Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

# Procesy a nástroje pre bezpečnú správu zariadení

Bezpečná správa zariadení (Blok V)

**Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe**

Mgr. Jana Uramová, PhD.

**KC KYB UNIZA,** https://kc.uniza.sk/

Jana.Uramova@fri.uniza.sk

# Obsah

- Oboznámiť sa s procesmi a nástrojmi pre bezpečné riadenie zariadení a ich bezpečnosti
  - Nástroje pre manažovanie aktív, rizík, zraniteľností, záplat, mobilných zariadení, konfigurácií
- Reálne ukážky z nástrojov na bezpečnú správu a riadenie
  - Nástroje pre manažovanie aktív, rizík

# Konext a význam správy zariadení

# Kontext a význam správy zariadení

Správa aktív = základný pilier kybernetickej bezpečnosti

Bez presnej evidencie aktív nie je možné:

- **správne vyhodnocovať riziká** – riziko vždy súvisí s konkrétnym aktívom a jeho hodnotou pre organizáciu,
- **identifikovať a odstraňovať zraniteľnosti** – zraniteľnosť má význam iba v kontexte aktíva, na ktorom sa nachádza,
- **plniť legislatívne a normatívne požiadavky** – ISO/IEC 27001, ISO/IEC 27005 a smernica **NIS2** vyžadujú vedenie inventára aktív ako povinnú súčasť riadenia bezpečnosti.

Neznáme alebo neevidované aktívum = **nezabezpečené aktívum**, ktoré môže byť ľahko zneužité útočníkom.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

## Prečo sú procesy a nástroje pre správu zariadení potrebné?

# Správa zariadení = kľúč pre kybernetickú bezpečnosť (KB)

**Strategické dôvody:**

- **Správa zariadení je základným pilierom KB** každej organizácie
  - Bez riadnej správy IT aktív nie je možné efektívne chrániť dáta, procesy a kritickú infraštruktúru.
- **Moderné kybernetické hrozby sú čoraz sofistikovanejšie**
  - a útočníci systematicky vyhľadávajú slabé miesta práve v oblasti správy zariadení.
- **Organizácie**, ktoré **zanedbávajú správu zariadení**, čelia:
  - zvýšenému riziku úniku citlivých dát,
  - narušeniu prevádzky,
  - finančným stratám.
- **Nedostatočná správa vedie k:**
  - neautorizovanému prístupu,
  - strate dôvery zákazníkov
  - a vážnym reputačným škodám.

## Prečo sú procesy a nástroje pre správu zariadení potrebné?

# Správa zariadení = kľúč pre kybernetickú bezpečnosť

### Ciele bezpečnej správy zariadení

- **Ochrana citlivých údajov –** prevencia únikov a neoprávneného prístupu
- **Zabezpečenie kontinuity procesov –** minimalizácia výpadkov a incidentov
- **Ochrana infraštruktúry –** zabezpečenie kritických systémov
- **Súlad a audit –** splnenie regulačných požiadaviek
- **Riadenie rizík –** proaktívna identifikácia a mitigácia hrozieb

Zlyhanie v správe zariadení môže viesť k strate údajov, reputácie a k značným finančným škodám. Prevencia je vždy efektívnejšia ako riešenie následkov incidentu.



Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Normy a legislatívne rámce pre správu zariadení

- **ISO/IEC 27001:2022** – ISMS (Information Security Management System) je strategické rozhodnutie organizácie pre zachovanie **dôvernosti, integrity a dostupnosti** informácií pomocou procesného riadenia rizík.
  - Vyžaduje, aby organizácia **vedela, čo vlastní a spravuje** – teda mala aktuálny **zoznam aktív** (Asset Register).
  - Aktuálny register aktív je základ pre všetky ďalšie procesy ISMS (napr. riadenie rizík, patch management, change management, business continuity).

- **ISO/IEC 27005:2022** – špecifikuje proces riadenia rizík v oblasti informačnej bezpečnosti a v kapitole **8.2 zdôrazňuje potrebu identifikovať a evidovať všetky aktíva organizácie** (hardvér, softvér, siete, dáta, služby, ľudské zdroje). Bez správneho zoznamu aktív nie je možné riziká efektívne vyhodnocovať ani ich primerane ošetrovať.

- **Zákon č. 69/2018 Z. z.** – prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb sú povinní zavádzať a udržiavať bezpečnostné opatrenia, **vrátane správy aktív, riadenia rizík a riadenie zraniteľností a záplat** (§ 19 – § 21).

- **NIS2 smernica (EU 2022/2555)** – od 2024 sprísňuje požiadavky, rozširuje pôsobnosť na viac sektorov, zavádza osobnú zodpovednosť manažmentu a vyššie pokuty.
  - Zavádza povinnosť nielen „mať opatrenia“, ale aj **ich preukázať** – t. j. mať evidenciu aktív a konfigurácií, ktorá sa dá auditovať.

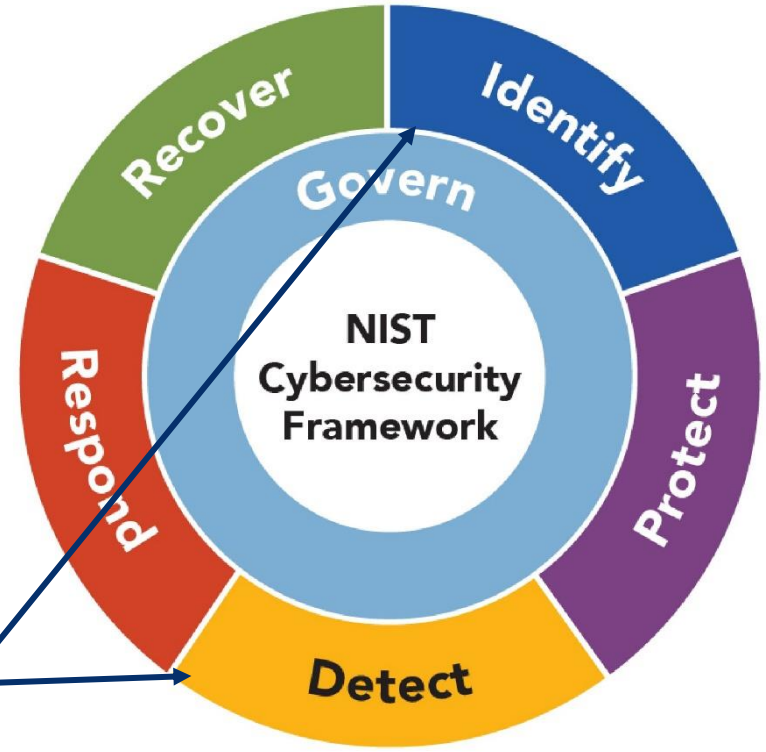


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# NIST CSF – prepojenie na správu aktív a monitoring

NIST Cybersecurity Framework definuje 5 základných funkcií:

- **Identify** – identifikácia aktív, prostredia, rizík
- **Protect** – zavedenie bezpečnostných opatrení
- **Detect** – odhaľovanie anomálií a incidentov (monitoring).
- **Respond** – reakcia na incidenty
- **Recover** – obnova služieb a procesov




Pre správu aktív a zariadení – sa zameriame na:

- **Identify** – evidovanie a kategorizáciu aktív (napr. NetBox, Lansweeper, LibreNMS, GLPI),
- **Detect** – monitoring a detekcia (LibreNMS, Greenbone).

NIST uvádza: „**Prvým krokom k efektívnej kybernetickej obrane je poznanie toho, čo vlastne chránime.**“



Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

## Prečo sú procesy a nástroje pre správu zariadení potrebné?

# Procesný pohľad – PDCA cyklus

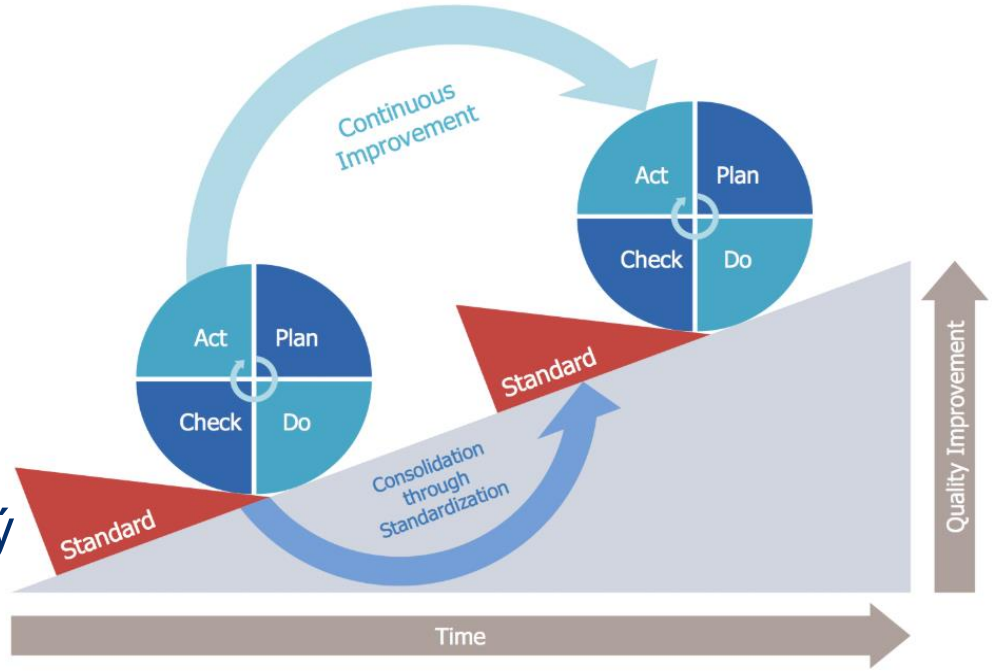
**PDCA** cyklus je **iteratívna metóda** riadenia, ktorá sa skladá zo štyroch krokov **Plan-Do-Check-Act**. **Používa sa na riadenie** podnikových procesov, výrobných procesov, alebo procesov kontinuálneho zlepšovania.

hypotéza → skúmanie → vyhodnotenie

- **Plan** (Naplánuj)– plánovanie: identifikácia aktív, analýza rizík, návrh opatrení.
- **Do** (Vykonaj) – realizácia: implementácia opatrení, monitoring, patching.
- **Check** (Over)– kontrola: audity, skeny, reporting, interné hodnotenie.
- **Act** (Jednaj)– zlepšenie: nápravné opatrenia, aktualizácia politiky, zvyšovanie zrelosti.

V prípade **úspechu** sa cyklus **končí** a nové nastavenia sa štandardizujú, systém sa monitoruje a následne sa pripravuje ďalšie spustenie cyklu.
Ak fáza **check** zistí neočakávané výsledky, iniciuje sa nový cyklus PDCA s cieľom odstrániť chybu.

**Riadenie bezpečnosti je neustály proces**, nie jednorazová úloha.
ISO/IEC 27001 používa cyklus PDCA:



# Čo je aktívum?

- Aktívum (assets) = čokoľvek, čo má hodnotu pre organizáciu, a preto si vyžaduje ochranu.
- Pri identifikácii aktív rozlišujeme 2 druhy aktív:
  - **Primárne aktíva**
    - Majú **najvyššiu hodnotu pre organizáciu** – priamo súvisia so zameraním, činnosťami a cieľmi.
    - Ich strata alebo kompromitácia má **okamžitý dopad na fungovanie organizácie**.
  - **Sekundárne (podporné) aktíva**
    - Všetky aktíva, ktoré umožňujú fungovanie primárnych aktív (procesov a informácii).
    - Každé podporné aktívum môže obsahovať zraniteľnosti, ktoré môžu byť zneužité hrozbami.

**Kompletný prehľad**
Evidencia všetkých aktív vrátane evidencie ich aktuálneho stavu.

**Väzby a závislosti**
Mapovanie vzťahov medzi aktívami a ich napojenie na kritické obchodné služby.

**Centrálna databáza**
Jednotný prehľad o všetkých aktívach a ich konfiguráciách – vždy aktuálne a konzistentné údaje.

**Riadenie rizík**
Identifikácia kritických aktív a určenie priorít pre ich ochranu.



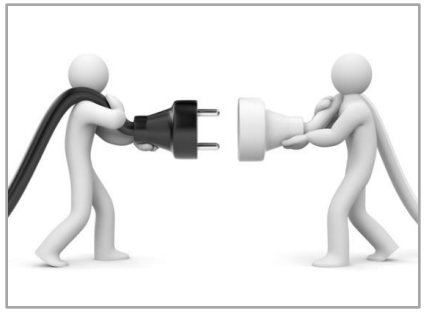
Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

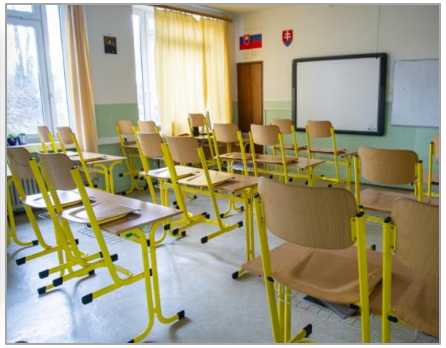
# Primárne vs. sekundárne aktíva

## Primárny proces: Výučba informatiky v učebni

Sekundárne aktíva, ktoré musia fungovať, aby mohla prebiehať výučba.









Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Primárne vs. sekundárne aktíva

*Primárny proces je závislý od celého ekosystému sekundárnych aktív. Ak zlyhá najmenší článok, ohrozený je celý proces.*

- Primárne = samotná **služba (výučba)**.
- Sekundárne = všetky „neviditeľné“ alebo podporné **veci**, **ktoré to umožňujú** (učebňa, stoličky, počítače, projektor, internet, elektrina, teplo, kľúče, učiteľ, učebné materiály…).

**Systém je taký silný, ako jeho najslabšia vrstva.**
Preto je dôležité identifikovať, chrániť a spravovať sekundárne aktíva rovnako ako primárne služby.

**Primárny proces je možný len vtedy, ak funguje množstvo sekundárnych aktív.**

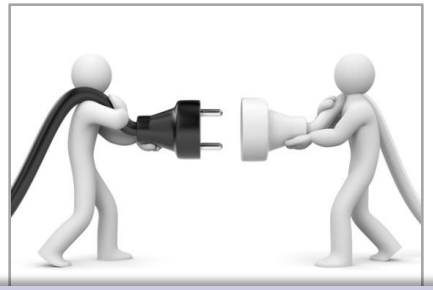
Ak zlyhá jedno z nich (napr. elektrina, internet, učiteľ, učebňa), primárny proces sa nemusí dať realizovať.

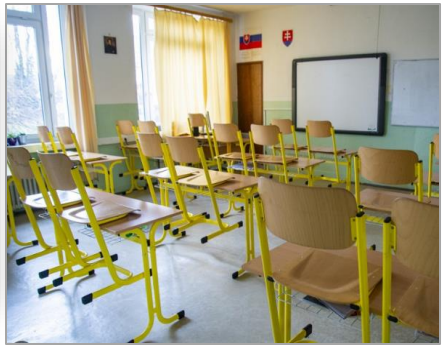


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

| Typ aktíva | Príklad | Poznámka |
|---|---|---|
| **Podporné informačné aktívum** | školský informačný systém, učebné dáta, notebook učiteľa | priamo spracúva alebo uchováva informácie |
| **Podporné fyzické aktívum** | serverovňa, dvere, zámok, UPS, klimatizácia | umožňuje bezpečné fungovanie IT prostredia |
| **Prevádzkové aktívum (neinformačné)** | stolička, osvetlenie, kúrenie | nemá priamy vplyv na bezpečnosť informácií |







**Fyzická bezpečnosť = súčasť informačnej bezpečnosti**, pretože chráni prostredie, v ktorom sú uložené alebo spracúvané informácie.

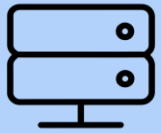
# Identifikácia primárnych aktív podľa ISO/IEC 27005

- Primárne aktíva sú 2 typov:
  - **Obchodné procesy (alebo subprocesy) a činnosti, zahrňujúce:**
    - **kritické procesy** – ich strata zastaví misiu/hlavnú činnosť organizácie,
    - **chránené procesy** – obsahujú tajné alebo patentované know-how,
    - **citlivé procesy** – zmena alebo manipulácia môže ohroziť plnenie cieľov,
    - **regulačne viazané procesy** – nevyhnutné pre splnenie zmluvných, právnych a regulačných povinností.
  - **Informácie, kde primárne informácie zahŕňajú najmä**
    - **kľúčové informácie** – potrebné na výkon misie a podnikania,
    - **osobné údaje** – vyžadujú ochranu podľa legislatívy (napr. GDPR),
    - **strategické informácie** – nevyhnutné pre dlhodobé ciele a orientáciu organizácie,
    - **vysoko nákladové informácie** – ich spracovanie a uchovávanie je finančne alebo časovo náročné.



Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

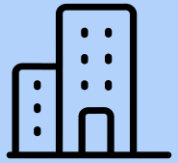
# Identifikácia sekundárnych aktív podľa ISO/IEC 27005



**Hardvér**
Fyzické zariadenia a komponenty

**Personál**
Ľudské zdroje a role

**Softvér**
Aplikácie a systémy



**Lokalita**
Fyzické priestory

**Sieť**
Komunikačná infraštruktúra

**Organizácia**
Štruktúra organizácie

***Hodnota podporného aktíva*** *je* ***odvodená od hodnoty primárnych aktív****, ktoré podporuje. Server sám o sebe „nemá hodnotu" – získava ju až tým, že poskytuje kritické služby alebo uchováva dôležité informácie.*



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Hardvér

**Hardvérové aktívum** nie je len „fyzické zariadenie“, ale **nositeľ dát, služieb a zodpovednosti.**

Správna evidencia umožňuje:

- rýchlo zistiť ***kde*** *sa zariadenie nachádza* (pri kontrole, audite, incidente),
- vedieť ***kto*** *zaň zodpovedá* a *kto ho spravuje*,
- definovať ***bezpečnostné opatrenia*** *podľa typu aktíva*,
- správne **plánovať *životný cyklus***, *nákup, výmenu, likvidáciu*,
- splniť požiadavky **ISO 27001 / GDPR / auditu**.

| Typ hardvéru | Príklad | Riziká |
|---|---|---|
| Aktívne zariadenia na spracovanie dát | PC, servery, sieťové prvky | Útoky, strata dát, malware |
| Prenosné zariadenia | Notebooky, tablety, mobily, PDA | Krádež, strata, neautorizovaný prístup |
| Fixné zariadenia | Servery v racku, prac. stanice | Fyzické poškodenie, poruchy HW |
| Periférie | Tlačiarne, skenery, externé disky | Únik dát cez tlač, odpojené médium |
| Médiá | USB, pásky, DVD, SSD | Nešifrované dáta, strata pri transporte |

kategórie hardvérových aktív



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Hardvér - aké údaje majú byť evidované

## Identifikačné údaje

- výrobca, model, typ zariadenia,
- sériové / inventárne číslo / asset ID / QR/RFID kód
- kategória aktíva (server, notebook, sieťové zariadenie…),
- dátum obstarania, cena, záruka.

## Technické údaje:

- BIOS verzia / firmware verzia / OS verzia,
- hardvérové parametre (CPU, RAM, storage, sieťové porty)
- pripojenie v sieti (IP, MAC, VLAN, hostname),
- zaznamenané zmeny (kedy bol vymenený disk, pridaná RAM atď.).

## Servis, podpora, SLA:

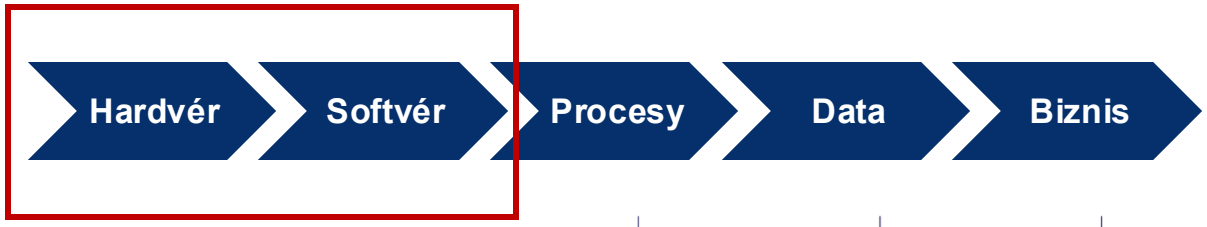
- servisná zmluva – typ podpory, reakčný čas (SLA), rozsah,
- záruka, dátum expirácie, možnosť predĺženia,
- história opráv a servisných zásahov.

## Umiestnenie a vlastníctvo:

- lokalita → budova → poschodie → miestnosť → rack / pracovisko,
- vlastník aktíva (Business Owner) – zodpovedá za dáta a prístupové práva,
- správca aktíva (IT Owner) – zodpovedá za technický stav, konfiguráciu.

## Informácie o bezpečnosti:

- Citlivosť aktíva (Low / Medium / High) podľa toho, aké dáta spracúva
- Je zariadenie šifrované? (BitLocker, TPM, FDE...)
- Fyzická bezpečnosť (zamknutý rack, monitoring, alarm)
- Prístupové práva a spôsob autentifikácie
- Záznam o incidentoch – bolo zariadenie stratené, napadnuté, zneužité?




Ak zlyhá základ (hardvér alebo softvér), biznis nefunguje.

# Hardvér - dobrá evidencia vs. chyby

| Pole | Príklad |
|---|---|
| Asset ID | HW-2024-01587 |
| Typ aktíva | Notebook – Lenovo ThinkPad T480 |
| Výrobné číslo | S/N: PF-1234-A56 |
| Vlastník | Oddelenie financií – M. Šimko |
| Správca | IT Support – J. Kováč |
| Umiestnenie | Budova B, 2. poschodie, kancelária 207 |
| OS / verzia | Windows 11 Pro – 23H2 |
| Zapnuté šifrovanie | Áno – BitLocker |
| Záruka / servis | OnSite NBD – do 12/2026 |
| Stav | Aktívne – v používaní |

**Časté chyby pri správe hardvérových aktív:**

❌ Registrovaný „notebook“, ale nevieme komu patrí.

❌ Servery bez záznamu o firmware alebo patchoch.

❌ USB disky mimo evidencie → riziko úniku osobných údajov.

❌ Aktívum evidované, ale v realite už dávno vyradené („mŕtve“ dáta v CMDB).

❌ Nikto nevie, či zariadenie ešte obsahuje dáta → problém pri GDPR.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Softvér a typy softvérových aktív

- Správa softvéru (SAM – Software Asset Management) rieši najmä:
  - bezpečnosť (aktualizácie, zraniteľnosti, patching),
  - legálnosť (licencie a audit),
  - prevádzku (podpora, kompatibilita, verzionovanie),
  - finančné plánovanie (opakovanie licenčných poplatkov, cloud/subskripcie).

**Softvér** je aktívum r**ovnako hodnotné ako hardvér**, ale je ťažšie viditeľné → preto musí byť evidované systematicky.

| Typ softvéru | Príklad | Riziká |
|---|---|---|
| Operačný systém | Windows, Linux, macOS | EOL verzia, nepatchované zraniteľnosti |
| Servisný/ zálohovací softvér | Zálohovacie SW, antivírus, monitoring | Neaktuálni agenti, nesprávna konfigurácia |
| Balíkový/ štandardný softvér | MS Office, Adobe, SAP klient | Nelegálna inštalácia, licenčný audit |
| Aplikačný softvér | CRM, ERP, HR systémy, intranet | Výpadok služby, chýbajúce SLA |
| Vlastný vývoj/ špecifické aplikácie | Interné systémy, webové portály | Neznáme knižnice, supply-chain riziká |

kategórie hardvérových aktív



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Softvér - aké údaje majú byť evidované

## Identifikačné údaje

- Názov softvéru + verzia + build (vnútorné vydanie, opravy, alebo konkrétny kompilát zdrojového kódu)
- Výrobca / dodávateľ
- Licenčný typ (per user, per device, subscription, open source)
- Pridelená licencia / počet zakúpených vs. počet používaných

## Väzba na hardvér:

- zoznam zariadení, kde je softvér nainštalovaný,
- počet inštancií vs. počet licencií,
- komu je softvér priradený (užívateľ, oddelenie, služba).

## Servis, podpora, SLA:

- Servisná zmluva / úroveň podpory (SLA, reakčný čas),
- Údržba (kto) / patchovanie (interný admin vs. vendor),
- Prevádzka (zodpovednosť) – business owner vs. IT owner.

## Bezpečnostné a prevádzkové logy:

- posledný aplikovaný patch / dátum aktualizácie,
- zraniteľnosti (CVEs) viazané na danú verziu,
- podpora / EOL dátum (End of Life / End of Support),
- je monitorovaný, loguje sa.

## Technické údaje:

- použité softvérové knižnice, frameworky, runtime (Java, .NET, Python…),
- použité Open Source komponenty → nutnosť sledovať CVE,
- závislosti medzi aplikáciami (API, databázy, integračné väzby),
- verzia aplikačného servera, DB servera, middleware,
- repozitár zdrojového kódu (Git, SVN) a jeho vlastníctvo.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Softvér - dobrá evidencia vs. chyby

| Pole | Príklad |
|---|---|
| Softvér | Microsoft SQL Server 2019 Standard |
| Verzia/build | 15.0.4322.2 |
| Výrobca | Microsoft |
| Licencia | Per Core – 4 cores, perpetual |
| Nainštalované na | SRV-FIN-DB01, SRV-FIN-DB02 |
| Vlastník | Oddelenie finančných systémov |
| Správca | IT – DBA tím |
| Posledný patch | KB5037140 (2024-02) |
| Zraniteľnosti | 1 aktívna CVE (stredná) |
| Servisná zmluva | Software Assurance – do 02/2026 |
| Stav | Aktívne - v prevádzke |

**Časté chyby pri správe softvérových aktív:**

❌ Nevieme, aké verzie sú v prevádzke → patching naslepo.

❌ Viac nainštalovaných licencií, než máme zakúpených.

❌ Softvér stále používaný, ale vendor už ukončil podporu.

❌ Open-source knižnice bez sledovania zraniteľností (Log4J, OpenSSL…).

❌ Softvér nainštalovaný, ale *bez vlastníka* → nikto ho neaktualizuje.



Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

# Sieť

Tvorí kritickú infraštruktúru organizácie. Jej zraniteľnosť často spočíva **nie v technológii, ale v nesprávnej konfigurácii**

- **Výpadok siete = automatický výpadok** všetkých služieb (ERP, email, databáza, cloud)
- Oproti hardvéru má sieť **kaskádový dopad incidentu** → ovplyvní stovky aktív naraz
- Útok na sieť je častejšie zneužitie chyby v konfigurácii ako zlý hardvér:

| Typ rizika | Príklad |
|---|---|
| Nesprávna konfigurácia | otvorené porty, default heslá, vypnuté logovanie |
| Neautorizovaný prístup | slabé Wi-Fi heslo, nezabezpečená VPN |
| Dostupnosť | DoS/DDoS, výpadok switcha, prerušený kábel |
| Integrita | MITM útok, ARP spoofing, BGP hijacking |
| Oslabená dôvernosť | nenašifrovaná komunikácia, sniffing paketov |



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Personál

- **Ľudský faktor je najslabší článok bezpečnosti.**
  - **Rozhodovatelia:** Manažment, vedenie – osoby s právomocou schvaľovať zmeny a investície
  - **Používatelia:** Koncový personál – zamestnanci využívajúci IT systémy v dennej práci
  - **Prevádzkový personál:** IT administrátori, technici – osoby zodpovedné za chod infraštruktúry
  - **Vývojári:** Programátori, architekti – tím vyvíjajúci a upravujúci softvér
  - **Bezpečnostný tím:** CISO, security analytici – špecialisti na kybernetickú bezpečnosť

# Lokalita

- **Externé prostredie:** Okolie budovy, prístupové cesty, parkoviská
- **Budovy:** Kancelárske priestory, dátové centrá, sklady
- **Zóny:** Rozdelenie na verejné, vyhradené a vysoko chránené oblasti
- **Fyzická bezpečnosť:** Kontrola prístupu, kamerové systémy, alarmy



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Inventarizácia aktív

## Hlavný význam:

- Základný pilier bezpečnostného riadenia a SOC operácií
- Poskytuje prehľad o všetkých zariadeniach, systémoch, aplikáciách a cloudových zdrojoch

**V prostredí SOCaaS umožňuje** (služba externým dodávateľom formou mesačného predplatného):

- Centrálne sledovanie infraštruktúr rôznych zákazníkov
- Kategorizáciu, stav aktív a ich bezpečnostný kontext
- Jednotné monitorovanie a reporting

## Prečo je nevyhnutná:

- Z nej vychádza detekcia zraniteľností a kontext incidentov
- Podporuje analýzu dopadu, ticketing a prioritu riešení
- Umožňuje riadenie životného cyklu aktív (obnova, vyradenie, audit)
- Pomáha plniť legislatívne a regulačné požiadavky



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Hodnotenie aktív a analýza vplyvu

- **Cieľ hodnotenia aktív**
  - stanoviť hodnotu aktív ako vstup do procesu riadenia rizík,
  - pripraviť podklad pre určenie úrovne dopadu a priorít ošetrenia rizík.
- **Metódy hodnotenia podľa ISO 27005**
  - **Kvantitatívne hodnotenie** – finančné vyjadrenie dopadov (náklady, strata, ALE - Annualized Loss Expectancy)
  - **Kvalitatívne hodnotenie** – stupnica dopadov (nízke, stredné, vysoké, kritické)
- **Analýza vplyvu (Impact Analysis)**
  - hodnotenie následkov straty **dôvernosti, integrity, dostupnosti**,
  - zahrnuté dopady: finančné, legislatívne, reputačné, prevádzkové, bezpečnostné, zmluvné, strategické.

- **Požiadavky normy ISO/IEC 27005** (preukázateľné v audite)
  - identifikované a zdokumentované aktíva (informácie, služby, procesy, osoby, technológie),
  - definované a schválené **kritériá hodnotenia** (finančné, právne, prevádzkové, reputačné…),
  - používaná **stupnica hodnotenia** (kvantitatívna alebo kvalitatívna),
  - doložené **vzťahy a závislosti medzi aktívami** – vplyv závislých aktív na hodnotu,
  - pre každé aktívum určená **hodnota a dopad kompromitácie** (CIA + ďalšie kritériá).



Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

## Prečo sú procesy a nástroje pre správu zariadení potrebné?

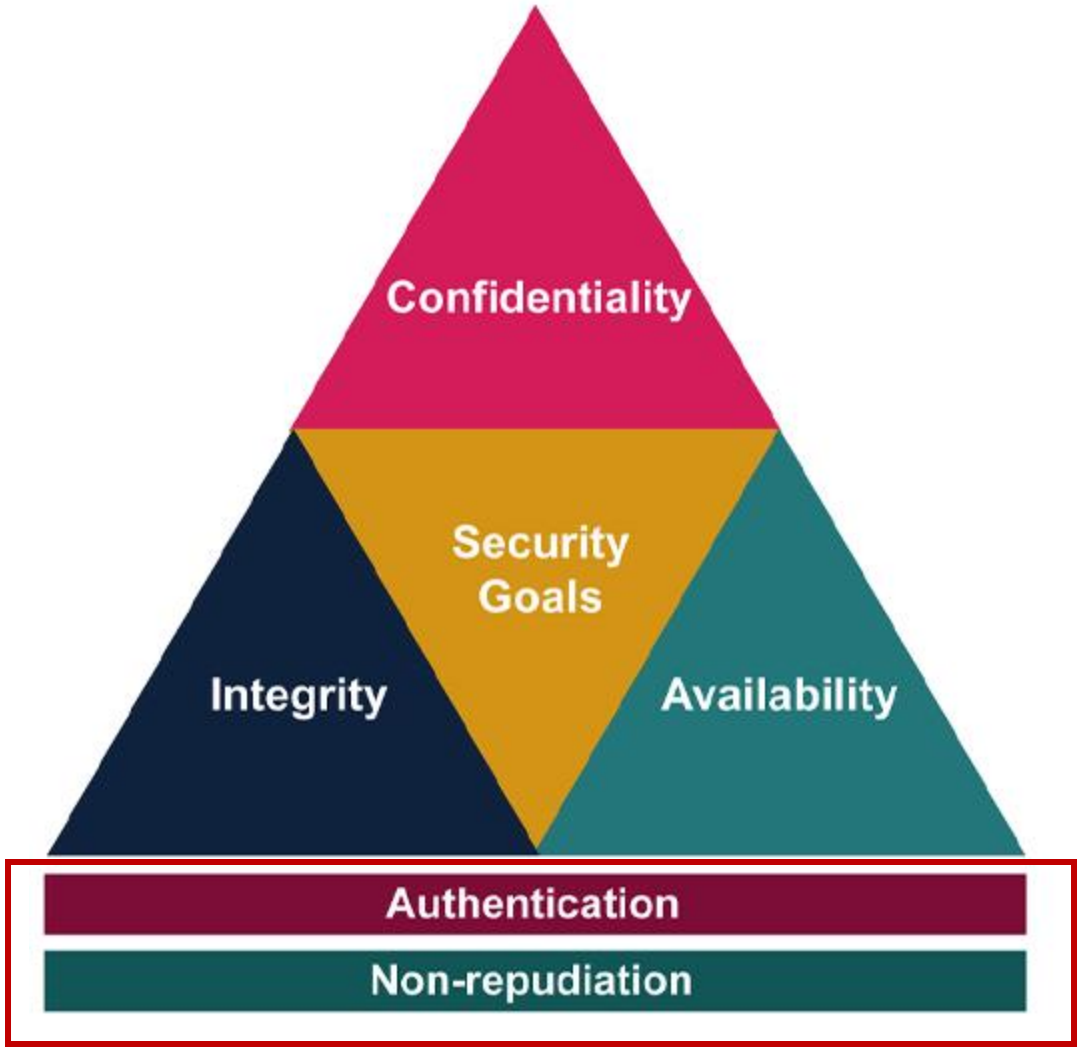
# CIA triáda (Dôvernosť, Integrita, Dostupnosť)

Každé aktívum musí byť chránené v súlade s princípmi CIA triády:

- **dôvernosť (confidentiality)** – informácie sú prístupné iba oprávneným osobám,
- **integrita (integrity)** – údaje musia zostať presné, úplné a chránené pred neoprávnenou zmenou,
- **dostupnosť (availability)** – služby a dáta musia byť dostupné vždy, keď ich organizácia potrebuje.

Rozšírené kritéria CIA+:

- **pravosť** (authenticity): zabezpečenie toho, že používateľ alebo systém je tým, za koho sa vydáva.
- **nepopierateľnosť** (non-repudiation): schopnosť dokázať, že určitá akcia alebo udalosť sa stala a kto ju vykonal






Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Nástroje pre bezpečné spravovanie a monitorovanie aktív

# Nástroje pre inventarizáciu aktív

- Výber správnych nástrojov je kritický
  - pre úspešnú implementáciu procesov správy zariadení.
- Moderné inventarizačné nástroje poskytujú:
  - automatizovaný prehľad o celej IT infraštruktúre
  - a tvoria základ pre ďalšie bezpečnostné aktivity.

**LibreNMS**

Open-source systém na monitoring a inventarizáciu s podporou SNMP a autodetekcie zariadení.

**netbox**

Nástroj na dokumentáciu a modelovanie infraštruktúry (IP adresy, racky, servery).

**Lansweeper**

Komerčný inventarizačný systém s agentmi, vhodný pre správu hardvéru a softvéru vo veľkých sieťach.

**GLPI**

Open-source inventarizačný systém s agentmi, vhodný pre správu hardvéru a softvéru vo veľkých sieťach.

**spiceworks**

Cloudová platforma určená na správu IT podpory, inventarizáciu zariadení a monitorovanie IT infraštruktúry.



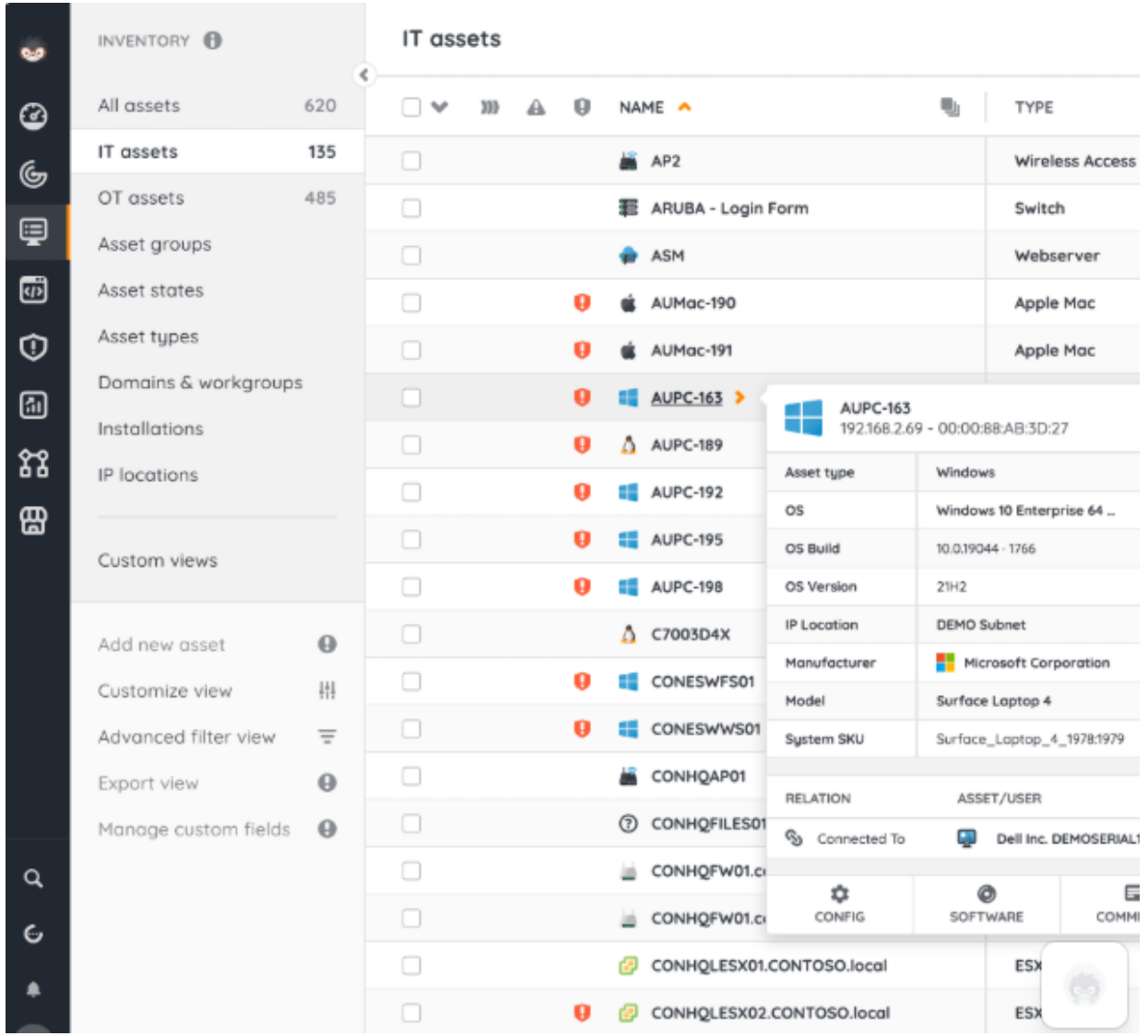
Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline


# Inventarizačný nástroj - Lansweeper

## Nástroje na správu a kategorizáciu aktív

# LanSweeper

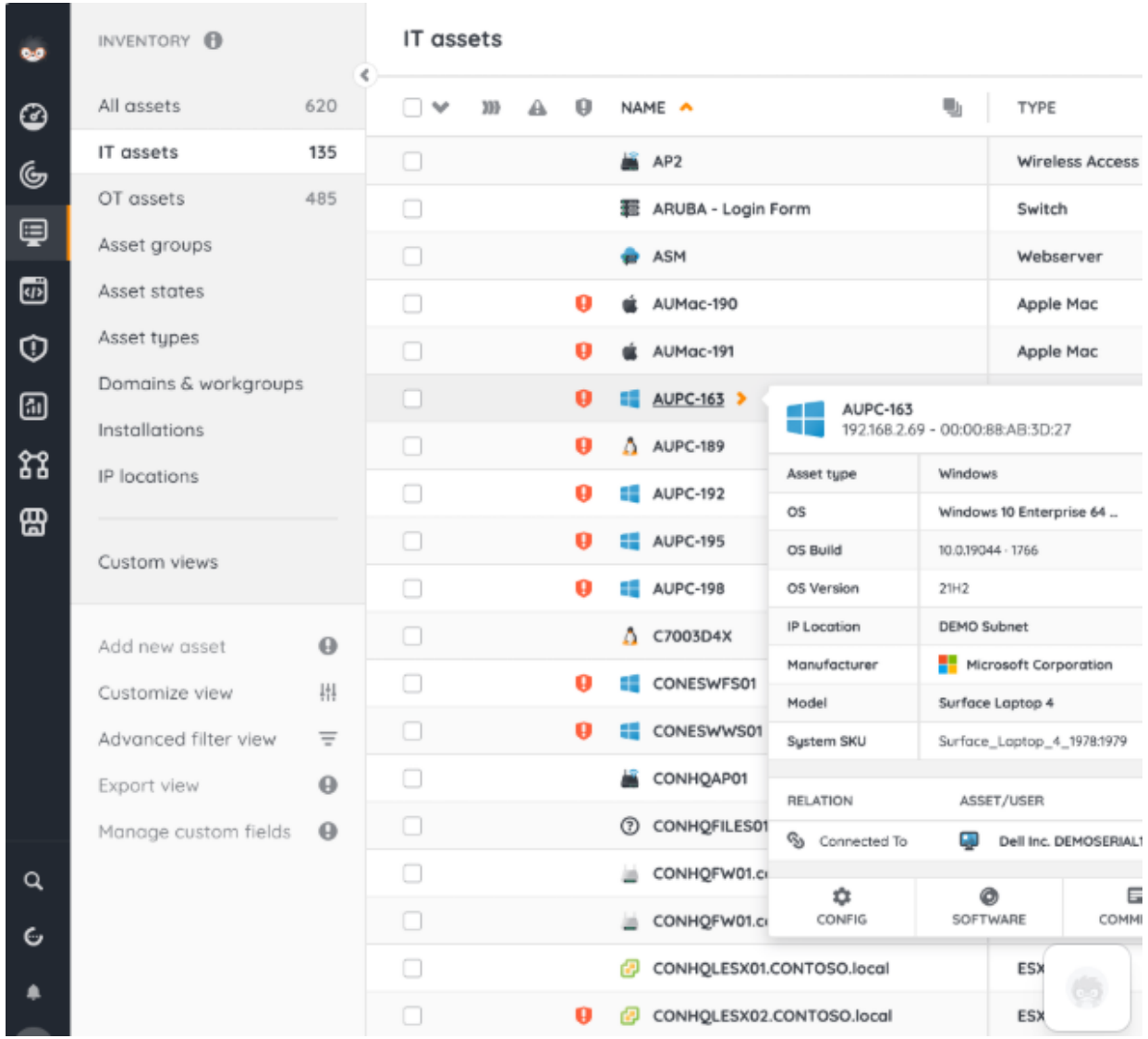
- Automaticky **objavuje** zariadenia - IT, OT, IoT, cloud,
  - detekuje HW,SW, používateľov, konfigurácie, umiestnenie zariadení a ich vzťahy.
  - OT = Operational Technology – technológie používané na riadenie a monitorovanie priemyselných procesov, infraštruktúry a výrobných zariadení.
    - Patria sem: PLC (programovateľné logické automaty), SCADA systémy, priemyselné siete, senzory, roboty, energetické riadiace systémy.
  - Pripomienka:
    - IT (Information Technology) → správa dát, aplikácií, systémov
    - OT (Operational Technology) → správa a riadenie fyzických procesov (výroba, distribúcia elektriny, doprava, zdravotnícka technika…)



## Nástroje na správu a kategorizáciu aktív

# LanSweeper

- Automaticky **objavuje** zariadenia
  - IT, OT, IoT, cloud,
- **Rôzne metódy skenovania:**
  - IP rozsahy,
  - domény AD,
  - agentov (napr. LsAgent, LsPush) / agent-less prístup.
- Informácie **ukladá do centrálnej databázy**
- Poskytuje:
  - prehľady
  - reporty
  - vizualizácie
- Umožňuje integráciu s inými systémami
  - ConnectWise PSA
  - HaloITSM
  - Jira Service Management (Jira Assets)
  - CMDB/ITAM systémami ako 4me



LanSweeper

# Komerčné riešenie

Lansweeper

## Free

Ideal for small teams who want to explore asset discovery. Start with 14 days of full access.

**€ 0**

Start free

- Asset Discovery & Inventory
- 14-day premium trial included
- Continue free with up to 100 assets
- Unlimited User Seats
- Community Support

## Starter

Everything you need to start discovering & managing your technology estate.

From
**€ 219** / month (billed annually)

Start free trial

Request a quote

- **Everything in Free**
- Includes 2,000 assets
- 1 Installation
- Service Desk Ticket Enrichment
- Single Sign-On (SSO)
- Starter Support

## Pro

Recommended

For IT leaders who need to reduce risk, stay compliant, and unlock full control. Why go Pro?

From
**€ 399** / month (billed annually)

Start free trial

Request a quote

- **Everything in Starter**
- Includes 2,000 assets
- Up to 3 installations
- Vulnerability & Lifecycle Insights
- All Integrations
- Pro Support

## Enterprise

For enterprises with global scale, governance, and support needs. Why go Enterprise?

**Contact Us**

Book a demo

Request a quote

- **Everything in Pro**
- Starts at 10,000 Assets
- More than 3 installations
- Full API Access
- Customer Success Manager
- Assistance for Global Deployments
- Concierge Service (Add-on)
- Enterprise Support

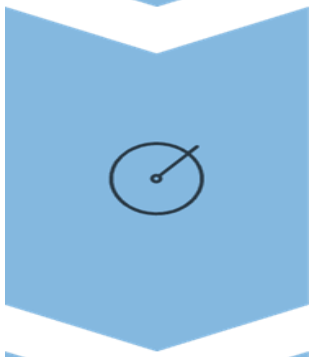
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

LanSweeper

# Metóda skenovania

## Scanning Target

skenovanie vopred definovanej skupiny aktív - IP range, konkrétne zariadenia alebo typy.



## Asset Radar

automatické zisťovanie nových zariadení odchytávaním komunikácie v sieti.

## Performance Scanning

monitorovanie zaťaženie CPU, pamäte, diskov a siete v reálnom čase.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# agentless vs. agent-based skenovanie

## Agentless skenovanie

- ideálne pre rýchle nasadenie, bez potreby inštalácie softvéru na koncových zariadeniach. Poskytuje okamžitý prehľad o celej sieti s minimálnym vplyvom na výkon.

- **Použitie:**
- **najvhodnejšie pre úvodné skenovanie siete** a inventarizáciu **infraštruktúrnych zariadení** (servery, sieťové prvky, SNMP zariadenia).

## Výhody:

- **okamžité nasadenie -** Nie je potrebná inštalácia na jednotlivých zariadeniach.
- **bez vplyvu na výkon -** Na cieľových zariadeniach nebežia žiadne procesy.
- **široké pokrytie -** Odhalí všetky typy zariadení – servery, switche, routery, IoT, zariadenia bez OS.

## Nevýhody:

- **obmedzenie sieťou -** Môže byť blokované firewallmi alebo vyžadovať prihlasovacie údaje.
- **škálovanie -** Pre veľké siete môže byť potrebné viac skenovacích serverov alebo konfigurácií.



Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# agentless vs. agent-based skenovanie

## Agent-based skenovanie

- vyžaduje inštaláciu malého agenta na zariadení, ktorý zbiera údaje a odosiela ich do systému. Umožňuje hĺbkový zber dát v reálnom čase – aj mimo hlavnej siete.

## Použitie:

- najvhodnejšie pre **mobilné a vzdialené zariadenia**, ktoré nie sú neustále pripojené k sieti.

## Výhody:

- **detailné dáta -** Zhromažďuje kompletné informácie priamo zo zariadenia.
- **funguje mimo siete -** zber údajov z notebookov či zariadení mimo LAN.
- **ideálne pre koncové zariadenia -** Určené pre pracovné stanice, laptopy.

## Nevýhody:

- **nutná inštalácia -** Agent musí byť nainštalovaný na každom zariadení.
- **nároky na výkon -** Mierne zaťažuje hostiteľské zariadenie
- **zložitejšia správa -** Vyžaduje viac úsilia na nasadenie a údržbu.



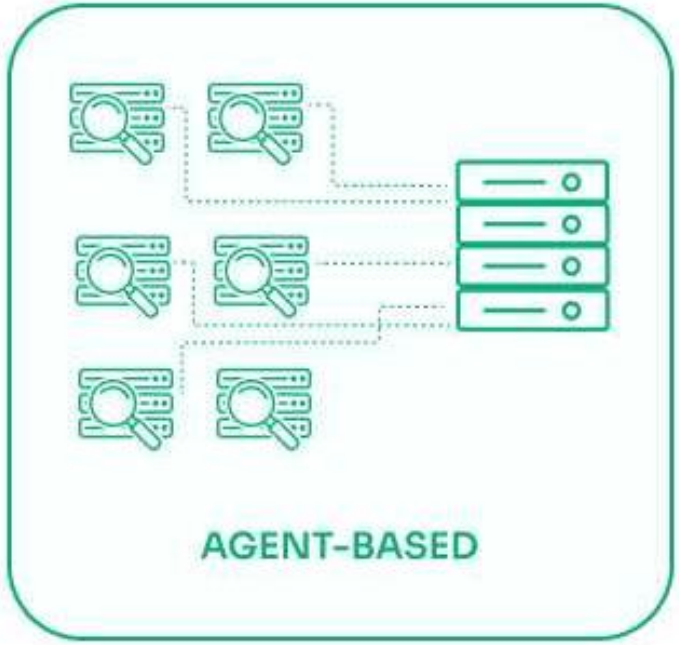
Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

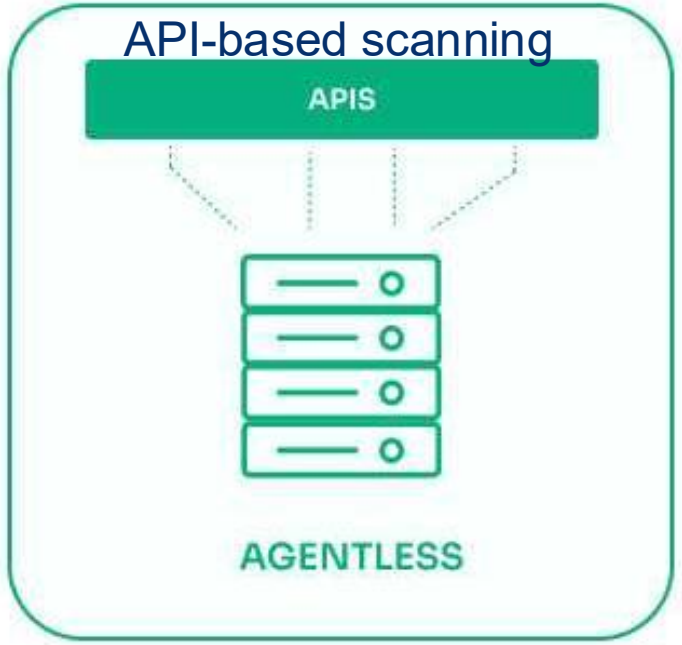
# Odporúčaná prax

**Kombinácia oboch metód:**

- **Agentless** – na široké pokrytie a rýchlu detekciu infraštruktúry.
- **Agent-based** – na hĺbkové dáta z endpointov mimo siete.

Táto kombinácia zaručuje **kompletný prehľad o IT aktívach** a **spoľahlivé dáta pre bezpečnostnú analýzu**.



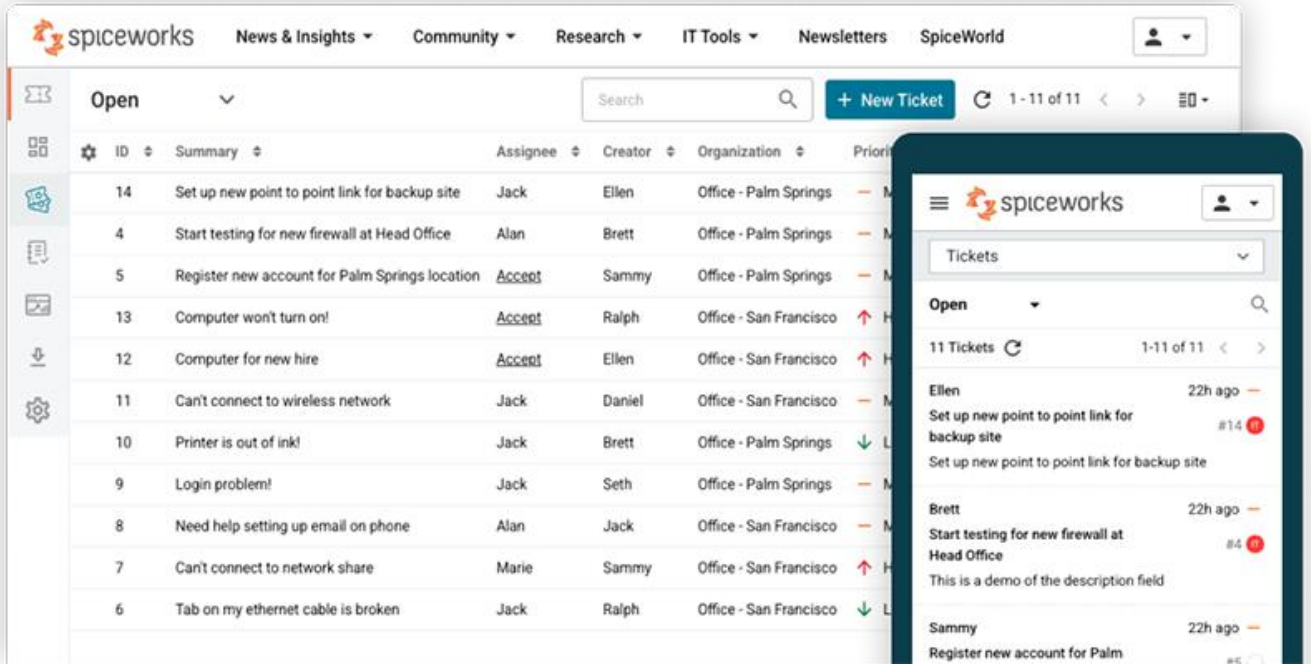




# Inventarizačný nástroj - SpiceWorks

## Nástroje na správu a kategorizáciu aktív

# SpiceWorks

- **Cloudové riešenie** na správu IT požiadaviek a incidentov, určené **pre interné IT tímy**.
- Umožňuje centralizované vytváranie, **priraďovanie a sledovanie tiketov cez** webové rozhranie alebo **e-mail**.
- Podporuje **automatizáciu procesov**, vrátane kategorizácie, prioritizácie a smerovania tiketov.
- **Obsahuje vstavané reporty** a **analytiku** na monitorovanie výkonnosti IT podpory.
- **Integruje sa so systémami inventarizácie IT aktív** – podporuje **prepojenie** medzi **helpdeskom** a **správou majetku**.






Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

## SpiceWorks

# Licencia

**Dva licenčné modely**:

- **Core (Free)** – bezplatný, financovaný reklamou
- **Premium (Paid)** – bez reklám, rozšírené funkcie

**Rovnaký základ funkcionality** v oboch plánoch:

- Správa IT incidentov a tiketov
- Podpora viacerých používateľov a zariadení
- Cloudové nasadenie

**Core plán**

- Pre menšie tímy alebo nízke požiadavky
- Obsahuje všetky základné funkcie
- S reklamami v používateľskom rozhraní

**Premium plán**

- Pre profesionálne IT oddelenia a väčšie tímy
- Odstránené reklamy + pokročilé nástroje (tasklisty, bulk akcie, live podpora)
- Škálovateľný, s vyššími SLA

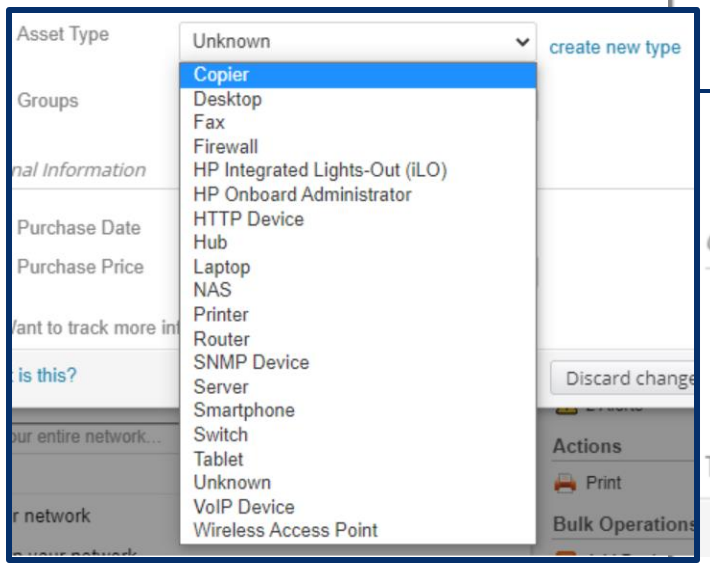
| | Core Plan (Free) | Premium Plan |
|---|---|---|
| Cena | Zadarmo | 5 USD na technika mesačne (pri ročnej platbe) / 6 USD mesačná platba |
| Počet technikov | 1–5 | Neobmedzený počet |
| Reklamy | Obsahuje reklamy | Bez reklám |
| Tasklists (zoznamy úloh) | ❌ | ✅ |
| Bulk Actions (hromadné akcie nad ticketmi) | ❌ | ✅ |
| Live Chat podpora 24/5 | ❌ | ✅ |

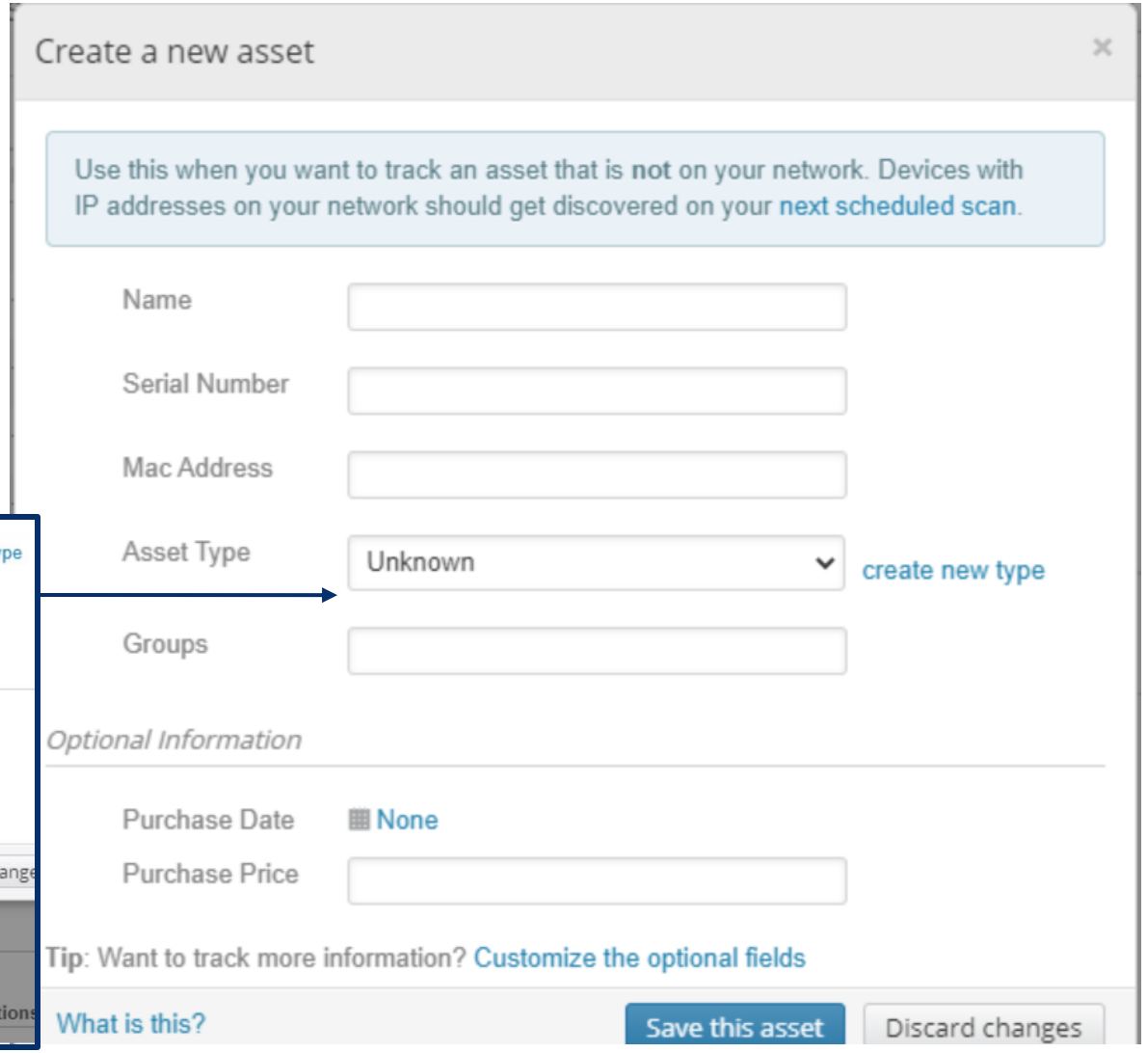


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Manuálne pridávanie aktív

- Spiceworks **ponúka 3 možnosti pridávanie aktív:**
  - manuálne,
  - import,
  - sken siete.
- Potrebné údaje **na vyplnenie**:
  - názov,
  - sériové číslo,
  - MAC adresa,
  - typ aktíva (preddefinované),
  - skupina.



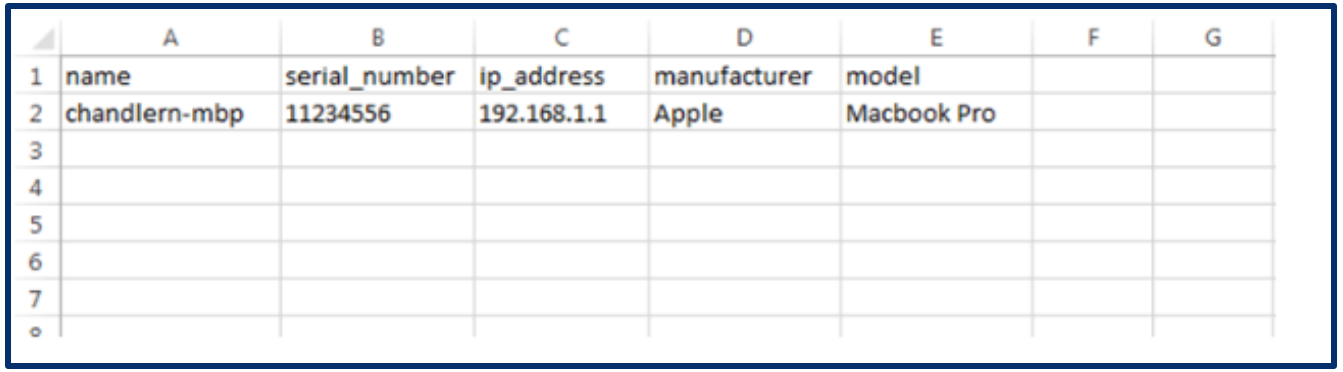
# Import a Export aktív

## Import aktív

- podporovaný je **import zariadení** vo formáte CSV,
- importný súbor musí zodpovedať definovanej šablóne,
- import sa vzťahuje **iba na hardvérové aktíva** – softvér nie je možné importovať touto formou
- šablóna CSV je dostupná v dokumentácii Spiceworks.

## Export dát:

- možnosť exportu do formátov **CSV, XLS, PDF,**
- exportovateľné entity: zariadenia, softvér, používatelia, nákupy, tikety, cloudové služby,
- export podporuje **pokročilé filtrovanie** podľa atribútov (napr. zariadenia s antivírusom, tikety s určitou prioritou).



| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | name | serial_number | ip_address | manufacturer | model | | |
| 2 | chandlern-mbp | 11234556 | 192.168.1.1 | Apple | Macbook Pro | | |
| 3 | | | | | | | |
| 4 | | | | | | | |
| 5 | | | | | | | |
| 6 | | | | | | | |
| 7 | | | | | | | |



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

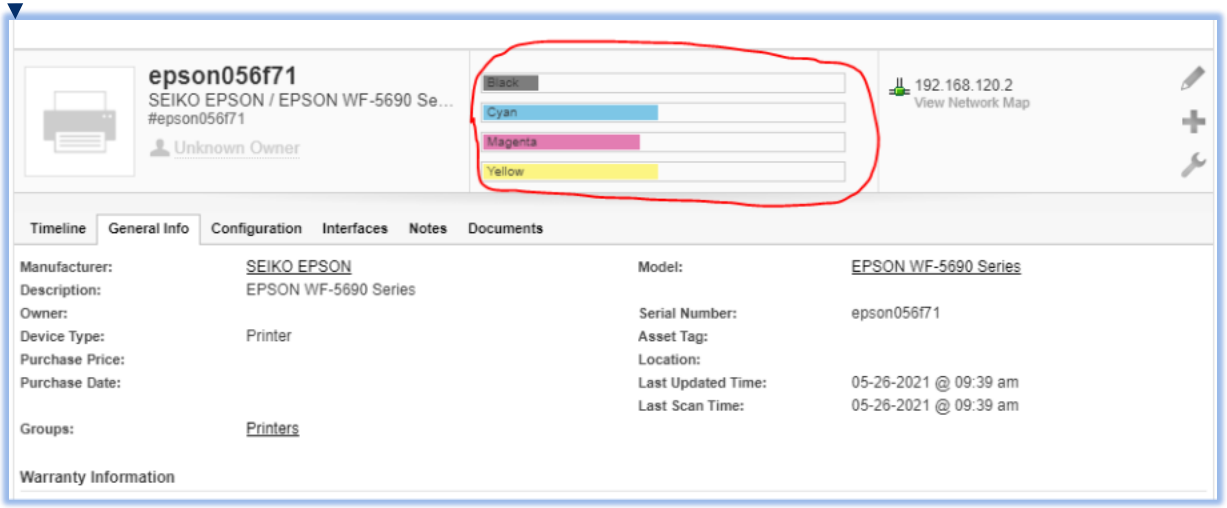
# Skenovanie aktív zo siete

## Bez použitia agenta

- Nie je potrebné mať na zariadeniach nainštalovaný klientsky softvér.
- Sieť sa prehľadá na základe zadaného IP rozsahu.
- Výsledky obsahujú **iba základné údaje** o zariadeniach:
  - IP adresa, MAC adresa, výrobca, typ zariadenia, v niektorých prípadoch aj sériové číslo.
- Tento spôsob je vhodný pre rýchly prehľad, no neposkytuje detailné inventarizačné údaje.

## S použitím agenta

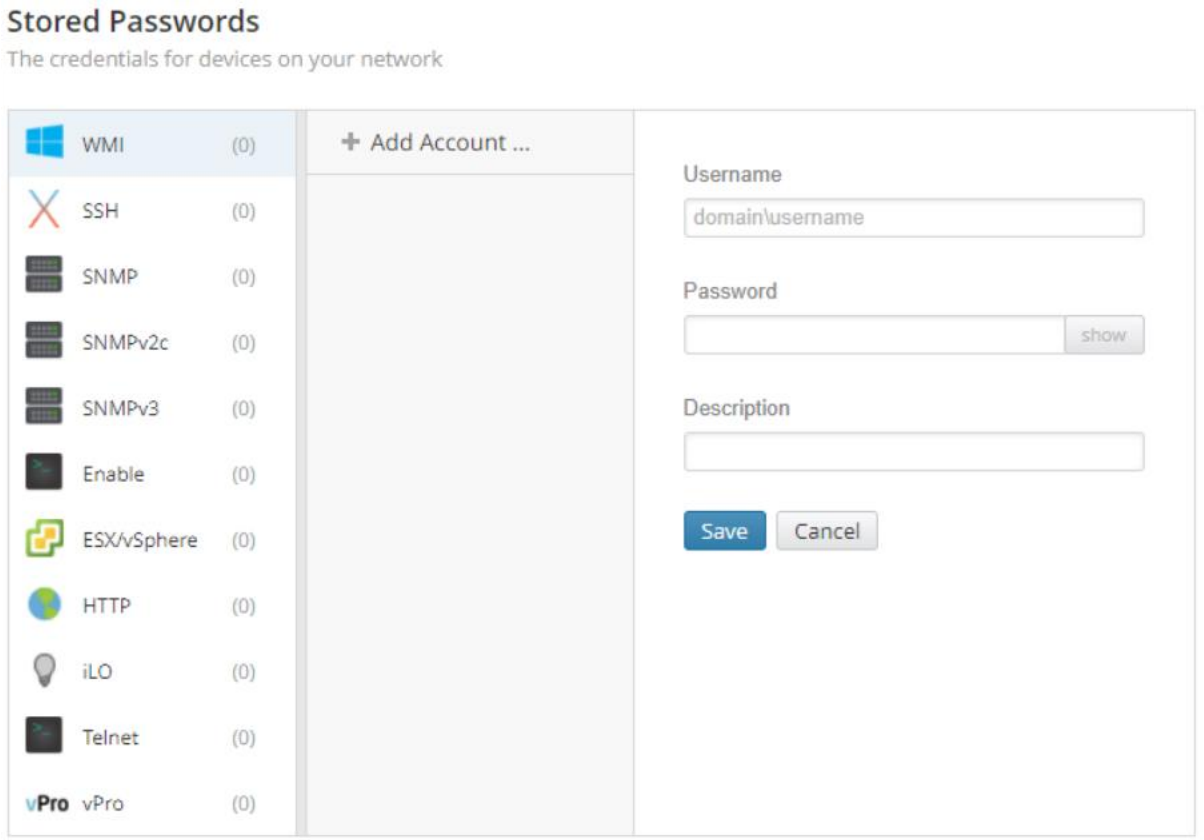
- Na koncové zariadenia sa nainštaluje agent, ktorý beží na pozadí.
- Agent poskytuje **detailné informácie o hardvéri, softvéri, používateľovi, stave zariadenia a pod.**
- Vhodné pre presnú inventarizáciu a priebežné monitorovanie.



SpiceWorks

# Skenovanie aktív zo siete

- Na získanie podrobnejších výsledkov je možné vytvoriť **databázu prihlasovacích údajov (credentials)**, ktoré sa pri skenovaní automaticky použijú na overenie zariadení.
- Podporované typy prístupov zahŕňajú napr.:
  - WMI, SSH, SNMP, ESX/vSphere, HTTP, Telnet, iLO, vPro a ďalšie.
- Tento mechanizmus umožňuje získať **detailnejšie a autentifikované údaje** zo zariadení nachádzajúcich sa v sieti.
- Údaje sú uložené v šifrovanej forme a priraďujú sa automaticky pri skenovaní podľa protokolu alebo typu zariadenia.



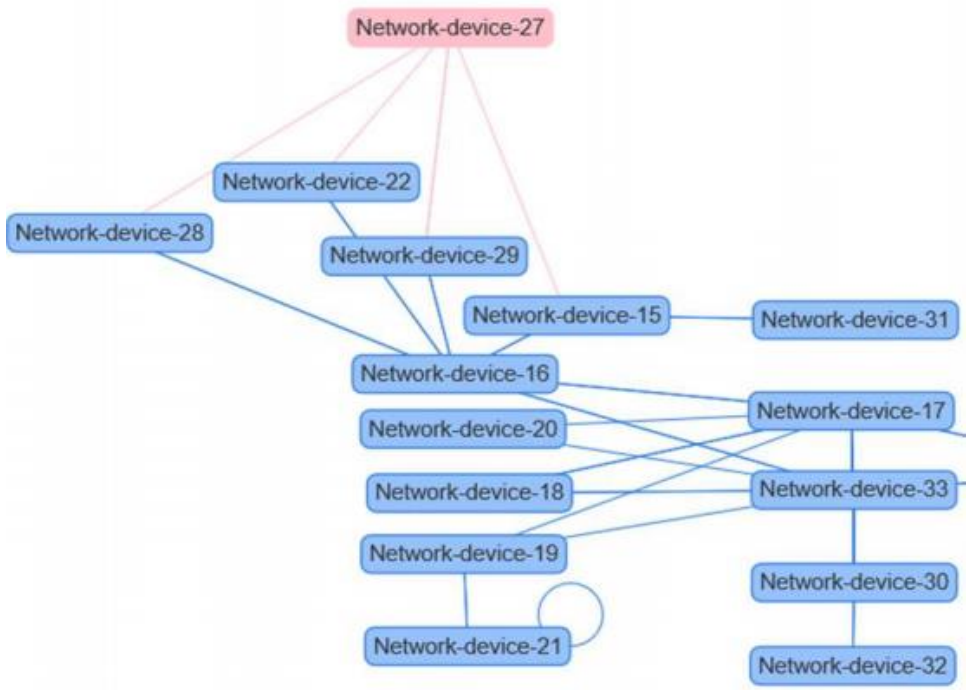



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE


# Inventarizačný nástroj - LibreNMS

# LibreNMS

- Open-source nástroj pre **mapovanie, monitorovanie a správu sieťových zariadení** (pomocou **SNMP**).
- Webové rozhranie v PHP, dostupné pre Linux, Windows, FreeBSD.
- Podporuje zariadenia od výrobcov (stovky):
  - Cisco,
  - Juniper,
  - Brocade,
  - HP, Dell, Fortinet, Ubiquiti, Synology, Arista, MikroTik a ďalšie.
- Grafické znázornenie siete a jej väzieb
  - **automaticky generovaná sieťová mapa**




LibreNMS nie je len monitoring – je to nástroj na **identifikáciu a kategorizáciu sieťových aktív v reálnom čase**

# Hlavné kategórie zariadení podporované v LibreNMS

1. **Sieťové zariadenia** – switche, routre, firewally, AP, load balancery
2. **Bezdrôtové a Wi-Fi zariadenia** – kontroléry, AP, bezdrôtové mosty
3. **Servery a OS** – Linux, FreeBSD, UNIX-like systémy
4. **Storage zasobníky** – NAS/SAN a iné úložné systémy
5. **UPS a napájacie zariadenia** – UPS, PDU, generátory
6. **Telekomunikačné a optické zariadenia** – PTP, rádia, optické prepínače

1. **IP kamerové a bezpečnostné zariadenia** – IP kamery,NVR
2. **Tlačiarne a multifunkčné zariadenia** – rôzne značky tlačiarní
3. **Environmentálne senzory a senzory HW** – senzory teploty, vlhkosti, zdravotné senzory
4. **Virtualizačné a cloudové platformy** – virtuálne zariadenia a hypervízory
5. **Softvérové služby a aplikácie** – SNMP-exponované služby, SW komponenty
6. **Iné SNMP-zariadenia** – generické SNMP zariadenia a IoT typy

# Hlavné funkcionality

## Auto Discovery

## Mapovanie

Vizualizácia topológie siete s grafickým zobrazením prepojení medzi zariadeniami

## Zber údajov

Kontinuálny zber dát zo zariadení a ich následné vykreslenie do prehľadných grafov

*Systém **LibreNMS** funguje výhradne pomocou protokolu **SNMP**, preto je potrebné aby mali **všetky** sieťové **zariadenia zapnutý SNMP protokol** a nakonfigurovaný správny **komunitný kľúč.***

LibreNMS podporuje viacero tzv. *discovery protocols*:

- **LLDP** – IEEE štandard, univerzálny pre väčšinu moderných zariadení,
- **CDP** – Cisco,
- **FDP** – Foundry/Brocade,
- **EDP** – Extreme Discovery Protocol (Extreme Networks),
- **NDP** – Nortel Discovery Protocol.

Tieto protokoly umožňujú LibreNMS automaticky generovať **sieťové mapy** a **vzťahy medzi portmi a zariadeniami** bez manuálneho zadávania.

# Prečo áno ?

**Výhody**

- Open-source (bez poplatkov)
- Automatické objavenie zariadení
- Podpora viacerých výrobcov
- Vizualizácia siete a grafy
- API a rozšíriteľnosť

**Nevýhody**

- Len sieťové aktíva
- Vyššie nároky SNMP a údržbu
- Vizualizácie nie sú vždy stabilné
- Náročnejšie ladenie



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

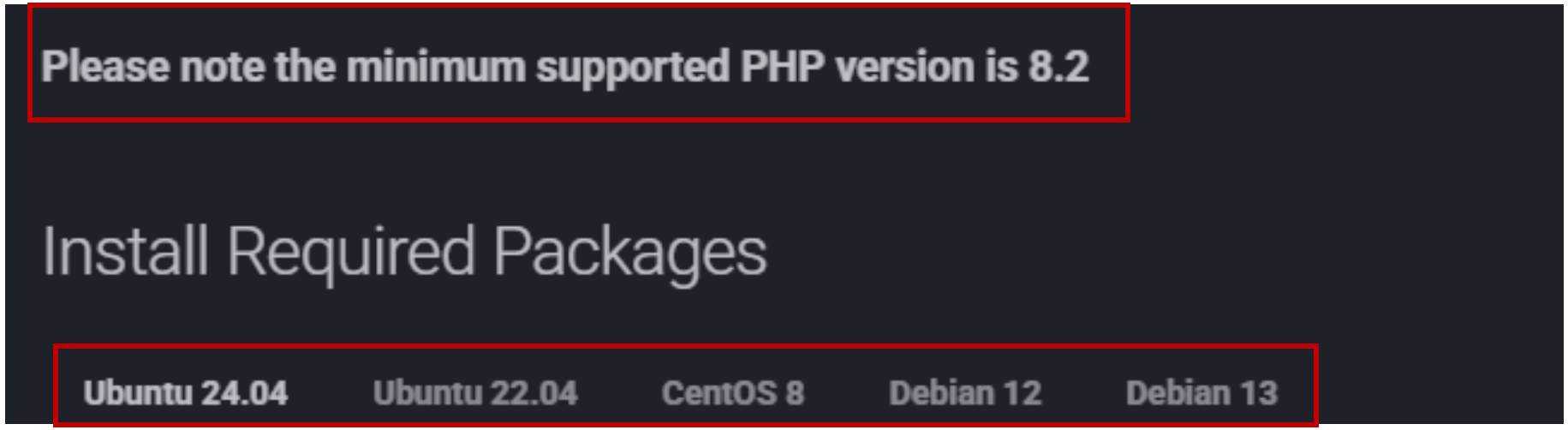
# Inštalácia

## Podporované distribúcie

- Ubuntu
- Debian
- RHEL/CentOS Stream / Rocky Linux / AlmaLinux
- Fedora, Arch Linux, Alpine Linux, openSUSE/SLES

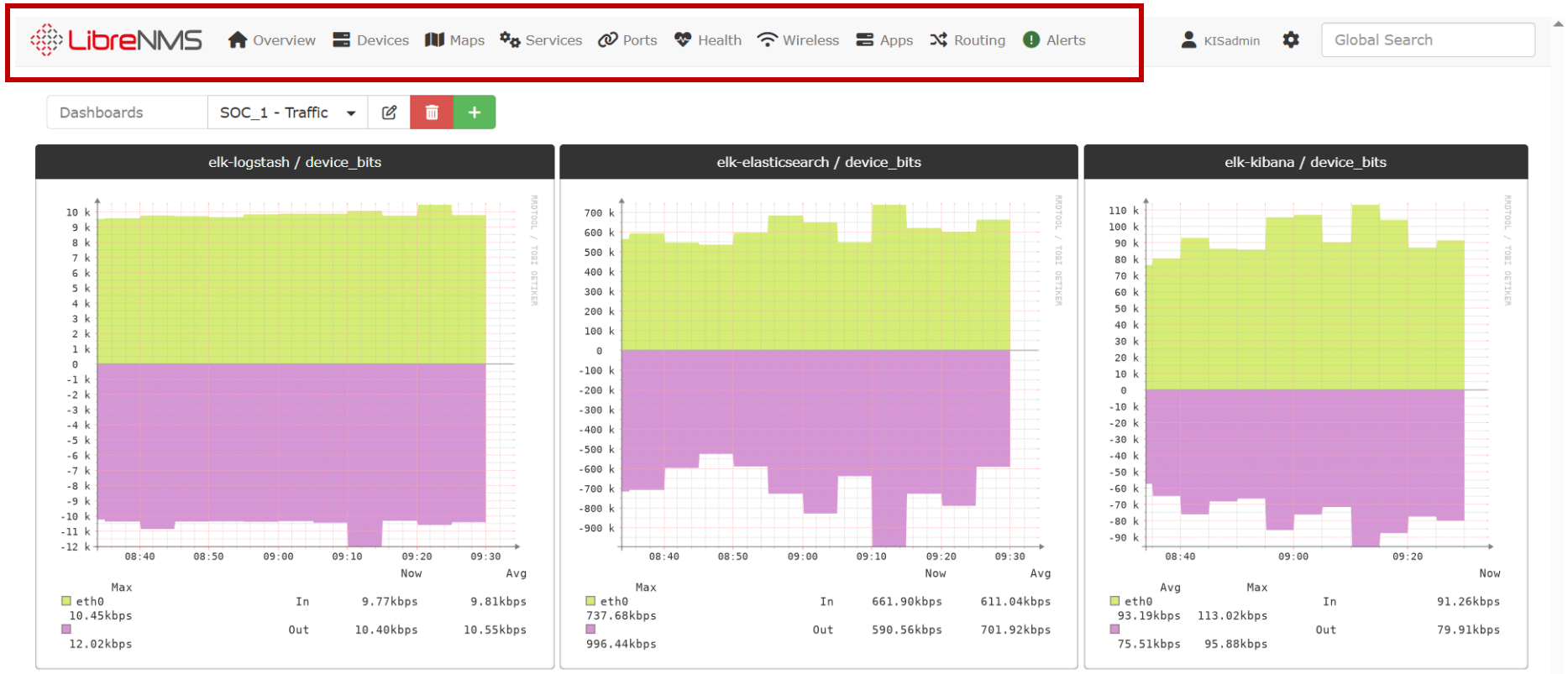
## Technické požiadavky

- Webový server (odporúčaný NGINX)
- PHP verzia 8.2 alebo vyššia
- Databázový server



# Webové používateľské rozhranie

- Prihlásenie do Web UI prebieha cez IP adresu vo webovom prehliadači

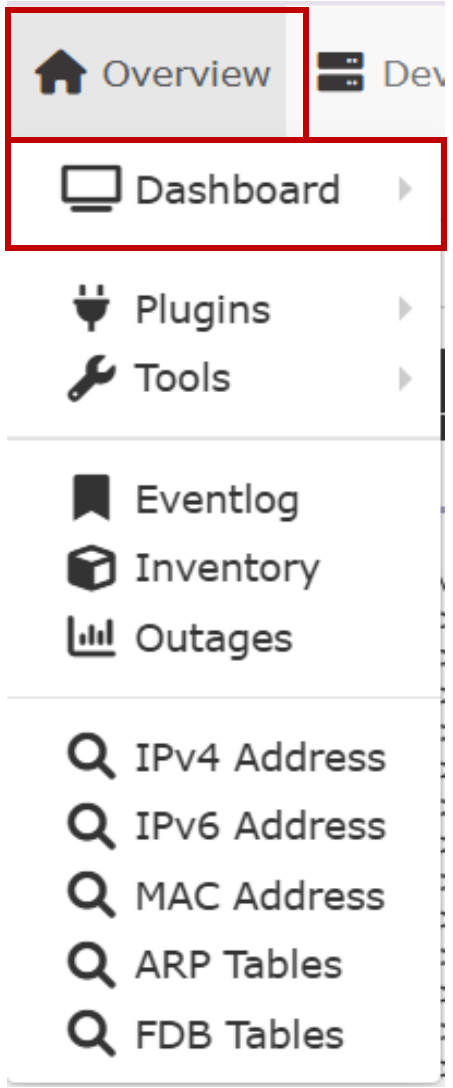


# Hlavné menu - Overview

**Overview (prehľad systému):**

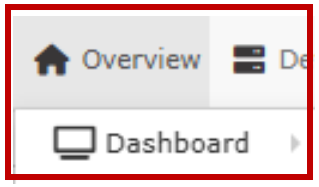
- dashboard, grafy, štatistiky, trendy,
- rýchly stav siete a zariadení,
- výstrahy a kritické udalosti.

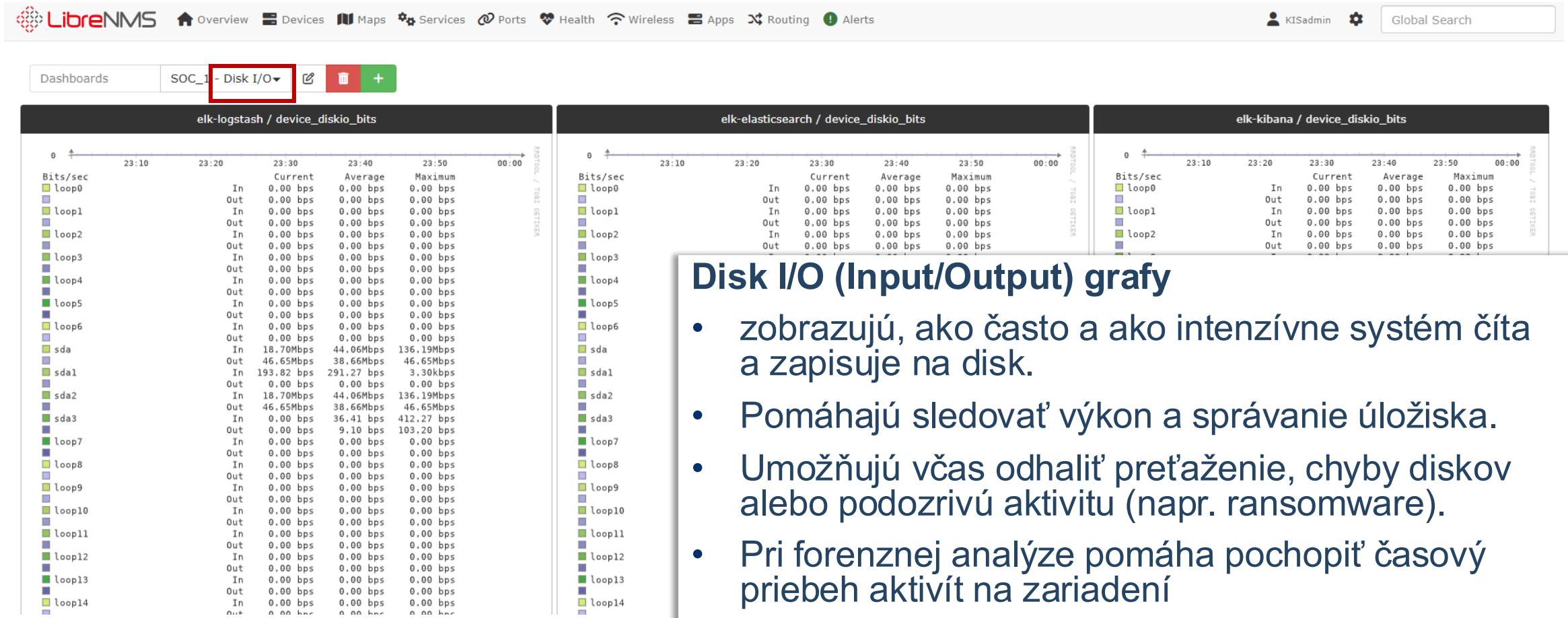
**Bezpečnostný význam:**
**→ rýchla detekcia prevádzkových problémov - preťaženia, výpadkov alebo podozrivého správania.**



LibreNMS

# Diskové IO grafy




## Disk I/O (Input/Output) grafy

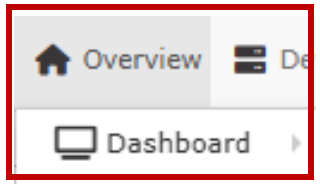
- zobrazujú, ako často a ako intenzívne systém číta a zapisuje na disk.
- Pomáhajú sledovať výkon a správanie úložiska.
- Umožňujú včas odhaliť preťaženie, chyby diskov alebo podozrivú aktivitu (napr. ransomware).
- Pri forenznej analýze pomáha pochopiť časový priebeh aktivít na zariadení
- LibreNMS tieto dáta získava cez SNMP a zobrazuje ich ako časové grafy (MB/s, IOPS).

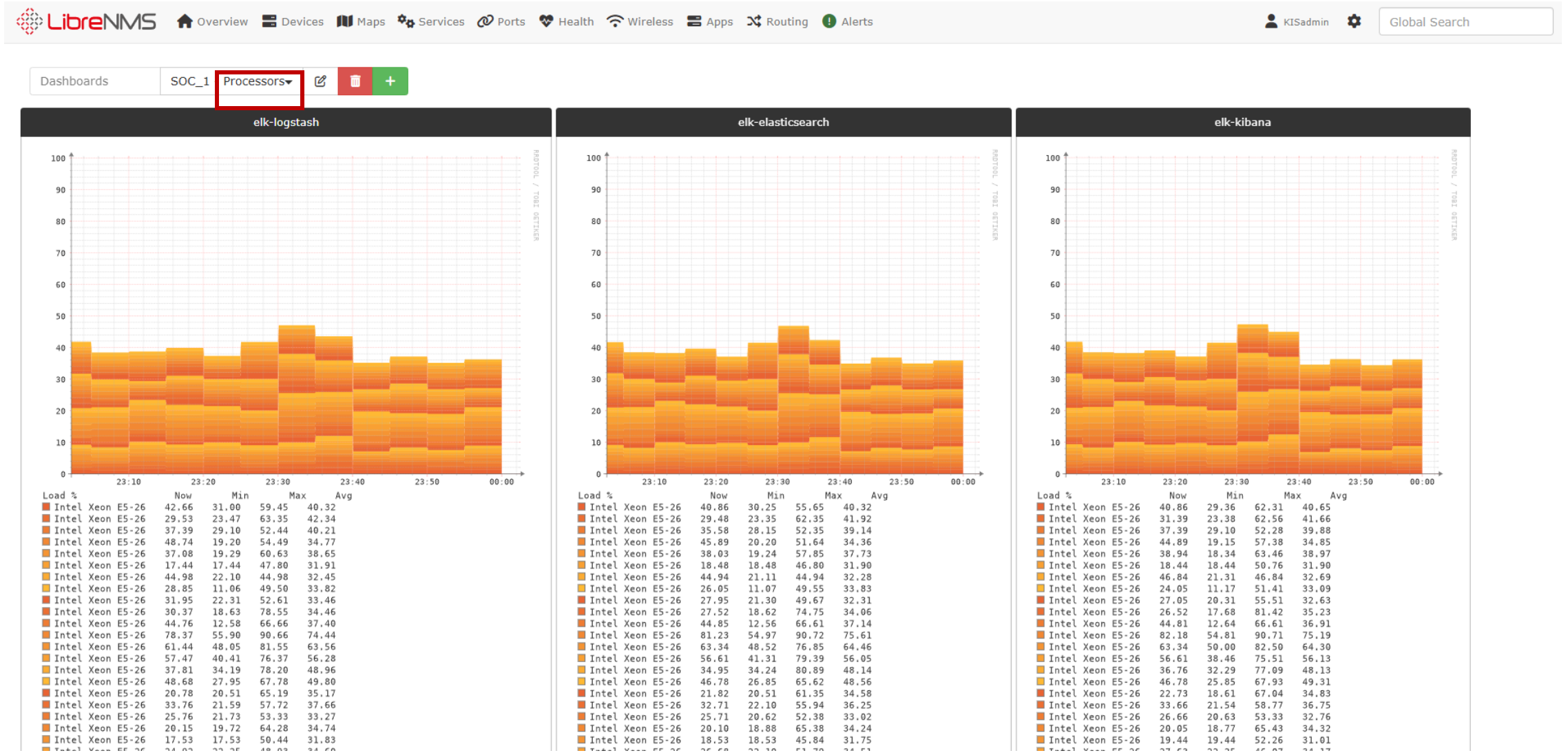


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

LibreNMS

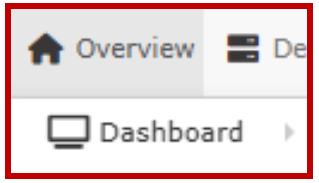
# Využitie CPU

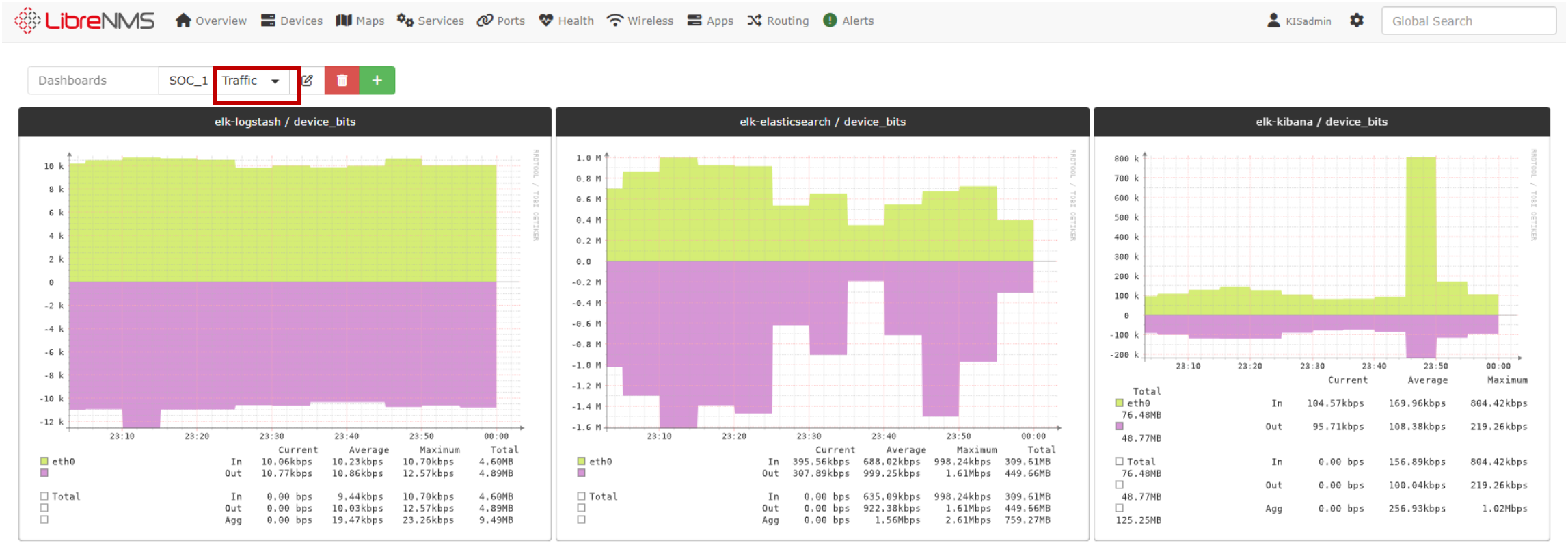


LibreNMS

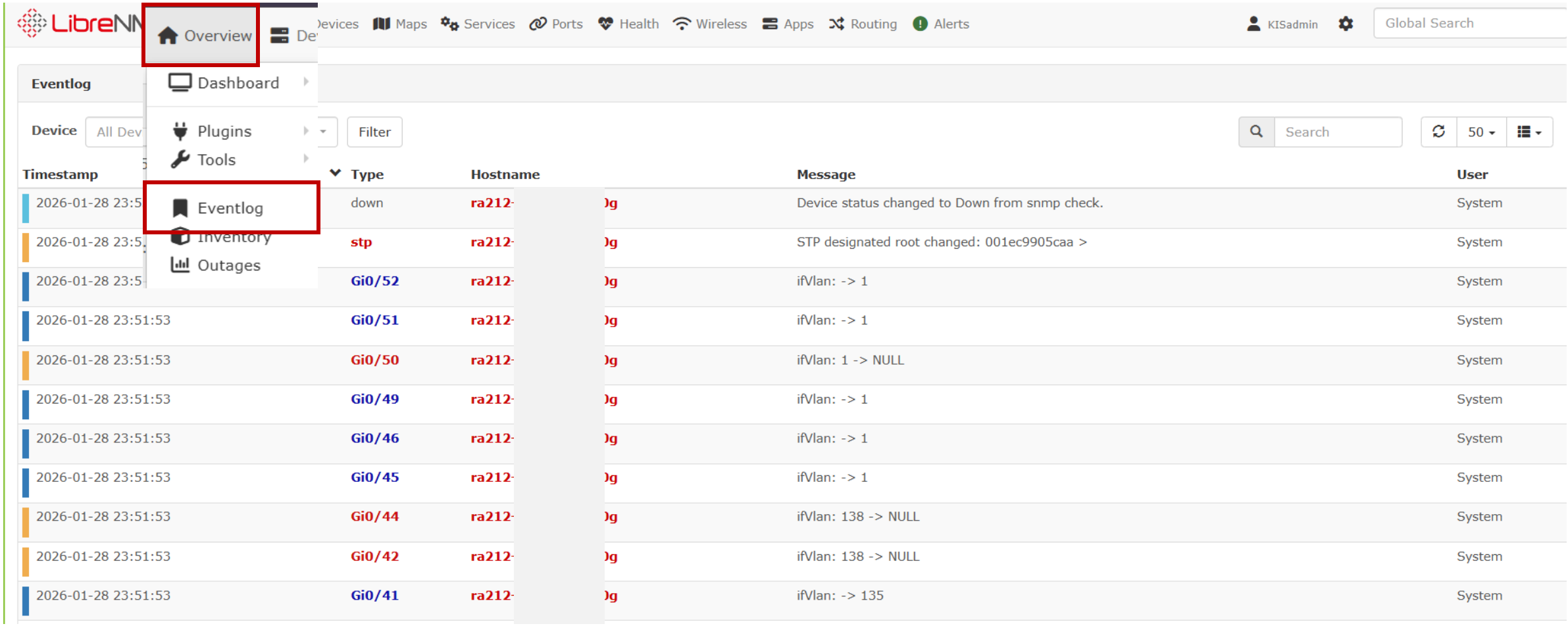
# Sieťová prevádzka



LibreNMS

# Eventlog



# .Overview - Logs

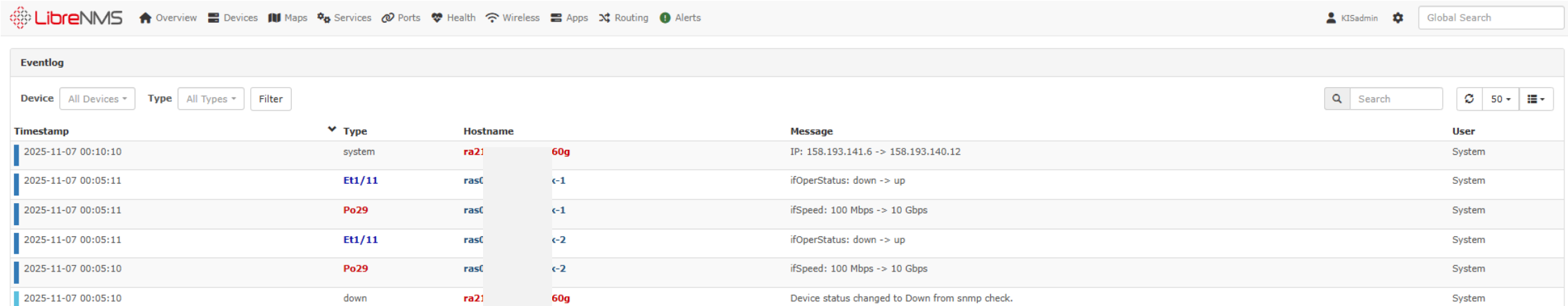
- EventLog v LibreNMS je **interný logovací mechanizmus**, ktorý:
  - zbiera informácie cez SNMP dotazy (polling) zo zariadení,
  - zaznamenáva interné udalosti systému LibreNMS (zmeny stavu, dostupnosti, verzie OS, služby, portov, atď.).
- Tieto údaje sa neposielajú zariadeniami ako syslog správy, ale LibreNMS ich sám zisťuje pri pravidelnom monitoringu (polling interval, typicky každých 5 minút).
- **Čo to znamená prakticky**
  - Ak sa **zmení stav zariadenia** (napr. SNMP prestane odpovedať → „Device down“), LibreNMS to zistí pri ďalšom pollingu a zapíše udalosť do *eventlog* tabuľky v databáze.
  - Ak sa **zmení stav rozhrania** (napr. port „Gi0/1“ ide DOWN), LibreNMS porovná novú SNMP hodnotu s predchádzajúcou a loguje to ako udalosť.
  - Ak sa **zistí nová verzia OS**, zmena IP, hostname, modulov – LibreNMS vytvorí záznam.

LibreNMS

# .Overview - Logs

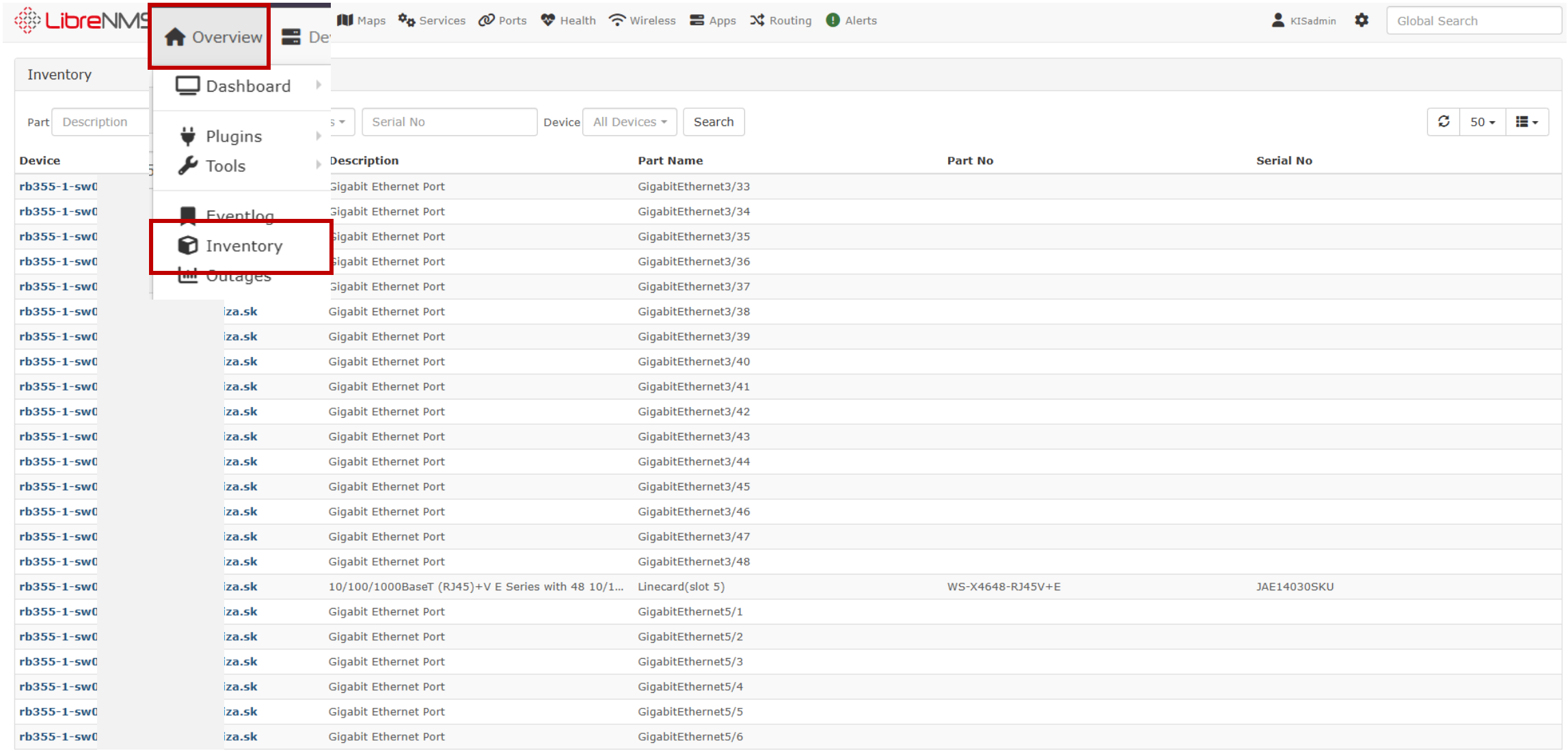
## Na uvedomenie si: EventLog vs Syslog

| Vlastnosť | **EventLog (LibreNMS)** | **Syslog (napr. syslog-ng, Rsyslog, ... )** |
|---|---|---|
| Zdroj dát | SNMP dotazy, interné udalosti | Udalosti posielané zariadením cez UDP/TCP |
| Smer toku | LibreNMS → zariadenie (polling) | Zariadenie → server (push) |
| Čas reakcie | závisí od intervalu pollingu (napr. 5 min) | okamžitý (real-time) |
| Obsah | zmeny stavu, výpadky, inventárne zmeny | logy systému, aplikácií, chýb, IDS alerty |
| Uloženie | databáza LibreNMS (tabuľka `eventlog`) | log súbory alebo databáza syslog servera |
| Použitie | prehľad o stave zariadení a ich zmien | detailná forenzná analýza, bezpečnostné udalosti |



LibreNMS

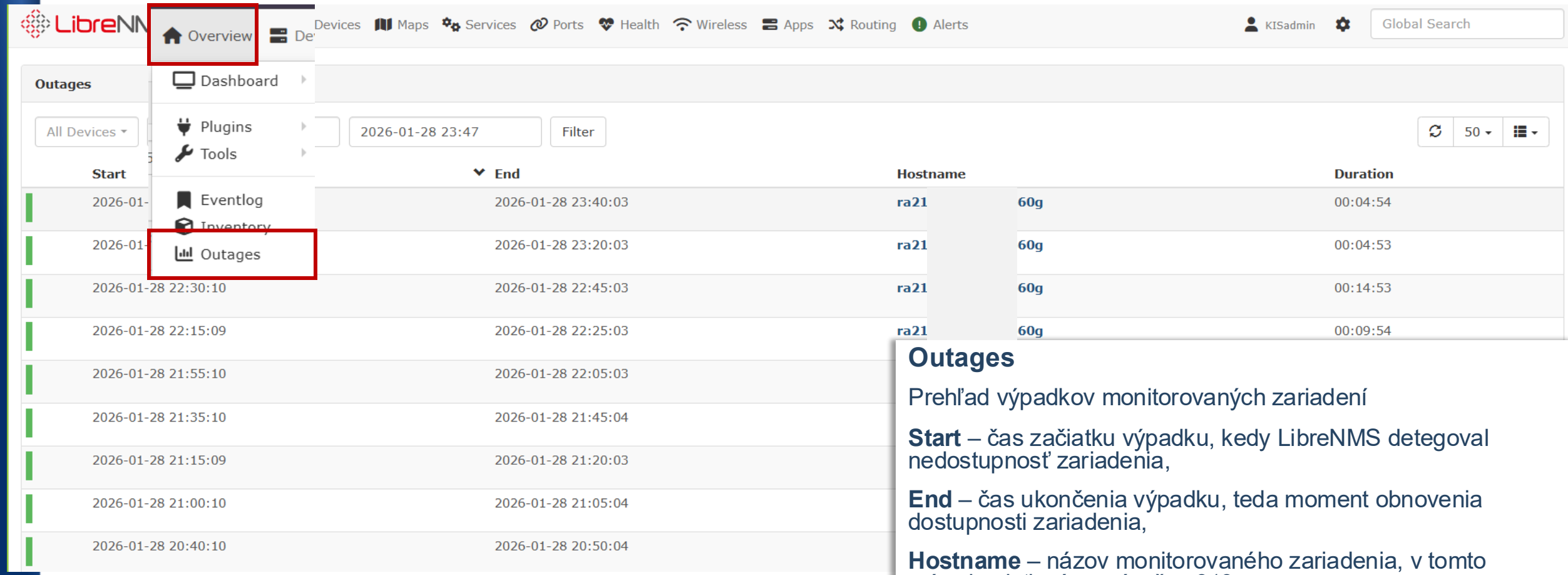
# Inventár




| Device | Description | Part Name | Part No | Serial No |
|---|---|---|---|---|
| rb355-1-sw0 | Gigabit Ethernet Port | GigabitEthernet3/33 | | |
| rb355-1-sw0 | Gigabit Ethernet Port | GigabitEthernet3/34 | | |
| rb355-1-sw0 | Gigabit Ethernet Port | GigabitEthernet3/35 | | |
| rb355-1-sw0 | Gigabit Ethernet Port | GigabitEthernet3/36 | | |
| rb355-1-sw0 | Gigabit Ethernet Port | GigabitEthernet3/37 | | |
| rb355-1-sw0 iza.sk | Gigabit Ethernet Port | GigabitEthernet3/38 | | |
| rb355-1-sw0 iza.sk | Gigabit Ethernet Port | GigabitEthernet3/39 | | |
| rb355-1-sw0 iza.sk | Gigabit Ethernet Port | GigabitEthernet3/40 | | |
| rb355-1-sw0 iza.sk | Gigabit Ethernet Port | GigabitEthernet3/41 | | |
| rb355-1-sw0 iza.sk | Gigabit Ethernet Port | GigabitEthernet3/42 | | |
| rb355-1-sw0 iza.sk | Gigabit Ethernet Port | GigabitEthernet3/43 | | |
| rb355-1-sw0 iza.sk | Gigabit Ethernet Port | GigabitEthernet3/44 | | |
| rb355-1-sw0 iza.sk | Gigabit Ethernet Port | GigabitEthernet3/45 | | |
| rb355-1-sw0 iza.sk | Gigabit Ethernet Port | GigabitEthernet3/46 | | |
| rb355-1-sw0 iza.sk | Gigabit Ethernet Port | GigabitEthernet3/47 | | |
| rb355-1-sw0 iza.sk | Gigabit Ethernet Port | GigabitEthernet3/48 | | |
| rb355-1-sw0 iza.sk | 10/100/1000BaseT (RJ45)+V E Series with 48 10/1... | Linecard(slot 5) | WS-X4648-RJ45V+E | JAE14030SKU |
| rb355-1-sw0 iza.sk | Gigabit Ethernet Port | GigabitEthernet5/1 | | |
| rb355-1-sw0 iza.sk | Gigabit Ethernet Port | GigabitEthernet5/2 | | |
| rb355-1-sw0 iza.sk | Gigabit Ethernet Port | GigabitEthernet5/3 | | |
| rb355-1-sw0 iza.sk | Gigabit Ethernet Port | GigabitEthernet5/4 | | |
| rb355-1-sw0 iza.sk | Gigabit Ethernet Port | GigabitEthernet5/5 | | |
| rb355-1-sw0 iza.sk | Gigabit Ethernet Port | GigabitEthernet5/6 | | |

LibreNMS

# Sieťová prevádzka




## Outages

Prehľad výpadkov monitorovaných zariadení

**Start** – čas začiatku výpadku, kedy LibreNMS detegoval nedostupnosť zariadenia,

**End** – čas ukončenia výpadku, teda moment obnovenia dostupnosti zariadenia,

**Hostname** – názov monitorovaného zariadenia, v tomto prípade sieťový prepínač *ra212-....*

**Duration** – celkové trvanie výpadku vyjadrené v hodinách, minútach a sekundách.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Nájdenie a monitorovanie zariadení

Objavenie zariadení v sieti a ich pridanie do zoznamu prebieha na základe procesu **auto-discovery**, ktorý beží v pravidelných intervaloch. Po objavení zariadenia je možné ho nájsť v zozname na záložke **Devices – All Devices.**

| 01 | 02 | 03 |
|---|---|---|
| **Auto-Discovery** | **Pridanie do zoznamu** | **Detail zariadenia** |
| Automatické objavenie zariadení v sieti pomocou SNMP protokolu | Zariadenie sa zobrazí v zozname so základnými informáciami | Zobrazenie podrobných grafov a monitorovacích údajov |

# Auto discovery vs polling

## Auto Discovery

- Proces vyhľadávania a pridávania nových zariadení alebo komponentov do systému
- Využíva sieťové protokoly ako CDP, LLDP, OSPF, BGP, SNMP, ARP

## Polling

- Proces dopytovania sa už pridaných zariadnení na ich aktuálny stav
- Zbiera metriky ako: vyťaženie CPU, prenosy na portoch,...

| Funkcia | Auto discovery | Polling |
|---|---|---|
| Účel | Hľadanie nových cieľov | Zber metrík existujúcich cieľov |
| Hlavný protokol | CDP/LLDP/SRP/SNMP | SNMP |
| Predvolený čas | 6 hodín | 5 minút |
| Príkaz (cli) | ./discovery.php -h all | ./poller.php -h all |

# Nájdenie a monitorovanie zariadení

V **zozname** máme k dispozícii **základné informácie**

- výrobca,
- meno/IP zariadenia,
- operačný systém.

Po **kliknutí ľavým tlačidlom myši na zariadenie** sa zobrazí jeho **detail** so základnými grafmi a monitorovacími údajmi.

Pre **monitorovanie stavu** zariadenia, máme k dispozícii kartu Health:

- **teplota** – monitorovanie teploty komponentov zariadenia,
- **výkon CPU** – sledovanie zaťaženia procesorov,
- **pamäť** - kontrola využitia operačnej pamäte.



Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

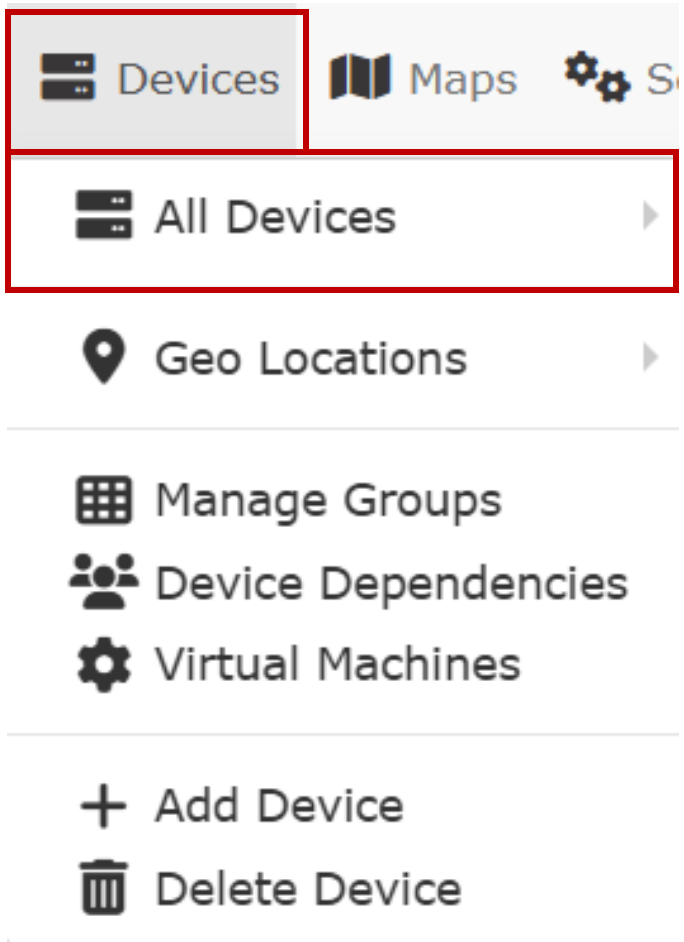
# Hlavné menu - Devices

**Devices (monitorovanie zariadení):**

- zoznam a stav všetkých zariadení (smerovače, prepínače, servery…),
- OS, IP, verzia SNMP, dostupnosť.

**Bezpečnostný význam:**

**→ identifikácia neautorizovaných zariadení,**
**→ kontrola OS a firmvérových verzií,**
**→ monitoring dostupnosti kritických prvkov.**



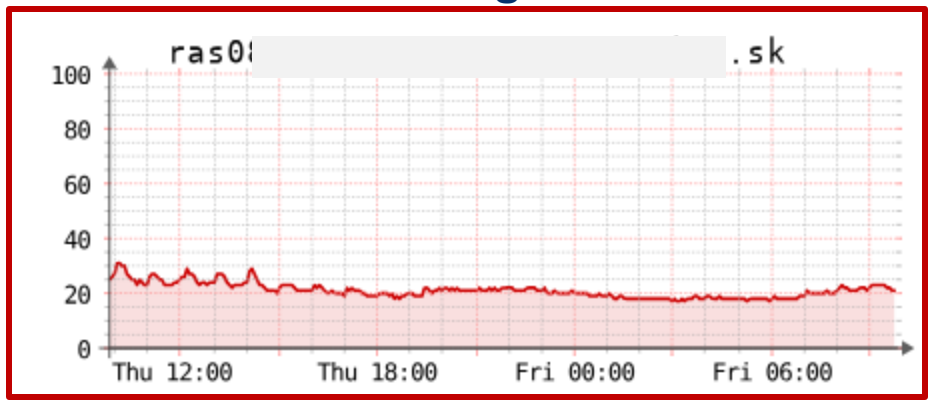
LibreNMS

# Hlavné menu - Devices

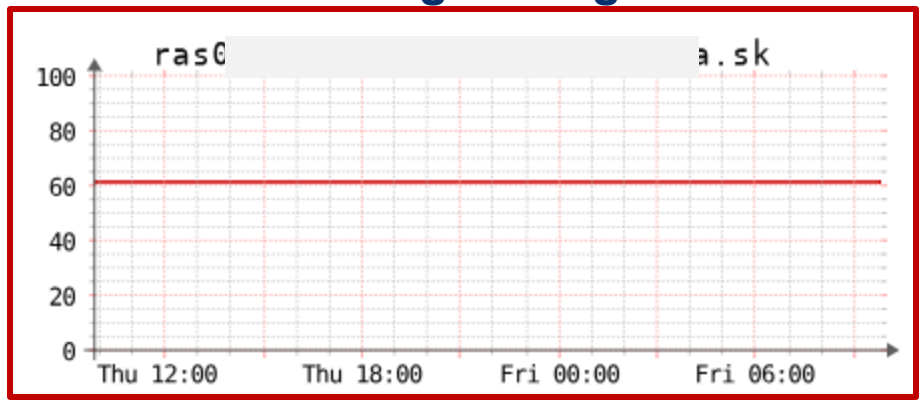
## Zobrazenie podsekcie **All devices**

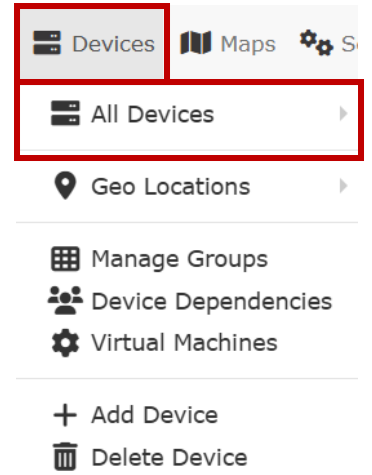
| S. | Id | M. | Vendor | Device | Metrics | Platform | Operating System | Time | Location | Actions |
|---|---|---|---|---|---|---|---|---|---|---|
| | 62 | | cisco | ras0 158. a.sk | 57 5 | Catalyst 3750G (WS-C3750G-48TS-S) | Cisco IOS 15.0(2)SE11 (IPSERVICESK9) | 1mo 2d 22h | | |
| | 40 | | cisco | rb00 158. a.sk | 55 5 | Catalyst 3560G (WS-C3560G-48TS-S) | Cisco IOS 12.2(55)SE12 (IPBASEK9) | 4mos 3w 6d | | |
| | 59 | | cisco | rc02 158. a.sk | 34 5 | Cat37xx Stacking | Cisco IOS 12.2(50)SE5 (IPBASEK9) | 10mos 2w 20h | | |
| | 47 | | cisco | ra32 158. a.sk | 35 5 | Catalyst 2960X (WS-C2960X-24TS-L) | Cisco IOS 15.2(2)E6 (UNIVERSALK9) | 10mos 2w 19h | | |
| | 60 | | cisco | ras0 158. a.sk | 62 5 | Cat37xx Stacking | Cisco IOS 15.0(2)SE11 (IPSERVICESK9) | 10mos 1w 1h | | |
| | 63 | | cisco | ras0 158. za.sk | 47 17 | Catalyst 3750E (WS-C3750E-24TD-E) | Cisco IOS 15.0(2)SE11 (UNIVERSALK9) | 10mos 2w 20h | | |

**monitoring CPU**



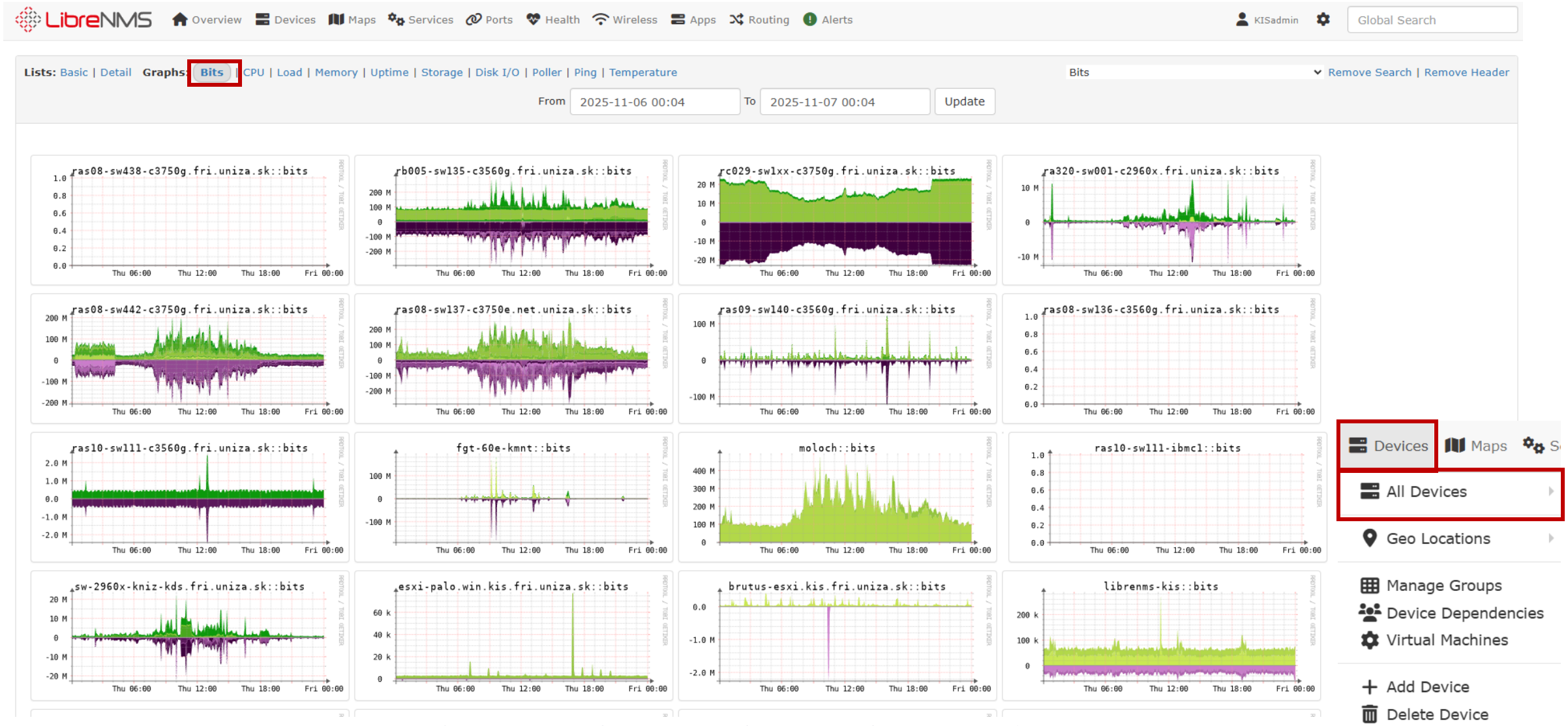

**monitoring storage**



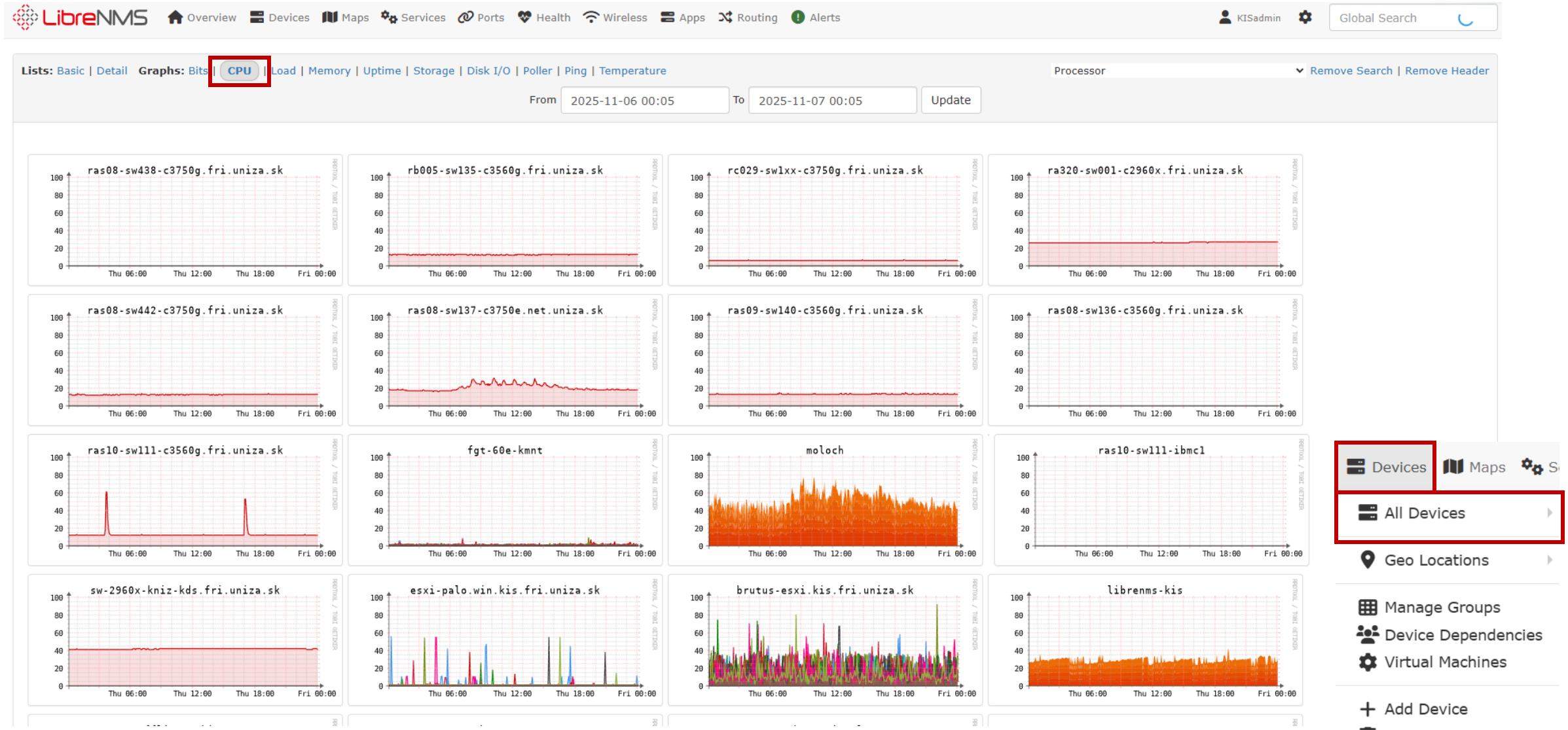



LibreNMS

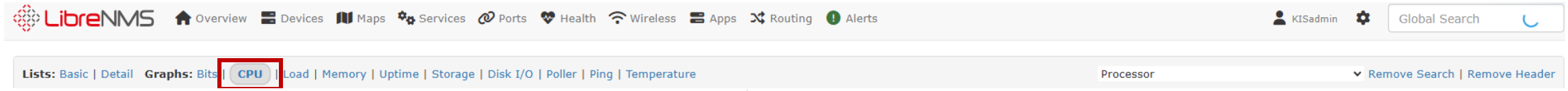
# Zariadenia - Sieťová prevádzka

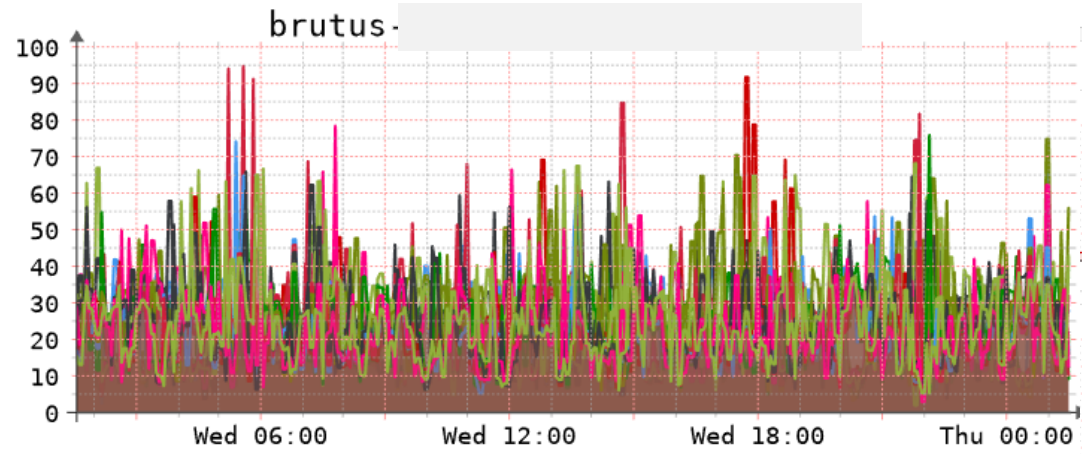


# Zariadenia - Zaťaženie CPU

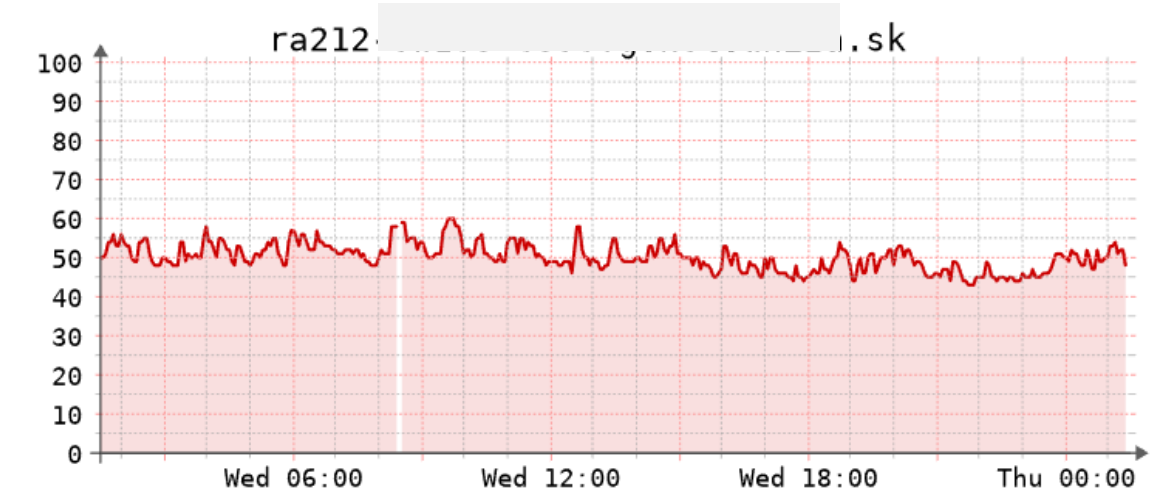


# Zariadenia - Zaťaženie CPU

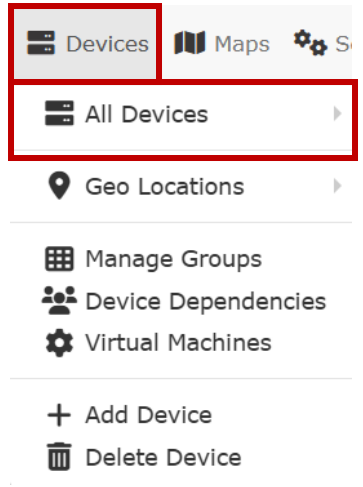



| Load % | Now | Min | Max | Avg |
|---|---|---|---|---|
| Pkg/ID/Node: 0 | 18.49 | 9.13 | 78.71 | 21.47 |
| Pkg/ID/Node: 0 | 42.05 | 4.20 | 52.01 | 17.85 |
| Pkg/ID/Node: 0 | 27.86 | 6.33 | 56.74 | 20.47 |
| Pkg/ID/Node: 0 | 18.79 | 5.42 | 46.86 | 20.12 |
| Pkg/ID/Node: 0 | 19.21 | 7.07 | 68.67 | 19.90 |
| Pkg/ID/Node: 0 | 21.93 | 5.42 | 55.86 | 21.73 |
| Pkg/ID/Node: 0 | 17.93 | 8.14 | 66.42 | 19.69 |
| Pkg/ID/Node: 0 | 18.00 | 7.67 | 58.97 | 21.92 |
| Pkg/ID/Node: 0 | 18.07 | 4.61 | 46.00 | 19.27 |
| Pkg/ID/Node: 0 | 19.35 | 4.07 | 53.04 | 21.86 |
| Pkg/ID/Node: 0 | 16.84 | 2.40 | 65.80 | 21.34 |
| Pkg/ID/Node: 0 | 55.91 | 3.35 | 64.76 | 22.03 |
| Pkg/ID/Node: 0 | 20.42 | 3.83 | 84.71 | 20.34 |

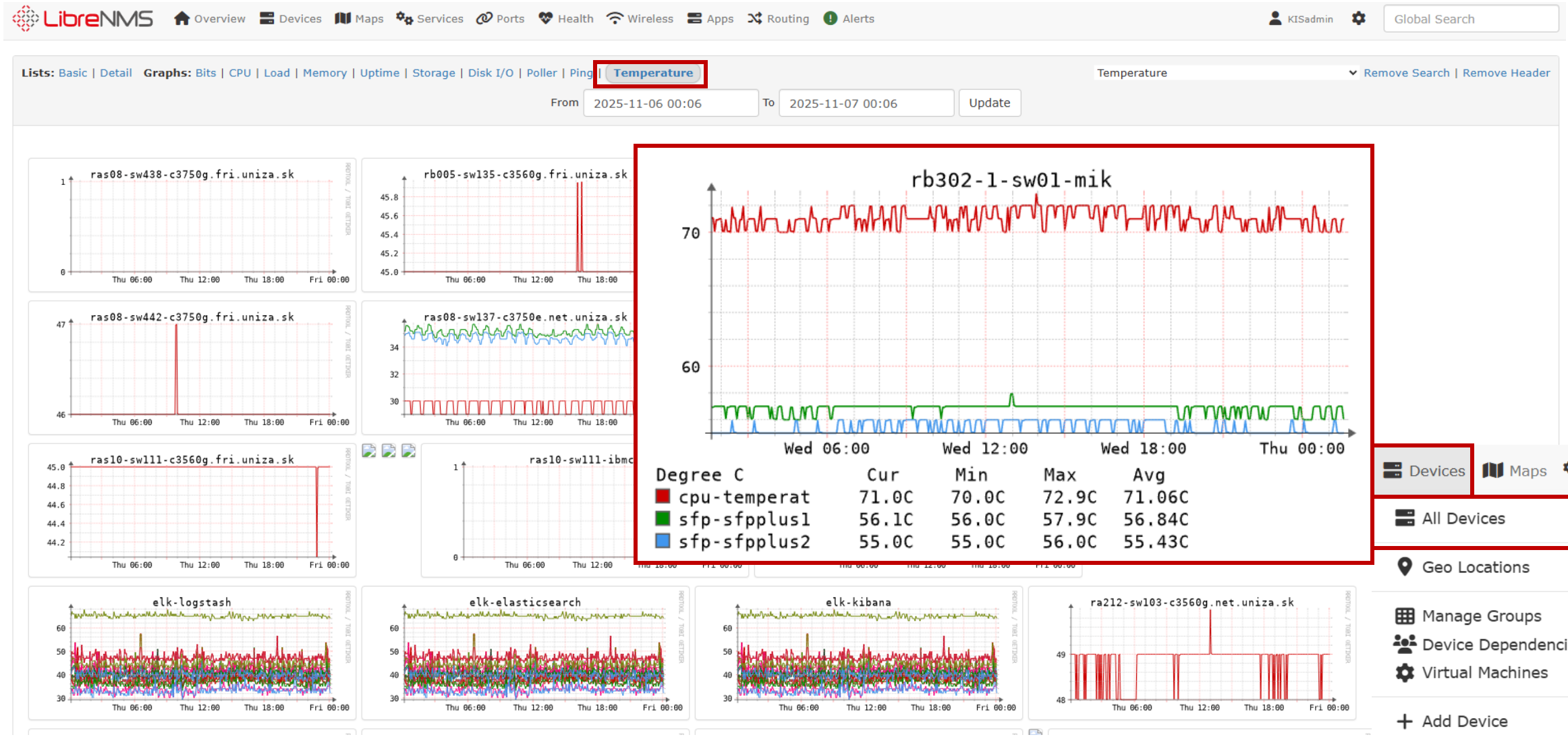



| Load % | Now | Min | Max | Avg |
|---|---|---|---|---|
| Processor 1 | 48.06 | 43.00 | 60.00 | 50.07 |



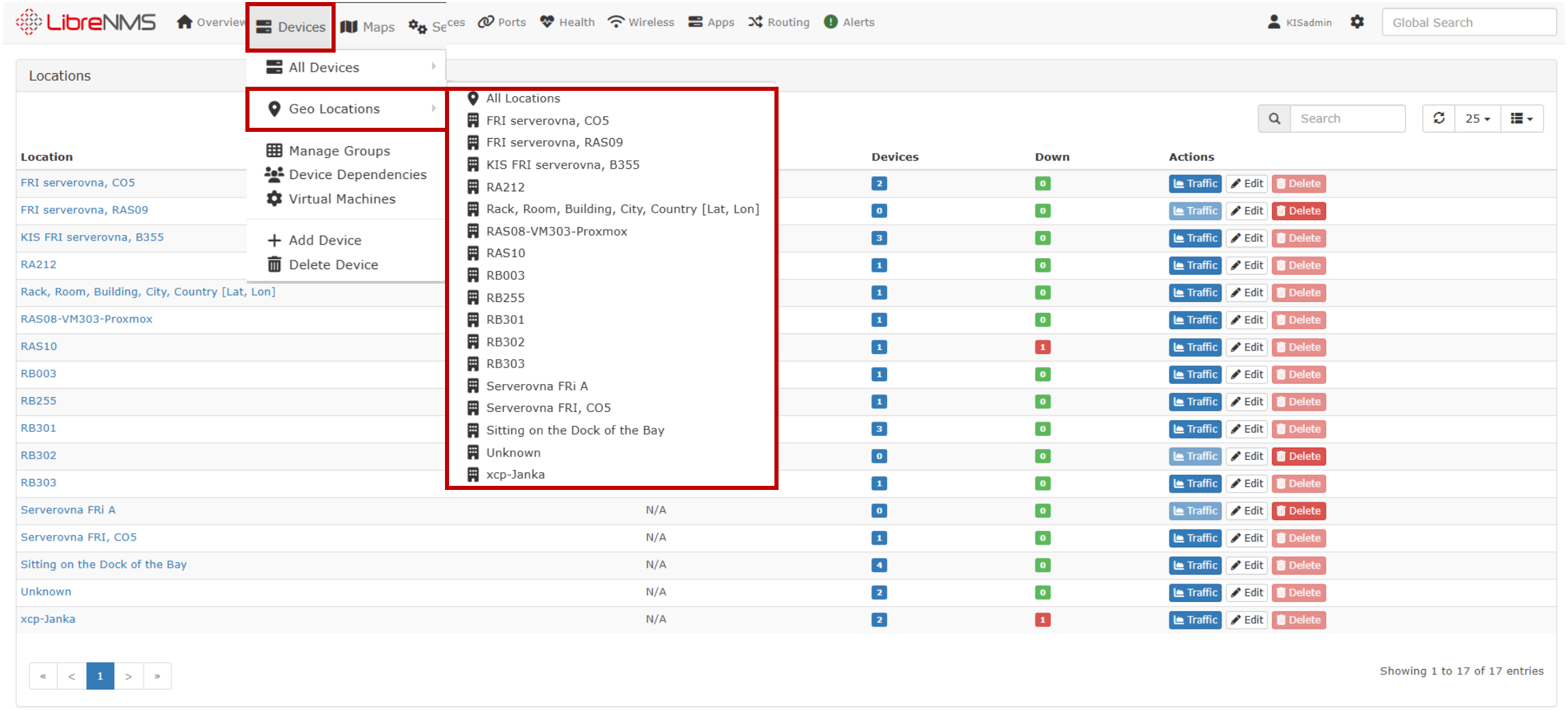
LibreNMS

# Teplota zariadení



LibreNMS

# Zariadenia - Lokácia zariadení



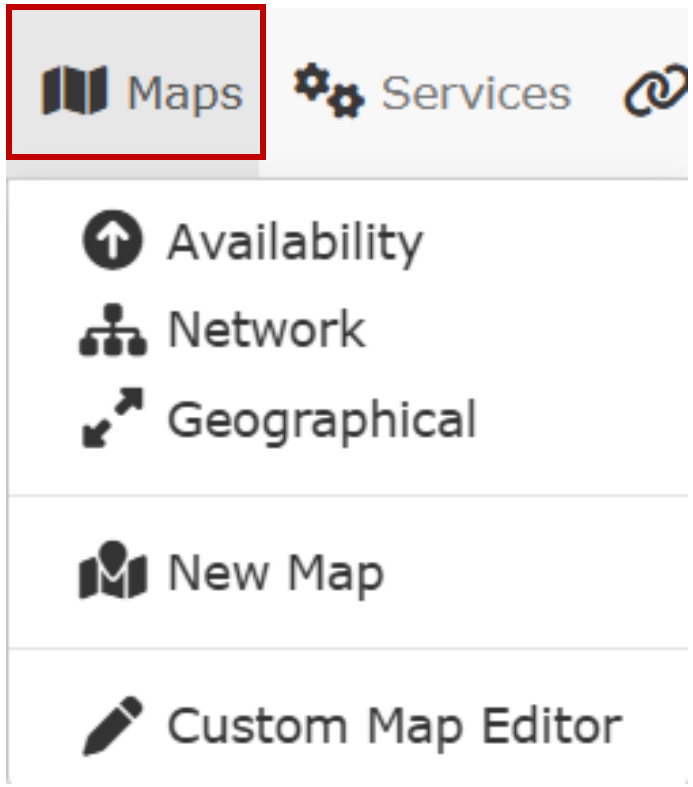
# Hlavné menu - Maps

## Maps (topológia siete)

- Grafické zobrazenie prepojení medzi zariadeniami
- Automaticky generované alebo ručne definované mapy

**Bezpečnostný význam:**

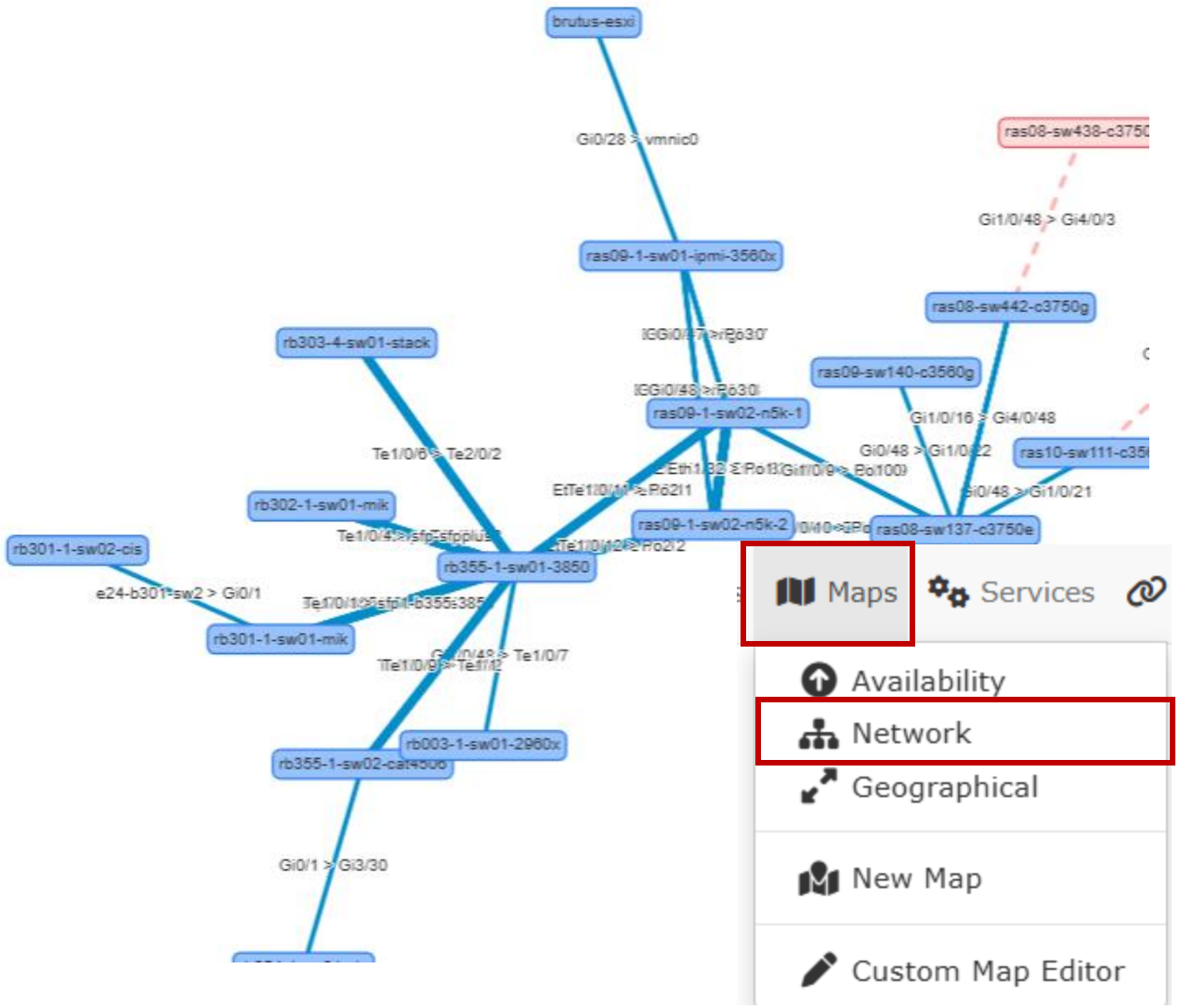
**→ Odhalenie neznámych spojení**
**→ Vizualizácia segmentácie siete**
**→ Overenie správneho smerovania tokov**



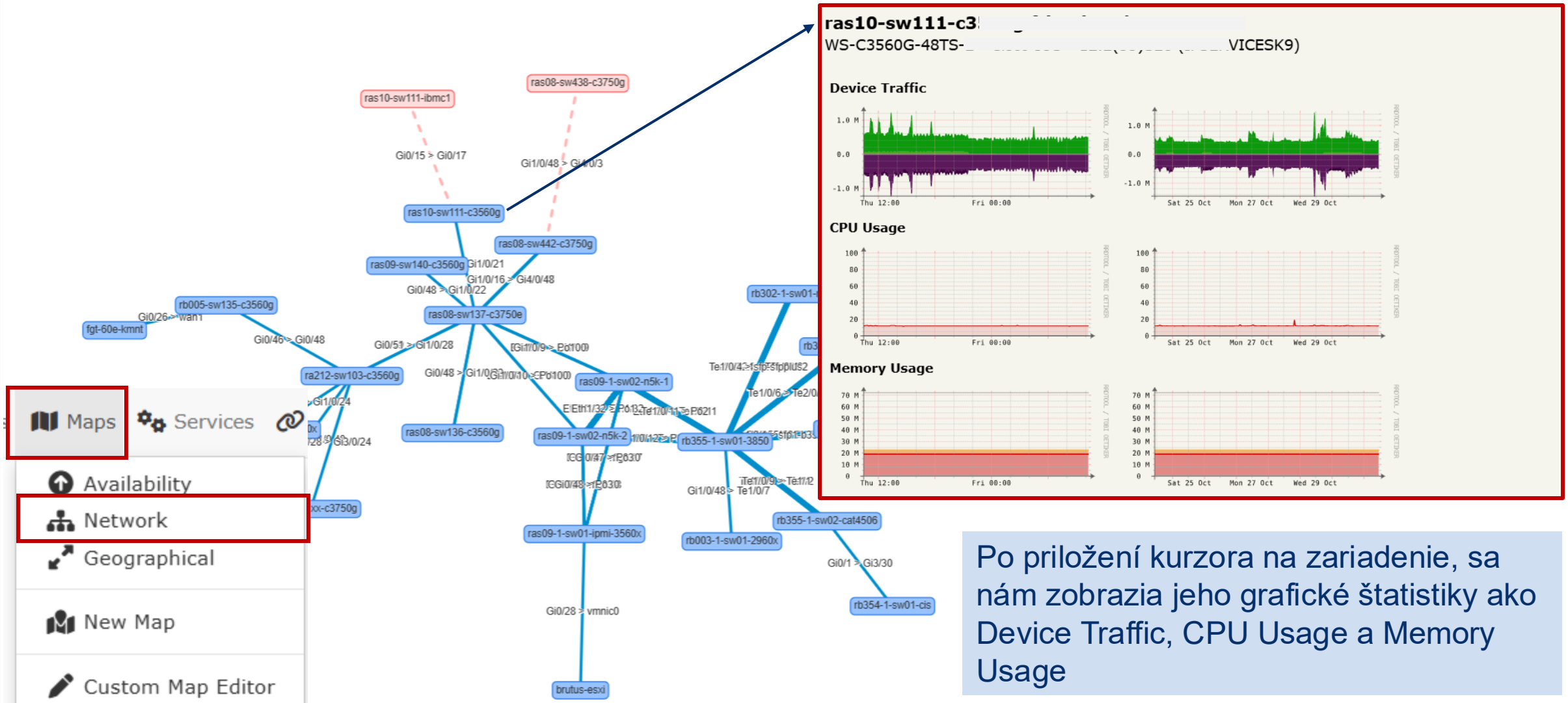
# Topologická mapa siete

- Jednou z dôležitých funkcionalít, ktoré LibreNMS poskytuje, je zobrazenie **topologickej mapy**.
  - Je možné ho nájsť na karte **Maps – Network.**

- Najväčším problémom topologickej mapy je v súčasnosti náhodné určovanie pozícií zariadení
  - čo má za následok nesúrodé vykresľovanie pri obnovení stránky



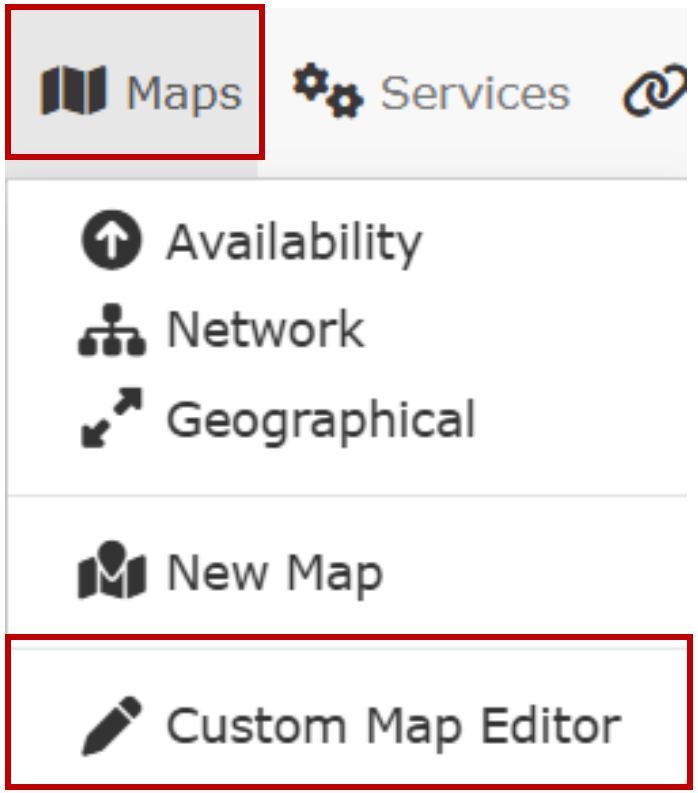
# Hlavné menu - Maps




Po priložení kurzora na zariadenie, sa nám zobrazia jeho grafické štatistiky ako Device Traffic, CPU Usage a Memory Usage

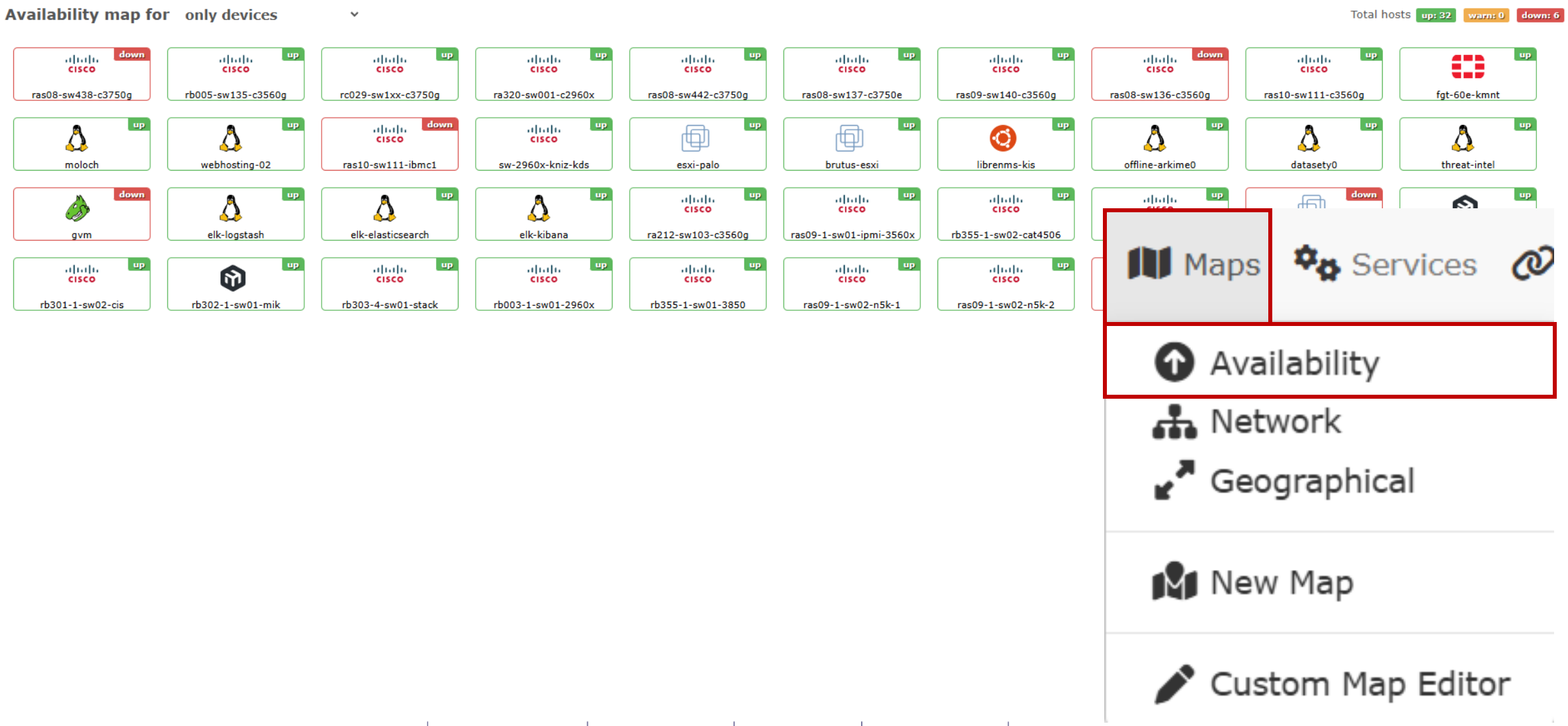
# Custom Map Editor

- Možnosť vytvoriť vlastnú mapu
- definujeme:
  - Názov, šírku a výšku mapy v pixeloch, zarovnanie uzlov – po pridaní nových zariadení ich táto funkcia zarovná do neviditeľnej mriežky - vylepší to custom vzhľad mapy
- Pridanie zariadenia:
  - Po pridaní zariadenia nás librenms vyzve aby sme si vybrali bod na mape, kde má byť zariadenie zobrazené
- Pridanie hrany
  - Prepojenie medzi zariadeniami môžeme zakresliť manuálne kliknutím na dve zariadenia, ktoré chceme prepojiť - definujeme: od, do, port, smer portu, štýl čiary, percentuálne využitie linky, ...
- Uloženie zmien + Uloženie mapy
  - Po uložení sa nová verzia zobrazí všetkým používateľom
  - Po  obnovení stránky by sa nemalo zmeniť rozloženie zariadení



LibreNMS

# .Maps - Dostupné zariadenia



# Hlavné menu – ports, health, alerts

## Ports

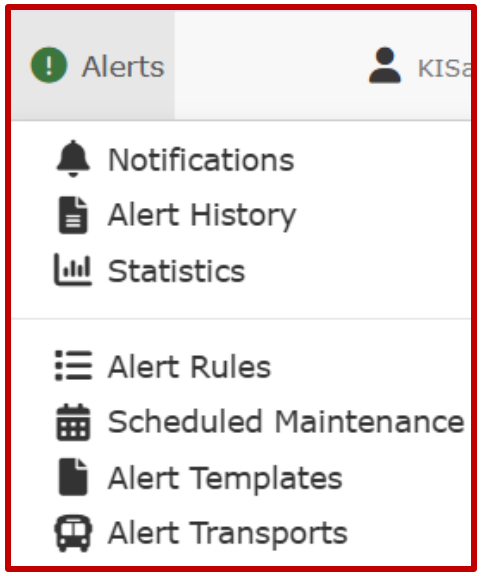
- sleduje stav a priepustnosť sieťových portov,
- deteguje výpadky, neautorizované pripojenia a zmeny konfigurácie,
- umožňuje identifikovať chybné alebo neaktívne porty.

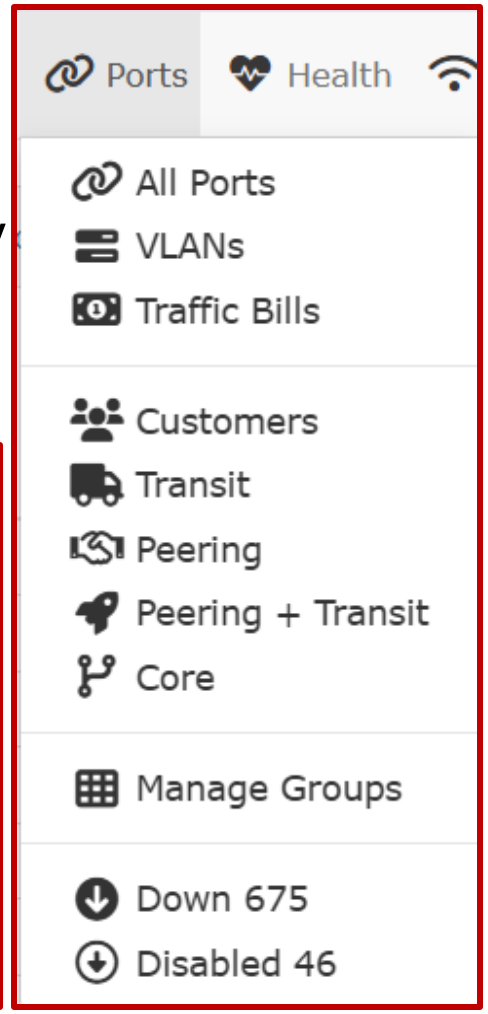
## Health

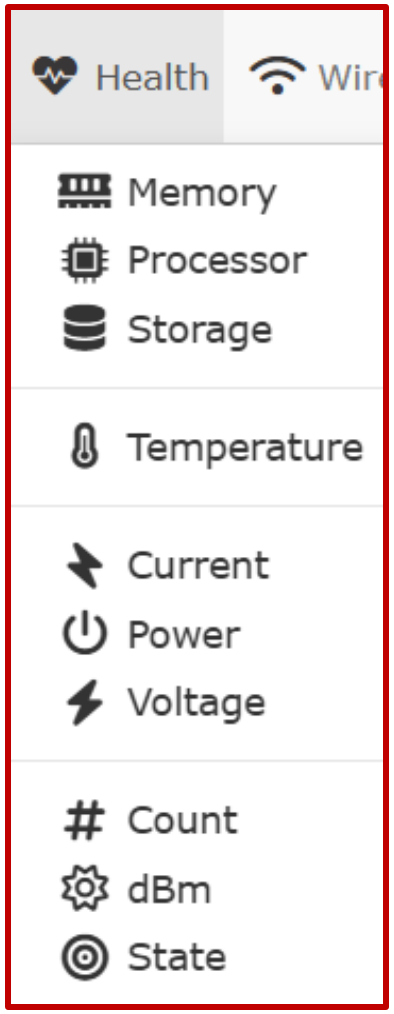
- monitorovanie **výkonu zariadení**: napr. pamäť, procesor, úložisko.
- poskytuje prehľad o stave zariadenia v reálnom čase.

## Alerts

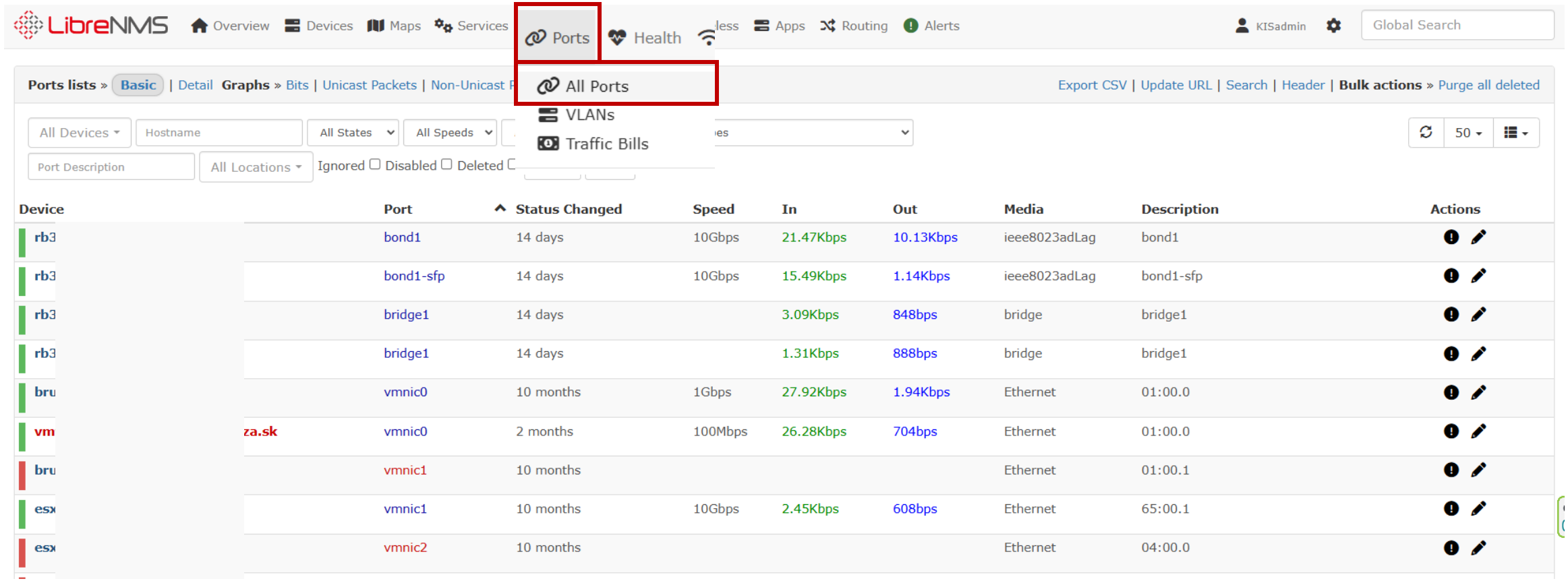
- automatické upozornenia,
- podporuje plánovanie údržby a reakcie na incidenty.



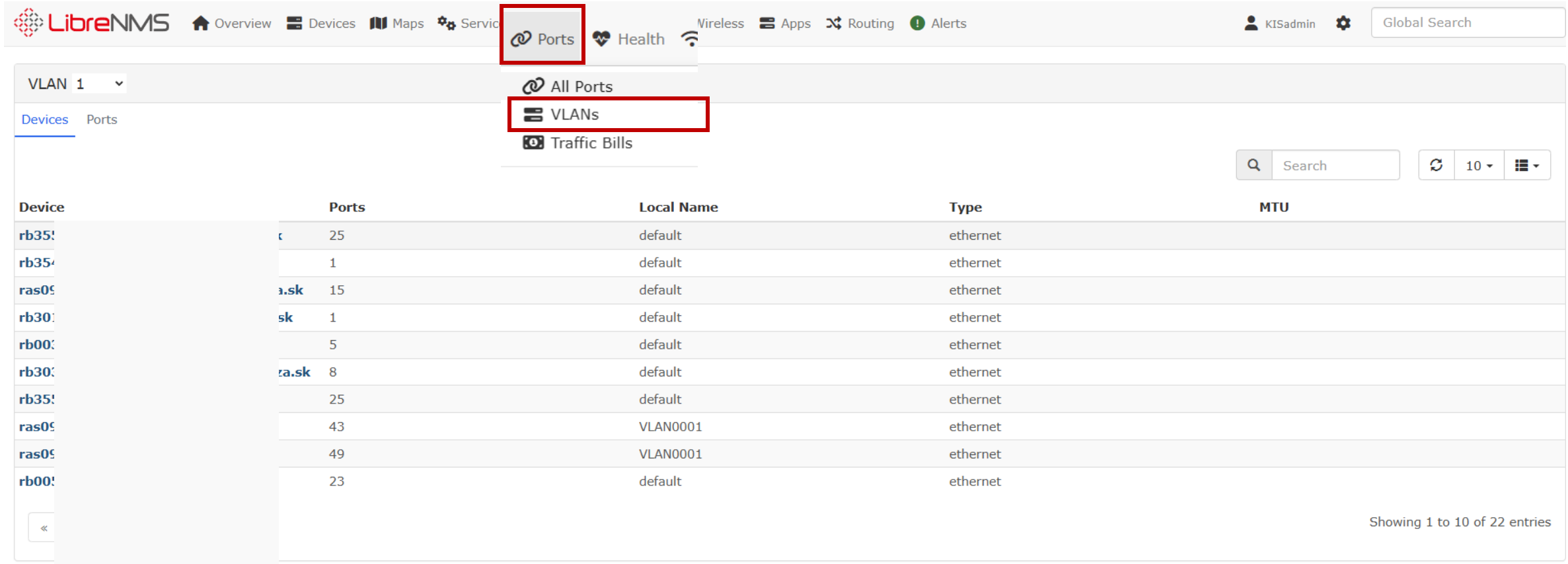



# LibreNMS
# .Ports



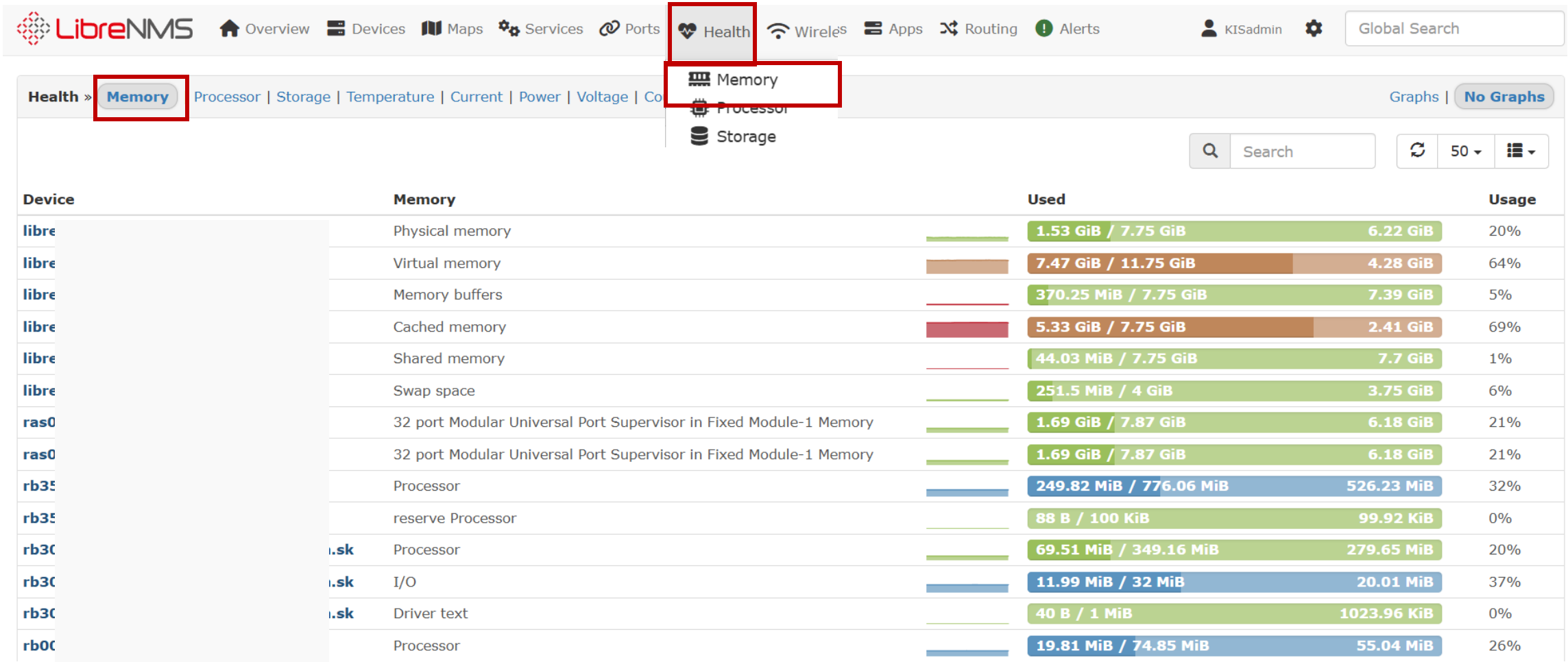
LibreNMS

# Virtuálne siete



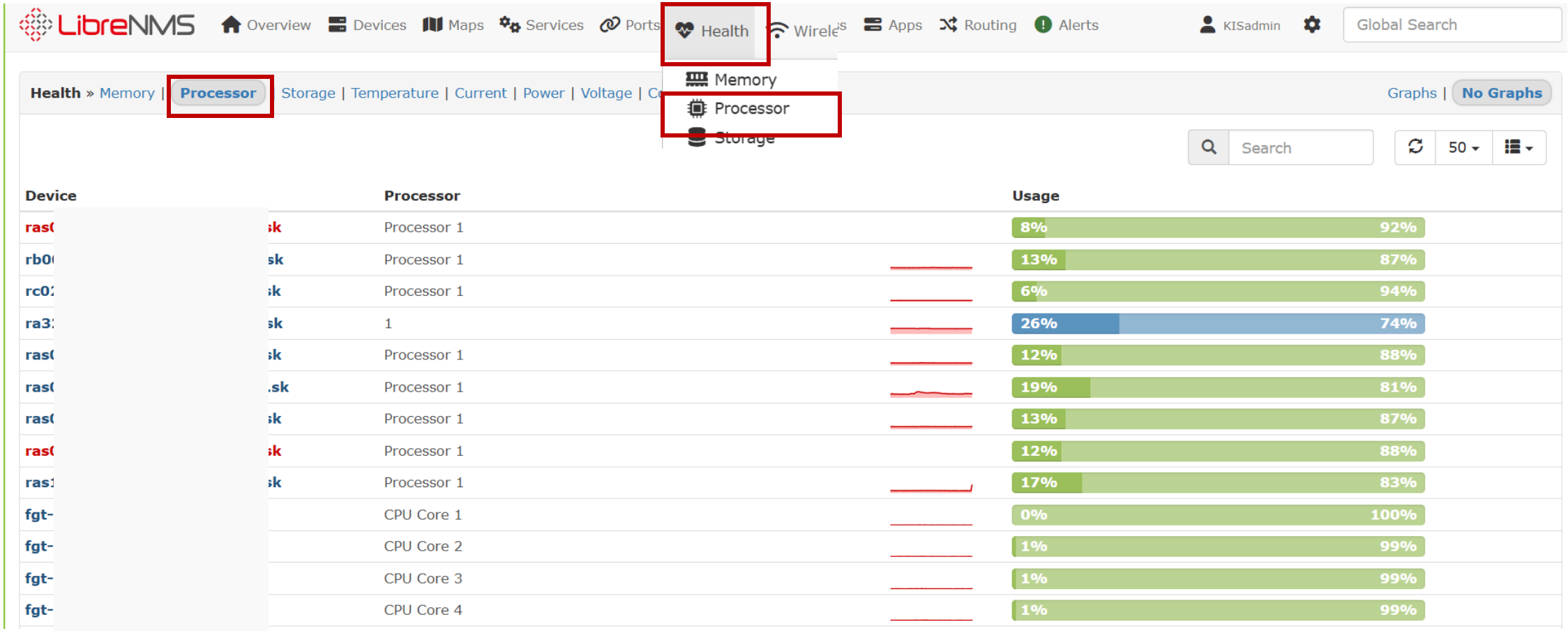
LibreNMS

# Health - Memory



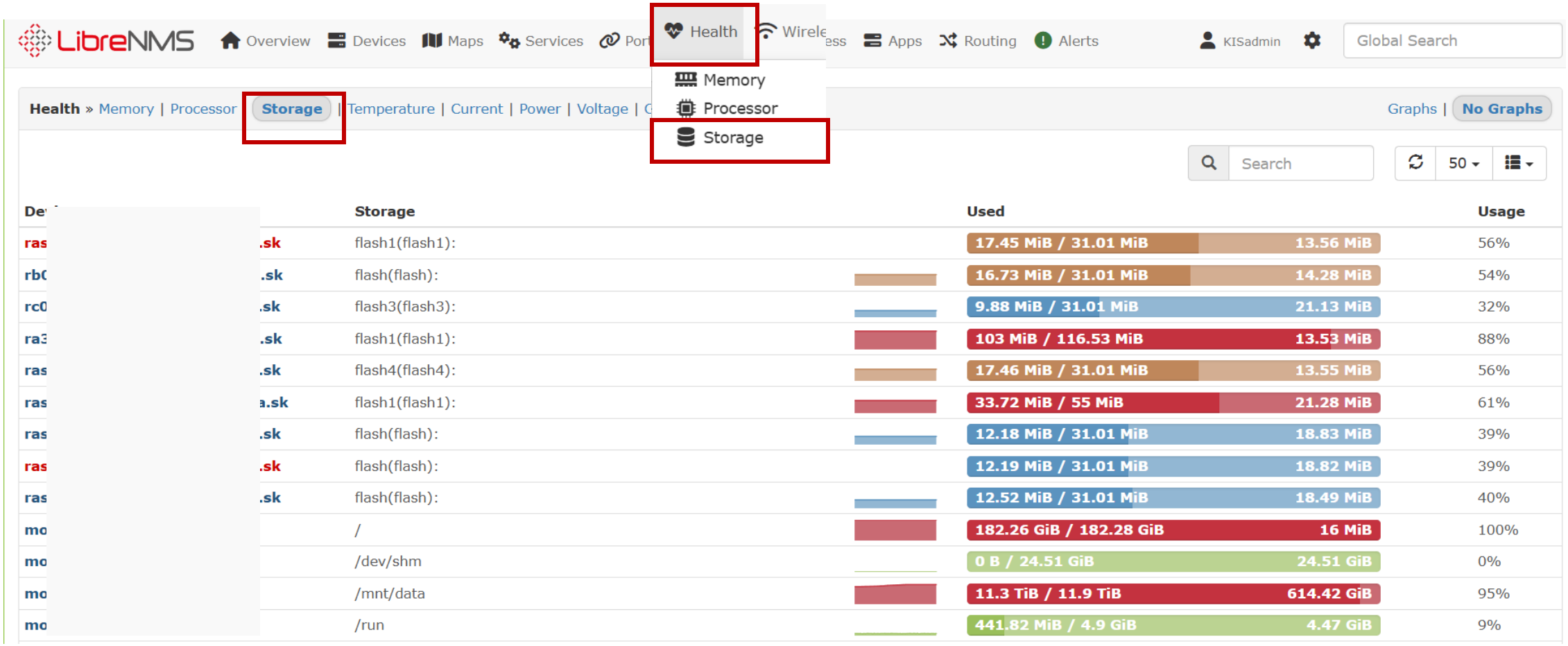
LibreNMS

# Health - Processor



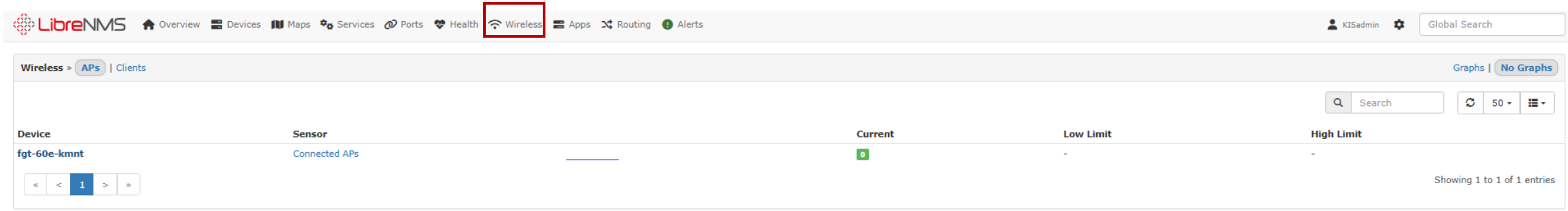
LibreNMS

# Health - storage



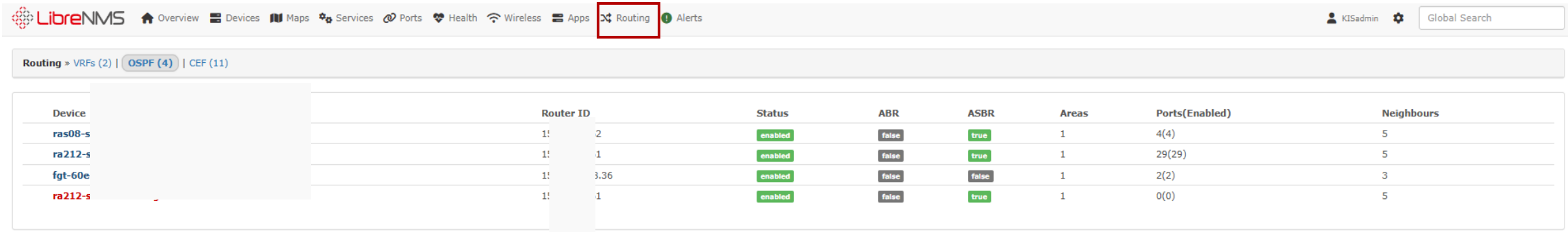
LibreNMS

# Wireless - AP



LibreNMS

# VRF, OSPF zariadenia



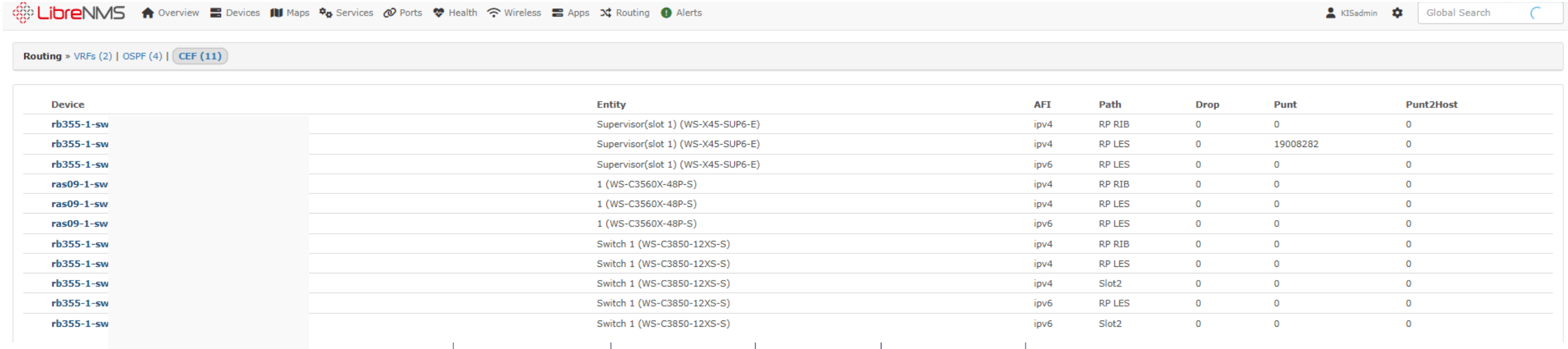

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# .Routing - Cisco CEF

**Cisco zariadenie** (napr. router alebo L3 switch) s povoleným SNMP, dokáže načítať a zobraziť informácie o **stavoch a štatistikách CEF**

- CEF si **predpočítava** informácie o smerovaní a ukladá ich do **Forwarding Information Base (FIB)** a **Adjacency Table**

| Parameter | Význam |
|---|---|
| **FIB entries** | počet záznamov vo Forwarding Information Base – t. j. koľko smerovacích ciest má zariadenie predpočítaných |
| **Adjacency entries** | počet susedných zariadení alebo rozhraní, pre ktoré sú pripravené cesty |
| **CEF switching statistics** | počty prepnutých paketov, chybovosť, CPU využitie pri forwarding operáciách |
| **CEF interface states** | stav CEF na jednotlivých sieťových rozhraniach (či je zapnutý/vypnutý, aktívny/neaktívny) |




| Device | Entity | AFI | Path | Drop | Punt | Punt2Host |
|---|---|---|---|---|---|---|
| rb355-1-sw | Supervisor(slot 1) (WS-X45-SUP6-E) | ipv4 | RP RIB | 0 | 0 | 0 |
| rb355-1-sw | Supervisor(slot 1) (WS-X45-SUP6-E) | ipv4 | RP LES | 0 | 19008282 | 0 |
| rb355-1-sw | Supervisor(slot 1) (WS-X45-SUP6-E) | ipv6 | RP LES | 0 | 0 | 0 |
| ras09-1-sw | 1 (WS-C3560X-48P-S) | ipv4 | RP RIB | 0 | 0 | 0 |
| ras09-1-sw | 1 (WS-C3560X-48P-S) | ipv4 | RP LES | 0 | 0 | 0 |
| ras09-1-sw | 1 (WS-C3560X-48P-S) | ipv6 | RP LES | 0 | 0 | 0 |
| rb355-1-sw | Switch 1 (WS-C3850-12XS-S) | ipv4 | RP RIB | 0 | 0 | 0 |
| rb355-1-sw | Switch 1 (WS-C3850-12XS-S) | ipv4 | RP LES | 0 | 0 | 0 |
| rb355-1-sw | Switch 1 (WS-C3850-12XS-S) | ipv4 | Slot2 | 0 | 0 | 0 |
| rb355-1-sw | Switch 1 (WS-C3850-12XS-S) | ipv6 | RP LES | 0 | 0 | 0 |
| rb355-1-sw | Switch 1 (WS-C3850-12XS-S) | ipv6 | Slot2 | 0 | 0 | 0 |


# Inventarizačný nástroj - GLPI

GLPI

# Účel

GLPI je **open-source** platforma na riadenie **IT služieb** (ITSM) a **IT aktív** (ITAM), ktorá umožňuje organizáciám efektívne **spravovať incidenty, požiadavky, majetok, projekty a procesy IT.**

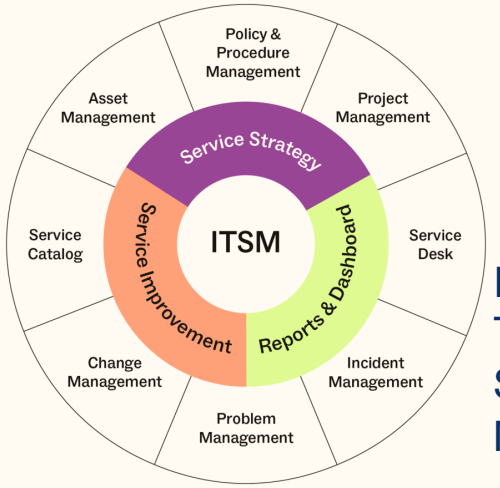
## Hlavné oblasti ITSM, ktoré GLPI pokrýva

- Incident & Request Management
- Problem Management
- Change Management
- Knowledge Base
- SLA management
- Asset & Configuration (CMDB)
- Supplier Management
- Projektový manažment
- Plánovanie zdrojov & time tracking
- Finančný manažment a rozpočty
- Rezervácie vybavenia a miestností

## Prečo je GLPI vhodné riešenie aj pre veľké organizácie?

- GDPR anonymizácia dát
- Multitenant/organizácia - oddelenie dát medzi entitami
- Podporuje zložité firemné štruktúry
- Rozšíriteľnosť - pluginy, API, integrácie

**Podporované oblasti mimo ITSM**




Information Technology Service Management

GLPI

# Prehľad kľúčových funkcionalít

| Funkcionalita | Popis |
|---|---|
| Vytváranie incidentov z e-mailov | Automatické generovanie incidentov z prichádzajúcich e-mailov. |
| Jednoduché (bez-kódové) vytváranie formulárov | Umožňuje používateľom vytvárať formuláre bez znalosti programovania. |
| Schvaľovanie prostredníctvom e-mailu | Uľahčuje schvaľovacie procesy cez e-mail. |
| Sledovanie času SLA a OLA | Monitoruje časy dohodnutých úrovní služieb a prevádzkových úrovní služieb. |
| CMDB (Databáza pre správu konfigurácií) | Databáza pre správu konfiguračných položiek a ich vzťahov. |
| Správa licencií | Sledovanie softvérových licencií. |
| Používateľsky prispôsobiteľné rozhranie | Umožňuje používateľom personalizovať rozhranie GLPI. |
| Plánovanie rozpočtu | Nástroje pre plánovanie a riadenie IT rozpočtov. |
| Plánovanie a alokácia zdrojov | Funkcie pre efektívne riadenie zdrojov. |



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Prehľad kľúčových funkcionalít

| Funkcionalita | Popis |
|---|---|
| Sledovanie času a nákladov | Monitorovanie času a výdavkov súvisiacich s IT aktivitami. |
| API pre vývojárov | Aplikačné programovacie rozhranie pre vývojárov na integráciu s GLPI. |
| Automatizačné pravidlá | Definovanie pravidiel pre automatizáciu IT procesov. |
| Podpora Single Sign-On | Zabezpečenie možnosti jednotného prihlásenia. |
| Firemná hierarchia organizácií s oddelením dát | Podpora komplexných organizačných štruktúr so segregáciou dát. |
| Anonymizácia (GDPR) | Funkcie pre anonymizáciu dát v súlade s predpismi GDPR. |
| Integrácia s monitorovaním cez API | Pripojenie k monitorovacím systémom ako Zabbix. |
| Používateľsky konfigurovateľné Kanban tabule | Prispôsobiteľné Kanban tabule pre správu úloh (To Do, In Progress, Review, Testing, Done, ...). |
| Preddefinované reporty a integrácia s Metabase (open-source platforma pre business intelligence, BI) | Poskytovanie štandardných reportov a integrácia s Metabase pre pokročilé reportovanie. |

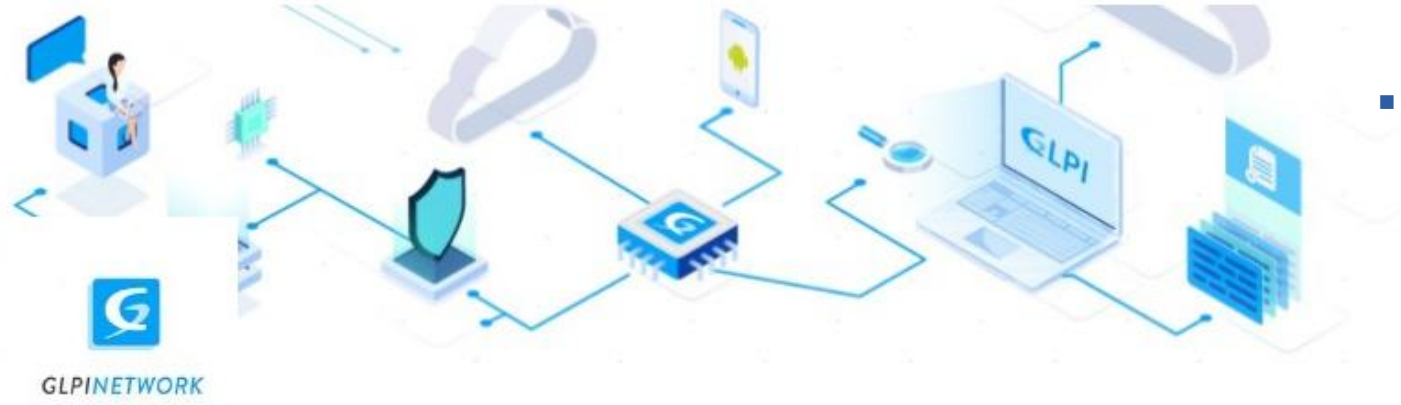
# Komunikácia s rôznymi platformami

- Email (Microsoft Exchange, Office 365, Gmail)
- LDAP vrátane SSO (Active Directory)
- Inventár (MS SCCM, FusionInventory, OCS Inventory)
- Monitorovanie (Zabbix, Nagios)
- Reportovanie (Metabase, Microsoft Power BI )
- Automatizácie biznis procesov (ProcessMaker)
- Kolaborácia a komunikácia (MS Teams, Slack, Telegram)


- **SCCM (System Center Configuration Manager)**
  - **SCCM** = nástroj od **Microsoftu** na **správu počítačov, softvéru a aktualizácií** v organizácii.
  - **Funkcie:**
    - inventarizácia hardvéru a softvéru,
    - centrálna inštalácia aplikácií (napr. Office, antivírus),
    - nasadzovanie aktualizácií a záplat (patch management),
    - vzdialená správa zariadení,
    - integrácia s **Active Directory** a **Intune** (pre hybridné prostredia).
  - **Prínosy:**
    - automatizuje správu tisícok zariadení,
    - znižuje riziko nezaplátaných systémov,
    - umožňuje kontrolu súladu (compliance).

# Komunikácia s rôznymi platformami

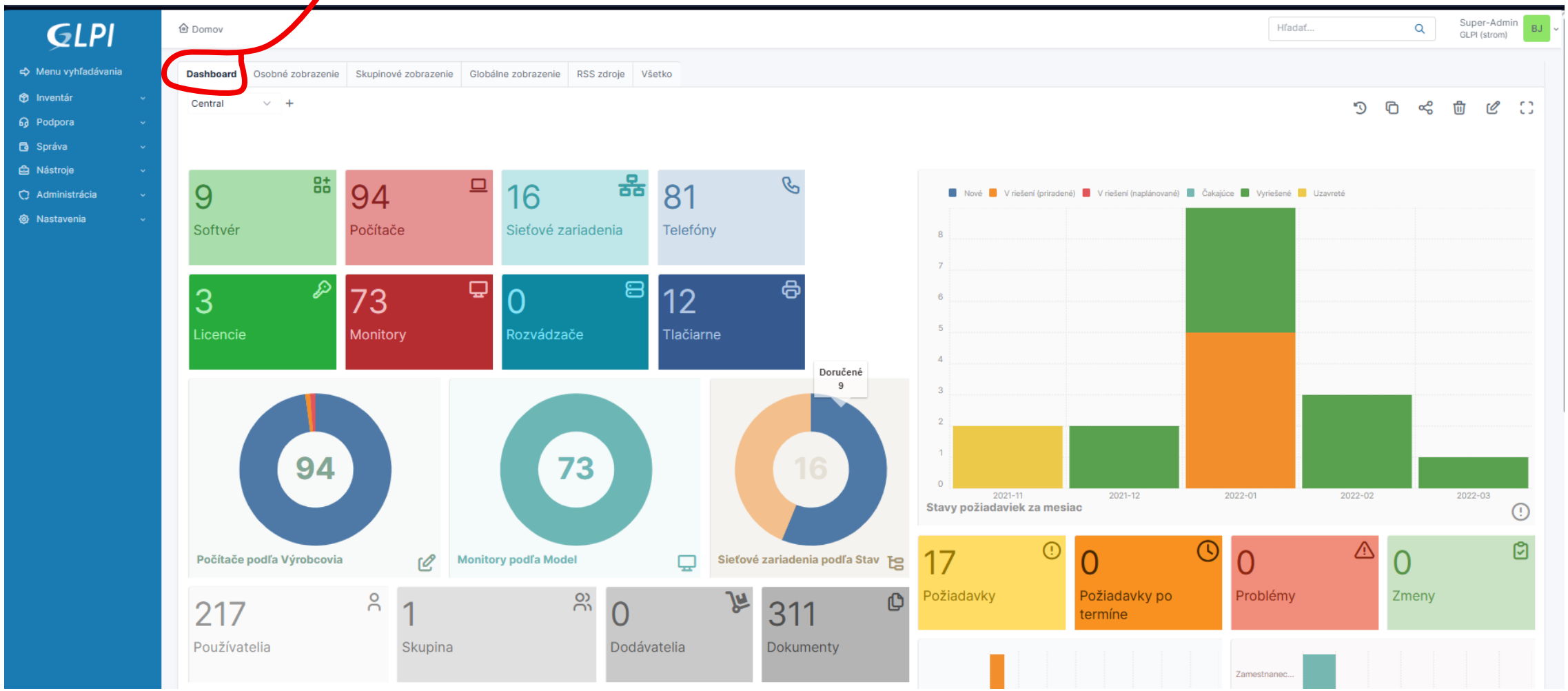
- Email (Microsoft Exchange, Office 365, Gmail)
- LDAP vrátane SSO (Active Directory)
- Inventár (MS SCCM, FusionInventory, OCS Inventory)
- Monitorovanie (Zabbix, Nagios)
- Reportovanie (Metabase, Microsoft Power BI )
- Automatizácie biznis procesov (ProcessMaker)
- Kolaborácia a komunikácia (MS Teams, Slack, Telegram)



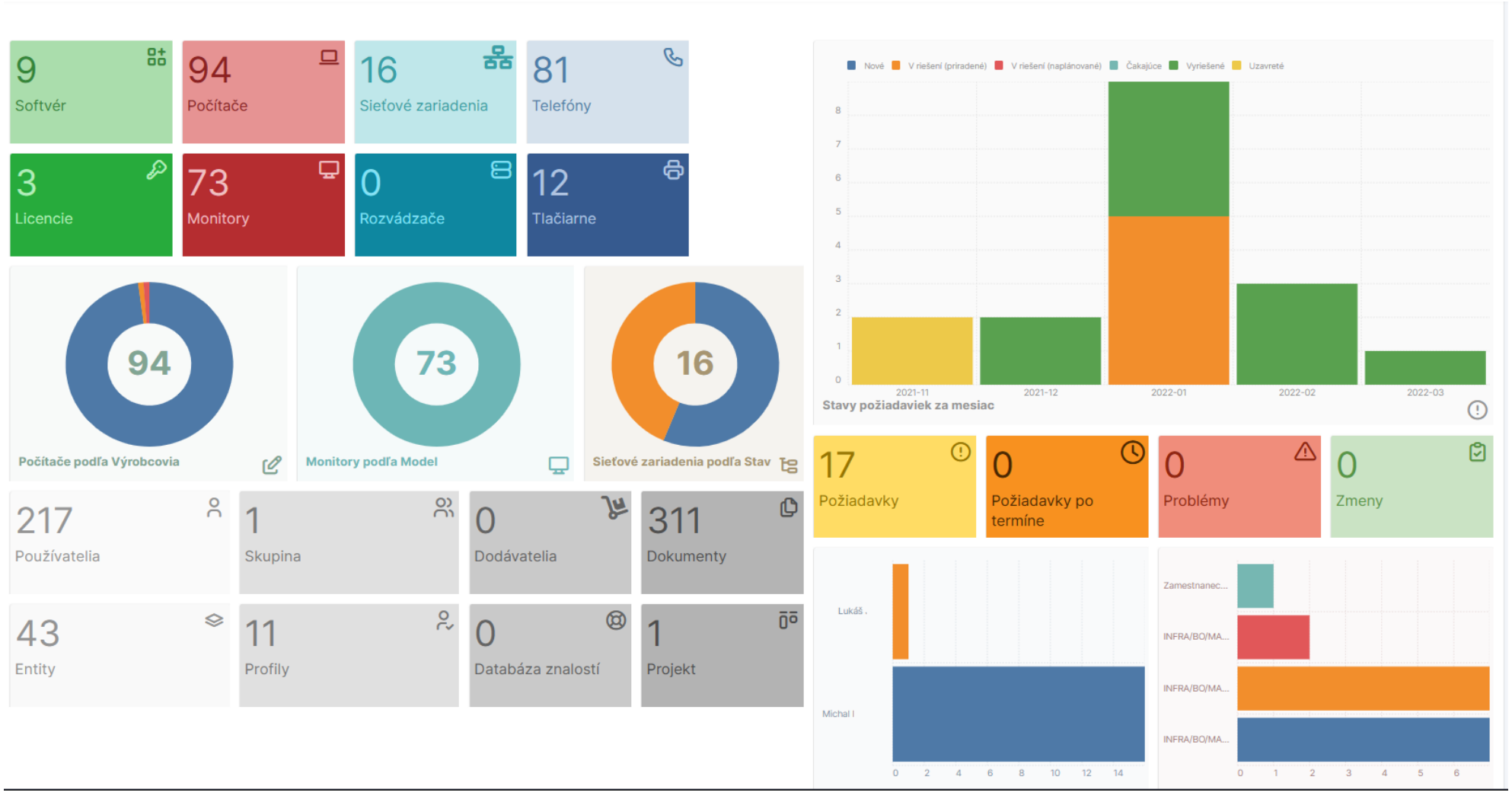

- **FusionInventory**
  - **FusionInventory** je **open-source nástroj** na **inventarizáciu IT aktív** a **nasadenie softvéru**, ktorý sa často používa ako **rozšírenie pre GLPI**.
  - **Funkcie:**
    - automaticky zisťuje a zapisuje zariadenia (PC, tlačiarne, servery, sieťové prvky),
    - zhromažďuje informácie o hardvéri, softvéri, OS, IP adresách, používateľoch,
    - podporuje **agentov** – malé programy inštalované na klientoch, ktoré pravidelne posielajú dáta,
    - umožňuje **nasadenie softvéru** alebo skriptov na diaľku,
    - dáta sa ukladajú priamo do **GLPI databázy**.
  - **Prínosy:**
    - úplná a automatická inventarizácia,
    - integrácia s GLPI (ITSM, Helpdesk, Asset management),
    - open-source alternatíva k drahým komerčným riešeniam ako SCCM.

GLPI

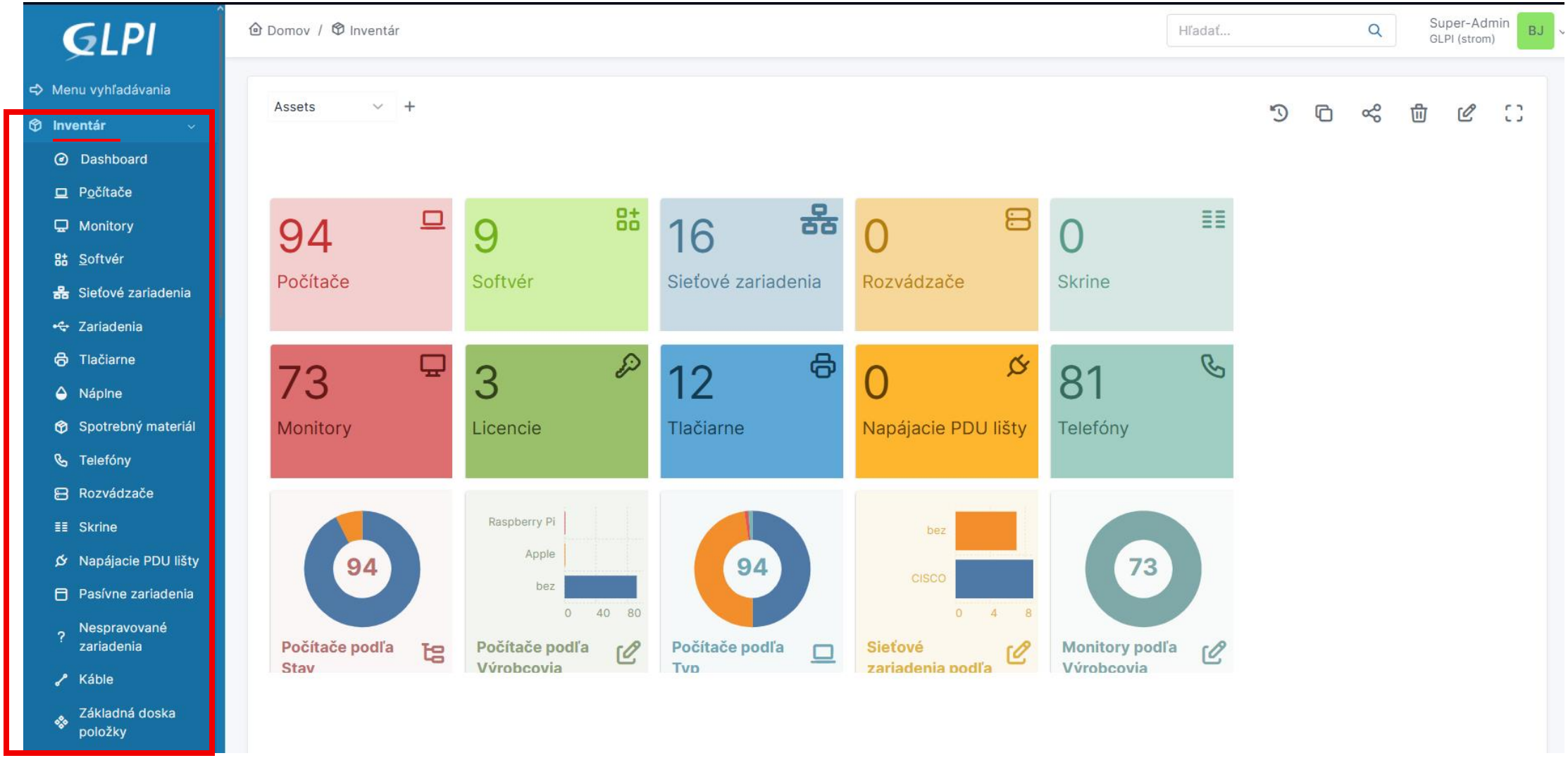
# Dashboard



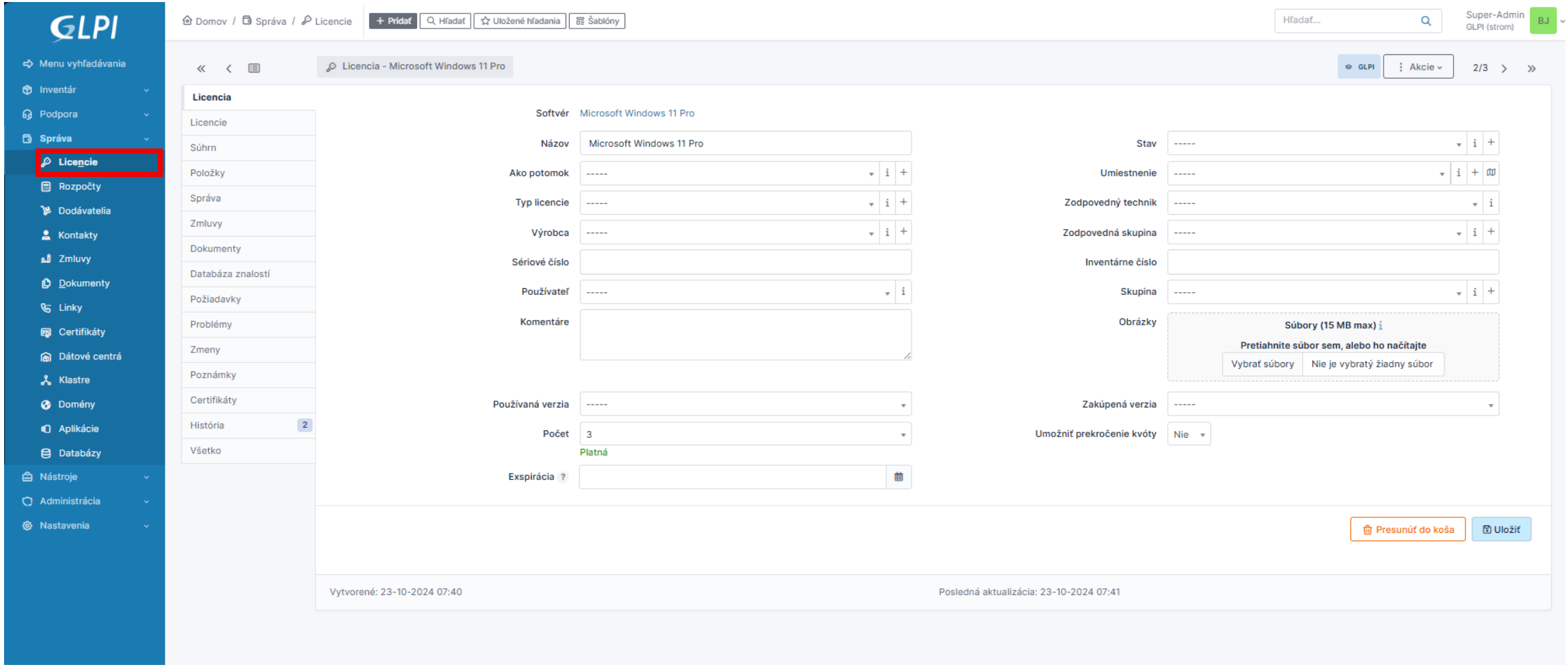
# Dashboard


9
Softvér
94
Počítače
16
Sieťové zariadenia
81
Telefóny
3
Licencie
73
Monitory
0
Rozvádzače
12
Tlačiarne
94
Počítače podľa Výrobcovia
73
Monitory podľa Model
16
Sieťové zariadenia podľa Stav
217
Používatelia
1
Skupina
0
Dodávatelia
311
Dokumenty
43
Entity
11
Profily
0
Databáza znalostí
1
Projekt
Nové
V riešení (priradené)
V riešení (naplánované)
Čakajúce
Vyriešené
Uzavreté
2021-11
2021-12
2022-01
2022-02
2022-03
Stavy požiadaviek za mesiac
17
Požiadavky
0
Požiadavky po termíne
0
Problémy
0
Zmeny
Lukáš .
Michal I
Zamestnanec...
INFRA/BO/MA...
INFRA/BO/MA...
INFRA/BO/MA...

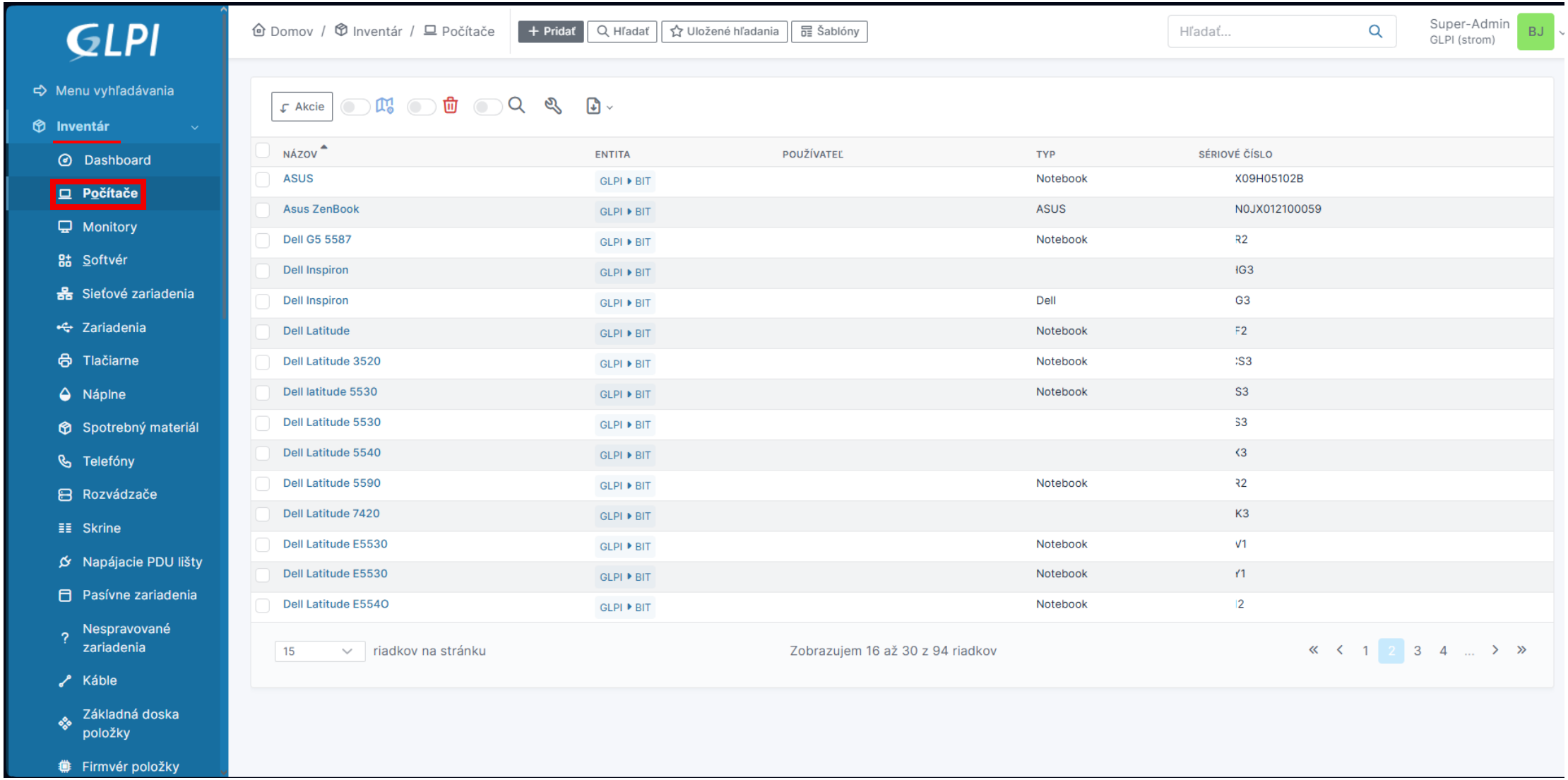
# Dashboard – Inventár (Assets)



# Dashboard – Správa - Licencia

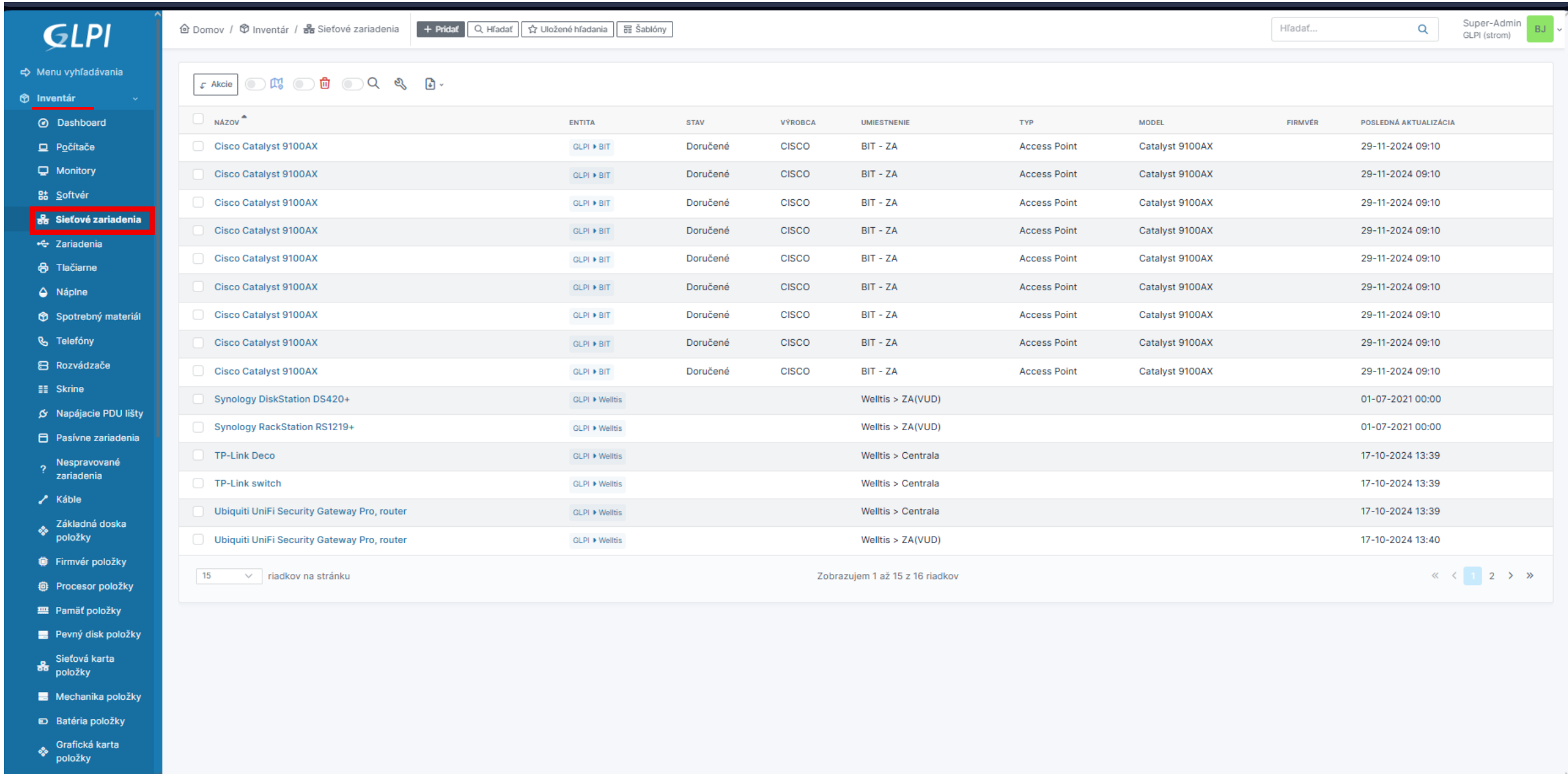


# Dashboard - Inventár - Počítače

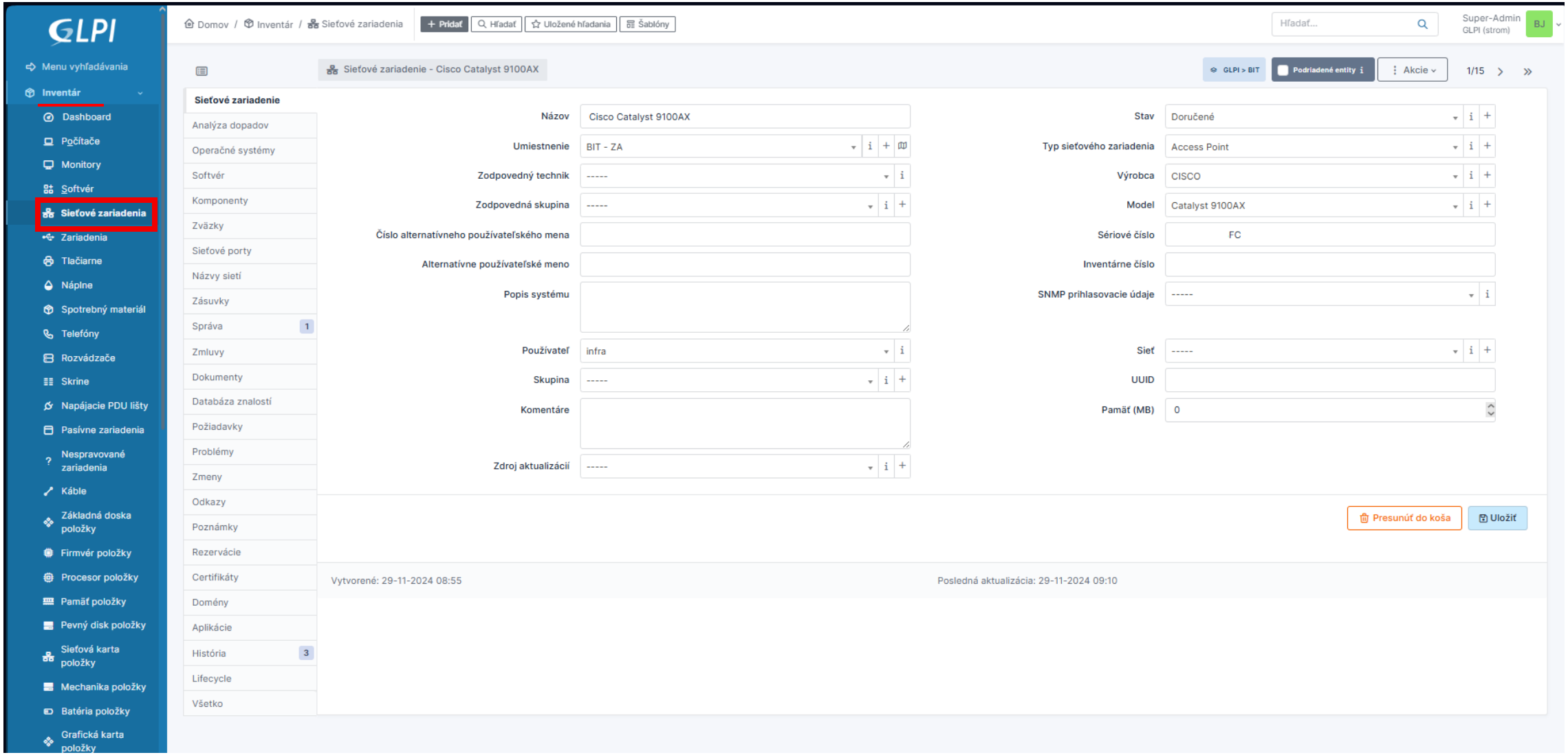


GLPI

# Dashboard - Inventár - Sieťové zariadenia

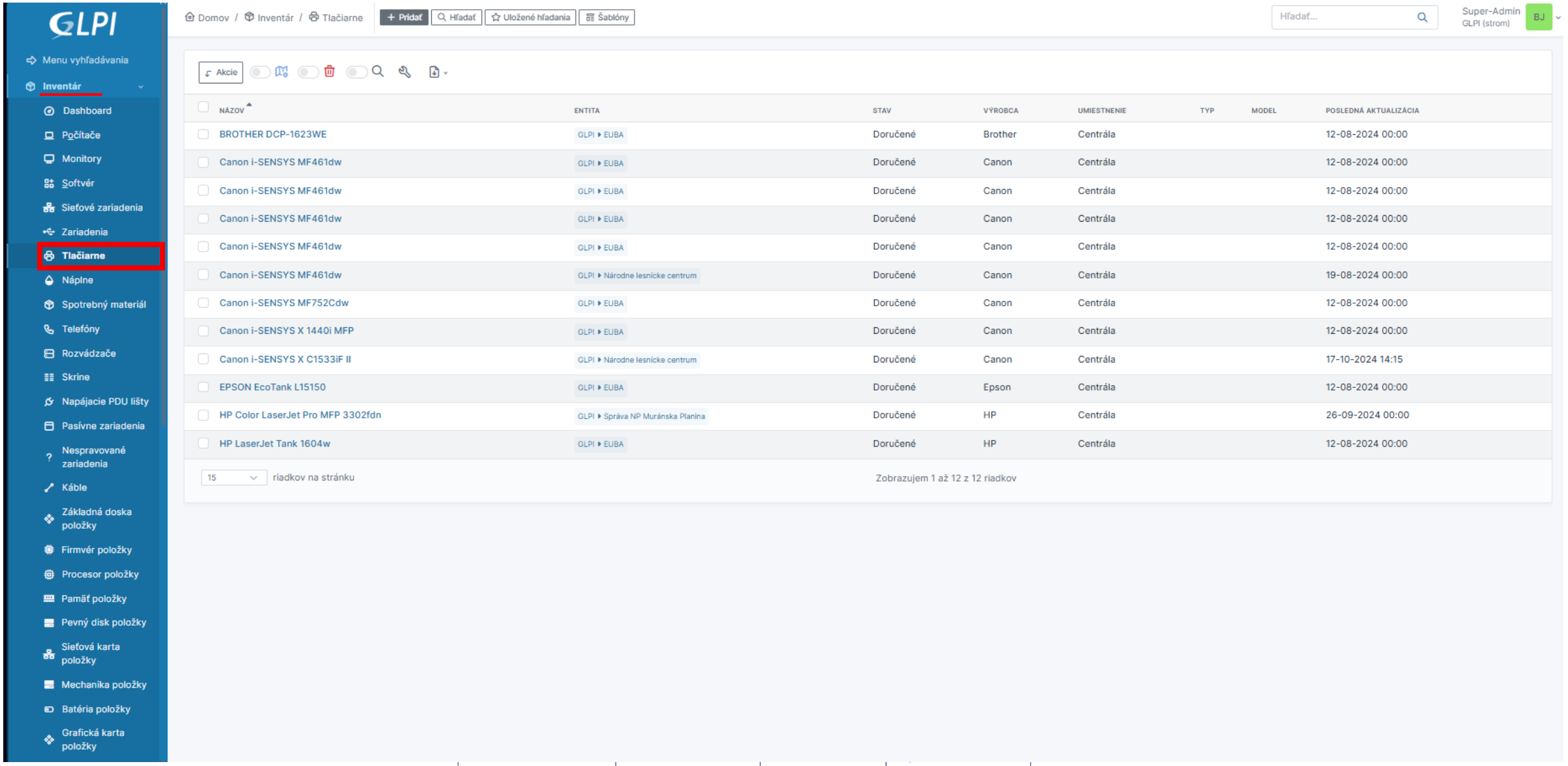


# Dashboard - Inventár - Sieťové zariadenie náhľad



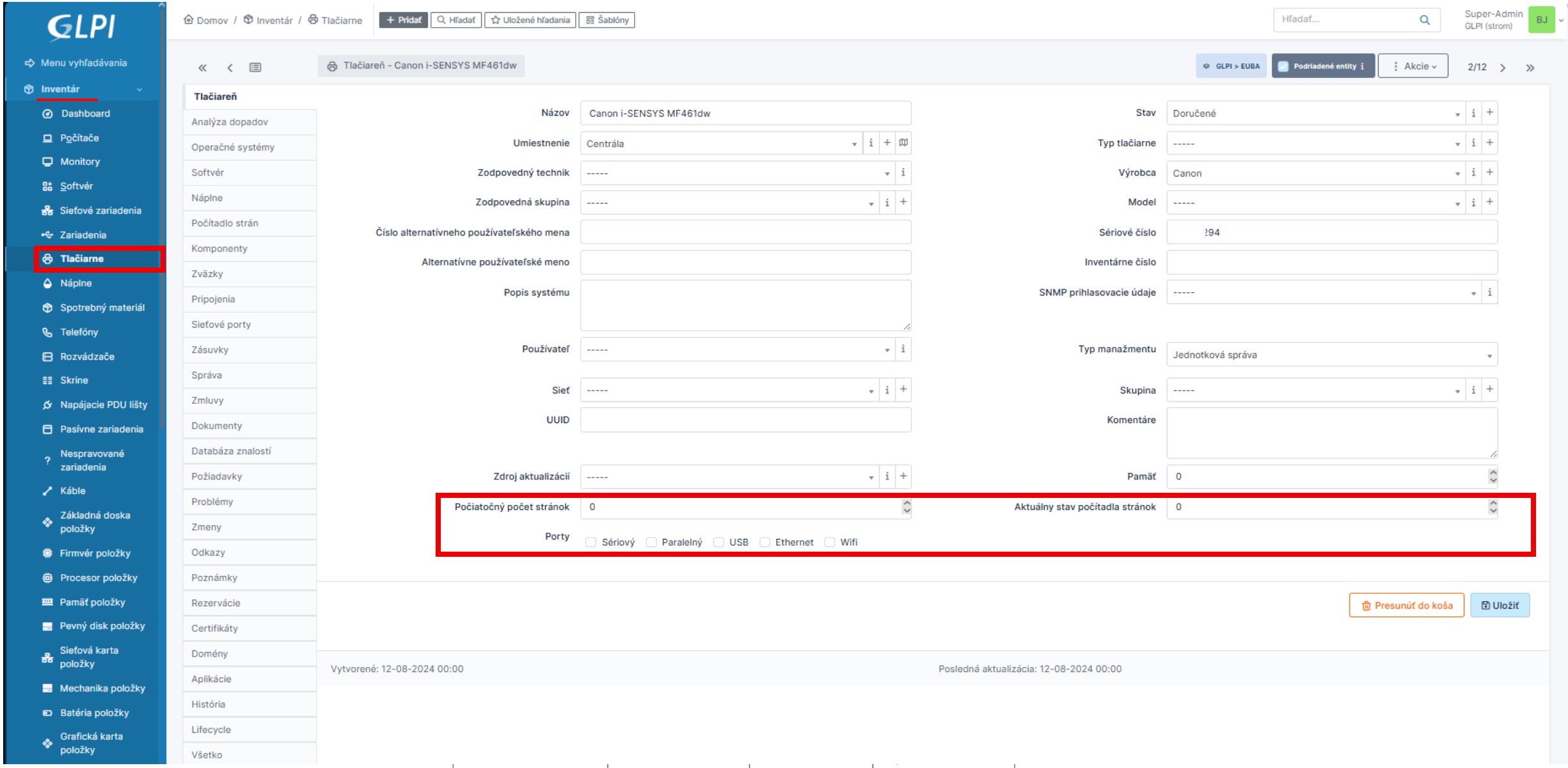
GLPI

# Dashboard - Inventár - Tlačiarne

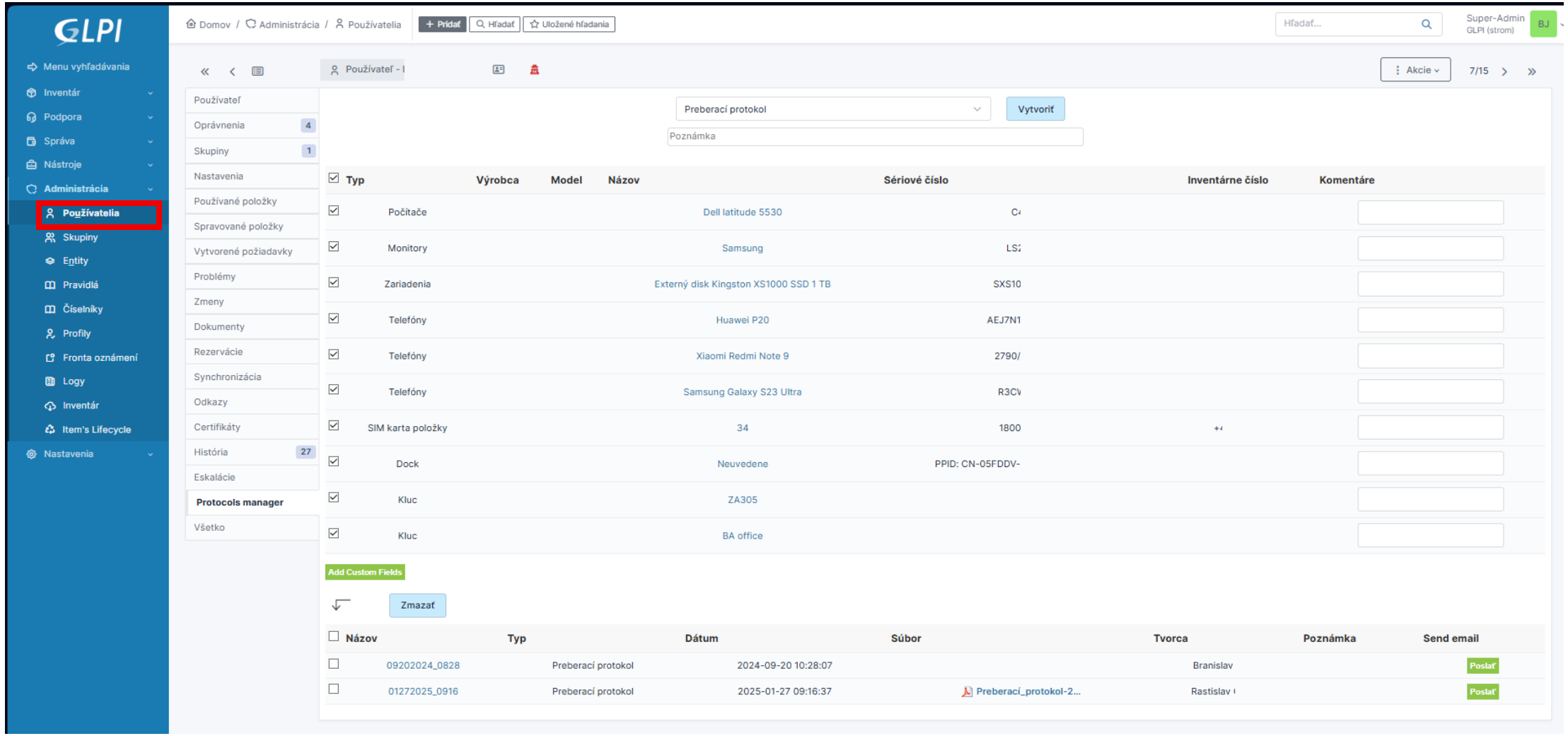


GLPI

# Dashboard - inventár - tlačiareň - náhľad



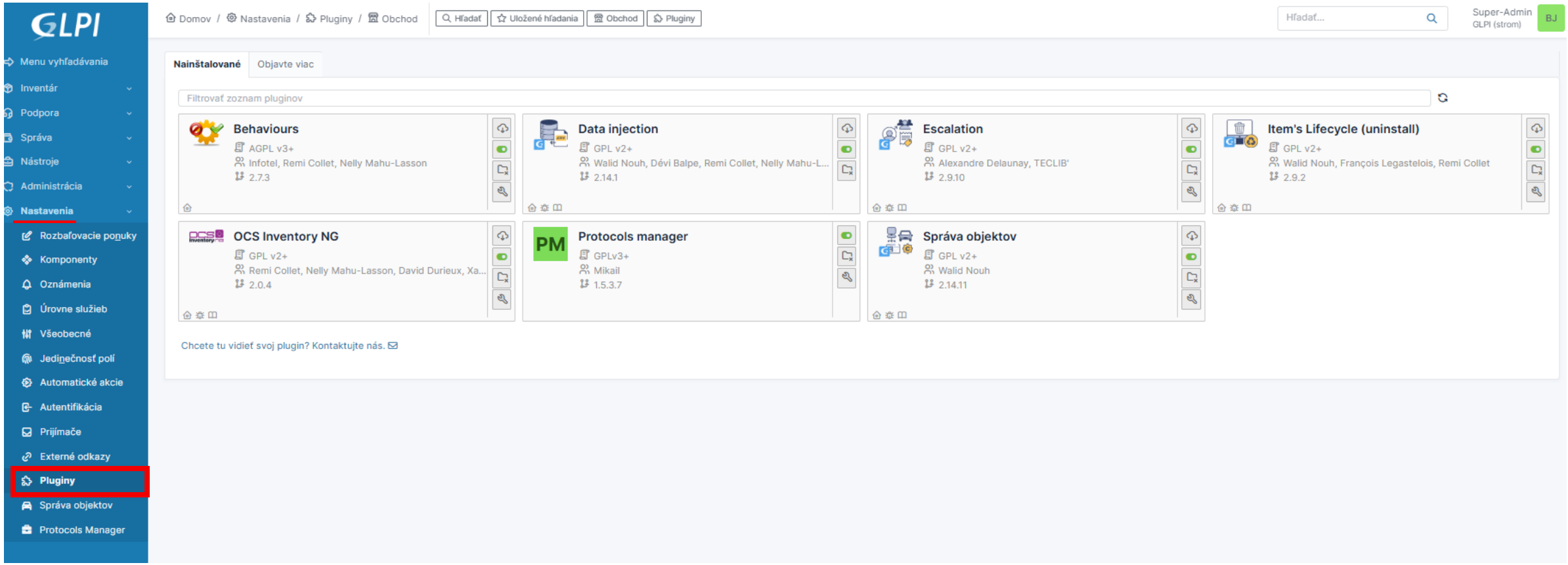
# Dashboard - Inventár - podľa osoby



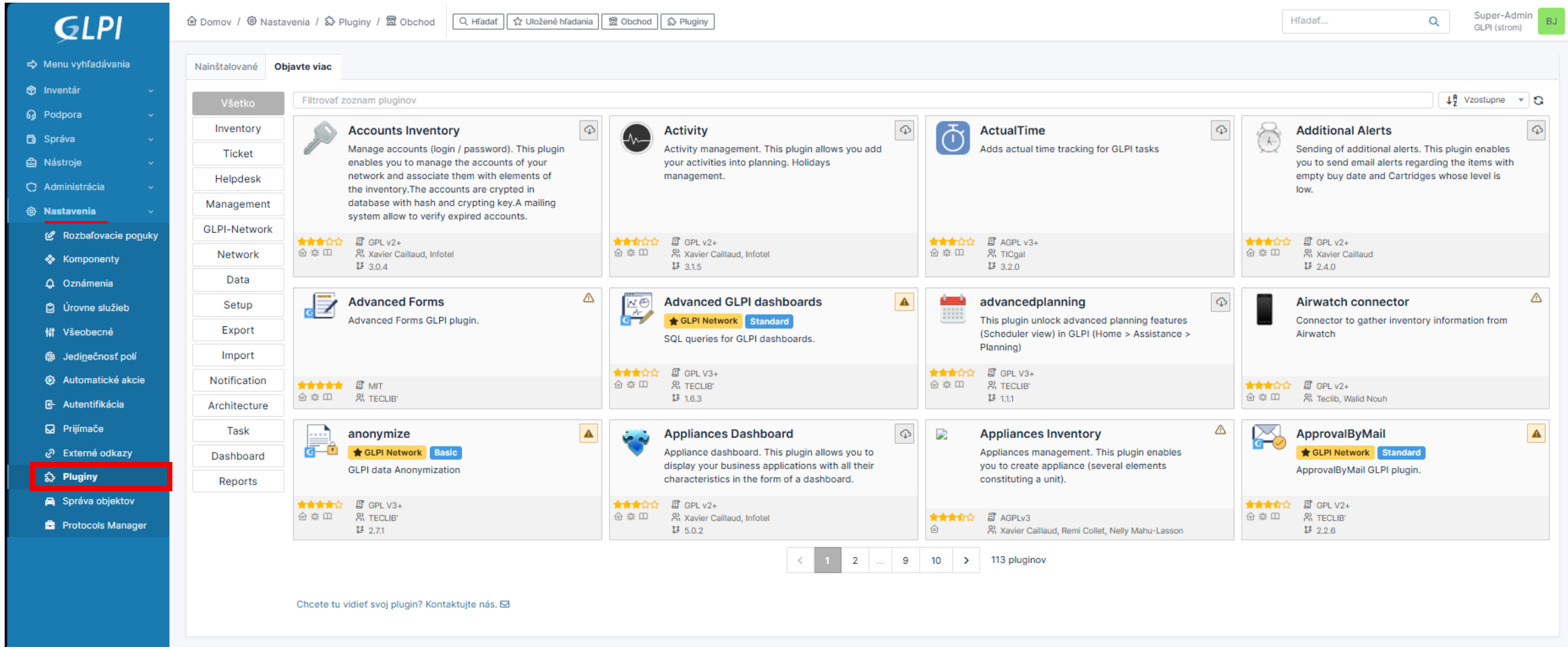



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Dashboard – Nastavenia - Pluginy

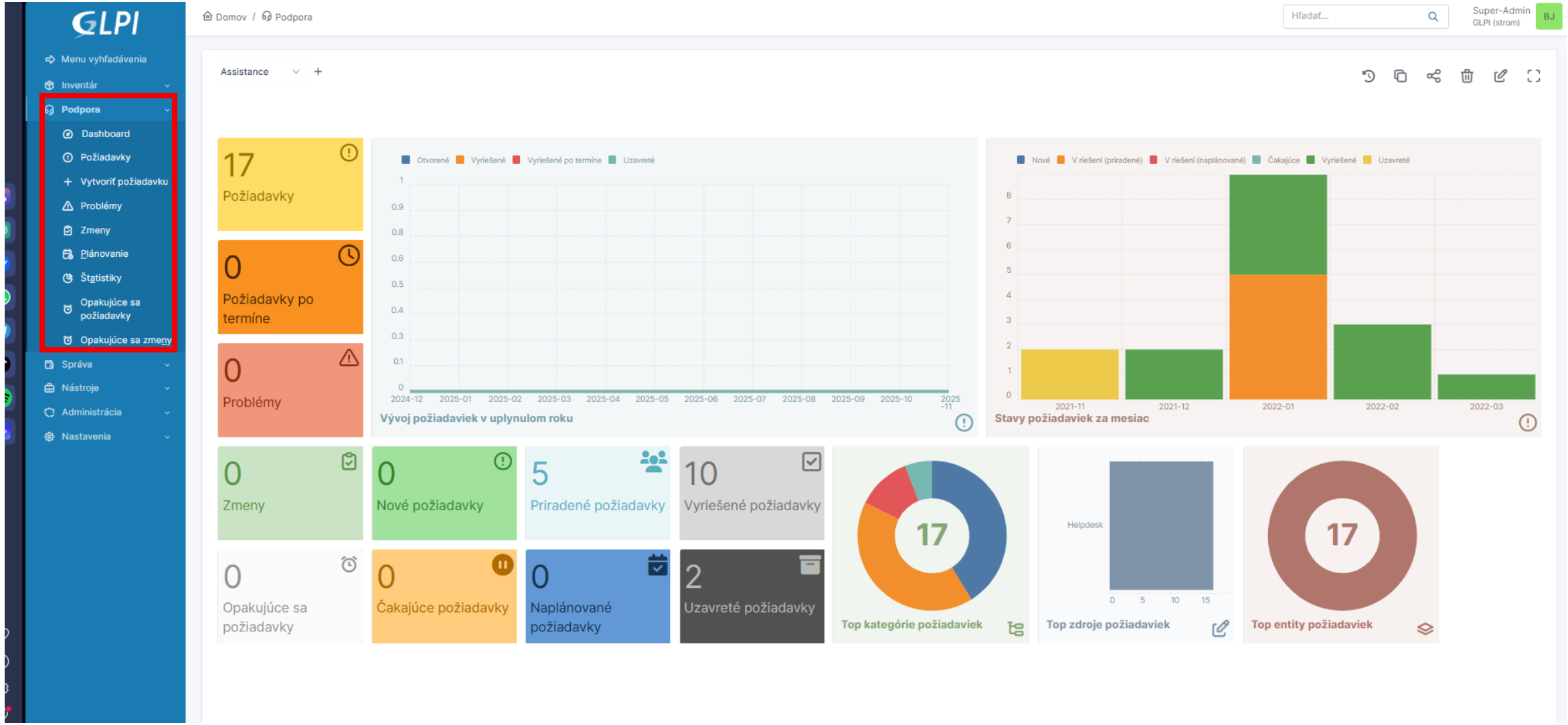


# Dashboard- Nastavenia - Pluginy obchod



GLPI

# Dashboard - Podpora (systém pre správu požiadaviek)

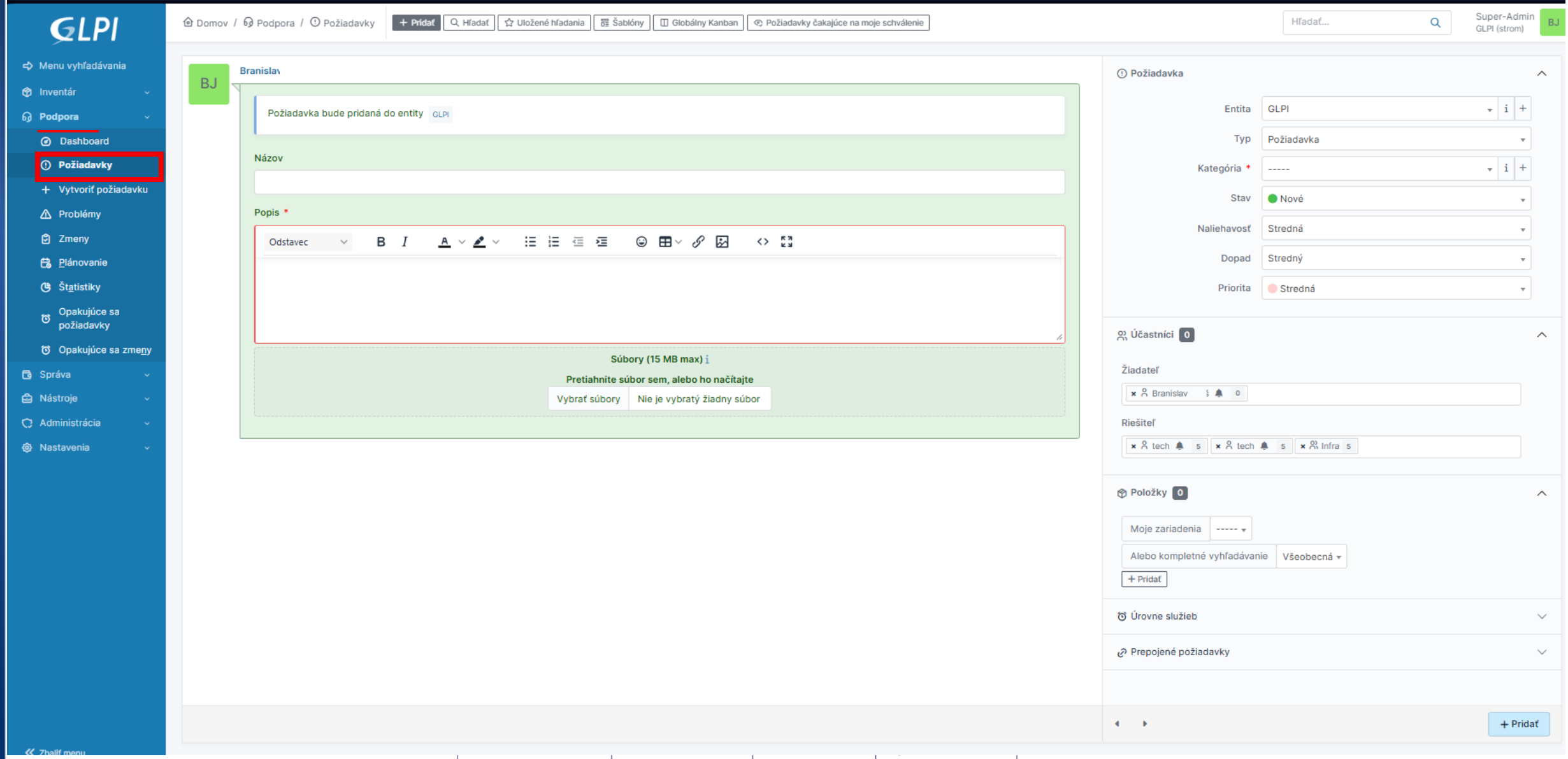




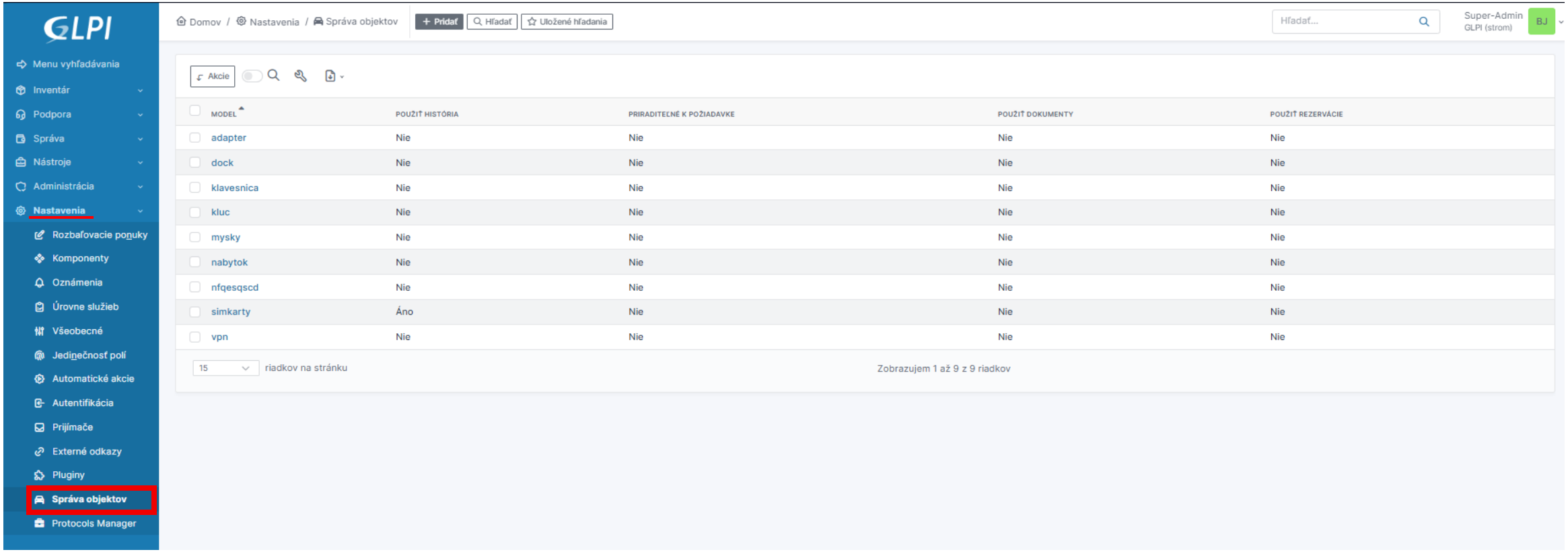

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

GLPI

# Dashboard - Podpora - Požiadavky

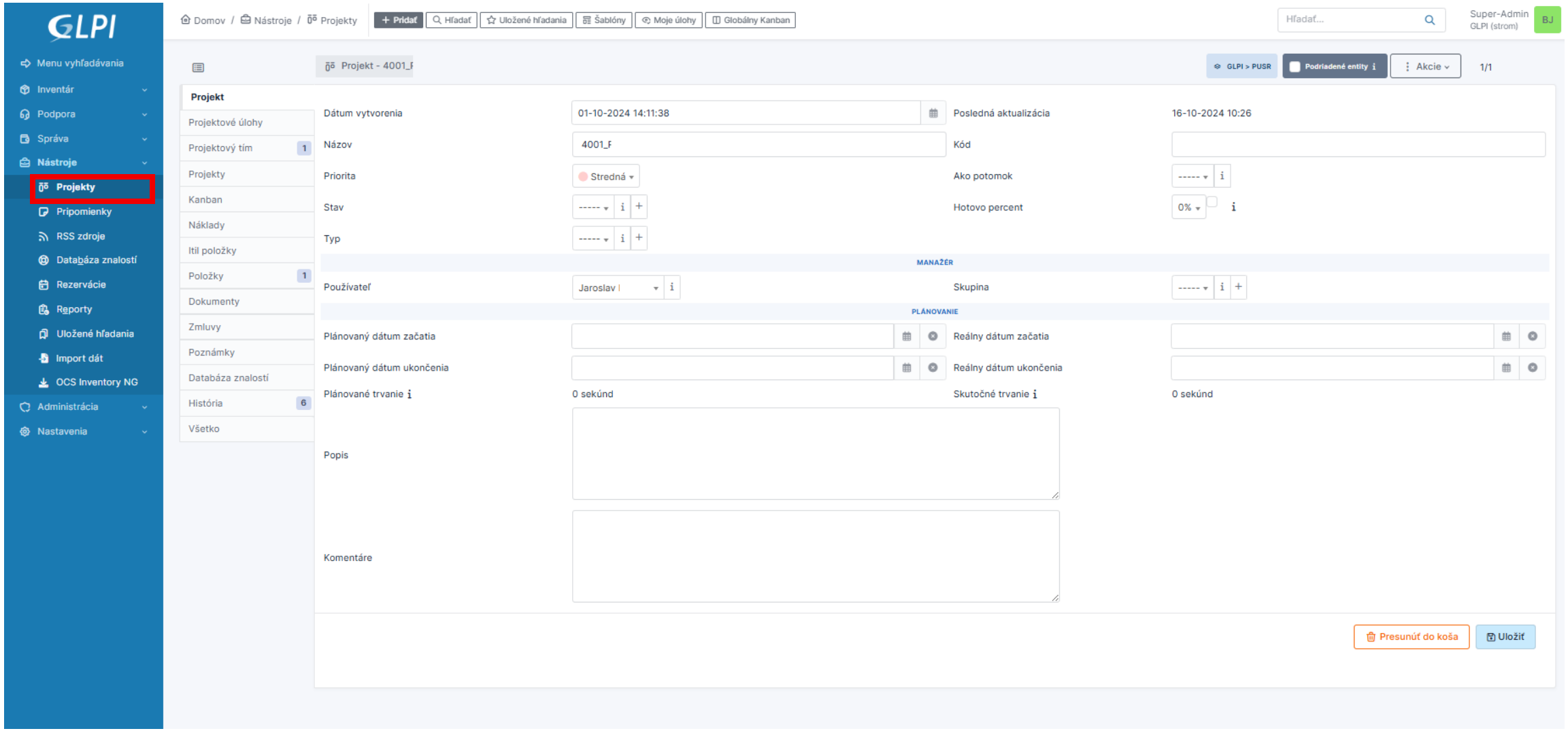


# Dashboard - Inventár - Pridanie položky

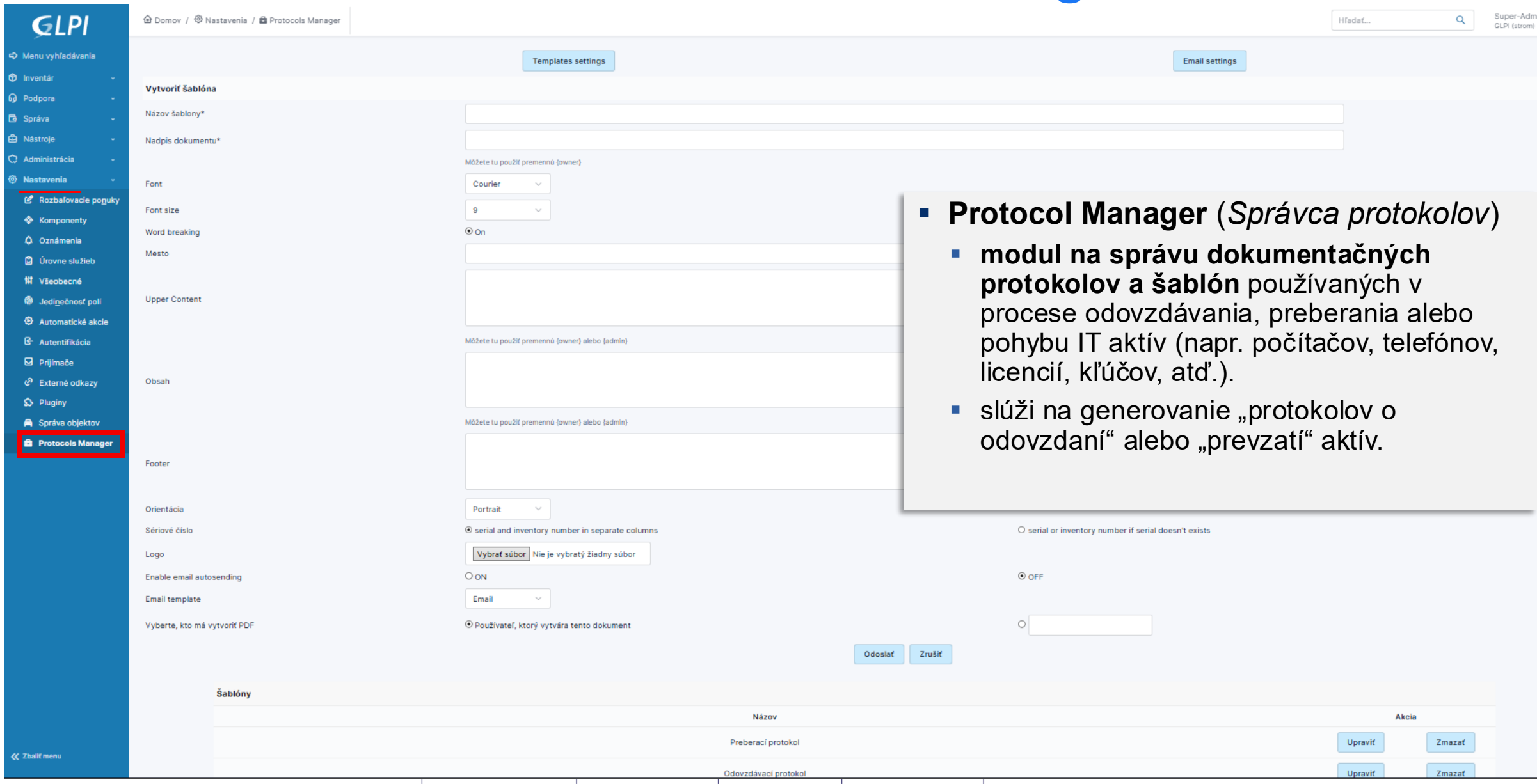


GLPI

# Dashboard- Nástroje - Projekt



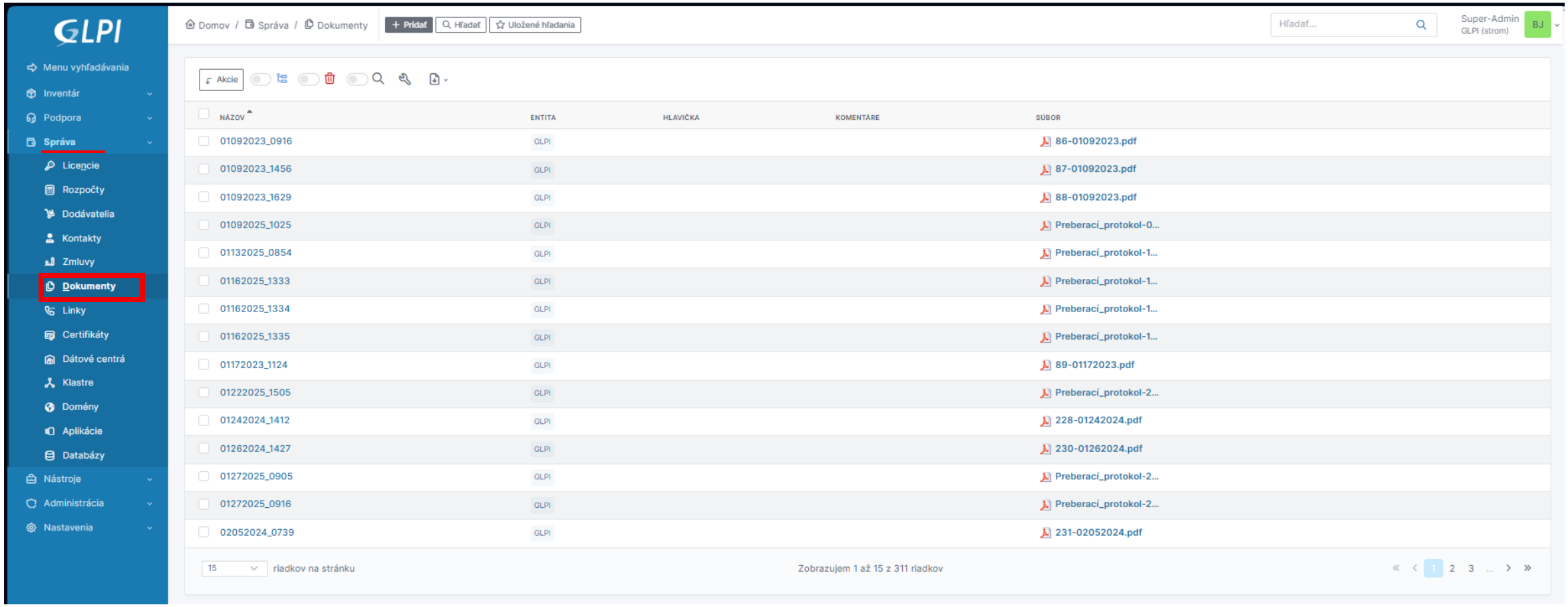
# Dashboard - Nastavenia - Protocol manager




- **Protocol Manager** (*Správca protokolov*)
  - **modul na správu dokumentačných protokolov a šablón** používaných v procese odovzdávania, preberania alebo pohybu IT aktív (napr. počítačov, telefónov, licencií, kľúčov, atď.).
  - slúži na generovanie „protokolov o odovzdaní“ alebo „prevzatí“ aktív.

GLPI

# Správa dokumentov






Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Licenčné podmienky

- GLPI je distribuované pod **GNU General Public License v3 (GPLv3)**
  - ide o **plne open-source softvér**
  - bez licenčných poplatkov, s otvoreným zdrojovým kódom.

- **GPLv3 neumožňuje bez splnenia podmienok**
  - **Uzavrieť kód**
    Ak GLPI upravíme a poskytneme iným, upravený kód musí byť **stále verejne prístupný** (nemôžeš si ho „privlastniť“ ako proprietárny).
  - **Používať názov GLPI na komerčný produkt bez povolenia**

- **Integrácie a pluginy**
  - GLPI umožňuje používať aj **komerčné pluginy** alebo integrácie (napr. od spoločnosti *Teclib’*), ktoré môžu mať samostatné licenčné podmienky.
    - Teclib’ ponúka tzv. **GLPI Network** (platená „enterprise“ edícia GLPI), ktorá obsahuje:
      - profesionálny **technický support** (SLA – garantované časy reakcie),
      - **aktualizácie a bezpečnostné opravy** s overením kompatibility,
      - prístup k **oficiálnym overeným pluginom**,
      - možnosť **cloud hostingu** (GLPI Cloud) – Teclib spravuje celý systém za zákazníka,
      - **certifikované inštalácie** a školenia,
      - integráciu s externými systémami (Active Directory, SSO, Office365, Jira, CMDB, atď.).

# Na uvedomenie si...

## LibreNMS

- je primárne **NMS/monitoring** nástroj
- má natívne:
  - **autodiscovery** zariadení v sieti (SNMP discovery)
  - **polling** (pravidelný zber metrík: traffic, CPU, RAM, teploty, porty, linky, alerty)

## GLPI

- je primárne **ITSM/CMDB/ITAM** (tiketovanie + evidencia aktív)
- **autodiscovery a „polling“** vie mať, ale nie natívne ako LibreNMS:
  - cez doplnok **GLPI Agent** (inventarizácia endpointov)
  - alebo cez **FusionInventory / OCS Inventory** (discovery + inventory)
- zvyčajne to slúži skôr na **inventár/CMDB**, nie na kontinuálny monitoring výkonu



Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE


# Inventarizačný nástroj - Netbox

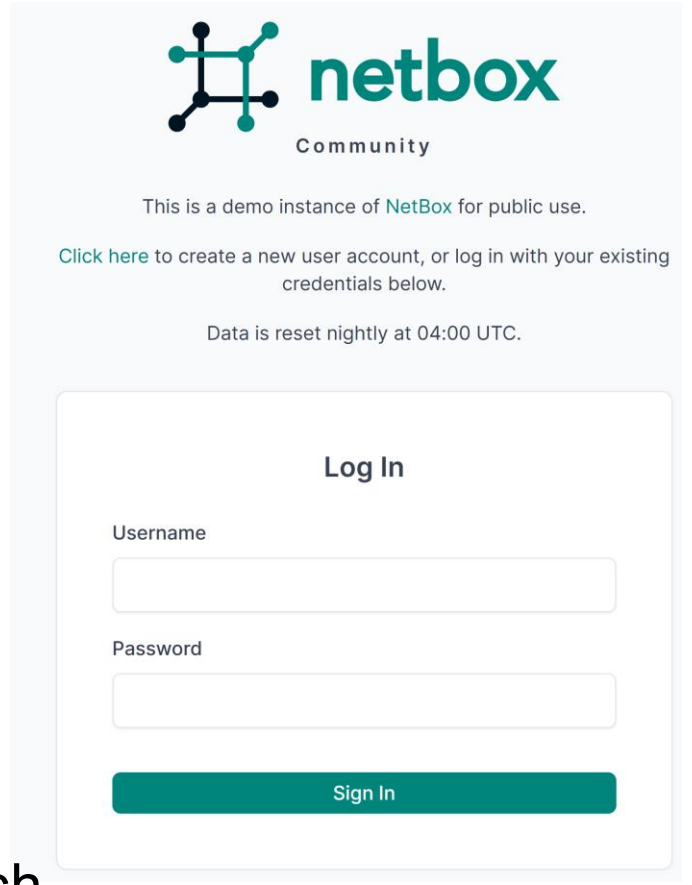
# Netbox

PONUKA DEMO NÁSTROJA

- NetBox je **nástroj na dokumentáciu reálnej IT infraštruktúry** (CMDB – configuration management database, v ITIL terminológii - Information Technology Infrastructure Library) – primárne na sieťovej úrovni.
- Umožňuje modelovať a ukladať informácie o:
  - zariadeniach, kabeláži, portoch, IP adresách, VLAN, rackoch, miestnostiach...
- Dokáže generovať vizuálne pohľady (napr. topológie a fyzické rozvádzače).
- Údaje sa ukladajú v štruktúrovaných objektoch, medzi ktorými sa definujú vzťahy.

NetBox slúži ako centrálny nástroj pre:

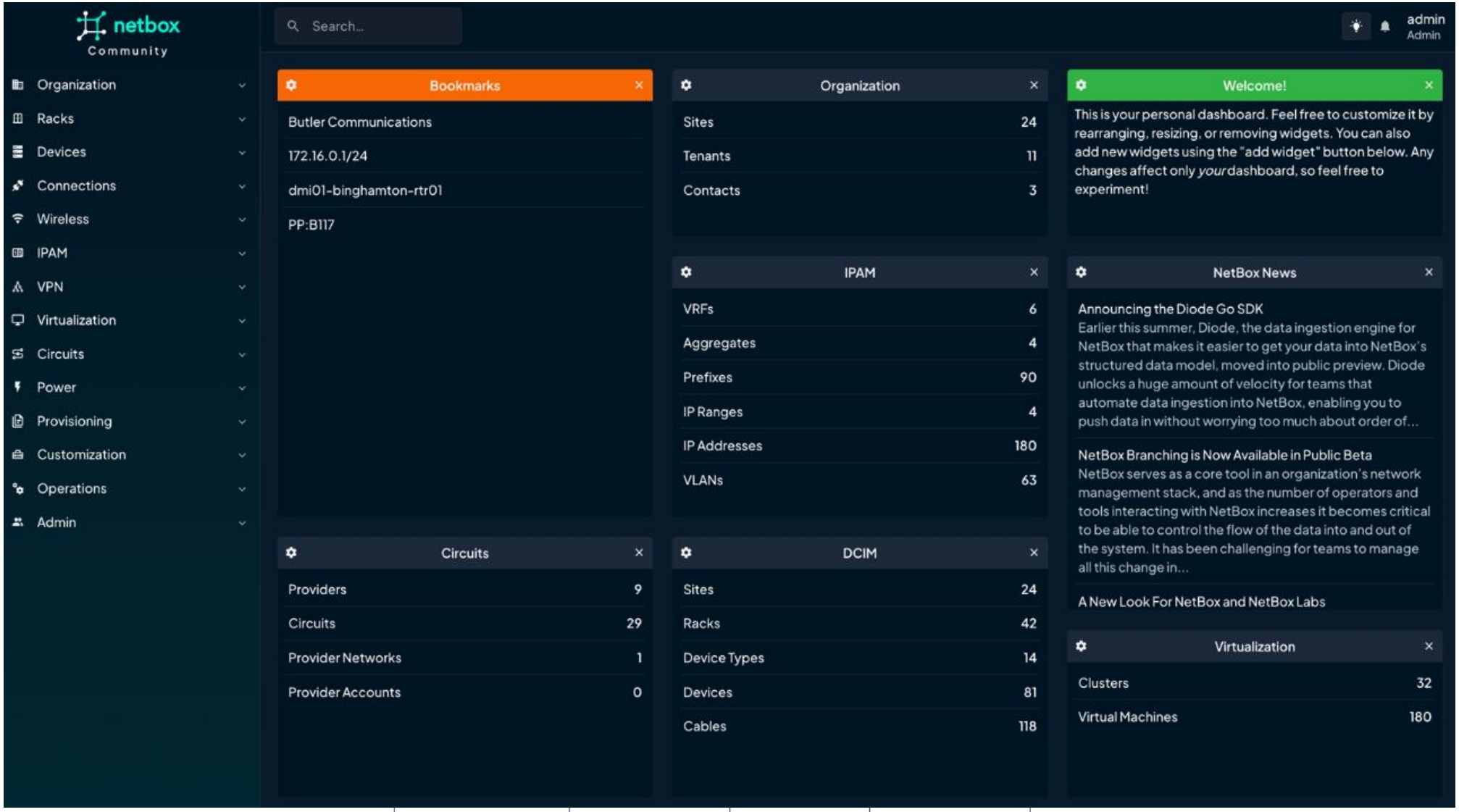
- dokumentáciu sieťovej infraštruktúry,
- DCIM (Data Center Infrastructure Management),
- integráciu s NetDevOps procesmi,
- využitie prvkov automatizácie,
- Iné - využitie rôznych pluginov a rozšírení.




Link: Home | NetBox

## Nástroje na správu a kategorizáciu aktív

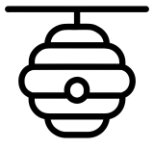
# Netbox



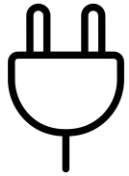
# Výhody

**Centralizovaná dokumentácia**
NetBox poskytuje jednotné miesto pre uchovávanie všetkých informácií o sieťovej infraštruktúre, zariadeniach, kábloch a IP adresách.

**Open-source riešenie**
Bezplatné, s aktívnou komunitou a možnosťou prispôsobenia špecifickým potrebám akademického prostredia.



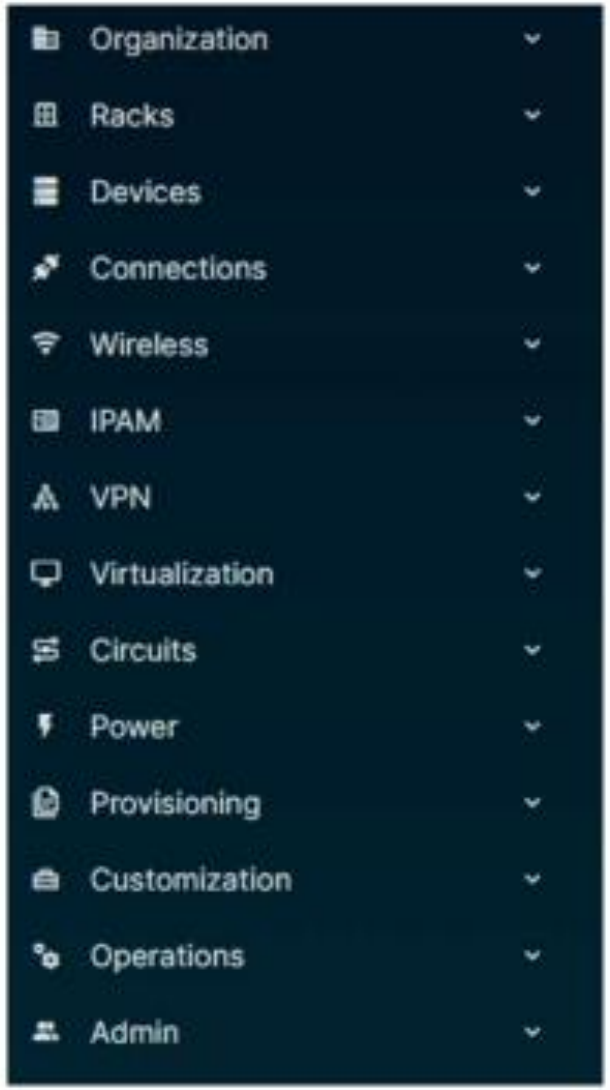
**API-first prístup**
Robustné REST API umožňuje jednoduchú integráciu s automatizačnými nástrojmi a inými systémami.



**Rozšíriteľnosť**
Podpora pluginov a rozšírení umožňuje pridávanie vlastných funkcií a integráciu s existujúcimi systémami.

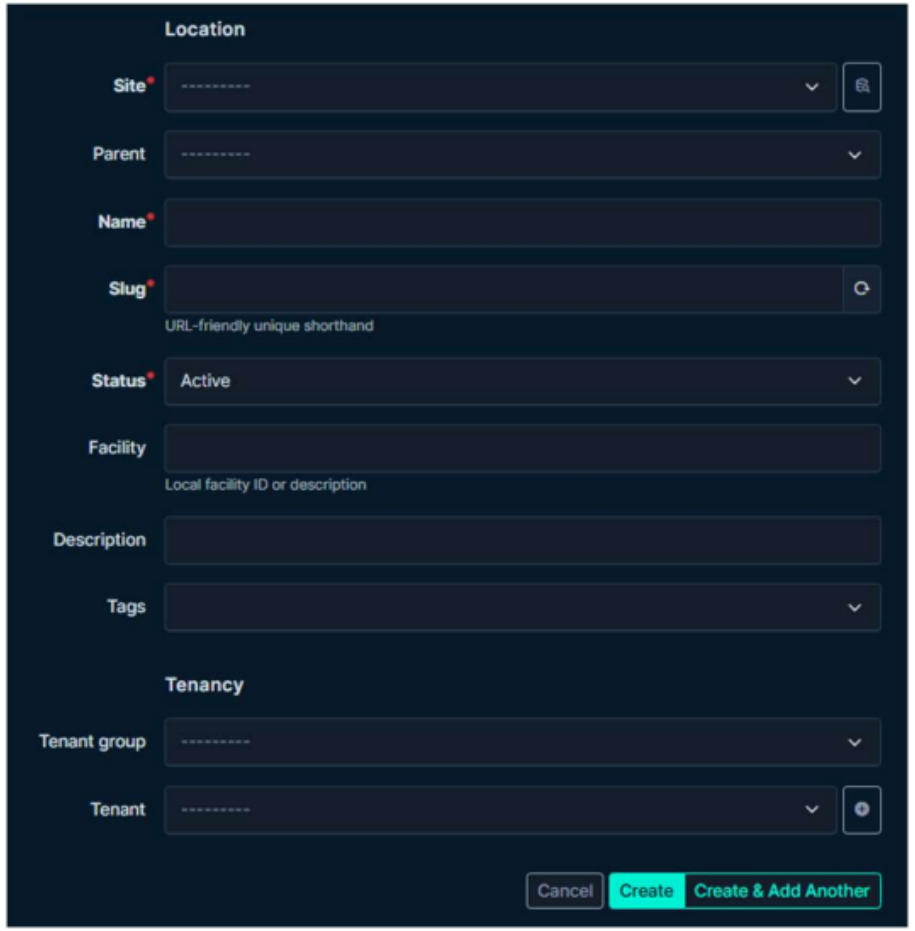
# Dokumentácia rôznych typov objektov

- Možná dokumentácia rôznych typov objektov podľa funkcie:
  - **organizácia** – miesto, miestnosť, vlastník,
  - **rozvádzače (Racks)** – reálne dátové skrine s U-pozíciami,
  - **zariadenia (Devices)** – prepínače, smerovače, servery, FW…,
  - **prepojenia (Cables)** – fyzické káble, optické alebo metalické,
  - **bezdrôtové siete** – SSID, typ šifrovania, VLAN,
  - **IPAM** – IP prefixy, adresy, VLAN, RIR, AS,
    - IPAM (IP Address Management) ako metóda na plánovanie, sledovanie a správu adresného priestoru internetových protokolov (IP) v sieti
  - **VPN, Virtualizácia, Napájanie** – doplnkové časti infraštruktúry.



# Pridávanie objektov/aktív

- Netbox **ponúka 3 možnosti pridávanie aktív:**
  - manuálne:
    - odporúčaný pri malom množstve dát / najjednoduchší spôsob
    - pri väčšom množstve dát - veľmi zdĺhavý proces
  - import:
    - využitie pri počatočnom naplnení databázy / rozsiahlych migráciach,
  - skriptovanie dát,
  - použitím rest API
    - využitie: po spojení netbox + discovery nástroj, vieme automaticky vytvárať objekty
    - automatizácia synchronizácie dát




Formulár pre vytvorenie učebne

# Pridávanie objektov/aktív

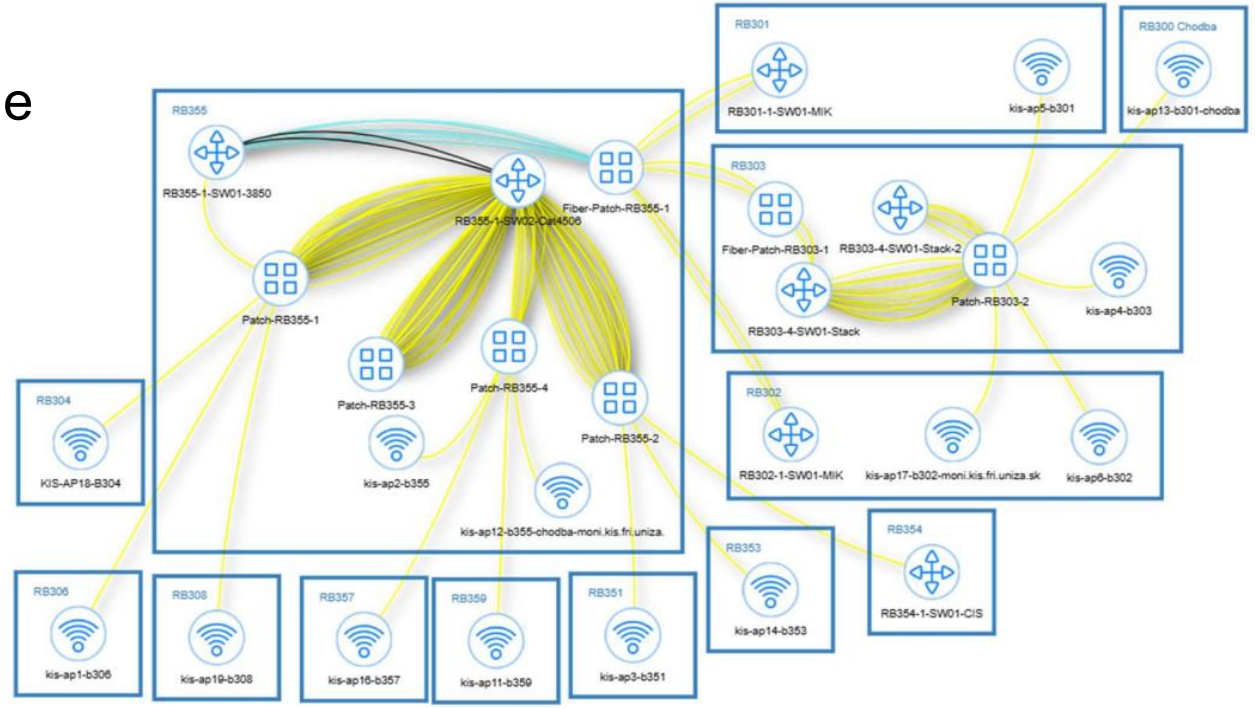
- Druhý spôsob je import dát.
- Definujeme si, aké parametre budú mať nové objekty (aktíva).
  - Ak súbor, ktorý nahrávame obsahuje ID čísla objektov, NetBox sa snaží upraviť existujúce objekty.
  - Ak objekt s daným ID neexistuje nahratie zmien sa nevykoná a nič sa nezmení.
- Podporované formáty sú YAML, CSV a JSON.
- Tretí spôsob je REST API:
  - **sieťové skenery** ukladajú naskenované údaje **priamo do NetBoxu** cez API,
  - **automatizačné skripty** môžu API využiť naobmedzené, opakovateľné úlohy pri dokumentova ní.

```yaml
- name: RB301
  site: FRI
  slug: rb301
  status: active
  description: RB301
  tenant: KIS
```

Textová definícia objektu

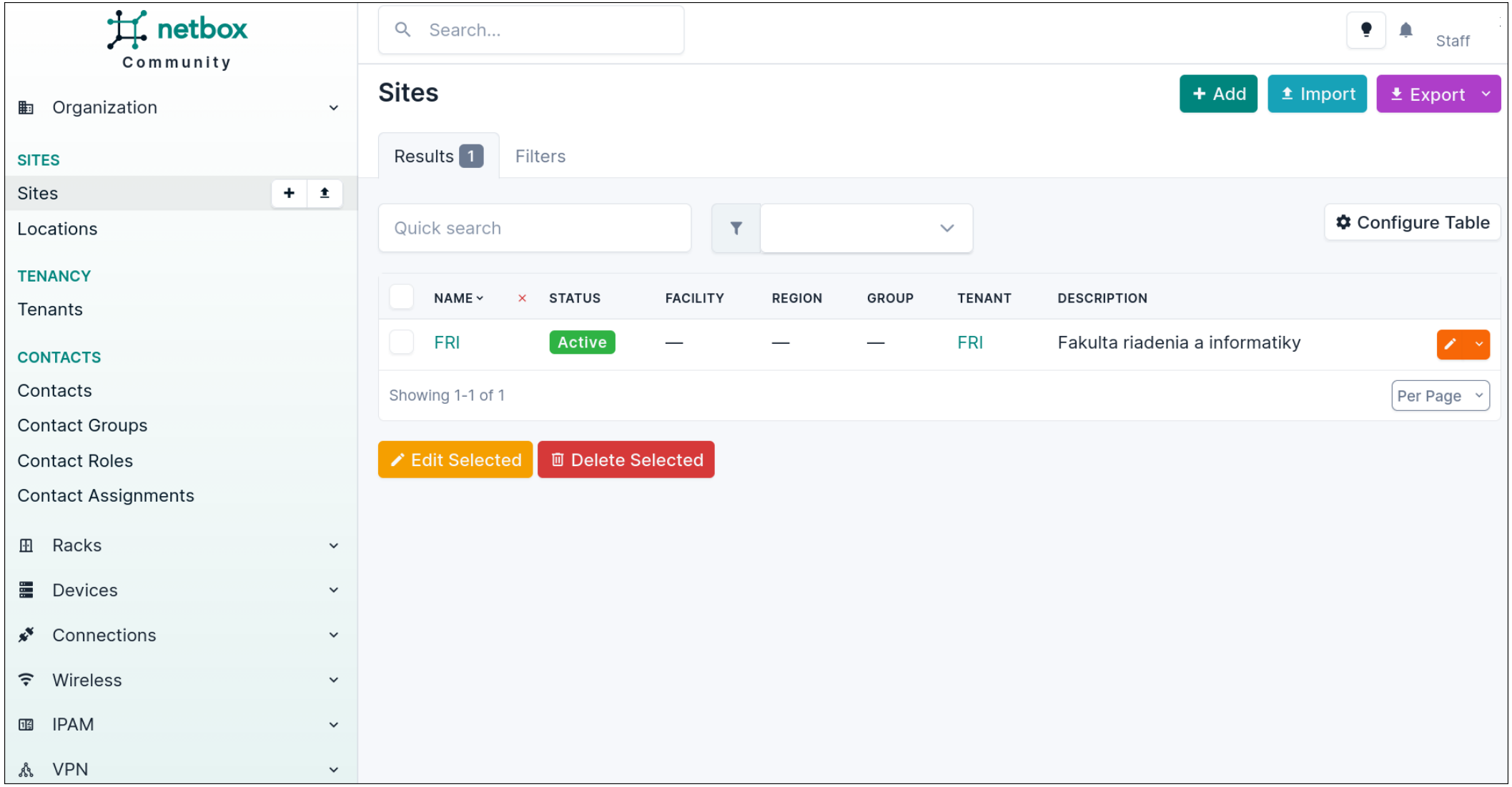
# Rozšírenie netbox-topology-views

- Vizualizačný plugin **`netbox-topology-views`** je možné použiť na automatické vykreslenie topológie siete
- Vygenerované diagramy:
  - Fyzická topológia serverov a prepínačov
  - VLAN väzby medzi zariadeniami
  - Fyzické prepojenia medzi lokáciami (napr. optika vs. metalika)
- Výhoda:
  **Topológia je dynamicky generovaná zo zadaných objektov**
  → ak sa **zmení fyzické prepojenie** (kábel, port) graf sa **automaticky aktualizuje**
  → **zmena IP adresy** sa prejaví **aktualizáciou údajov** objektu, **nie zmenou topológie**



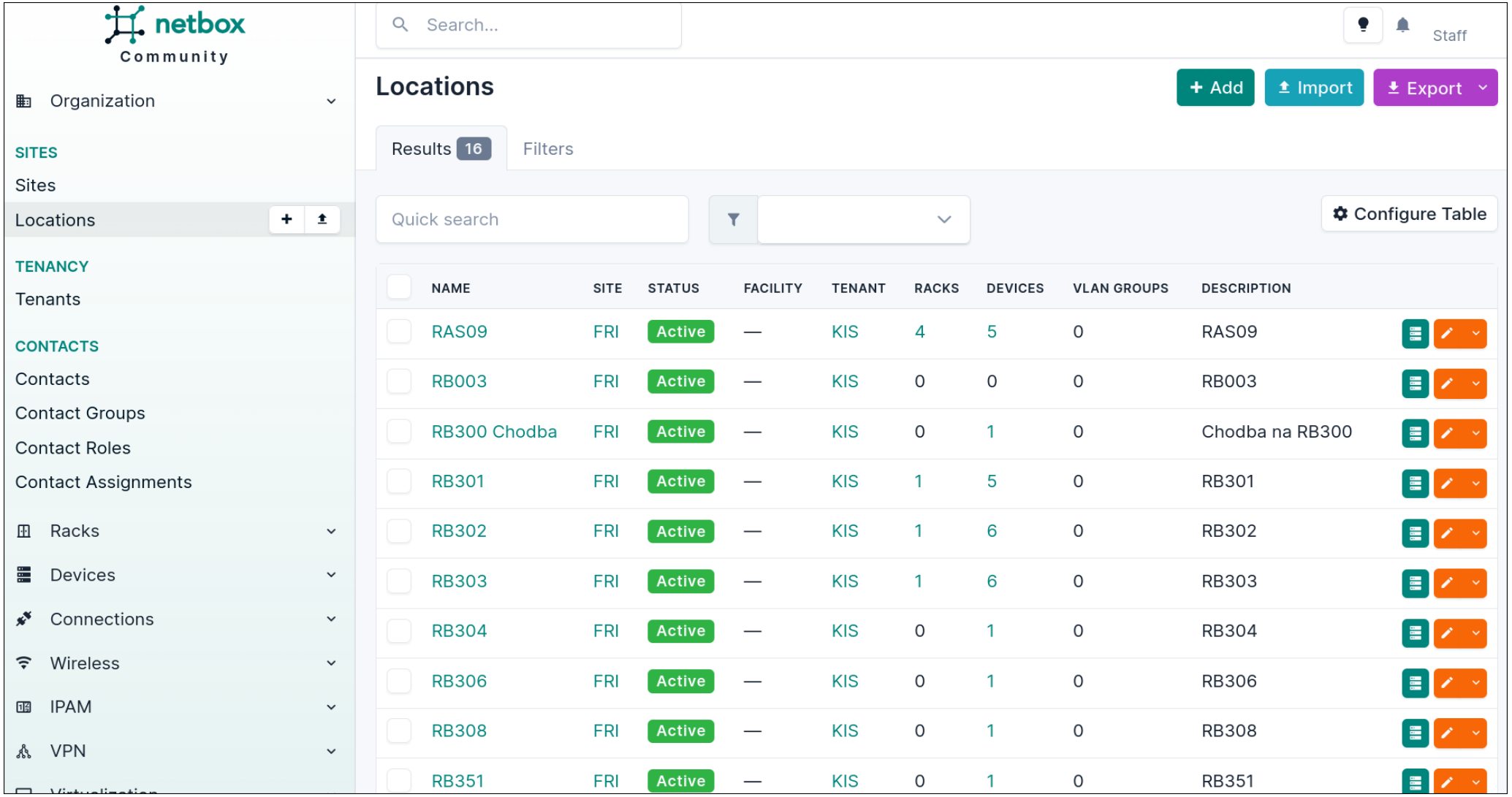
# Netbox

# Sites



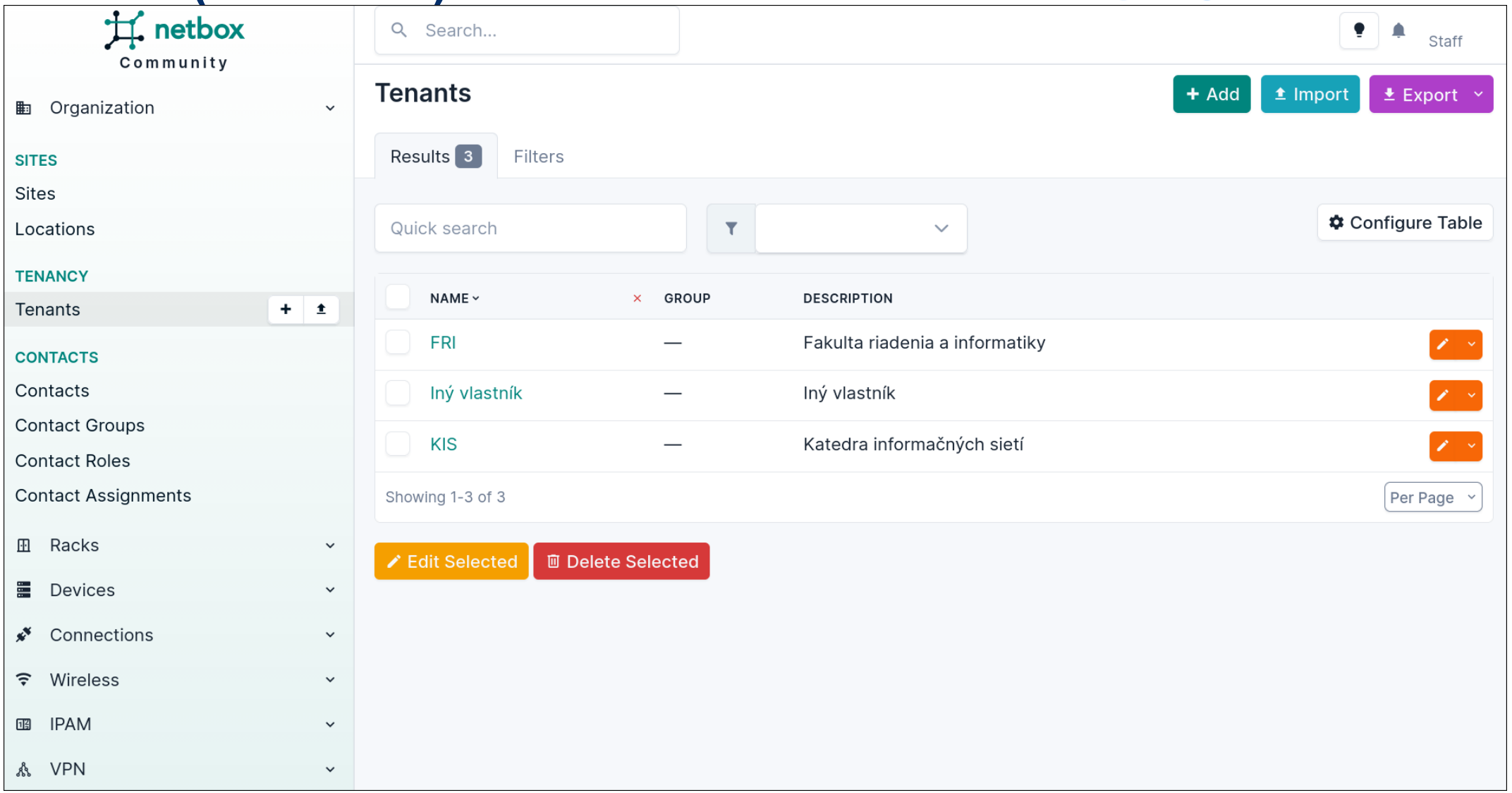
# Netbox

# Locations



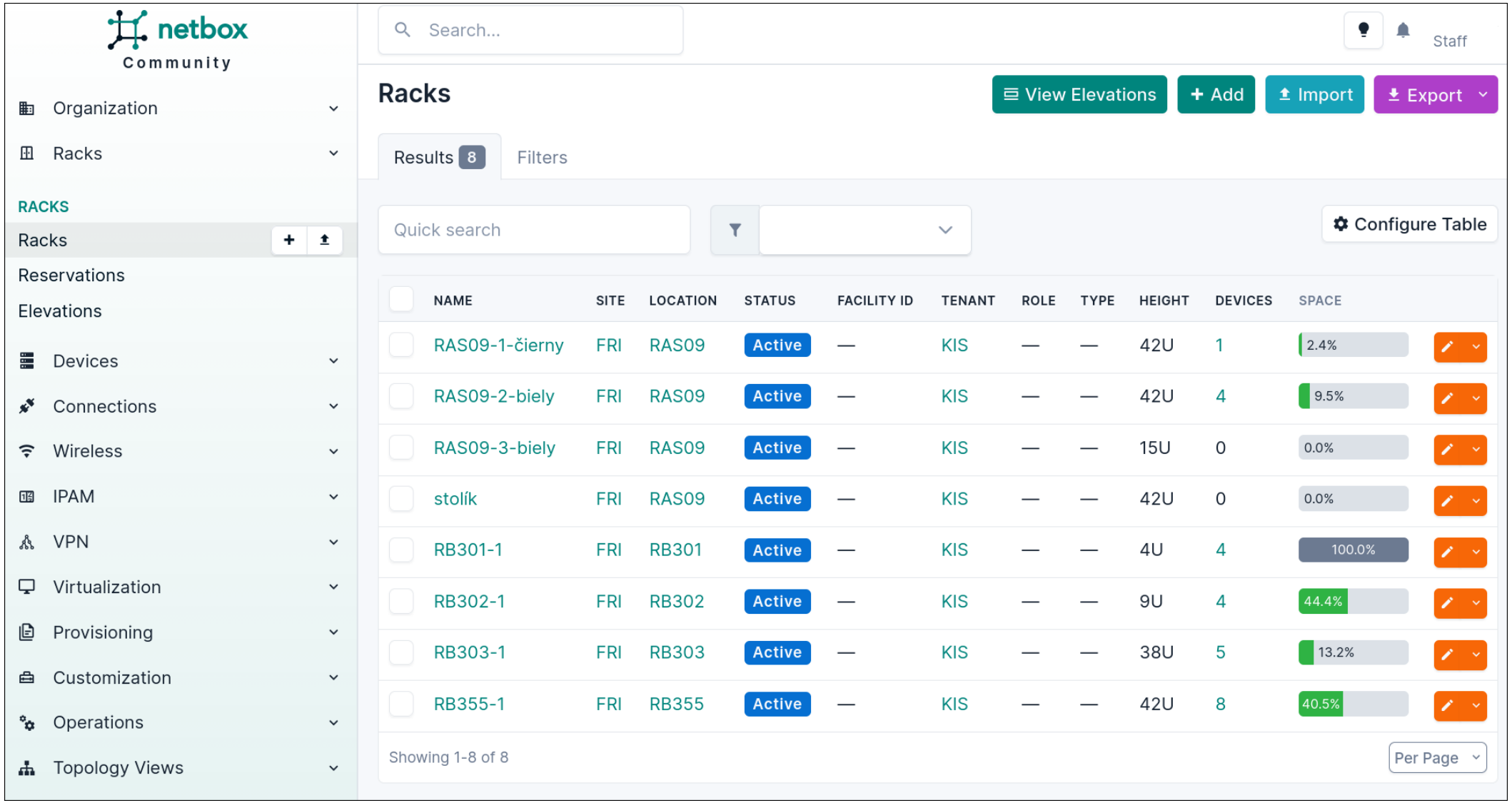
# Netbox

# Tenants (Vlastníci)



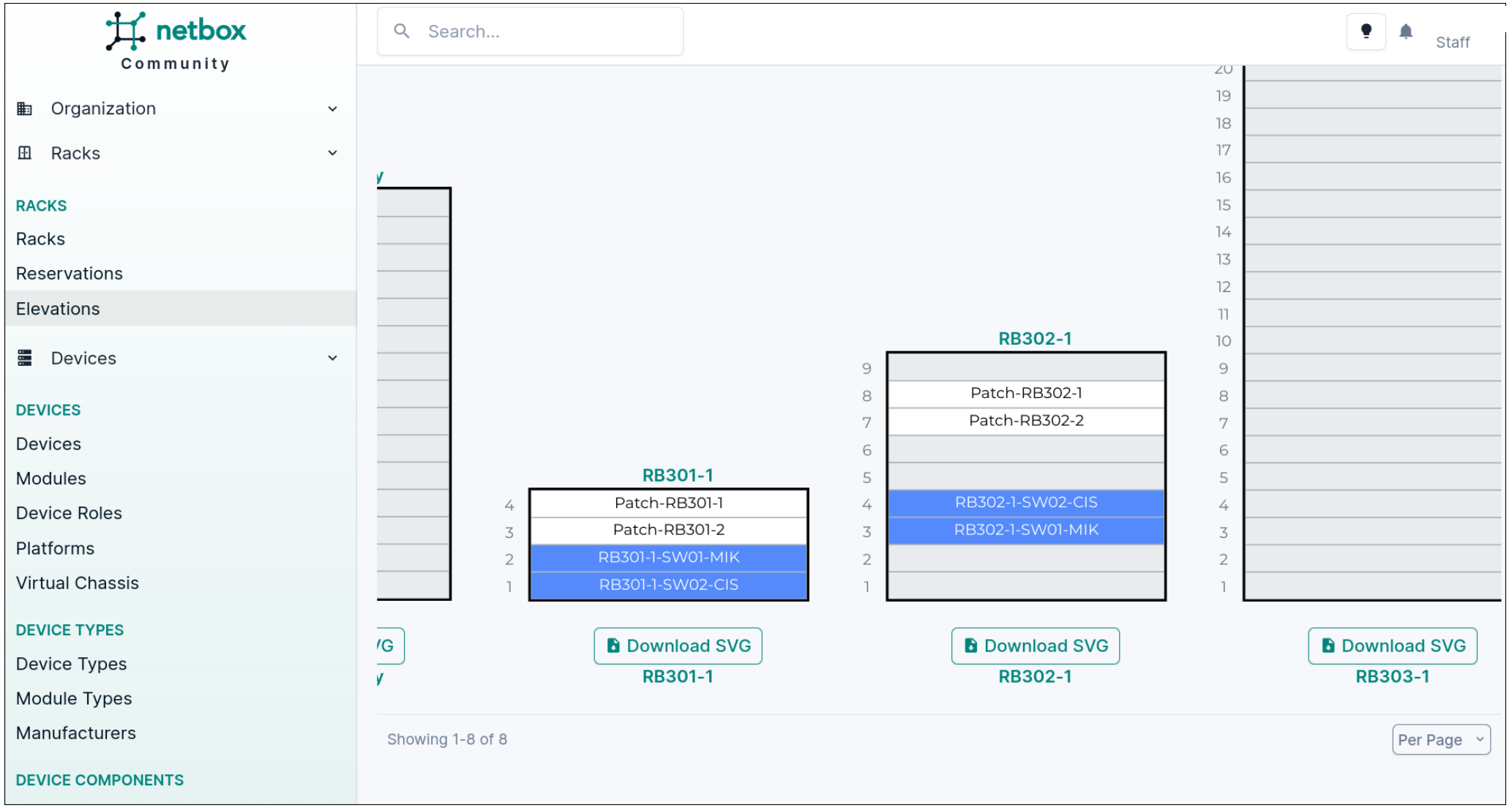
# Netbox

# Zoznam rack-ov



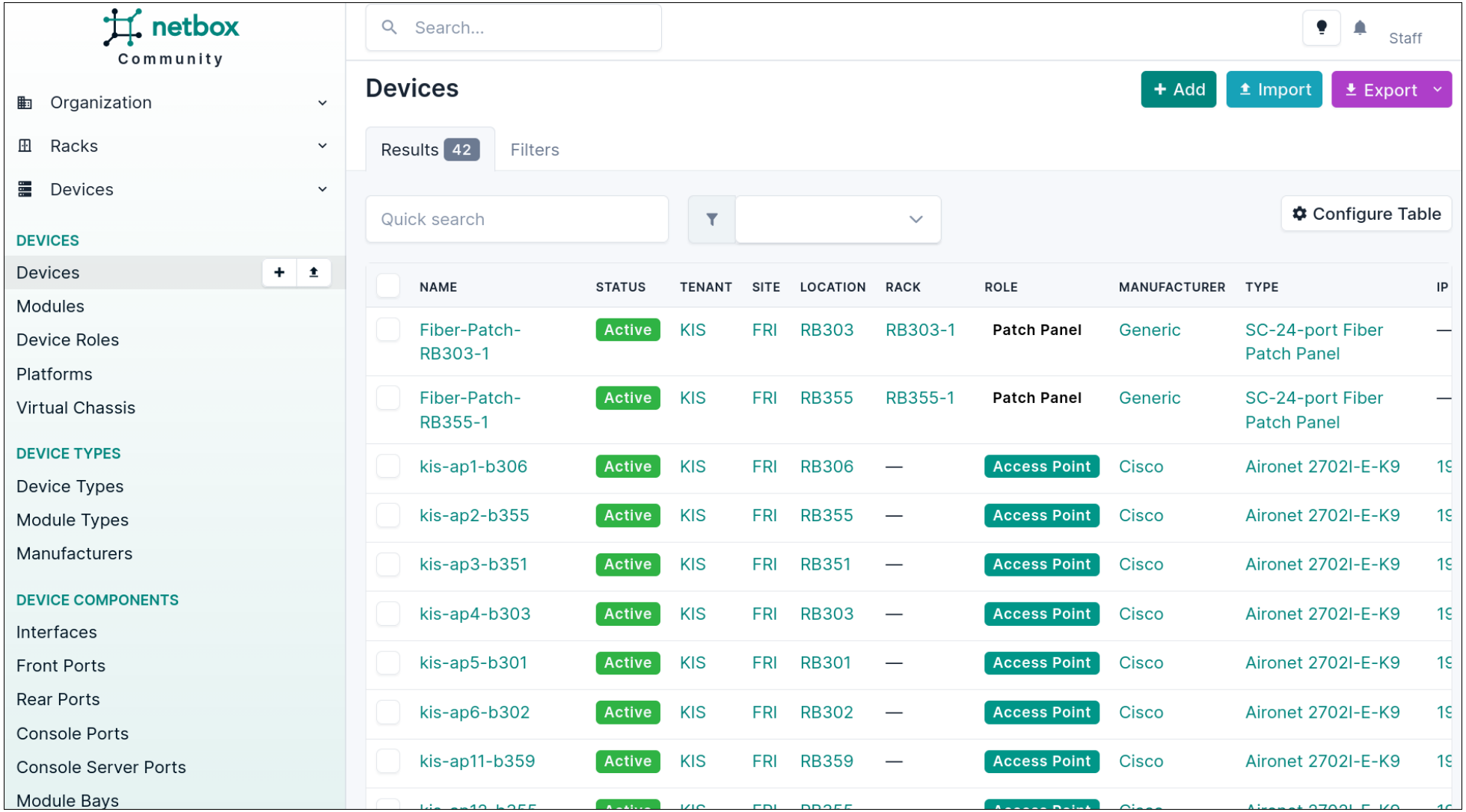
# Netbox

# Vizualizácia rack-ov (osadenie zariadení)

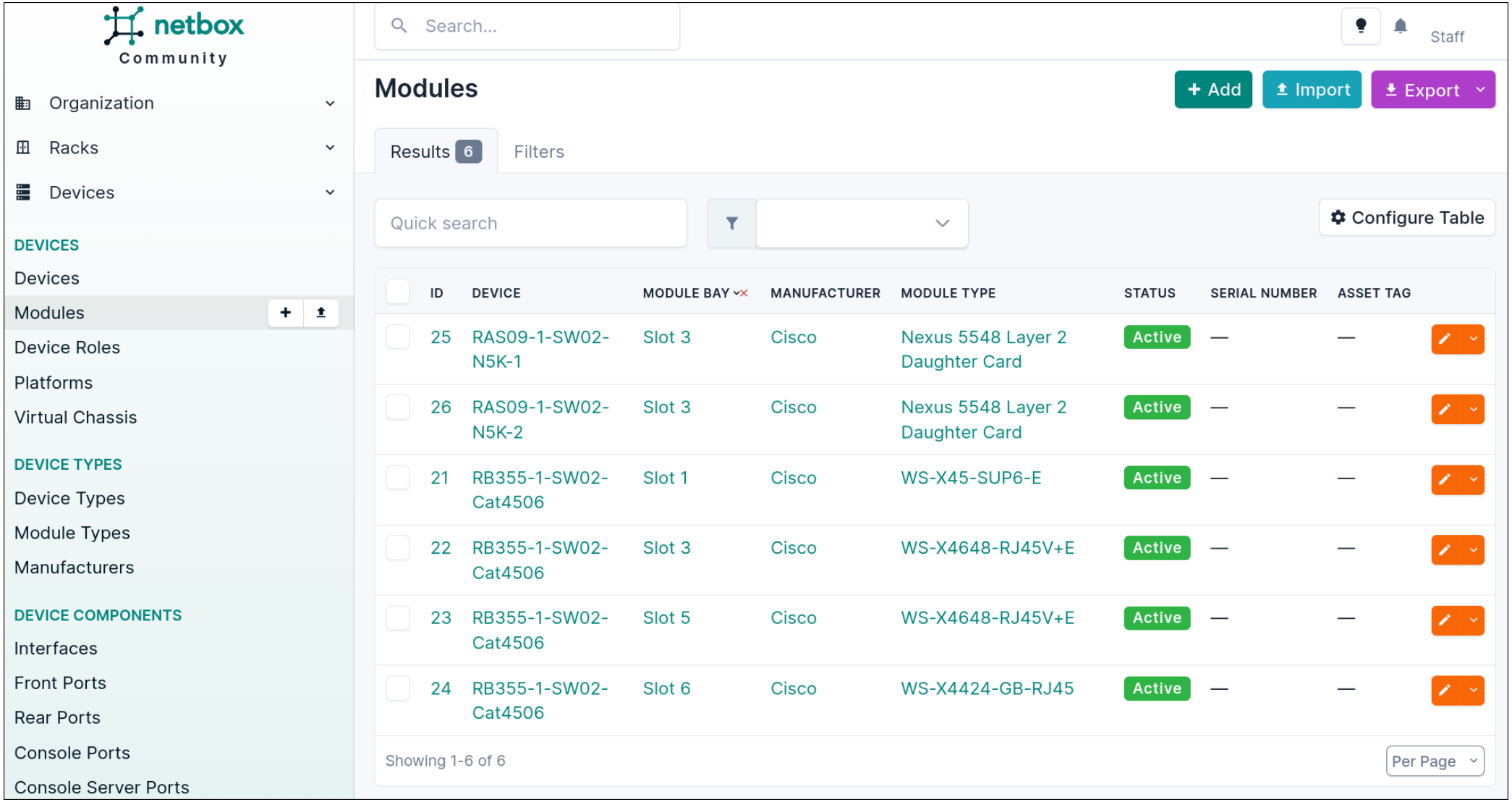


# Netbox

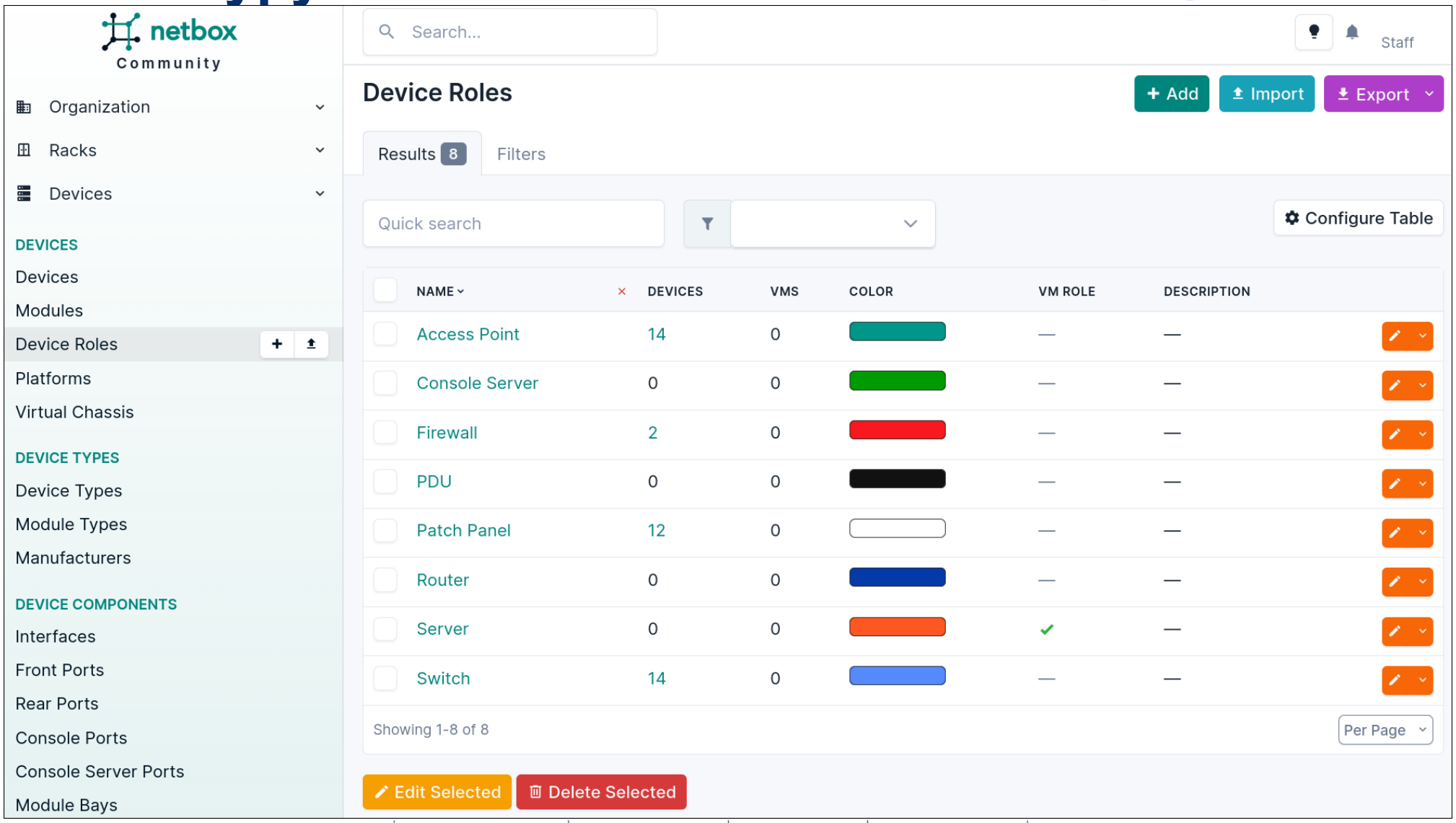
# Sieťové zariadenia



# Devices - Hardvérové moduly (karty)

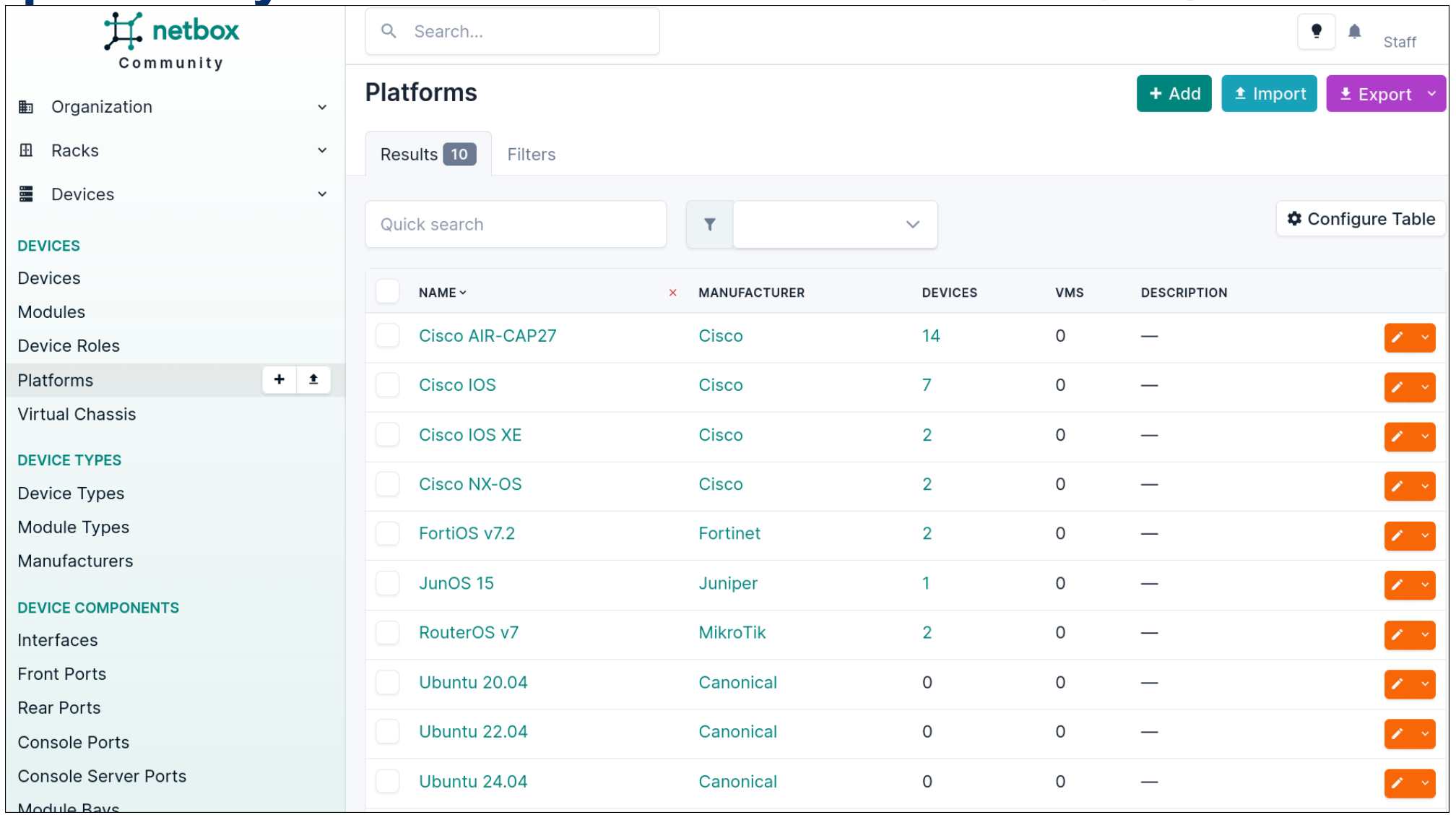


# Devices - Typy zariadení



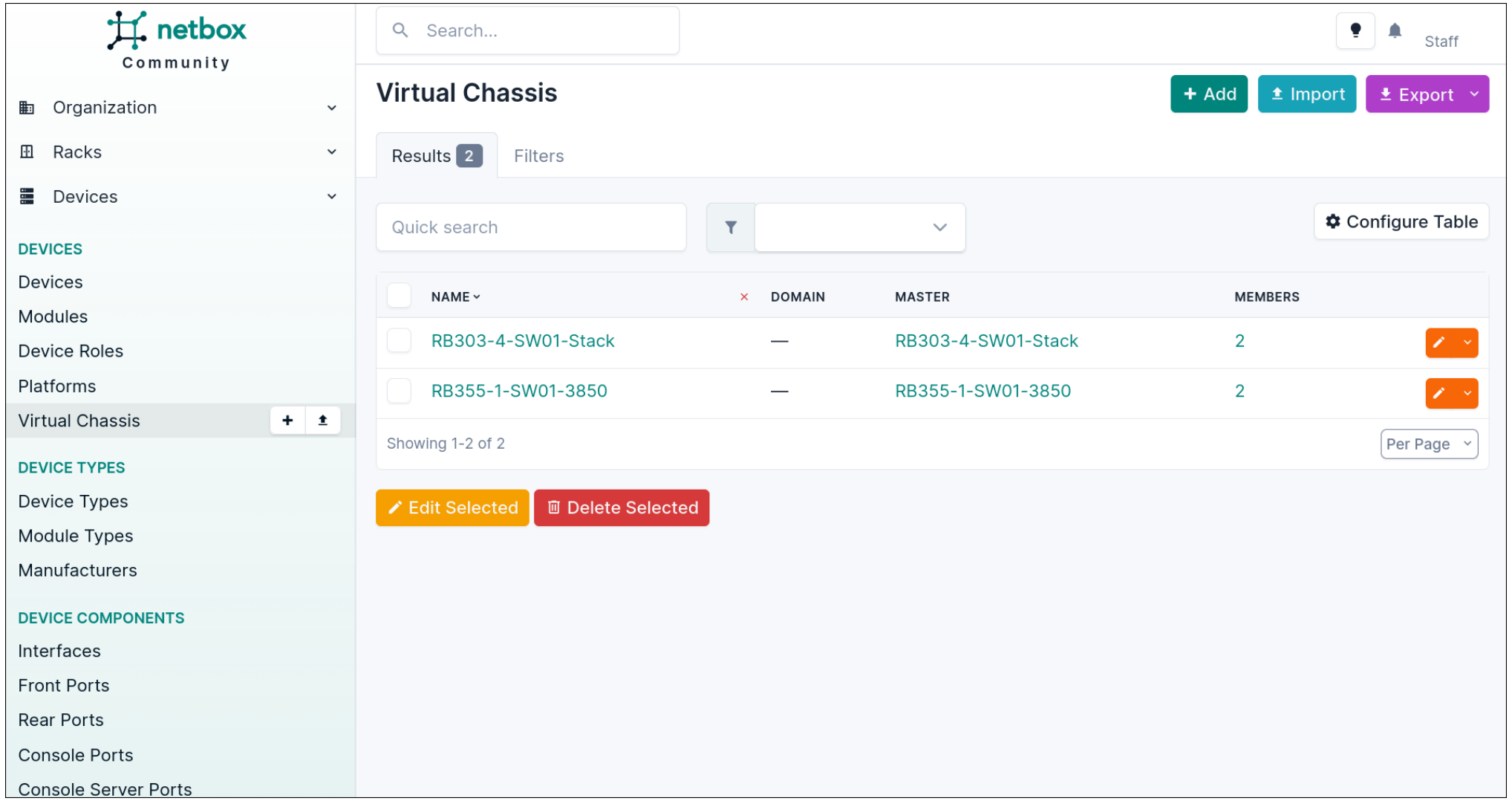
# Netbox

# OS platformy



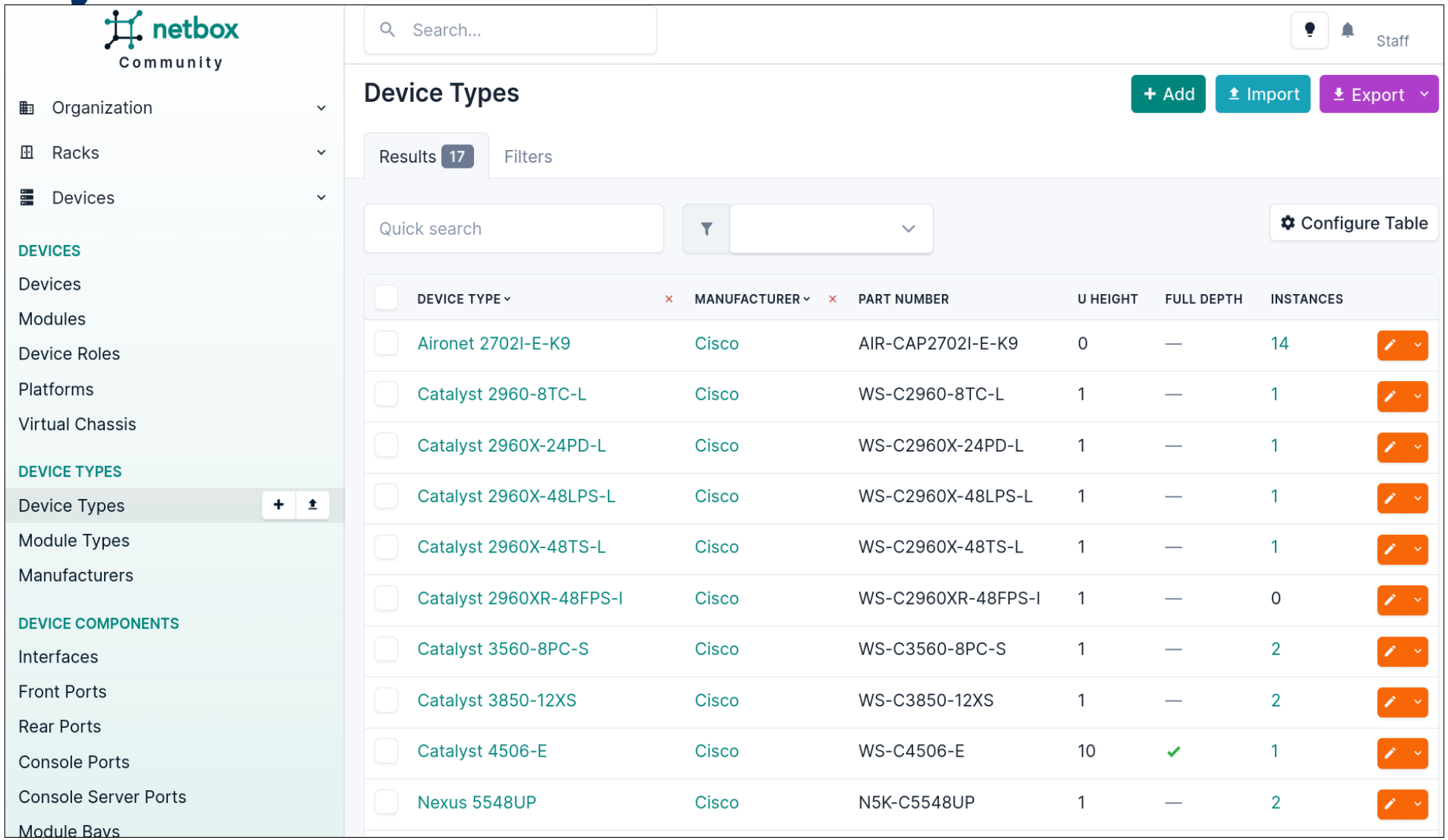
# Netbox

# Virtual chassis

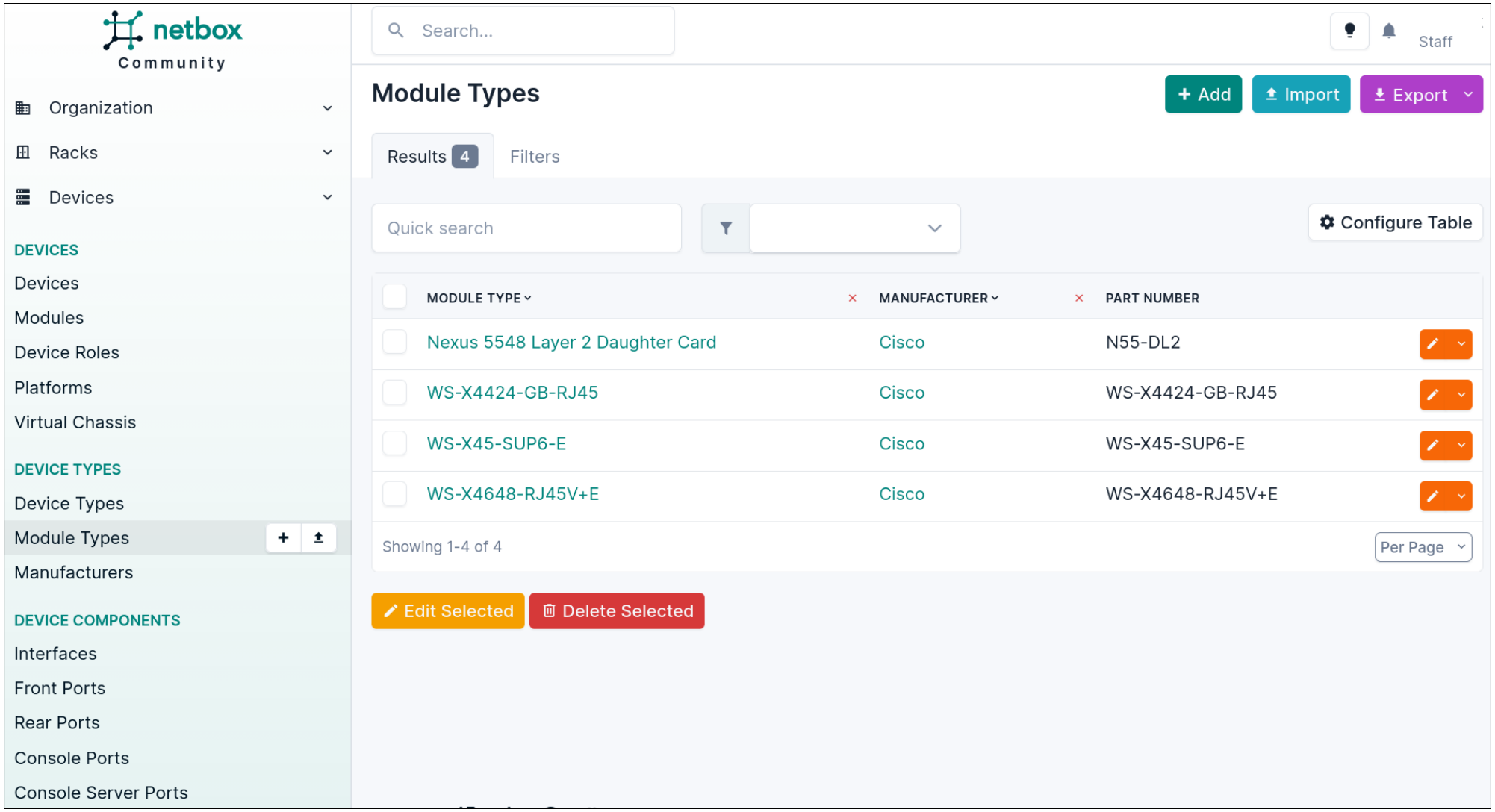


# Netbox

# Modely zariadení

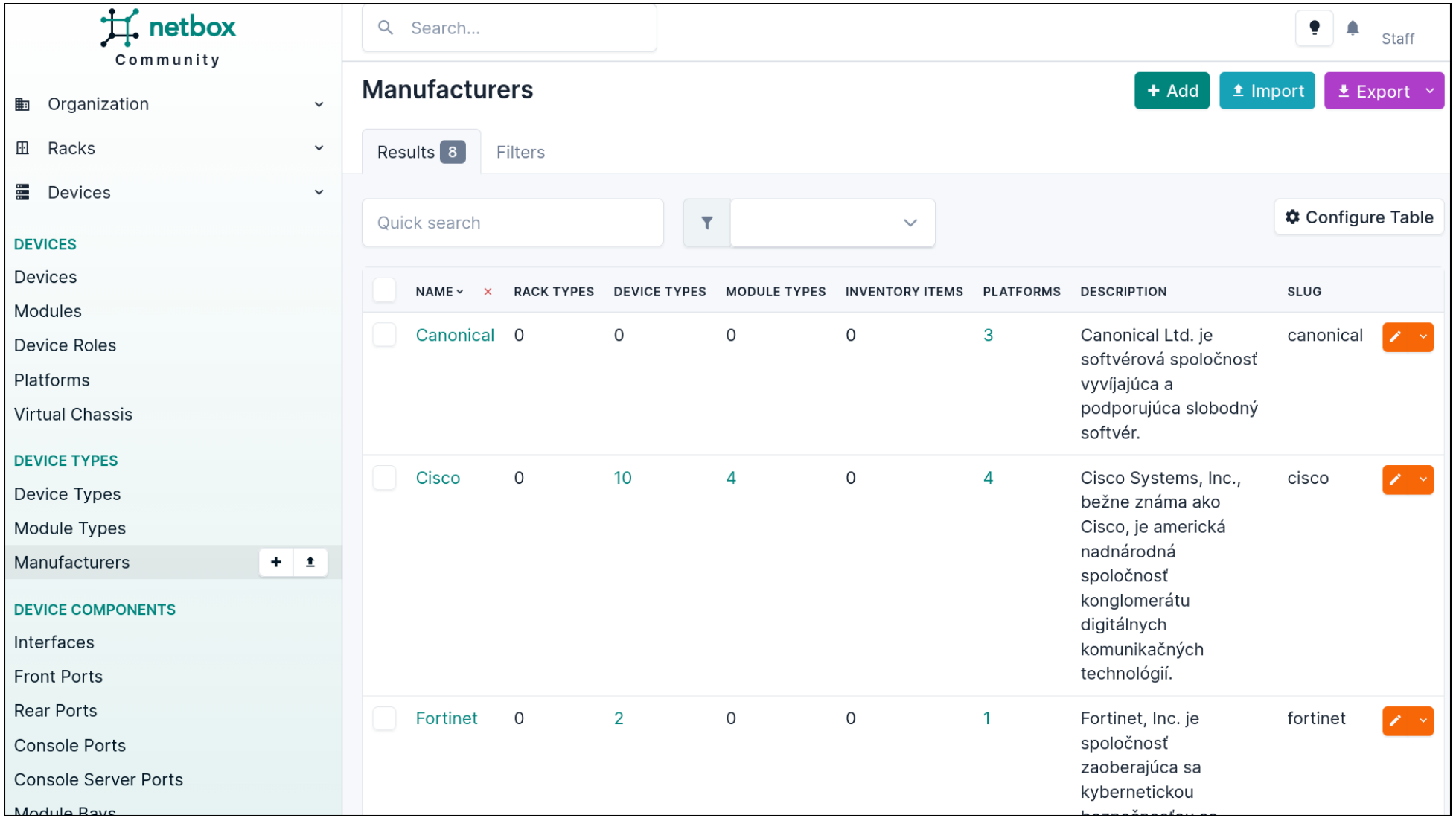


# Typy modulov (kariet)

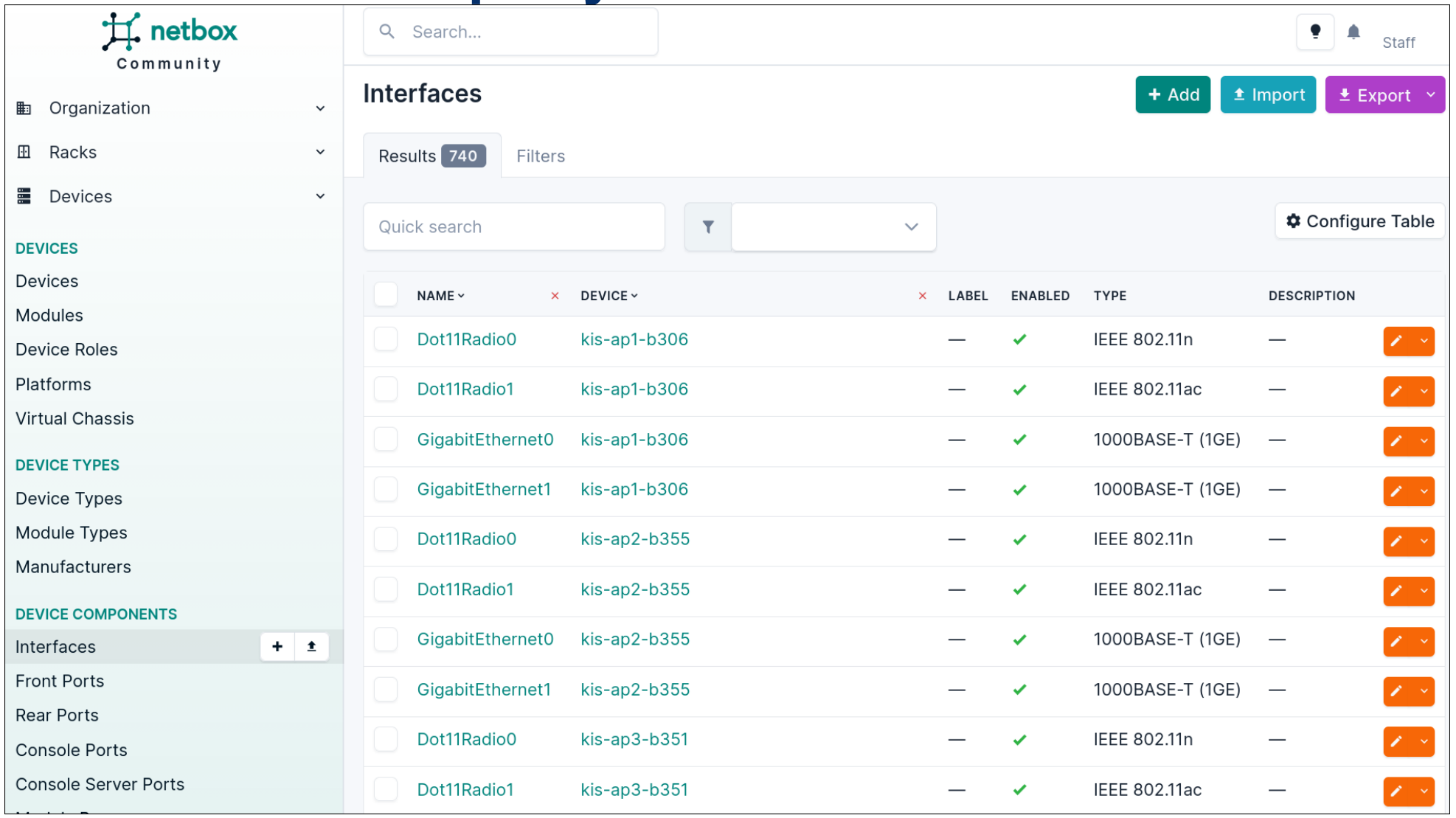


# Netbox

# Výrobcovia

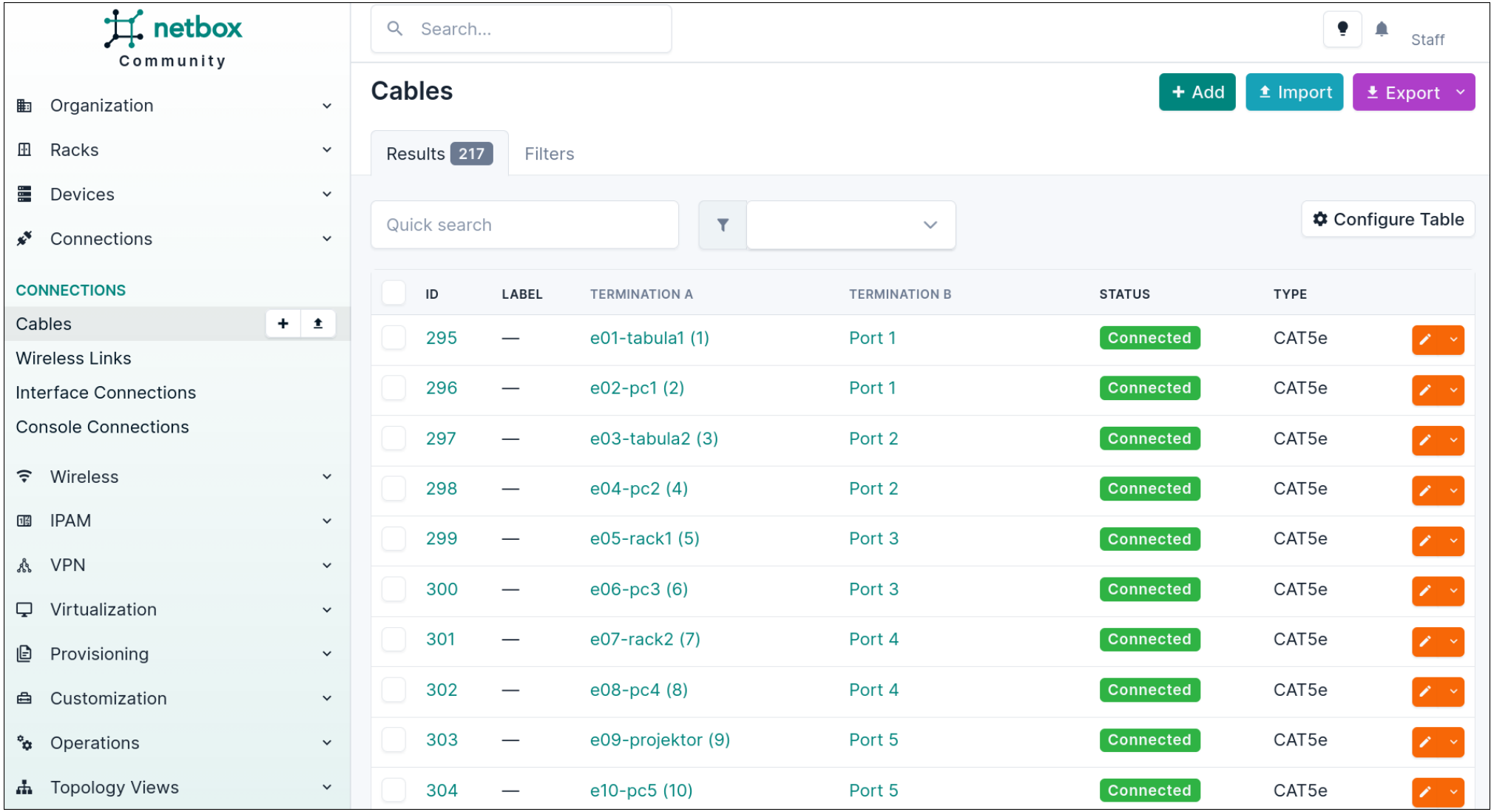


# Rozhrania / sieťové porty



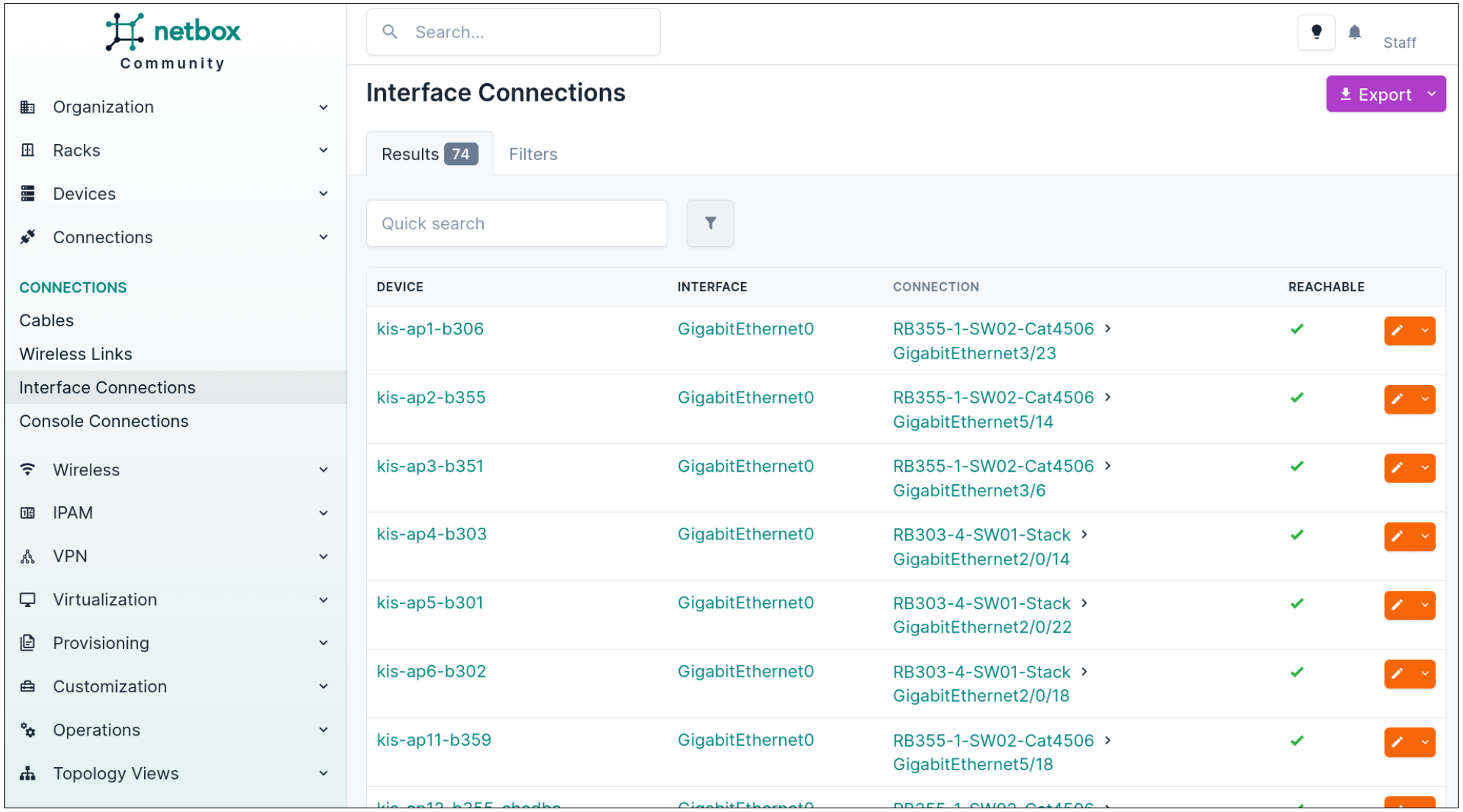
# Netbox

# Connections - Káble



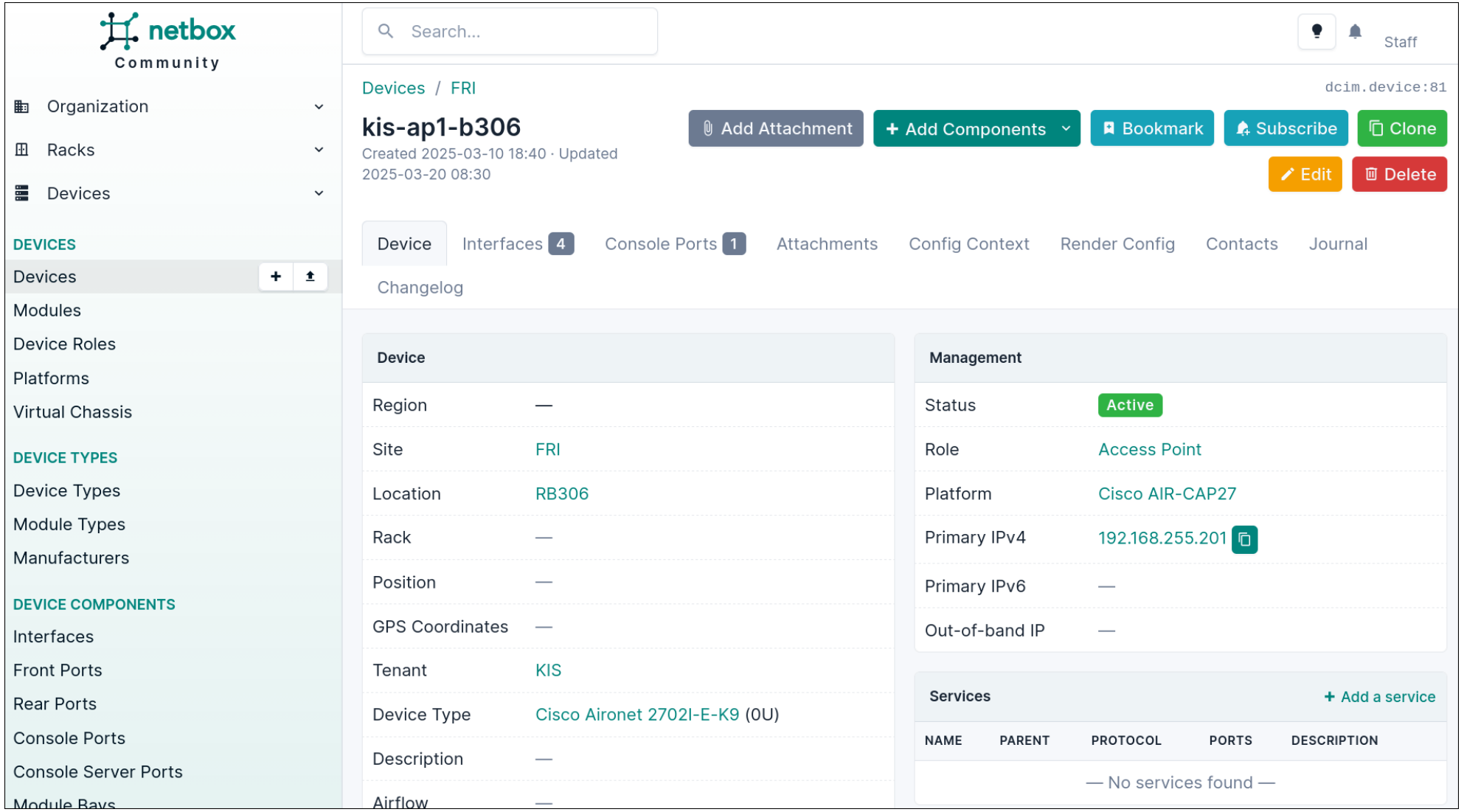
# Netbox

# Pripojenia rozhraní



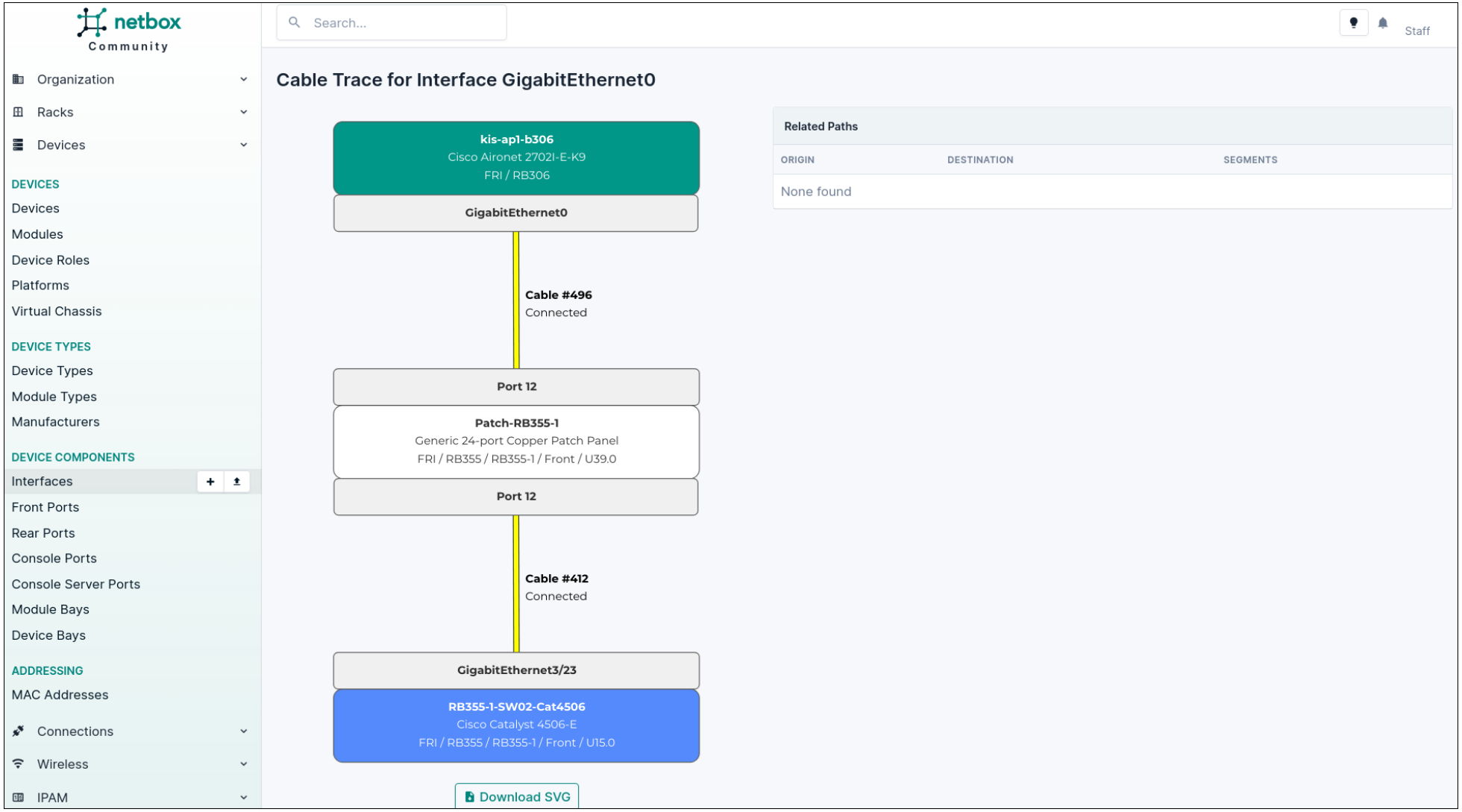
# Netbox

# Detail zariadenia



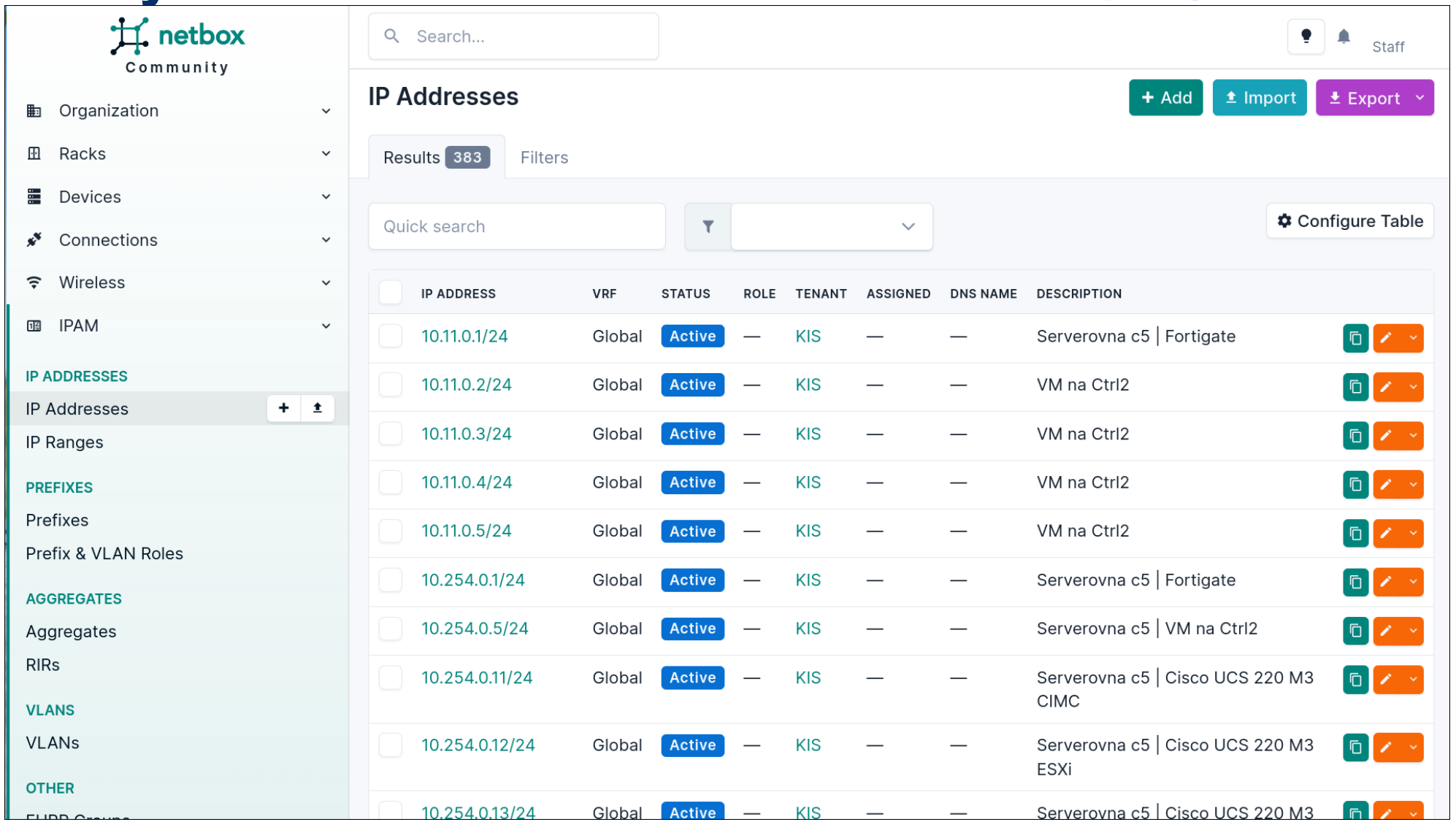
# Netbox

# Mapa spojenia



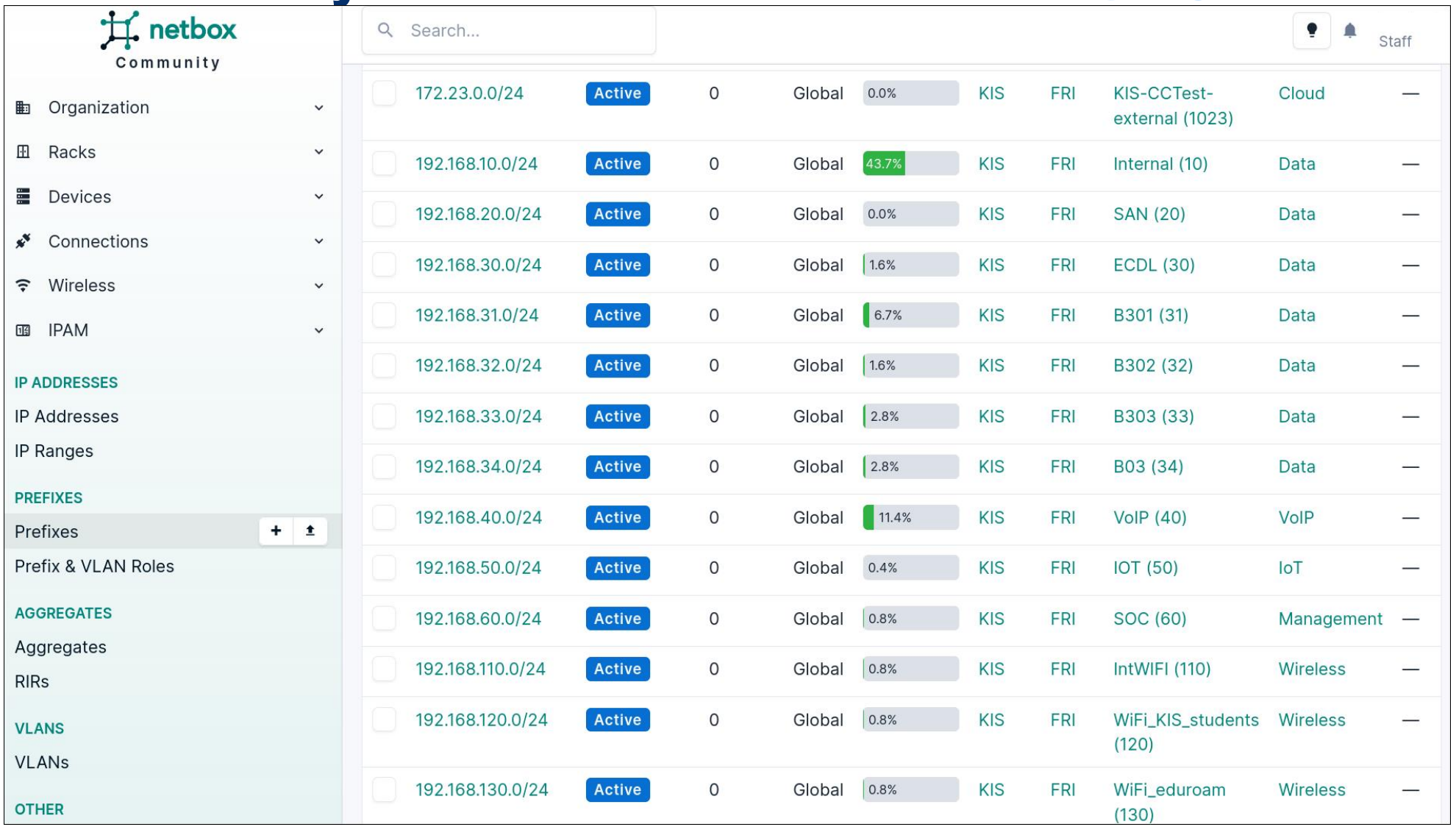
# Netbox

# IP adresy



# Netbox

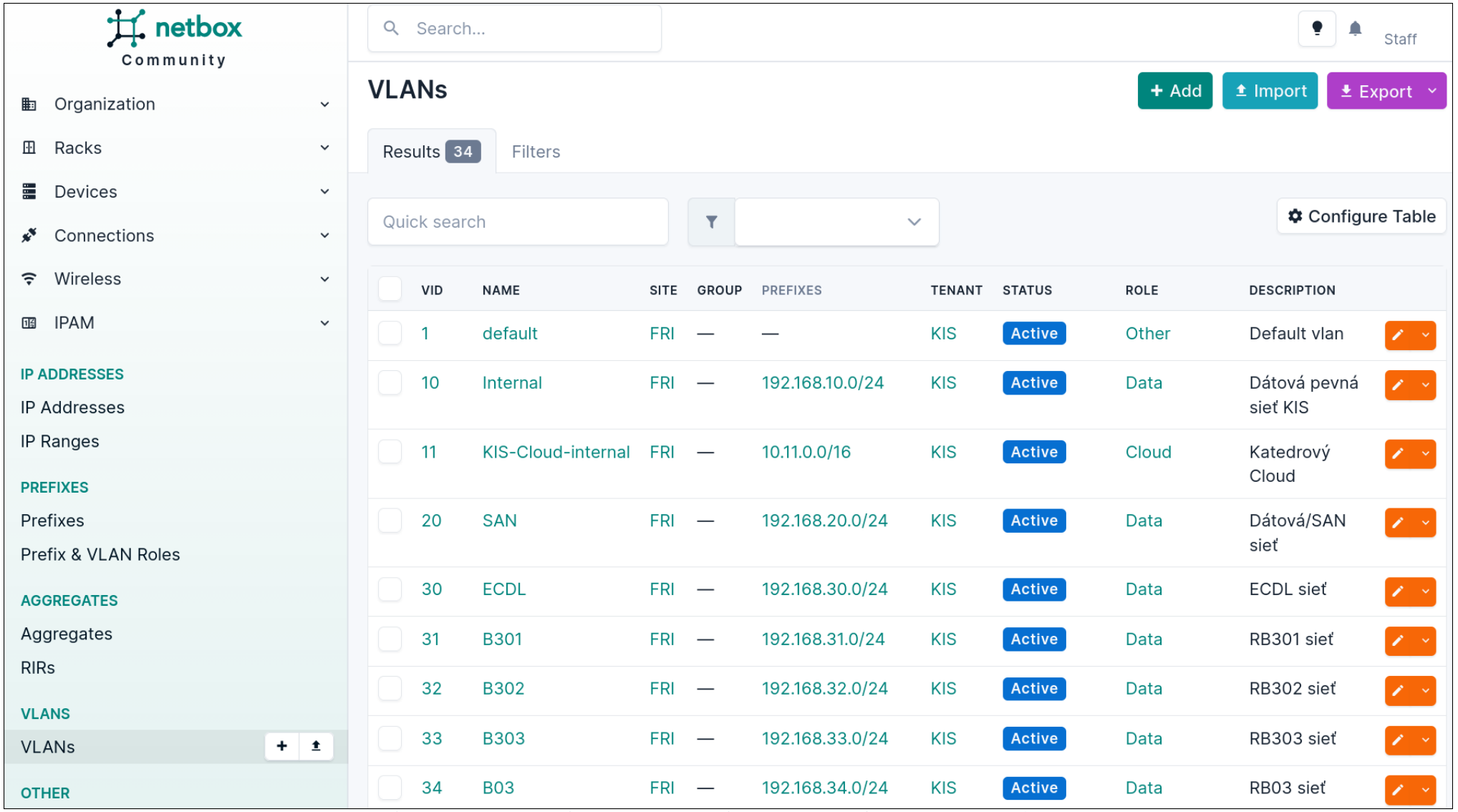
# Sieťové rozsahy




| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 172.23.0.0/24 | Active | 0 | Global | 0.0% | KIS | FRI | KIS-CCTest-external (1023) | Cloud | — |
| 192.168.10.0/24 | Active | 0 | Global | 43.7% | KIS | FRI | Internal (10) | Data | — |
| 192.168.20.0/24 | Active | 0 | Global | 0.0% | KIS | FRI | SAN (20) | Data | — |
| 192.168.30.0/24 | Active | 0 | Global | 1.6% | KIS | FRI | ECDL (30) | Data | — |
| 192.168.31.0/24 | Active | 0 | Global | 6.7% | KIS | FRI | B301 (31) | Data | — |
| 192.168.32.0/24 | Active | 0 | Global | 1.6% | KIS | FRI | B302 (32) | Data | — |
| 192.168.33.0/24 | Active | 0 | Global | 2.8% | KIS | FRI | B303 (33) | Data | — |
| 192.168.34.0/24 | Active | 0 | Global | 2.8% | KIS | FRI | B03 (34) | Data | — |
| 192.168.40.0/24 | Active | 0 | Global | 11.4% | KIS | FRI | VoIP (40) | VoIP | — |
| 192.168.50.0/24 | Active | 0 | Global | 0.4% | KIS | FRI | IOT (50) | IoT | — |
| 192.168.60.0/24 | Active | 0 | Global | 0.8% | KIS | FRI | SOC (60) | Management | — |
| 192.168.110.0/24 | Active | 0 | Global | 0.8% | KIS | FRI | IntWIFI (110) | Wireless | — |
| 192.168.120.0/24 | Active | 0 | Global | 0.8% | KIS | FRI | WiFi_KIS_students (120) | Wireless | — |
| 192.168.130.0/24 | Active | 0 | Global | 0.8% | KIS | FRI | WiFi_eduroam (130) | Wireless | — |

# Netbox

# Virtuálne siete



# Licencia


- NetBox je publikovaný pod **Apache License 2.0** – otvorená a benevolentná open-source licencia.
- Táto licencia **umožňuje:**
  - používať softvér bez obmedzenia (aj komerčne),
  - upravovať a integrovať ho s inými systémami,
  - využívať jeho API a exporty,
  - nasadiť ho v rámci akejkoľvek organizácie bez platenia poplatkov.

## Nástroje pre inventarizáciu aktív

# Možné hodnotiace kritériá

| | názov kritéria | stručný popis | vysvetlenie priradenia bodov |
|---|---|---|---|
| 1 | Vytvorenie, editácia a mazanie záznamov o aktívach | Schopnosť systému evidovať, upravovať a mazať informácie o jednotlivých aktívach. | 1 = Len základná evidencia bez úprav;<br>5 = Plná CRUD funkcionalita s kontrolou zmien a audit trail. |
| 2 | Rozlíšenie aktív podľa typu – hardvér, softvér, virtuálne, cloudové | Možnosť rozlišovať typy aktív pre lepšiu organizáciu a správu. | 1 = Len základné typy aktív;<br>5 = Rozšírené triedenie vrátane cloudových, kontajnerov a virtuálnych |
| 3 | Možnosť priradenia tagov, kategórií, vlastníkov a stavu (napr. aktívne, v údržbe, vyradené) | Pridávanie metadát pre efektívne triedenie a správu aktív. | 1 = Len pevne dané kategórie;<br>5 = Užívateľsky definovateľné tagy, stav a vlastníctvo. |
| 4 | Evidencia bezpečnostného stavu každého aktíva (napr. OS verzie, posledná aktualizácia) | Ukladanie informácií o zraniteľnostiach, patch úrovni a aktualizáciách systému. | 1 = Žiadne bezpečnostné atribúty;<br>5 = Automatizovaná evidencia bezpečnostného stavu. |
| 5 | Mapovanie aktív na lokality, VLANy, IP rozsahy, racky | Schopnosť mapovať fyzické a logické umiestnenie aktív v sieti. | 1 = Len názov lokality;<br>5 = Podpora komplexného mapovania IP, rack, VLAN, zón. |
| 6 | Väzby medzi aktívami (napr. server – služba – aplikácia) | Možnosť vizualizovať a spravovať prepojenia medzi komponentmi infraštruktúry. | 1 = Bez väzieb;<br>5 = Detailné mapovanie závislostí s grafickou reprezentáciou. |
| 7 | Integrácia s monitoringom, SIEM, ticketing systémom, EDR, skenerom zraniteľností, evidencia incidentov | Možnosť prepojenia s ďalšími nástrojmi SOC pre automatizáciu a zdieľanie údajov. | 1 = Žiadna integrácia;<br>5 = Viacúrovňová bidirekčná integrácia s relevantnými systémami. |



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

## Nástroje pre inventarizáciu aktív

# Možné hodnotiace kritériá

| | názov kritéria | stručný popis | vysvetlenie priradenia bodov |
|---|---|---|---|
| 8 | Možnosť filtrovania, fulltextového vyhľadávania a exportu | Efektívna práca s údajmi – vyhľadávanie podľa rôznych parametrov a exportovanie údajov. | 1 = Len základné vyhľadávanie;<br>5 = Pokročilé fulltextové vyhľadávanie + exporty (CSV, JSON). |
| 9 | Podpora API (REST, GraphQL) na správu aktív a integráciu | Možnosť spravovať a aktualizovať údaje o aktívach pomocou API. | 1 = Bez API;<br>5 = Dokumentované REST/GraphQL API pre všetky funkcie. |
| 10 | Možnosť tvorby vlastných polí, atribútov, pluginov (napr. NetBox/Django) | Užívateľská flexibilita pre prispôsobenie systému vlastným potrebám. | 1 = Pevne definovaná štruktúra;<br>5 = Plne prispôsobiteľná s podporou pluginov alebo skriptovania. |
| 11 | Automatizovaný discovery assetov v sieti (napr. SNMP, nmap, API z iných systémov) | Automatizovaný zber a aktualizácia údajov o aktívach zo siete a iných systémov. | 1 = Manuálny zber údajov;<br>5 = Automatizované discovery s plánovaním a API vstupmi. |
| 12 | Webové rozhranie s možnosťou úprav a prehľadnou správou | Používateľsky privetivé GUI pre správu assetov. | 1 = Neintuitívne alebo len CLI;<br>5 = Responzívne a používateľsky priateľské rozhranie. |
| 13 | Zaznamenávanie zmien na aktívach (kto, kedy, čo zmenil) | Auditovateľnosť všetkých zmien pre forenznú a prevádzkovú transparentnosť. | 1 = Žiadne logovanie zmien;<br>5 = Detailný audit trail s časovou pečiatkou a užívateľom. |
| 14 | Možnosť sledovať životný cyklus assetov (nasadenie – vyradenie) | Správa jednotlivých fáz životnosti aktíva – od zaradenia po vyradenie. | 1 = Bez životného cyklu;<br>5 = Komplexné sledovanie s upozorneniami a stavmi. |
| 15 | Upozornenia na zmenu stavu, expirácie, servisné intervaly | Automatické notifikácie pri zmene stavu alebo potrebe servisného zásahu. | 1 = Bez upozornení;<br>5 = Konfigurovateľné upozornenia podľa podmienok alebo kalendára. |



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE


# Reálna implementácia procesu riadenia rizík (MONARC)

## Implementácia procesu riadenia rizík

# MONARC

- **Open-source nástroj** na riadenie informačných a kybernetických rizík.
- Vyvíjaný a podporovaný **CIRCL (Computer Incident Response Center Luxembourg)**.
- Postavený na **metodike ISO/IEC 27005** a **EBIOS RM** (Expression of Needs and Identification of Security Objectives, spravuje ANSSI, francúzska agentúra pre KB, risk manag. metóda)
- Cieľ: umožniť organizáciám **systematicky identifikovať, hodnotiť a spravovať riziká**.

MONARC pomáha **plniť požiadavky zákona č. 69/2018 Z. z. (§20 – Riadenie rizík)** a normy ISO/IEC 27001 (kap. 6 – Riziká a príležitosti).

### Podporované distribúcie

- Primárne testovaný na Ubuntu verzii 18.04 LTS, pričom inštalácie sú možné na:
  - Ubuntu

### Technické požiadavky

- Git
- Apache
- MariaDB
- PHP verzia 8.1 alebo vyššia
  - PHP knižnice spravované composer-om
- Javascript
  - Javascript spravovaný composer-om

# Možnosti nasadenia

- MONARC sa skladá z 2 hlavných častí:
  - **Back office (BO)** – správa bezpečnostných modelov, FO serverov a klientov inštalácií MONARC
  - **Front office (FO)** – riadenie analýzy rizík, FO nepotrebuje využívať BO
- Celá architektúra obsahuje dodatočný reverzný proxy (RPX) a konfiguračný server (CFG). Je možné pripojiť viacero FO k jednému BO. Nasadenie je riadené pomocou ansible.
- **FO (Front Office)** – jednoduchšie nasadenie
  - **Stačí jeden server**, všetko prebieha v prostredí FO
  - **Nevyžaduje Back Office** ani reverzný proxy server
  - Ideálne pre **malé a stredné organizácie**
- **BO (Back Office)** – centralizovaná správa pre viac FO
  - Používa sa v **väčších prostrediach**, kde je potrebné riadiť rizikové analýzy **viacerých organizácií**
  - **FO slúži ako klient, BO spravuje modely, používateľov a analýzy**
  - Nasadenie BO si vyžaduje **vyššiu úroveň technických znalostí** (Linux, Docker, Ansible, sieťové služby)

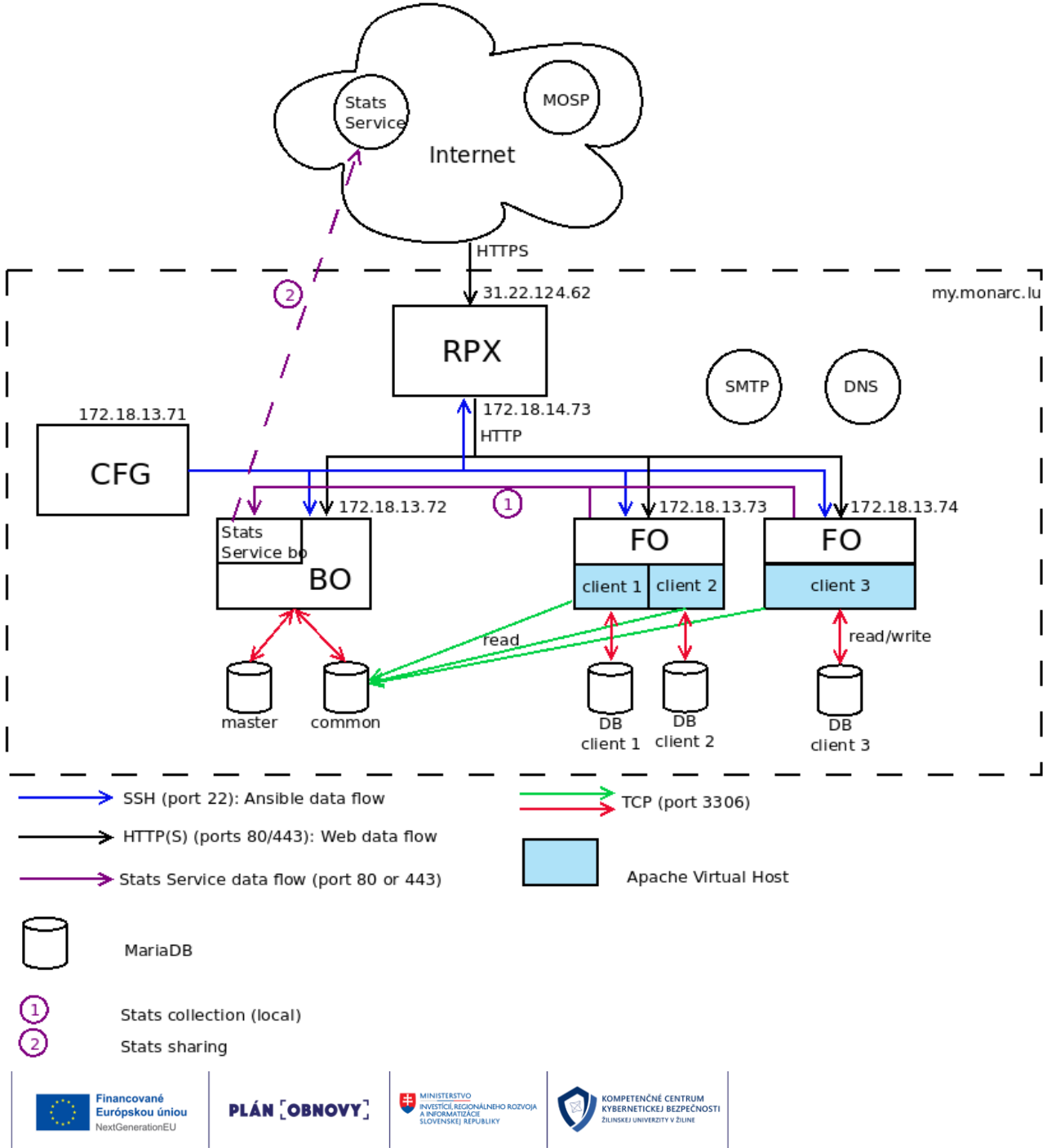


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

MONARC

# Back Office

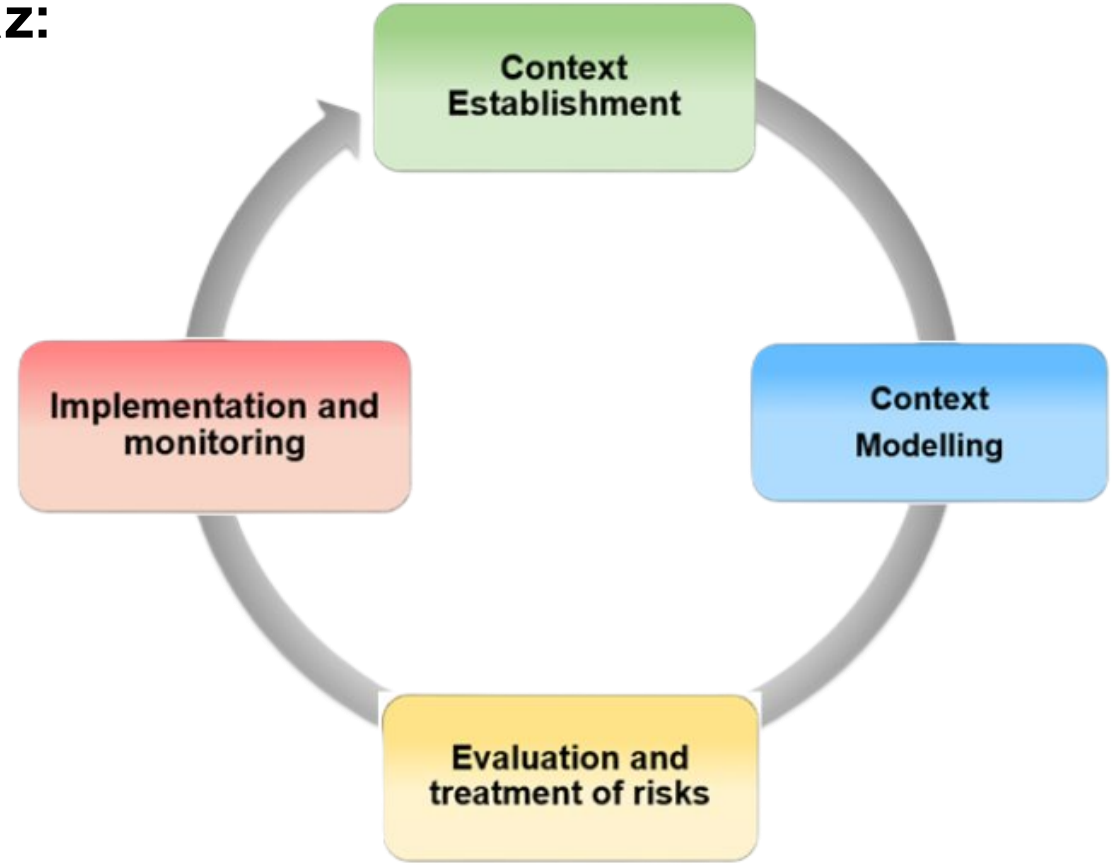
**Back Office** obsahuje **centrálny** databázový a **riadiaci uzol**, ku ktorému sa pripájajú všetky Front Office inštancie



# Analýza rizík v 4 fázach

- Monarc ponúka **iteratívnu** a **kvalitatívnu** metódu analýzy rizík, ktorá pozostáva zo **4 fáz:**

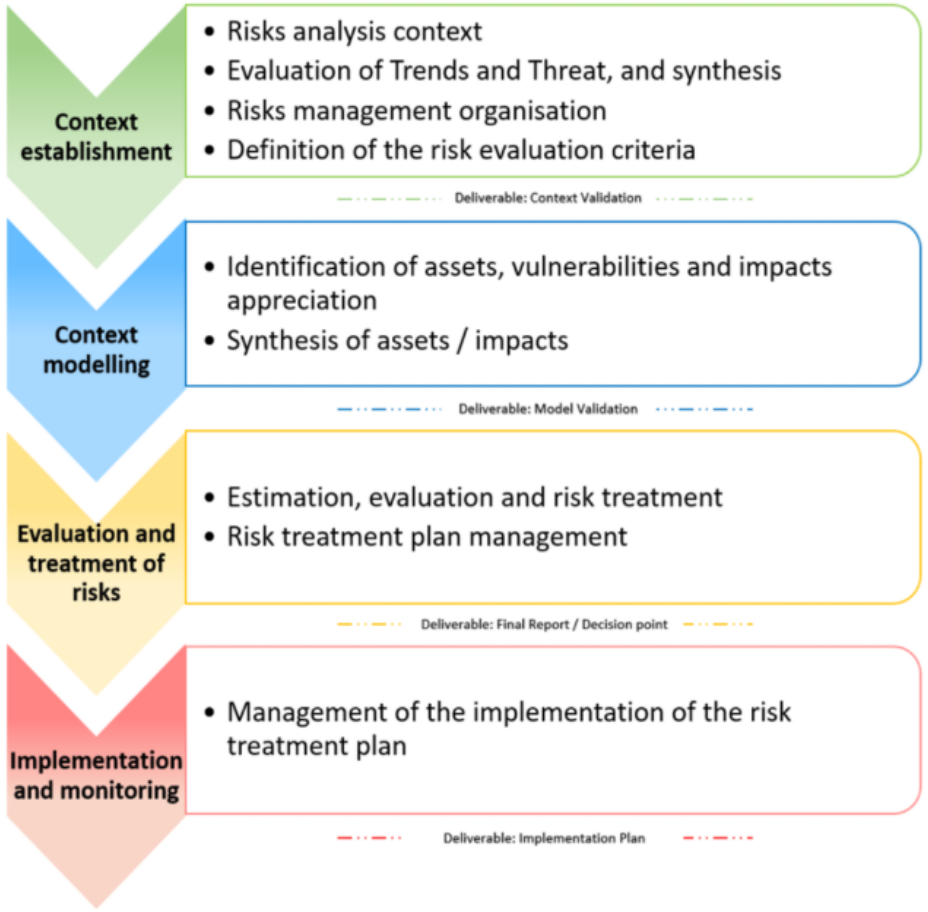
1. **stanovenie kontextu:**
   - určenie cieľa analýzy a definovanie prostredia
   - stanovenie kritérií a metodiky hodnotenia rizík
2. **modelovanie kontextu:**
   - identifikácia aktív a ich rozdelenie podľa priority
   - vytvorenie rizikového modelu pomocou databázy MONARC
3. **hodnotenie a ošetrenie rizík:**
   - posúdenie hrozieb, zraniteľností a úrovne rizík
   - návrh opatrení na zníženie významných rizík
4. **implementácia a monitorovanie:**
   - realizácia odporúčaných bezpečnostných opatrení
   - priebežné sledovanie zmien a aktualizácia analýzy



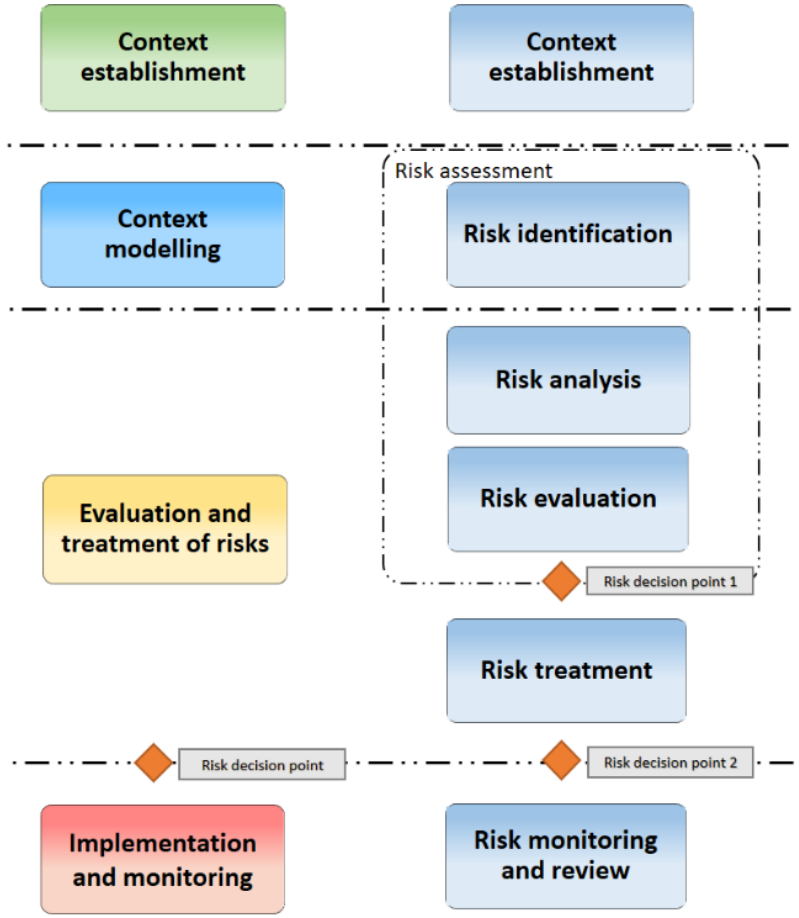
MONARC

# Analýza rizík v 4 fázach

## Fázy analýzy rizík v nástroji Monarc:



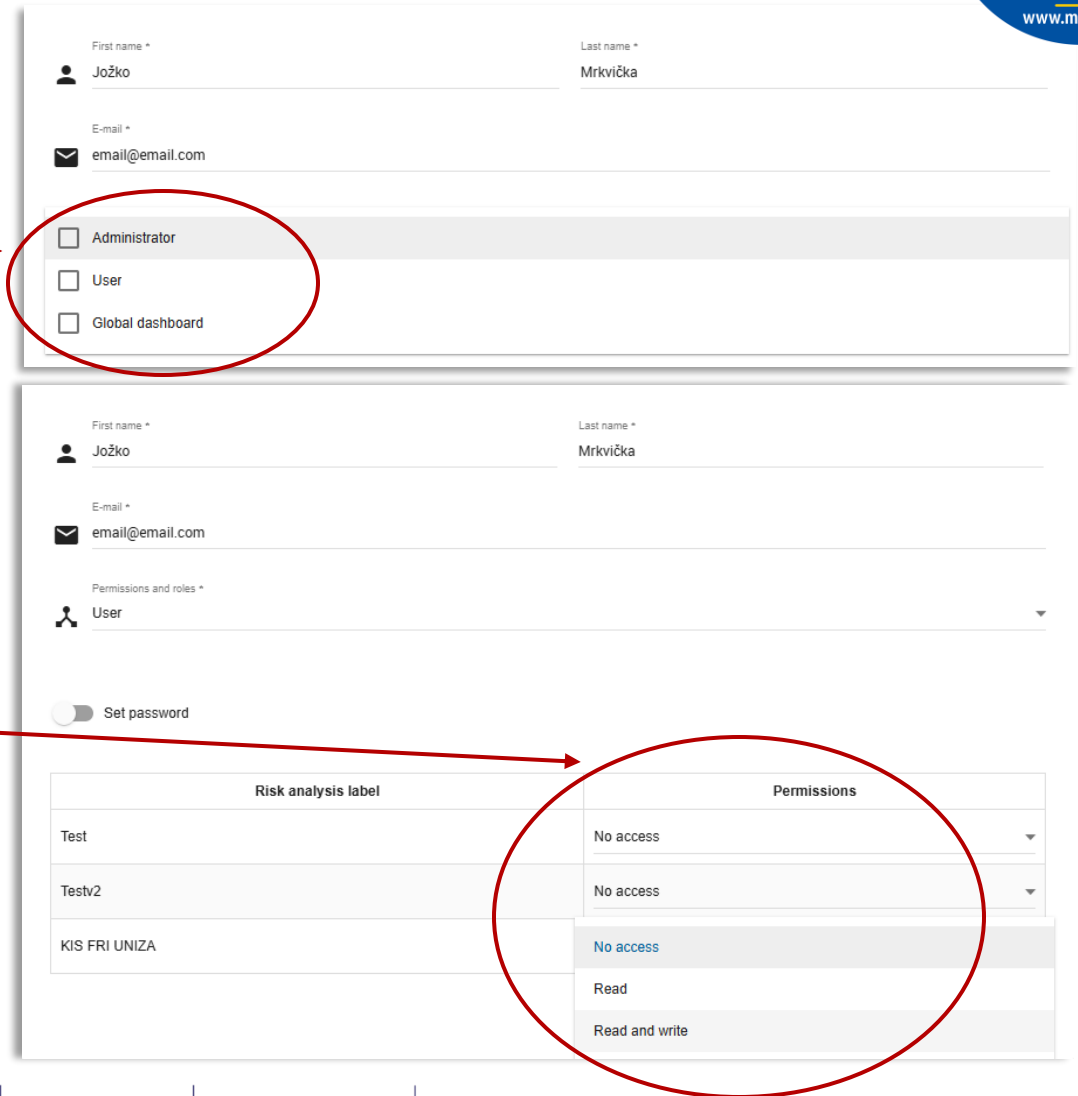

## Fázy uvedené v analýze rizík podľa Monarc, sú v súlade s normou ISO/IEC 27005:



# Prihlásenie do MONARC

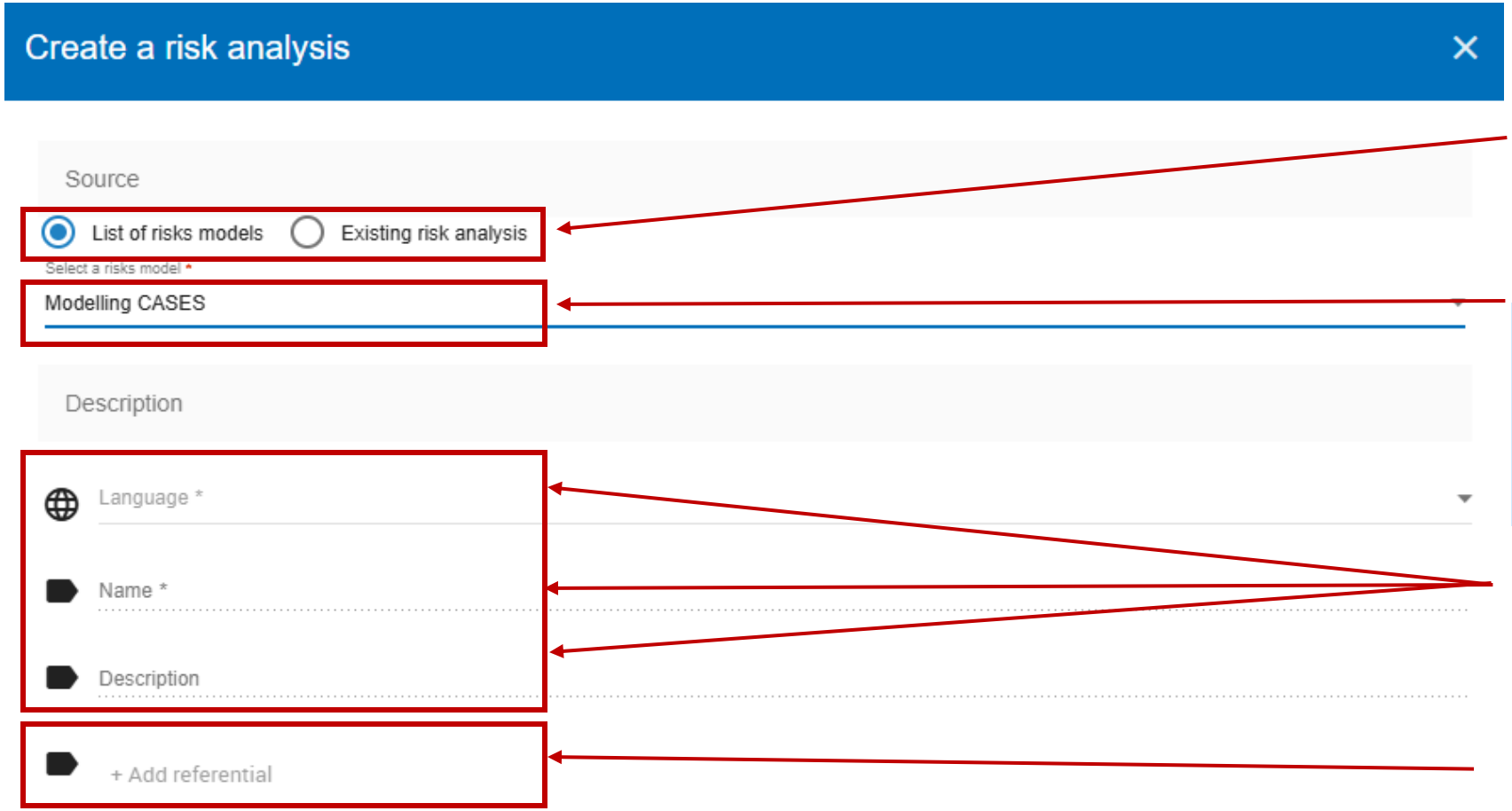
Po inštalácii - MONARC používa predvolené prihlasovacie údaje (`admin@admin.localhost` / `admin`)

- **Dostupné roly v systéme:**
  - **Administrator** – správa systému a používateľov
  - **User** – prístup k vlastným analýzam podľa pridelených práv
  - **Global dashboard** – vidí a spravuje globálne štatistiky všetkých analýz
- **Úrovne oprávnení pre analýzy:**
  - **No access** – bez prístupu
  - **Read** – iba na čítanie
  - **Read and write** – plný prístup k analýze



MONARC

# Nastavenie pri vytváraní projektu




Výber zo šablóny (viď nižšie) alebo vytvorím kópiu z existujúcej analýzy (reuse)

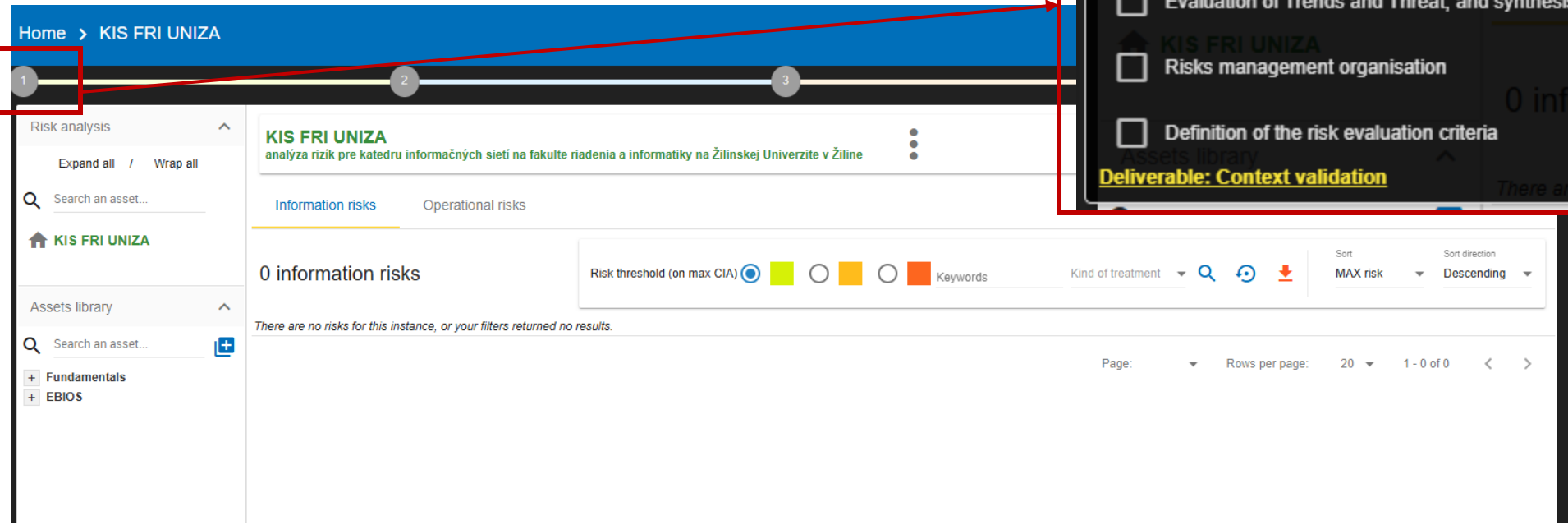
2 možnosti výberu modelu: blank project / modelling CASES (preddefinované rizikové scenáre)

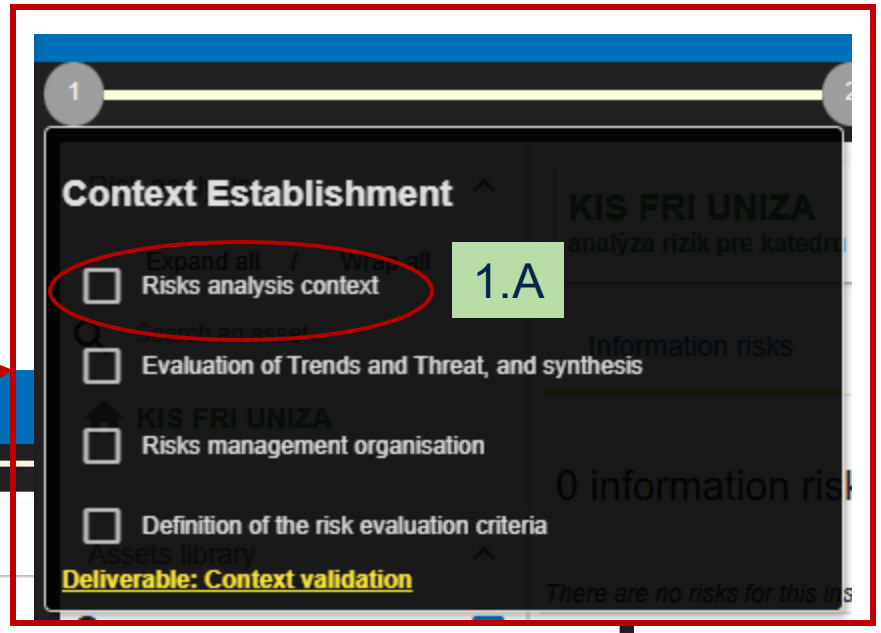
Vyberieme preferovaný jazyk, určíme názov a popis analýzy

Výber bezpečnostného štandardu, ktorý chceme pridať / podľa akej normy alebo rámca chceme hodnotiť a riadiť riziká

# 1. Stanovenie kontextu – 1.A Risk analysis context

- V tejto časti popisujeme **cieľ analýzy,**
- v textovom okne odpovieme **na 4 témy:**
  - všeobecné úvahy (general consideration),
  - prístup riadenia rizík (risk management approach),
  - základné kritériá (basic criteria),
  - rozsah a hranice (scope and boundaries).

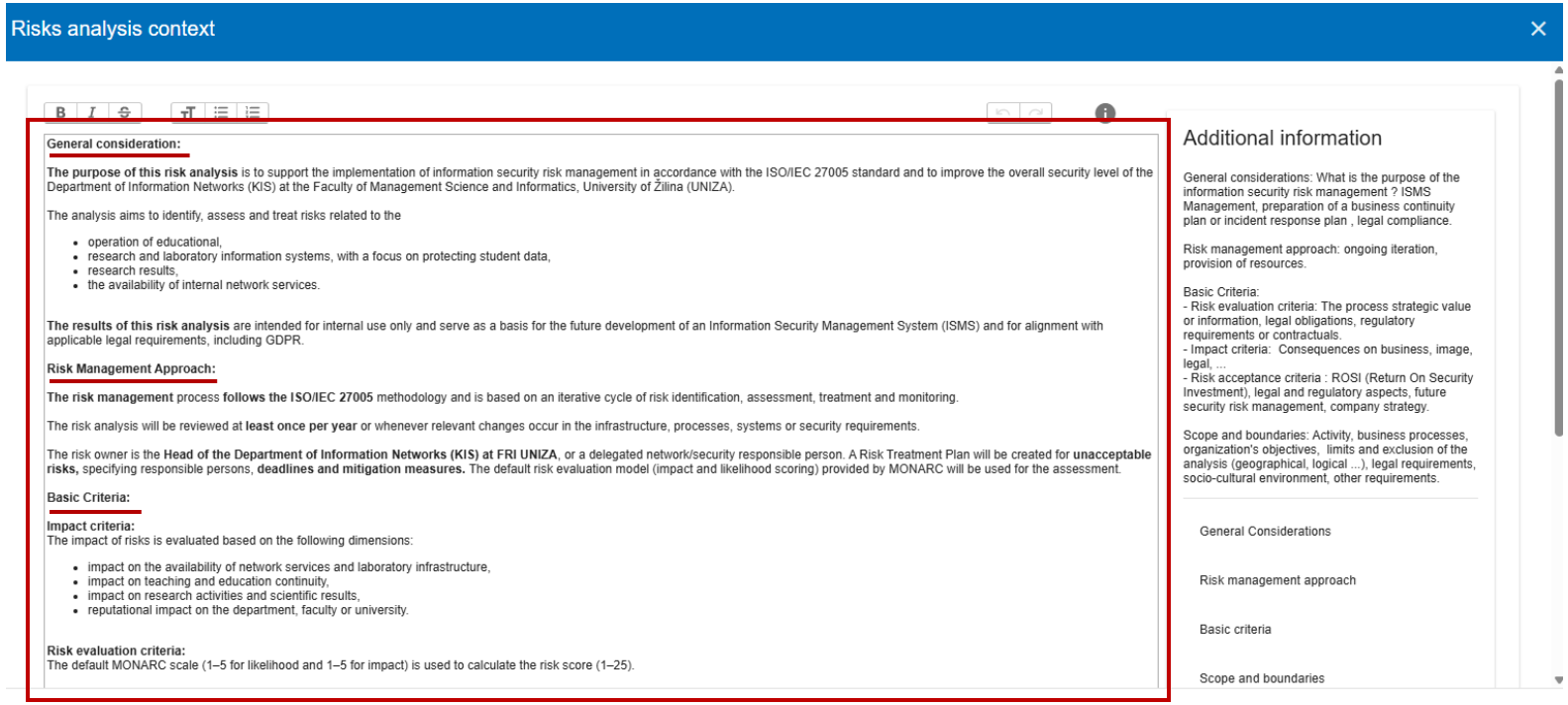


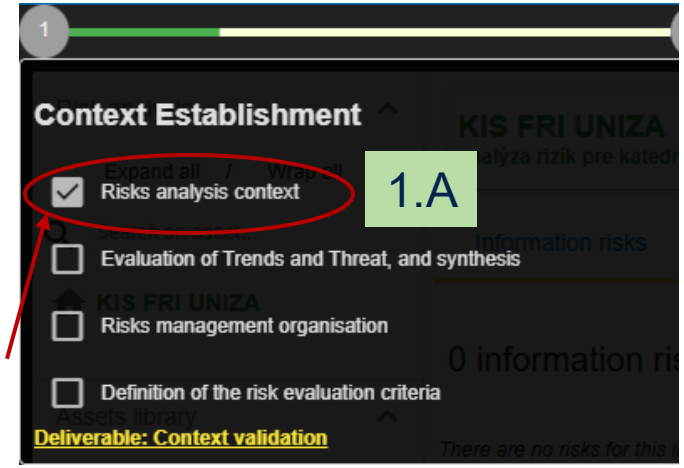



# 1. Stanovenie kontextu – 1.A Risk analysis context

Hlavné časti, ktoré sa v tomto kroku vypĺňajú:

- **všeobecné východiská** (general considerations) – účel analýzy (ISO 27005, ochrana dát, podpora ISMS…)
- **prístup k riadeniu rizík** (risk management approach) – ako sa bude riziko riadiť, prehodnocovať, kto je risk owner
- **základné kritériá hodnotenia** (basic criteria) – kritériá hodnotenia dopadu, matica rizík, akceptačné hranice
- **Rozsah a hranice analýzy** (scope and boundaries) – čo (nie) je zahrnuté v analýze (systémy katedry, nie osobné PC…)



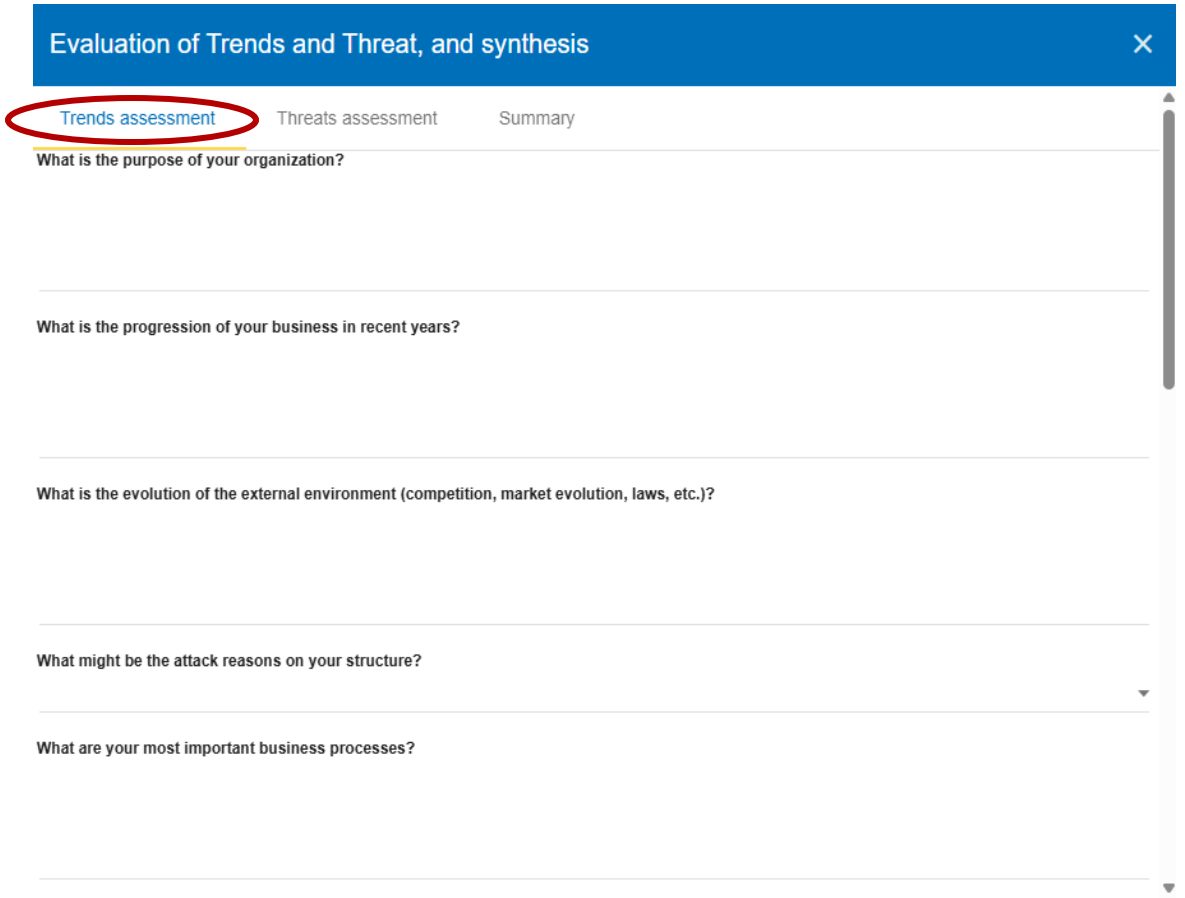
# 1. Stanovenie kontextu – 1.B Evaluation of Trends and Threat, and synthesis

Ďalšia fáza sa rozdeľuje do 3 sekcií:

| Sekcia | Popis |
|---|---|
| I. Trends assessment | Odpovedanie na otázky o charaktere organizácie, jej vývoji, hodnotách, externom prostredí a rizikových faktoroch. |
| II. Threats assessment | Posúdenie vopred definovaných typov hrozieb, ktoré nie sú viazané na konkrétne aktívum (30 hrozieb v MONARC), dopad na CIA (Confidentiality, Integrity, Availability) + určenie trendu hrozby. |
| III. Summary | Zhrnutie najvýznamnejších trendov, rizikových faktorov a najpravdepodobnejších hrozieb. Slúži ako vstup do ďalšej fázy – modelovania rizík. |

Sekcia I.

**Trends assessment:**



# 1. Stanovenie kontextu – 1.B Evaluation of Trends and Threat, and synthesis

| Názov hrozby | Popis hrozby | c | i | a |
|---|---|---|---|---|
| Chyba pri používaní | Chyba používateľa pri obsluhe, zadávaní údajov alebo nesprávnom používaní hardvéru alebo softvéru. | 1 | 1 | 1 |
| Porucha softvéru | Chyba návrhu, inštalácie alebo prevádzky softvéru spôsobujúca nesprávne fungovanie. | 0 | 1 | 1 |
| Porucha alebo zlyhanie zariadenia | Logická alebo fyzická udalosť spôsobujúca poruchu hardvéru. | 0 | 1 | 1 |
| Zneužitie identity (falšovanie práv) | Osoba sa vydáva za inú osobu s cieľom získať prístupové práva alebo spáchať podvod. | 1 | 1 | 1 |

# 1. Stanovenie kontextu – 1.B Evaluation of Trends and Threat, and synthesis

| Názov hrozby | Popis hrozby | c | i | a |
|---|---|---|---|---|
| Odpočúvanie komunikácie | Neoprávnené sledovanie alebo zachytávanie komunikácie. | 1 | 0 | 0 |
| Vzdialené špehovanie | Sledovanie činností používateľa na diaľku (napr. zadávanie hesla). | 0 | 0 | 0 |
| Manipulácia s hardvérom | Neoprávnená inštalácia zariadenia na zachytávanie alebo ničenie dát. | 1 | 1 | 0 |
| Neoprávnené kopírovanie softvéru | Nelegálne kopírovanie alebo používanie pirátskeho softvéru. | 1 | 0 | 1 |

MONARC

# 1. Stanovenie kontextu – 1.B Evaluation of Trends and Threat, and synthesis

| Názov hrozby | Popis hrozby | c | i | a |
|---|---|---|---|---|
| Poškodenie dát | Zásah do prenosu alebo obsahu dát (zničenie, zmena, vloženie). | 0 | 1 | 0 |
| Popretie vykonania činnosti | Osoba alebo subjekt popiera vykonanie činnosti | 0 | 1 | 0 |
| Nezákonné spracovanie údajov | Osoba vykonáva spracúvanie informácií, ktoré je zakázané zákonom alebo iným právnym predpisom. | 1 | 1 | 0 |
| Zachytenie elektromagnetických signálov | Rušivé signály z elektromagnetického zdroja vyžarované zariadením, ktoré sa šíria buď vedením po napájacích kábloch alebo uzemňovacích vodičoch, alebo vyžarovaním do voľného priestoru. | 1 | 0 | 0 |

# 1. Stanovenie kontextu – 1.B Evaluation of Trends and Threat, and synthesis

| Názov hrozby | Popis hrozby | c | i | a |
|---|---|---|---|---|
| Krádež alebo zničenie médií či zariadení | Odcudzenie alebo fyzické poškodenie zariadení alebo nosičov dát. | 1 | 0 | 1 |
| Získanie vyradených médií | Získanie dát z vyradených alebo recyklovaných nosičov. | 1 | 0 | 0 |
| Infekcia škodlivým softvérom | Nechcený softvér poškodzujúci systémy. | 1 | 1 | 1 |
| Zahltenie informačného systému | Úmyselné alebo neúmyselné preťaženie zdrojov systému. | 0 | 0 | 1 |

MONARC

# 1. Stanovenie kontextu – 1.B Evaluation of Trends and Threat, and synthesis

| Názov hrozby | Popis hrozby | c | i | a |
|---|---|---|---|---|
| Zneužitie oprávnení | Osoba s rozšírenými právami zneužije svoje oprávnenia. | 1 | 1 | 1 |
| Údaje z nedôveryhodných zdrojov | Použitie nesprávnych dát alebo zariadení z externých zdrojov. | 0 | 1 | 0 |
| Neoprávnené zverejnenie informácií | Úmyselné alebo nedbanlivé sprístupnenie informácií. | 1 | 0 | 0 |
| Nemožnosť údržby systému | Nedostatok odborných znalostí bráni údržbe a modernizácii. | 0 | 0 | 1 |

MONARC

# 1. Stanovenie kontextu – 1.B Evaluation of Trends and Threat, and synthesis

| Názov hrozby | Popis hrozby | c | i | a |
|---|---|---|---|---|
| Nedostupnosť personálu | Nedostatok kvalifikovaných alebo oprávnených pracovníkov. | 0 | 0 | 1 |
| Zničenie zariadení alebo médií | Udalosť vedúca k fyzickému zničeniu. | 0 | 0 | 1 |
| Požiar | Udalosti umožňujúce vznik požiaru. | 0 | 1 | 1 |
| Poškodenie vodou | Udalosti spôsobujúce škody vodou. | 0 | 1 | 1 |

# 1. Stanovenie kontextu – 1.B Evaluation of Trends and Threat, and synthesis

| Názov hrozby | Popis hrozby | c | i | a |
|---|---|---|---|---|
| Veľká havária | Udalosť vedúca k fyzickému zničeniu objektov. | 0 | 0 | 1 |
| Znečistenie | Prítomnosť prachu, plynov alebo toxických látok. | 0 | 1 | 1 |
| Zlyhanie telekomunikačných služieb | Výpadok alebo nesprávna kapacita telekomunikačných služieb. | 0 | 0 | 1 |
| Výpadok dodávky elektriny | Zlyhanie alebo nedostatočné napájanie zariadení. | 0 | 0 | 1 |

# 1. Stanovenie kontextu – 1.B Evaluation of Trends and Threat, and synthesis

| Názov hrozby | Popis hrozby | c | i | a |
|---|---|---|---|---|
| Zlyhanie klimatizácie | Nedostatočné chladenie alebo ventilácia. | 0 | 0 | 1 |
| Environmentálna katastrofa | Rozsiahla udalosť poškodzujúca priestory. | 0 | 1 | 1 |



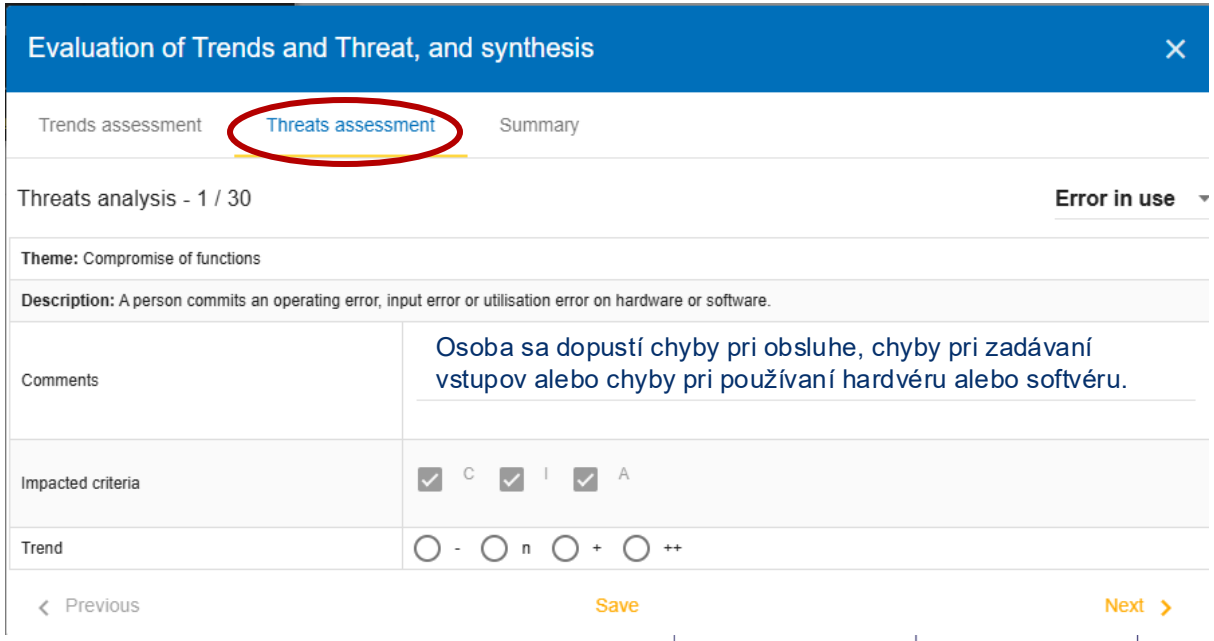
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# 1. Stanovenie kontextu – 1.B Evaluation of Trends and Threat, and synthesis

Sekcia II: **Threats assessment**

Posúdenie hrozieb je z pohľadu dopadu (na CIA) a aj na základe položky „Trend“ ktorá je definovaná takto:

- „-“ => Nikdy sa hrozba neobjavila, veľmi malá pravdepodobnosť
- „n“ => Neutrálny názor (No clear position, no opinion)
- „+“ => Hrozba sa už objavila
- „++“ => Hrozba sa objavila viac krát

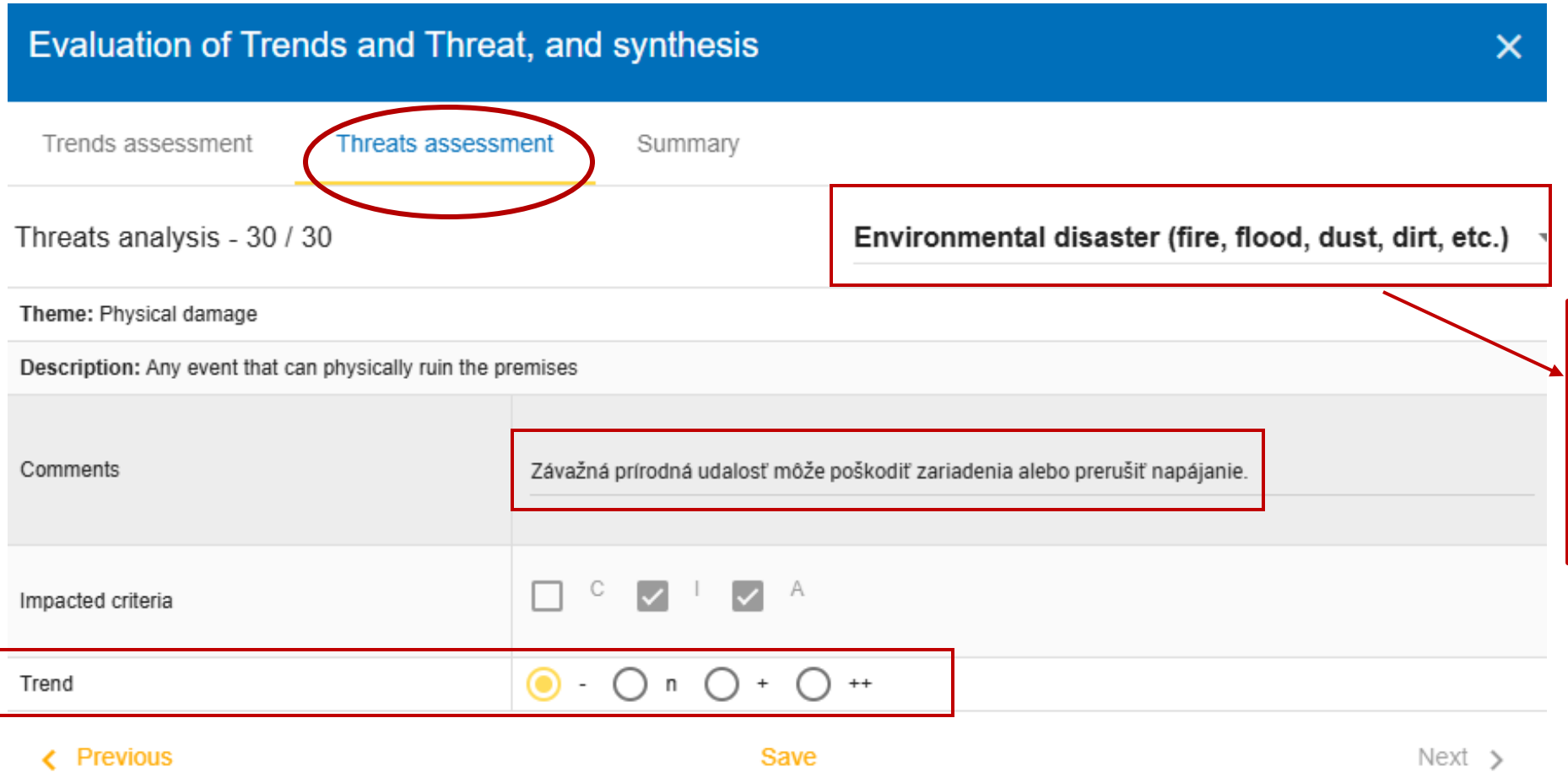



| Hrozba | Trend | Odôvodnenie |
|---|---|---|
| Malware infection | + | už sa vyskytlo (infikované zariadenie) |
| Loss of power supply | n | vyskytuje sa občas, ale nie pravidelne |
| Eavesdropping (odpočúvanie) | – | doteraz neevidované prípady |
| Error in use (ľudská chyba) | ++ | opakujúca sa chyba používateľov pri práci so systémami |
| Equipment failure | + | už sa vyskytla porucha zariadenia |

MONARC

# 1. Stanovenie kontextu – 1.B Evaluation of Trends and Threat, and synthesis

Sekcia II: **Threats assessment**

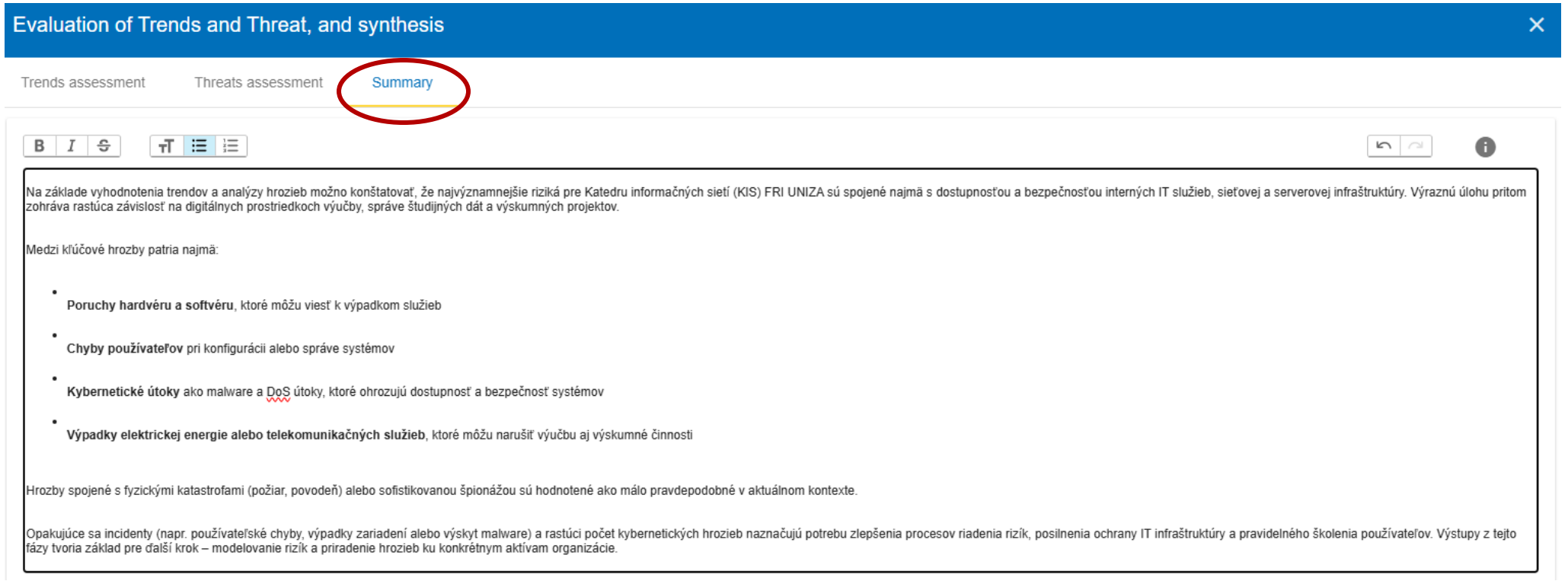



Výber z 30 hrozieb – postupne ku každému treba zadefinovať trend a komentár

# 1. Stanovenie kontextu – 1.B Evaluation of Trends and Threat, and synthesis

Sekcia III: **Summary**:

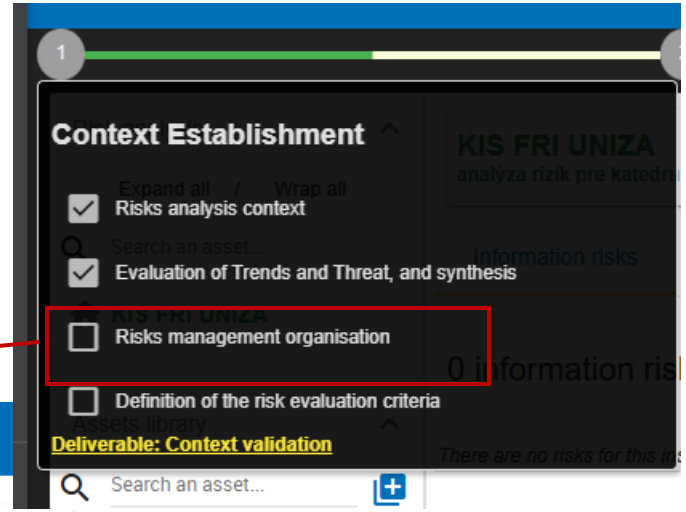
- Čo sme zistili pri hodnotení trendov a hrozieb
- Ktoré hrozby sú najkritickejšie
- Aké dopady to má na organizáciu



# 1. Stanovenie kontextu – 1.C Risk management organisation

Ďalšia fáza slúži na nastavenie organizačného rámca riadenia rizík, vypĺňame:

- **kto** je zodpovedný za riadenie rizík,
- **definujeme roly** (schvaľovanie, implementácia, hlásenie incidentov),
- **popis, ako** prebieha eskalácia a aktualizácia rizík




Risks management organisation

**Riadenie rizík na Katedre informačných sietí je súčasťou interného procesu zabezpečenia informačnej bezpečnosti a podpory prevádzky IT služieb.** Za koordináciu analýzy rizík a aktualizáciu hodnotenia je zodpovedný vedúci katedry alebo ním poverená osoba (správca IT infraštruktúry). Hodnotenie rizík sa vykonáva minimálne raz ročne alebo po výskyte významného incidentu.

**Roly a zodpovednosti:**

- **Rizikový manažér / vedúci katedry** – schvaľuje analýzu rizík a rozhoduje o prijatí alebo ošetrení rizík.
- **Správca IT infraštruktúry** – identifikuje technické riziká, navrhuje opatrenia a vykonáva implementáciu.
- **Výskumní a pedagogickí pracovníci** – hlásia incidenty, spolupracujú pri identifikácii rizík procesov a dát.
- **Študenti** – povinnosť dodržiavať stanovené bezpečnostné pravidlá (napr. používanie účtov, ochrana dát).

**Riešenie konfliktov a eskalácia:**
Ak vznikne rozpor v hodnotení rizík alebo zodpovednostiach, eskalácia prebieha na úroveň vedenia fakulty (prodekan pre IT alebo bezpečnosť). V prípade závažných incidentov sa postupuje podľa interného incident response plánu UNIZA.

Additional information

Ongoing risk assessment organization

Roles and responsibilities

Conflict resolution and escalation paths

# 1. Stanovenie kontextu – 1.C Risk management organisation

- V tomto kroku sa upravujú **všetky hodnotiace stupnice**, ktoré sa používajú pri analýze rizík
- Úpravy sú možné **iba na začiatku analýzy** – po hodnotení aktív ich už nie je možné meniť
- Je možné meniť **popisy bodových hodnôt** aj **pridávať nové úrovne dopadu**

| Skratka/Pojem | Význam |
|---|---|
| **CIA** | Confidentiality – Integrity – Availability (tradičná triáda informačnej bezpečnosti) |
| **ROLPF** | Regulatory / Organizational / Legal / Privacy / Financial dopady |
| **Threats** | Hrozby – hodnotia sa podľa pravdepodobnosti výskytu |
| **Impact** | Dopad – ako veľmi to poškodí aktívum alebo proces |

Rozdiel medzi **informačnými rizikami** a **operačnými rizikami:**

| Typ rizika | Čo znamená | Ako sa hodnotí | Príklady |
|---|---|---|---|
| **Informačné riziká** | Riziká, ktoré ohrozujú konkrétne aktívum (napr. server, dáta, proces, aplikáciu) | Kombináciou CIA triády + ROLPF a vždy sa berie najhoršia (max) hodnota | únik dát, strata integrity databázy, nedostupnosť servera |
| **Operačné riziká** | Riziká, ktoré sa týkajú fungovania organizácie ako celku, nie jedného aktíva | Hodnotia sa len podľa ROLPF atribútov a tiež cez max() | výpadok dodávateľa, zlé nastavené procesy, dlhá odozva systému |

**CIA = bezpečnostné vlastnosti informácií**
**ROLFP = dopady na fungovanie organizácie**

# 1. Stanovenie kontextu – 1.C Risk management organisation

Rozdiel medzi **informačnými rizikami** a **operačnými rizikami v metodike MONARC**

INFORMAČNÉ RIZIKÁ

- Viazané na konkrétne aktívum (server, databáza, aplikácia)
- Cieľ - ochrana informácii
- Hodnotenie dopadu:
  - **CIA (Confidentiality, Integrity, Availability)**
  - doplnkovo **ROLFP**
- Berie sa najhorší maximálny dopad

OPERAČNÉ RIZIKÁ

- týkajú sa **fungovania organizácie ako celku**
- nie sú viazané na jedno konkrétne aktívum
- hodnotenie dopadu:
  - **ROLFP (Regulatory, Organizational, Legal, Financial, Privacy/Personal)**
- CIA nie je primárnym hodnotiacim rámcom

Dlhá odozva systému - prečo kategória operačné riziko ?
Dlhá odozva znamená, že systém **reaguje, je dostupný,** ale reaguje pomaly.
Dostupnosť (Availability) preto nie je narušená, len je znížená kvalita.
Dopad sa prejavuje najmä v **procesoch (ľudia čakajú), financie (strata času, peňazí),** ..
Preto toto riziko berieme ako operačný dopad na procesy.

# 1. Stanovenie kontextu – 1.D Definition of the risk evaluation criteria

| Skratka | Význam |
|---|---|
| **CIA** | Confidentiality – Integrity – Availability (tradičná triáda informačnej bezpečnosti) |
| **ROLPF** | Regulatory / Organizational / Legal / Privacy / Financial dopady |
| **Threats** | Hrozby – hodnotia sa podľa pravdepodobnosti výskytu |
| **Impact** | Dopad – ako veľmi to poškodí aktívum alebo proces |

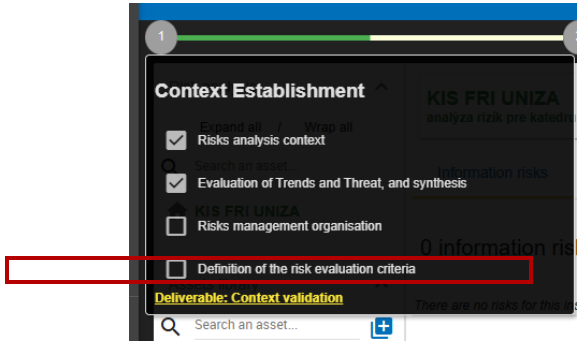
| Typ rizika | Čo znamená | Ako sa hodnotí | Príklady |
|---|---|---|---|
| **Informačné riziká** | Riziká, ktoré ohrozujú konkrétne aktívum (napr. server, dáta, proces, aplikáciu) | Kombináciou CIA triády + ROLPF a vždy sa berie najhoršia (max) hodnota | únik dát, strata integrity databázy, nedostupnosť servera |
| **Operačné riziká** | Riziká, ktoré sa týkajú fungovania organizácie ako celku, nie jedného aktíva | Hodnotia sa len podľa ROLPF atribútov a tiež cez max() | výpadok dodávateľa, zlé nastavené procesy, dlhá odozva systému |

V MONARC sa pri výpočte nepoužíva priemer ani súčet:

- Vezme sa **najhorší (najvyšší) hodnotený dopad**, lebo:
  - ak je riziko kritické z jedného pohľadu (napr. výpadok = A4 [Availability=4]), tak nezáleží, že z iného je nízke (C1, I2) [Confidentiality = 1; Integrity = 1]. Najhorší dopad = ten, ktorý treba riešiť. - Ak je niečo kritické z jedného pohľadu, je to kritické ako celok – preto funkcia MAX.

**Threats** = hodnotené podľa pravdepodobnosti
→ teda: **S akou pravdepodobnosťou môže nastať tento typ útoku alebo incidentu?**

**Impact** = úroveň dopadu na aktívum (CIA + ROLPF)
→ teda: **Ak sa to stane, aký veľký problém to spôsobí?**



# 1. Stanovenie kontextu – 1.D Definition of the risk evaluation criteria

Monarc ponúka preddefinované stupnice (Scale), ktoré je možné si upraviť podľa potreby. Stupnice pre:

Definition 1: **Impact scale** (Stupnica dopadov rizík)
Definition 2: **Likelihood scale** (Stupnica pravdepodobnosti hrozieb)
Definition 3: **Vulnerabilities scale** (Stupnica závažnosti zraniteľností)
Definition 4: **Acceptance thresholds of information risks** (Prahové hodnoty pre prijatie informačných rizík)
Definition 5: **Acceptance thresholds of operational risks** (Prahové hodnoty pre prijatie operačných rizík)

Definition 1:
Preddefinovaná stupnica pre dopady informačných rizík (dopady na CIA, ROLFP je na ďalšom snímku)

Ku stupnici dopadov (0–4) je možné pridávať alebo odstraňovať úrovne a upravovať popisy jednotlivých hodnôt pre hodnotenie dopadov jednotlivých rizík.

Definition 1

ROLFP

Impacts scale: [ 0 - 5 ]

Show hidden impacts

| | Confidentiality | Integrity | Availability | Reputation |
|---|---|---|---|---|
| 0 | Nonexistent impact.<br>The confidentiality criterion is not important. | Nonexistent impact.<br>The integrity criterion is not important. | Nonexistent impact.<br>The availability criterion is not important. | No consequences |
| 1 | Weak impact, insignificant.<br>Information leaks are negative to the organization's interests.<br>Examples:<br>- Internal information leaks which shouldn't be outside the company.<br>- Memorandum<br>- Internal phone directory | Weak impact, insignificant. Corruption easy to rectify without any consequences.<br>Example:<br>- Internal mail or letter. | Weak impact, insignificant.<br>Unavailability which is inconvenient, but not really harmful for the stakeholders. | Sporadic media critics |
| 2 | Average impact, acceptable.<br>Information leaks harm organization's interests.<br>Examples:<br>- Moderately sensitive information leaks which are only for a group of people.<br>- Internal networking scheme.<br>- Documentation or source code which is non-critical. | Average impact, acceptable.<br>Corruption which brings an inconvenience to the stakeholders. Recovery is easy.<br>Example:<br>- Informational web site. | Average impact, acceptable.<br>Unavailability which brings an inconvenience to the stakeholders.<br>Example:<br>- Maximum time periods consider as unbearable are not reached. | Temporary degradatio<br>or staff reputation.<br>Occasional media criti |
| 3 | Strong impact, hardly bearable.<br>Information leaks seriously harm organization's interest. Example:<br>- Confidential information leaks.<br>- Bank secrecy<br>- Sensitive personal data<br>- Security incident | Strong impact, hardly bearable.<br>Corruption which brings a considerable inconvenience to the stakeholders.<br>Example:<br>- Confusion between stakeholders. | Strong impact, hardly bearable.<br>Unavailability which bring a considerable inconvinience to the stakeholders.<br>Example:<br>- Maximum time periods consider as unbearable are reached. | Strong degradation of<br>staff reputation.<br>Serious and repeated |
| 4 | Really strong impact, unbearable.<br>Information leaks almost deadly harm organization's interest.<br>Example:<br>- Secret or really sensitive information leaks.<br>- Classified information by the law (the EU, NATO, national…) | Really strong impact, unbearable.<br>Corruption which can't be recovered or bring a permanent downtime. | Really strong impact, unbearable.<br>Unavailability which asks some drastic efforts to recover, or even final.<br>Example:<br>- Important maximums time periods consider as unbearable. | Death of someone.<br>Definitive degradation<br>staff reputation.<br>Internationnal media c |
| 5 | | | | |

# 1. Stanovenie kontextu – 1.D Definition of the risk evaluation criteria

Definition 1:

Preddefinovaná stupnica pre hodnotenie dopadov (Impact) **operačných rizík**
(5 stupňov: 0 - 4), **informačné** majú CIA + ROLFP, pričom stupnica pre ROLFP je tam rovnaká

Definition 1

Information risks | Operational risks | Compliance

**Impacts scale:** 5 **Levels**

Show hidden impacts

| | Reputation | Operational | Legal | Financial | Personal |
|---|---|---|---|---|---|
| 0 | No consequences | No consequences | No consequences | No consequences | No consequences |
| 1 | Sporadic media critics | Minor incidents without any impact on customers. | Small probability of any sentences, or really slight one.<br>Any prosecution should be futile. | Brings some marginal fees (more or less 1% of the sales revenue). | Some inconvenience which will be topped without difficulty (Time waste, procedure reiteration, irritation, etc.). |
| 2 | Temporary degradation of the company or staff reputation.<br>Occasional media critics | Isolated incidents with a manageable impact on customers. | Possible sentence for the company. | Brings some non-marginal fees (more or less 5% of the sales revenue). | Significative inconvenience which could be topped with some difficulties (Additional costs, denial of access to commercial delivery, fear, misunderstanding, stress, slight physical ailments, etc.). |
| 3 | Strong degradation of the company or staff reputation.<br>Serious and repeated media critics. | Interruption of a whole department. | Sentence for the company. | Brings some heavy fees which can affect the company (more or less 10% of the sales revenue). | Significative consequences which could be topped, but with some serious difficulties (funds embezzlement, bank ban, deterioration of goods, job loss.). |
| 4 | Death of someone.<br>Definitive degradation of the company or staff reputation.<br>Internationnal media coverage. | Complete stop of all services | Heavy sentence for the company. | Brings some deadly fees almost insurmontable (more or less 20% of the sales revenue). | Significative consequences almost irremediable, which can't be topped (financial distress, important financial debts, working impossibility, long periods psychological and physiological affection, death, etc.). |

# 1. Stanovenie kontextu – 1.D Definition of the risk evaluation criteria

| Úroveň | Reputačný dopad | Prevádzkový dopad | Právny dopad | Finančný dopad | Osobný dopad |
|---|---|---|---|---|---|
| 0 | Žiadne následky | Žiadne následky | Žiadne následky | Žiadne následky | Žiadne následky |
| 1 | Ojedinelá kritika v médiách | Menšie incidenty bez dopadu na zákazníkov | Veľmi mierne sankcie. Prípadné stíhanie by bolo neúspešné. | Vznikajú len marginálne náklady (cca 1 % z obratu). | Menšie nepríjemnosti, ktoré je možné bez problémov zvládnuť (strata času, opakovanie postupov, podráždenie a pod.). |
| 2 | Dočasné zhoršenie reputácie organizácie alebo zamestnancov. Príležitostná mediálna kritika. | Izolované incidenty so zvládnuteľným dopadom na zákazníkov. | Možnosť uloženia sankcie organizácii. | Vznikajú nezanedbateľné náklady (cca 5 % z obratu). | Významné nepríjemnosti, ktoré možno zvládnuť s určitými ťažkosťami (dodatočné náklady, obmedzenie prístupu k službám, strach, stres, mierne zdravotné problémy a pod.). |
| 3 | Výrazné zhoršenie reputácie organizácie alebo zamestnancov. Závažná a opakovaná mediálna kritika. | Prerušenie činnosti celého oddelenia. | Uloženie sankcie organizácii. | Vznikajú vysoké náklady, ktoré môžu významne ovplyvniť organizáciu (cca 10 % z obratu). | Závažné následky, ktoré je možné prekonať len s veľkými ťažkosťami (sprenevera finančných prostriedkov, zákaz bankových služieb, poškodenie majetku, strata zamestnania a pod.). |
| 4 | Trvalé poškodenie reputácie organizácie alebo zamestnancov. Medzinárodná mediálna pozornosť. Úmrtie osoby. | Úplné zastavenie všetkých služieb. | Vysoké (prísne) sankcie uložené organizácii. | Takmer neprekonateľné finančné straty (cca 20 % z obratu). | Takmer nenapraviteľné následky, ktoré nie je možné prekonať (vážne finančné problémy, vysoké dlhy, neschopnosť pracovať, dlhodobé psychické alebo fyzické následky, smrť a pod.). |

# 1. Stanovenie kontextu – 1.D Definition of the risk evaluation criteria

Definition 1:

Možnosť rozšírenia množiny dopadov (Impact) rizík, okrem predvolených CIA a ROLFP

| Financial | Personal | New column name |
|---|---|---|
| ences | No consequences | |
| : marginal fees (more or less 1% of the ue). | Some inconvenience which will be topped without difficulty (Time waste, procedure reiteration, irritation, etc.). | |
| : non-marginal fees (more or less 5% of venue). | Significative inconvenience which could be topped with some difficulties (Additional costs, denial of access to commercial delivery, fear, misunderstanding, stress, slight physical ailments, etc.). | |
| : heavy fees which can affect the ore or less 10% of the sales revenue). | Significative consequences which could be topped, but with some serious difficulties (funds embezzlement, bank ban, deterioration of goods, job loss.). | |
| : deadly fees almost insurmontable (more of the sales revenue). | Significative consequences almost irremediable, which can't be topped (financial distress, important financial debts, working impossibility, long periods psychological and physiological affection, death, etc.). | |

Je možné pridať si vlastný nový atribút (okrem CIA a ROLFP) pre vyjadrenie a následné hodnotenie dopadov rizík a určiť si preň vlastnú stupnicu a popísať jednotlivé stupne

# 1. Stanovenie kontextu – 1.D Definition of the risk evaluation criteria

Preddefinovaná stupnica (Scale) pre:

Definition 1: **Impact scale** (Stupnica dopadov rizík)

Definition 2: **Likelihood scale** (Stupnica pravdepodobnosti hrozieb)

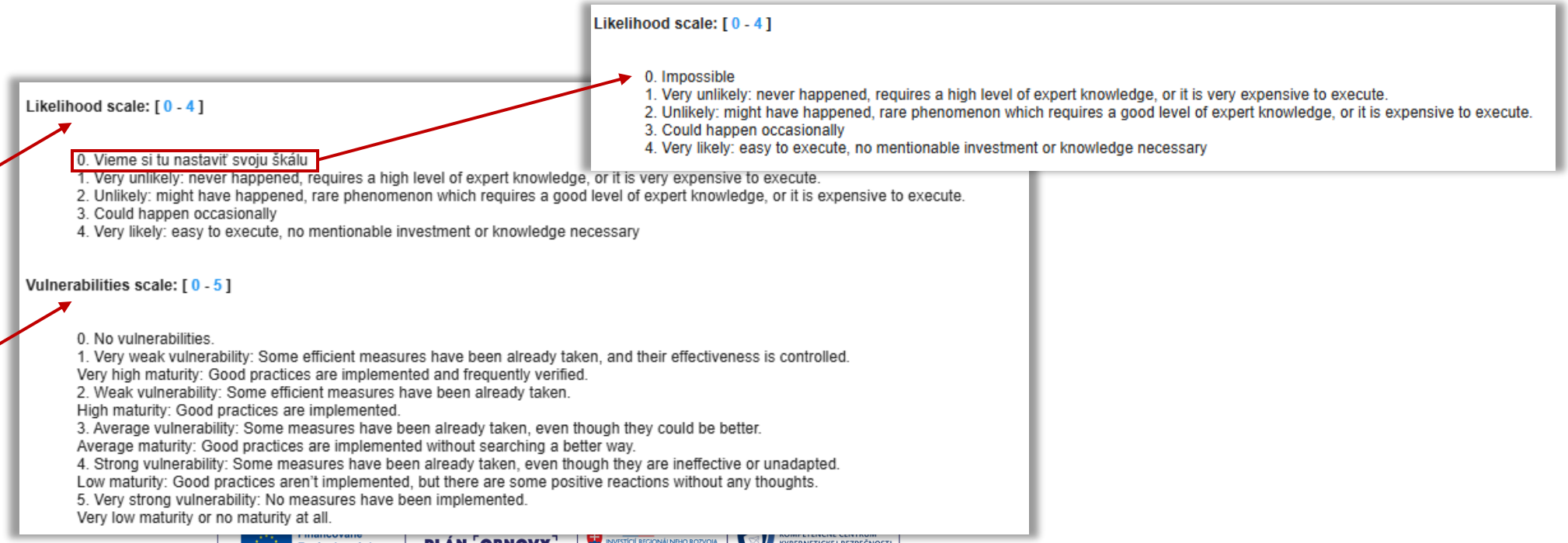
Definition 3: **Vulnerabilities scale** (Stupnica závažnosti zraniteľností)

Definition 4: **Acceptance thresholds of information risks** (Prahové hodnoty pre prijatie informačných rizík)

Definition 5: **Acceptance thresholds of operational risks** (Prahové hodnoty pre prijatie operačných rizík)

Definition 2

Definition 3



# 1. Stanovenie kontextu – 1.D Definition of the risk evaluation criteria

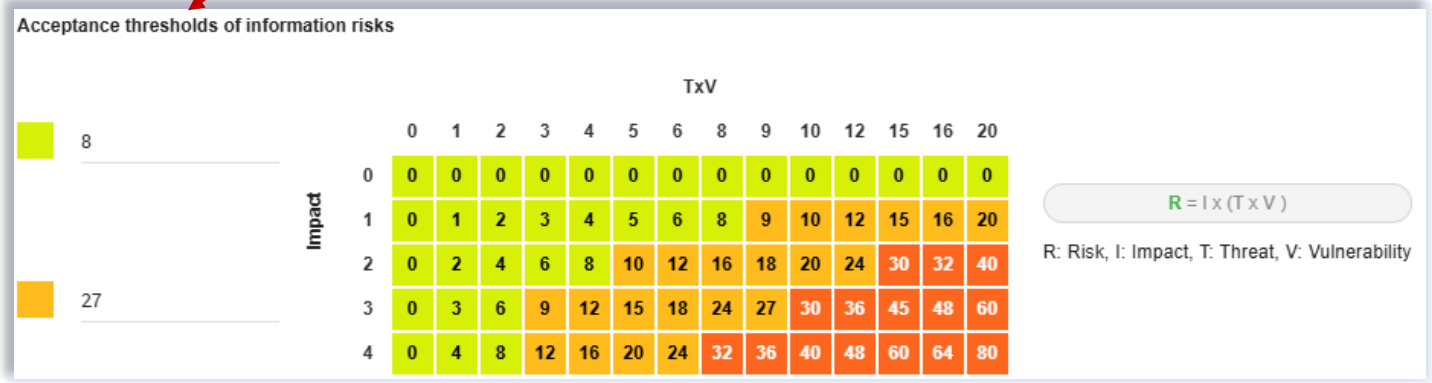
Definition 4: **Acceptance thresholds of information risks** (Prahové hodnoty pre prijatie informačných rizík)

- **Horizontálna os (T × V)** = kombinácia Threat (pravdepodobnosť hrozby) × Vulnerability (závažnosť zraniteľnosti aktíva)
- **Vertikálna os (Impact)** = dopad na aktívum (CIA + ROLPF)
  - Každá bunka v matici = **vypočítaná hodnota rizika R = Impact × (Threat × Vulnerability)**
- Čísla naľavo:
  - **8** → **max. skóre pre zelenú zónu (akceptované riziko)**
  - **27** → **hranica medzi oranžovou a červenou** (nad 27 je riziko neprijateľné)

**0 – 8 = prijateľné**
**9 – 27 = tolerované, ale je potrebné sledovanie**
**- 80 = neprijateľné, nutné riešenie**

| Farba | Význam | Stav |
|---|---|---|
| zelená | prijateľné riziko | nie je potrebná akcia |
| oranžová | treda sledovať / podmienečne akceptovať | môže vyžadovať opatrenie |
| červená | neprijateľné riziko | musí byť riešené (mitigácia / kontrola) |

Definition 4



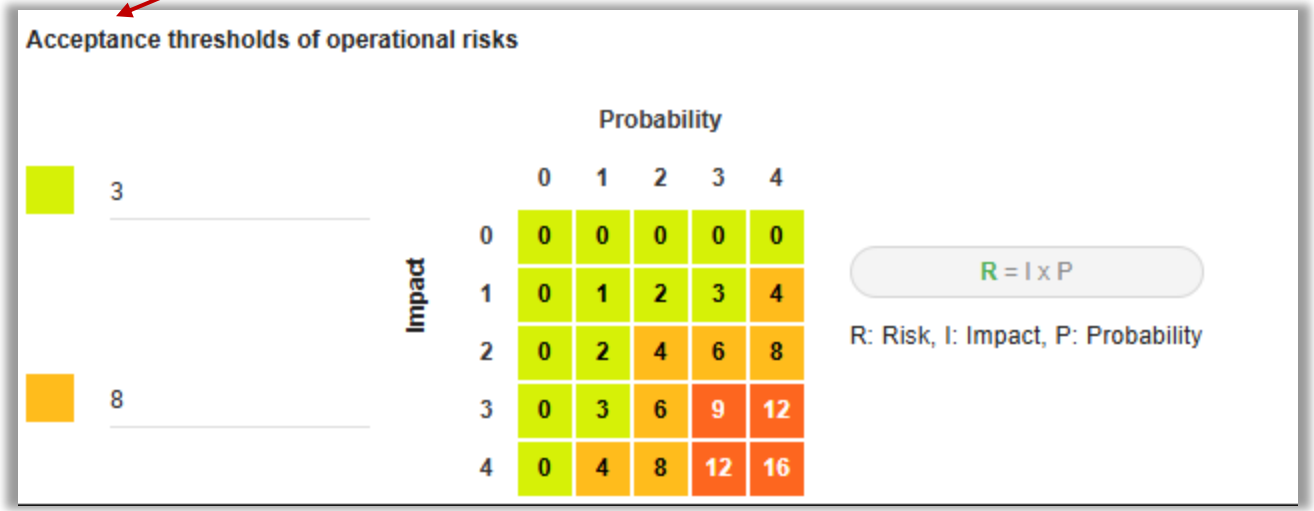
# 1. Stanovenie kontextu – 1.D Definition of the risk evaluation criteria

Definition 5: **Acceptance thresholds of operational risks** (Prahové hodnoty pre prijatie operačných rizík)

- **Horizontálna os (Probability)** = stupnica pravdepodobnosti výskytu operačného rizika
- **Vertikálna os (Impact)** = dopad rizika na prevádzku organizácie
- Hranice tolerancie rizika

**0 – 3 = prijateľné**
**4 – 8 = tolerované**
**9 – 16 = neprijateľné**

Definition 5




*V tejto fáze sa len nastavujú stupnice a prahové hodnoty.*
*Konkrétne hodnoty pravdepodobnosti a dopadu sa aplikujú až vo fáze 3.A.*

| Informačné riziká | Operačné riziká |
|---|---|
| R = Impact × (Threat × Vulnerability) | R = Impact × Probability |
| hodnotí sa cez CIA + ROLPF | hodnotí sa len dopad na prevádzku |
| komplexnejší model | zjednodušený model |

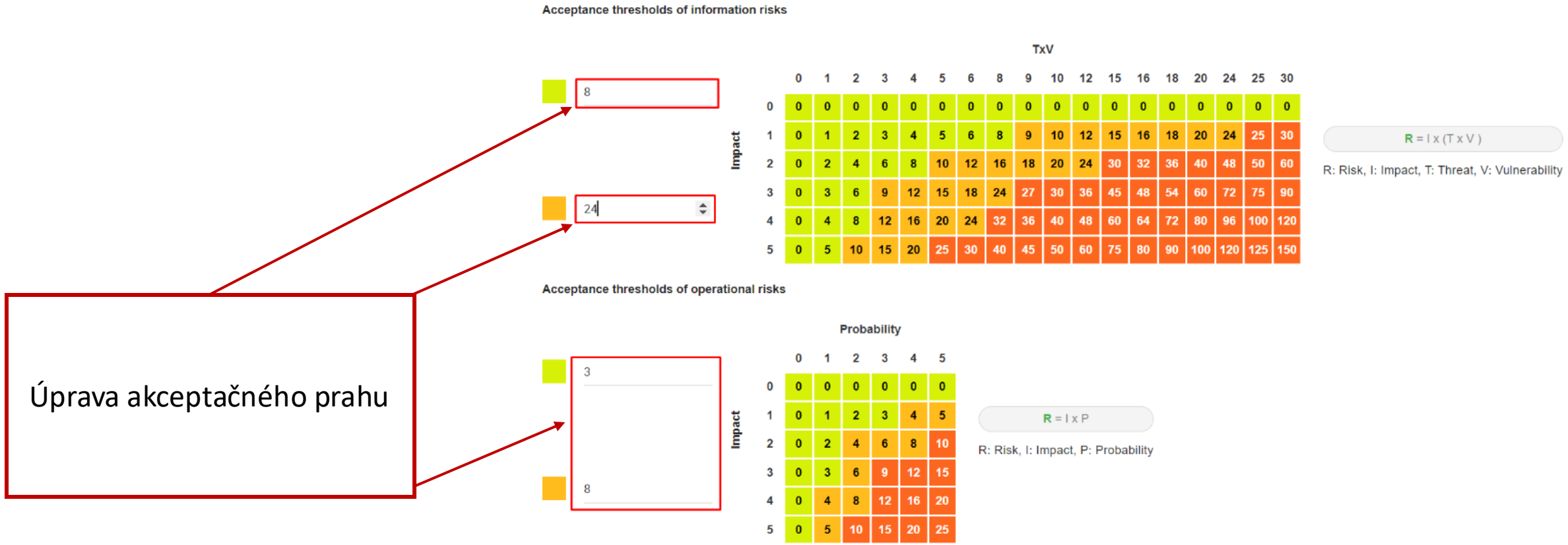
| Farba | Význam | Čo to znamená |
|---|---|---|
| zelená | prijateľné riziko | netreba opatrenia |
| oranžová | tolerované riziko | sledovať, zvážiť úpravy |
| červená | neprijateľné riziko | musí byť riešené |

MONARC

# 1. Stanovenie kontextu – 1.D Definition of the risk evaluation criteria

Definition 4: **Acceptance thresholds of information risks** (Treshold hodnoty pre prijatie informačných rizík)

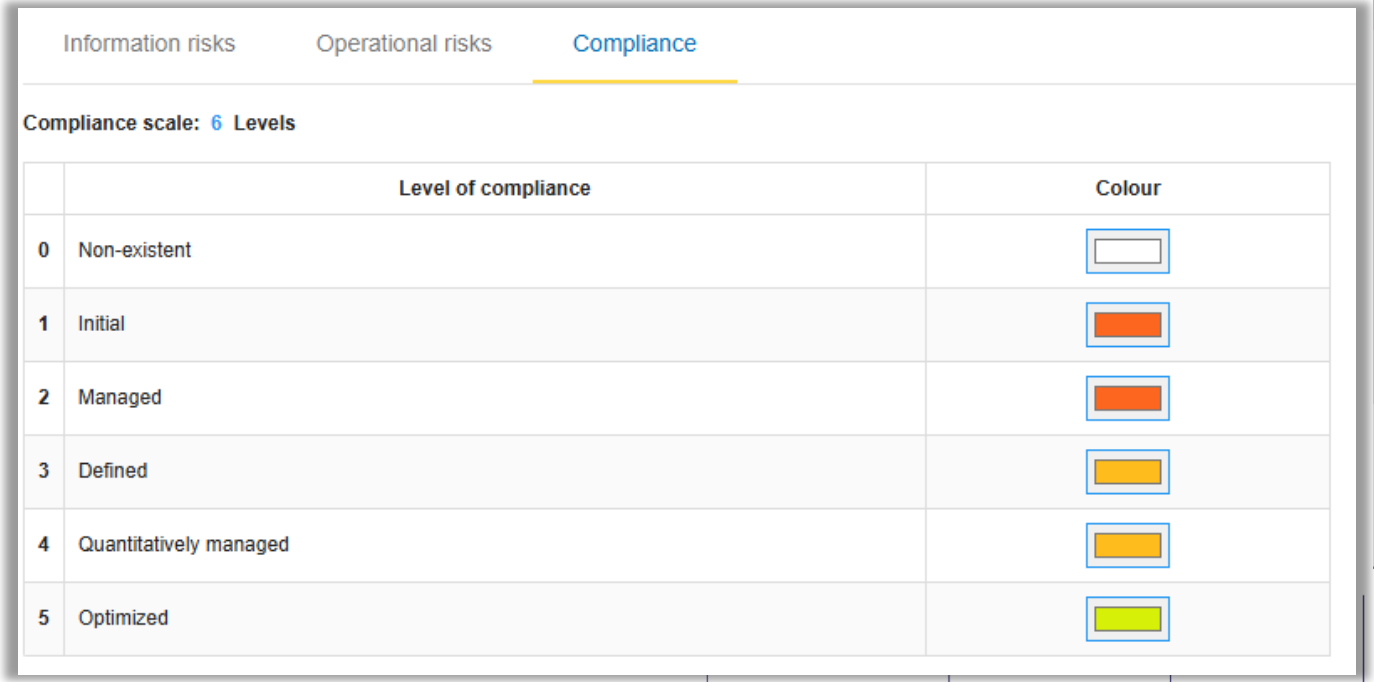
Definition 5: **Acceptance thresholds of operational risks** (Treshold hodnoty pre prijatie operačných rizík)




Úprava akceptačného prahu

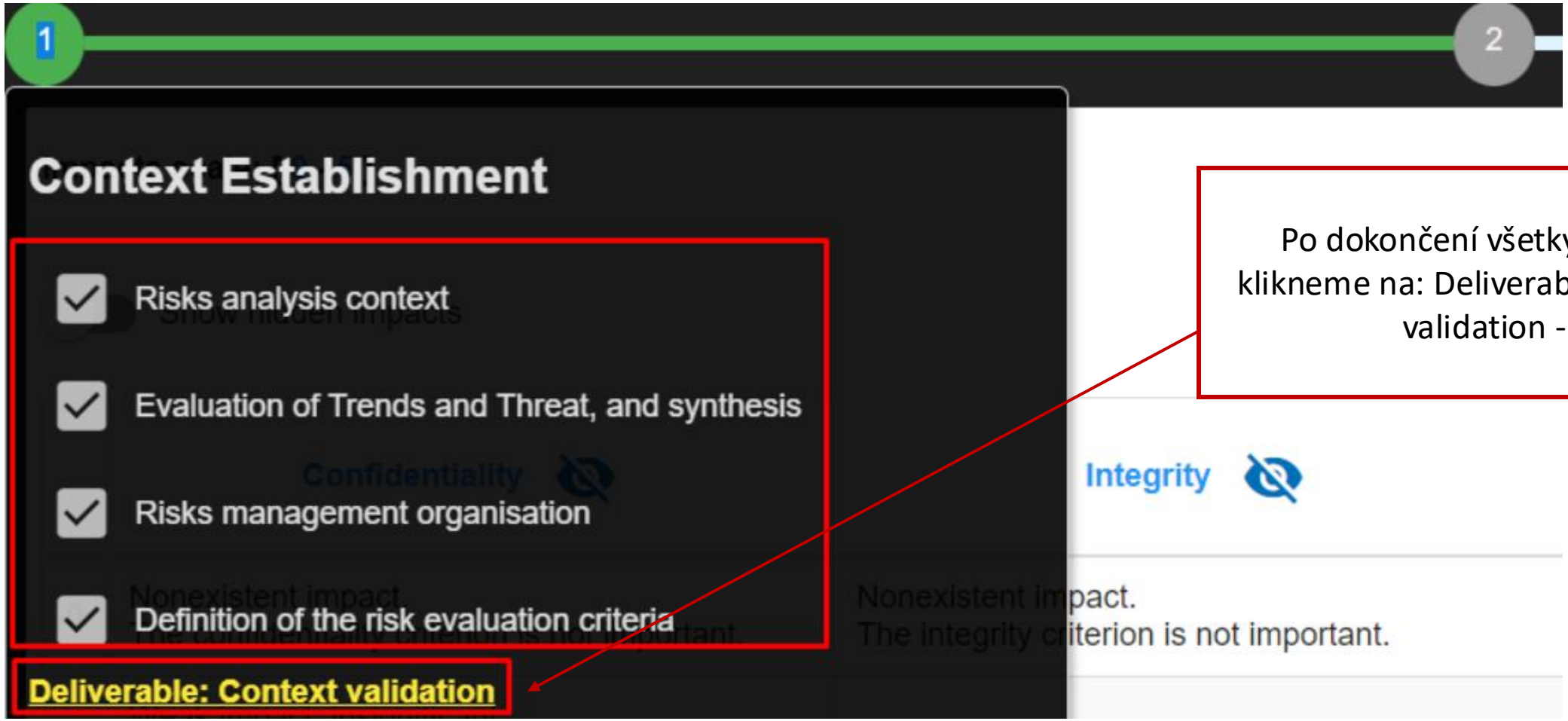
# 1. Stanovenie kontextu – 1.D Definition of the risk evaluation criteria

- úroveň zhody (súlad s normami, politikami, reguláciami).
- Používa sa na hodnotenie toho, **ako dobre je organizácia riadená z pohľadu kybernetickej a informačnej bezpečnosti**.
- Používa sa pri hodnotení **zvyškového rizika (residual risk)**
  - Pomáha určiť, ako kvalitne je organizácia schopná riadiť dané riziko
  - MONARC automaticky priraďuje farby k úrovniam zhody – ako pri semafórovej metóde




| Úroveň | Názov | Význam |
|---|---|---|
| 0 – Non-existent | Neexistujúca | Neexistujú žiadne pravidlá, procesy ani evidencia. |
| 1 – Initial | Počiatočná | Existujú ad-hoc postupy, ale nie sú formalizované. |
| 2 – Managed | Riadená | Procesy existujú, ale nie sú štandardizované ani monitorované. |
| 3 – Defined | Definovaná | Procesy sú zdokumentované a jednotné v celej organizácii. |
| 4 – Quantitatively managed | Kvantitatívne riadená | Zhoda sa meria pomocou metrík, prebieha monitorovanie a reporting. |
| 5 – Optimized | Optimalizovaná | Neustále zlepšovanie, automatizácia, riadené podľa best practice. |

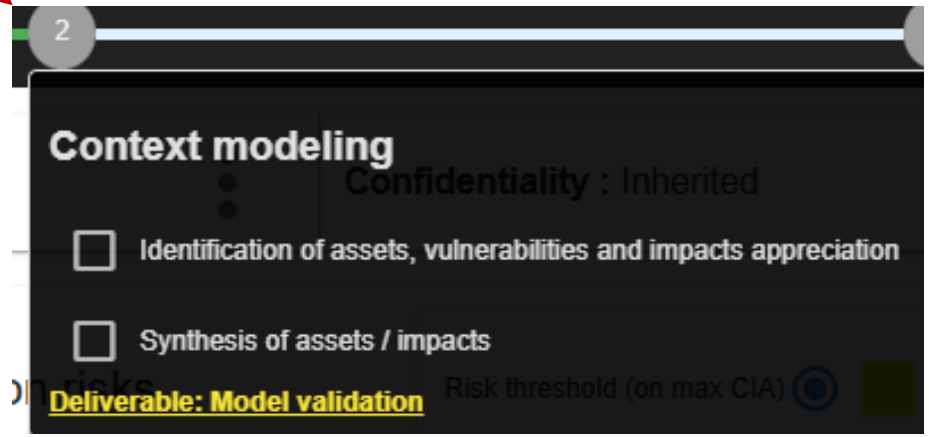
# 1. Stanovenie kontextu – Koniec prvej časti (1.A, 1.B, 1.C, 1.D)




Po dokončení všetkých častí klikneme na: Deliverable: Context validation -

# 2. Modelovanie kontextu – 2.A Identification of assets, vulnerabilities and impacts appreciation

1. **stanovenie kontextu:**
   - určenie cieľa analýzy a definovanie prostredia
   - stanovenie kritérií a metodiky hodnotenia rizík
2. **modelovanie kontextu:**
   - identifikácia aktív a ich rozdelenie podľa priority
   - vytvorenie rizikového modelu pomocou databázy MONARC
3. **hodnotenie a ošetrenie rizík:**
   - posúdenie hrozieb, zraniteľností a úrovne rizík
   - návrh opatrení na zníženie významných rizík
4. **implementácia a monitorovanie:**
   - realizácia odporúčaných bezpečnostných opatrení
   - priebežné sledovanie zmien a aktualizácia analýzy






Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# 2. Modelovanie kontextu – 2.A Identification of assets, vulnerabilities and impacts appreciation

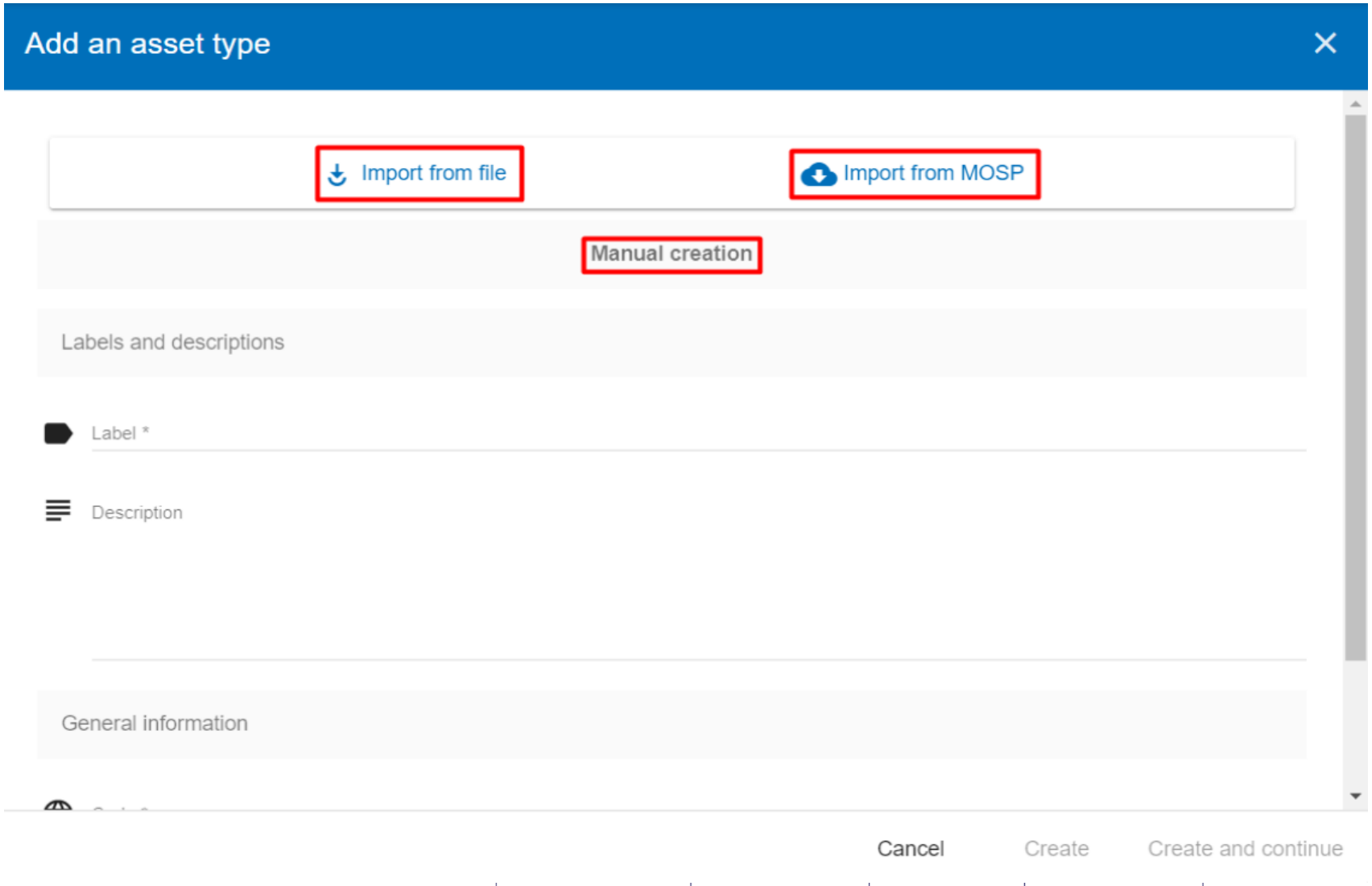
- Preddefinovaný zoznam **aktív**

Asset types | Search... | Show active only

| Status | Label | Code | Type | Description | Actions |
|---|---|---|---|---|---|
| ✓ | Backup | OV_BACKUP | Secondary | Backup | |
| ✓ | Building, office or premises | OV_BATI | Secondary | Building, office or premises | |
| ✓ | Business application | LOG_APP | Secondary | Custom business application or standard | |
| ✓ | Company directory | SYS_ANU | Secondary | Company directory | |
| ✓ | Container | CONT | Primary | Asset container | |
| ✓ | Decision maker | PER_DEC | Secondary | Decision maker | |
| ✓ | Desktop computer | OV_POSTE_FIXE | Secondary | Desktop computer | |
| ✓ | Developer | PER_DEV | Secondary | Developer | |
| ✓ | Electronic medium | MAT_SUPP | Secondary | CD ROM, back-up cartridge, removable hard disc, memory key, tape. | |

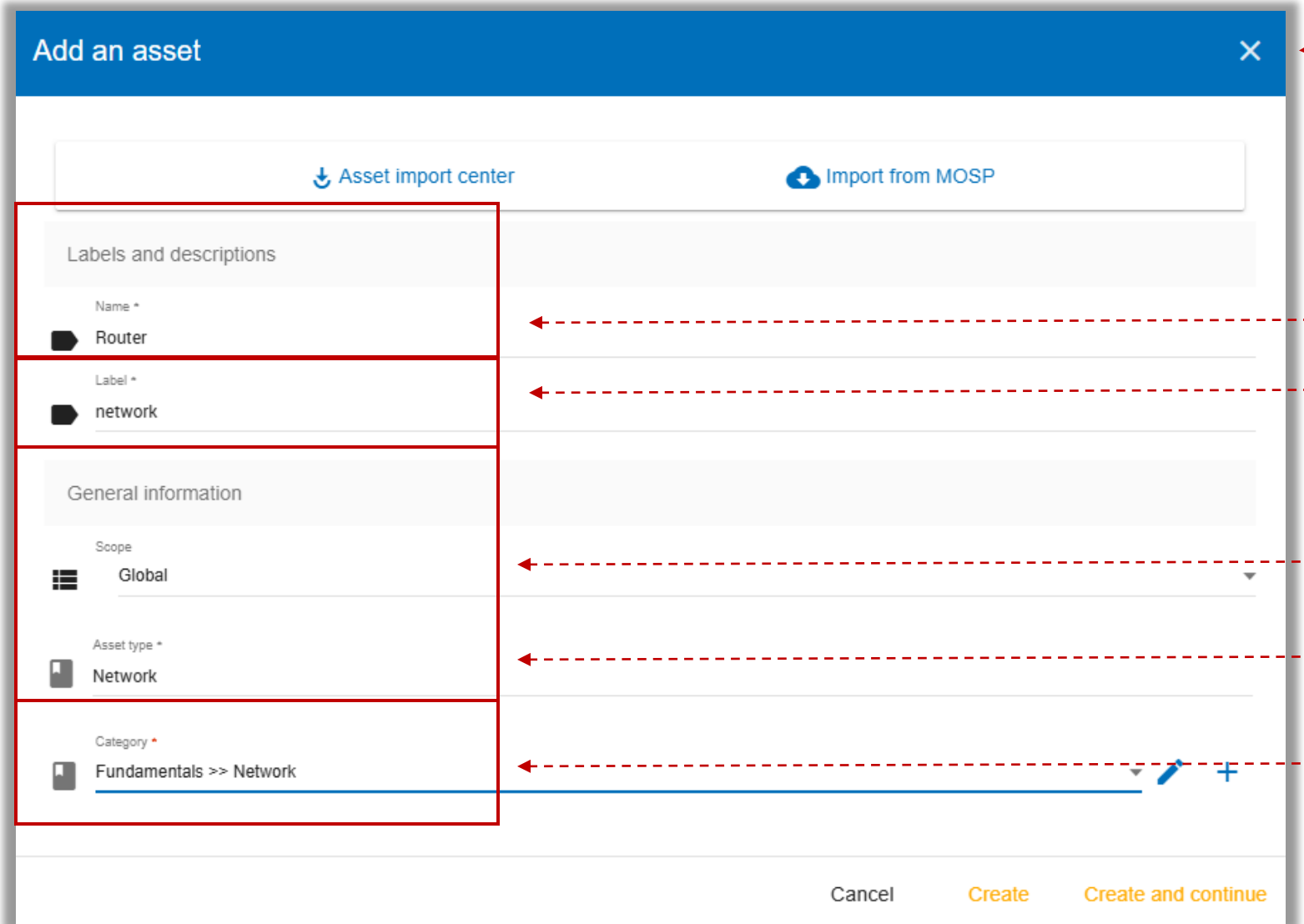
# 2. Modelovanie kontextu – 2.A Identification of assets, vulnerabilities and impacts appreciation

- 3 spôsoby pre vloženie aktív do analýzy



# 2. Modelovanie kontextu – 2.A Identification of assets, vulnerabilities and impacts appreciation

- 3 spôsoby pre vloženie aktív do analýzy:




1. spôsob:
**Manuálne vkladanie aktíva**

Jedinečný názov aktíva

Dodatočný popis, ktorý sa zobrazí keď podržíme kurzor nad daným prvkom

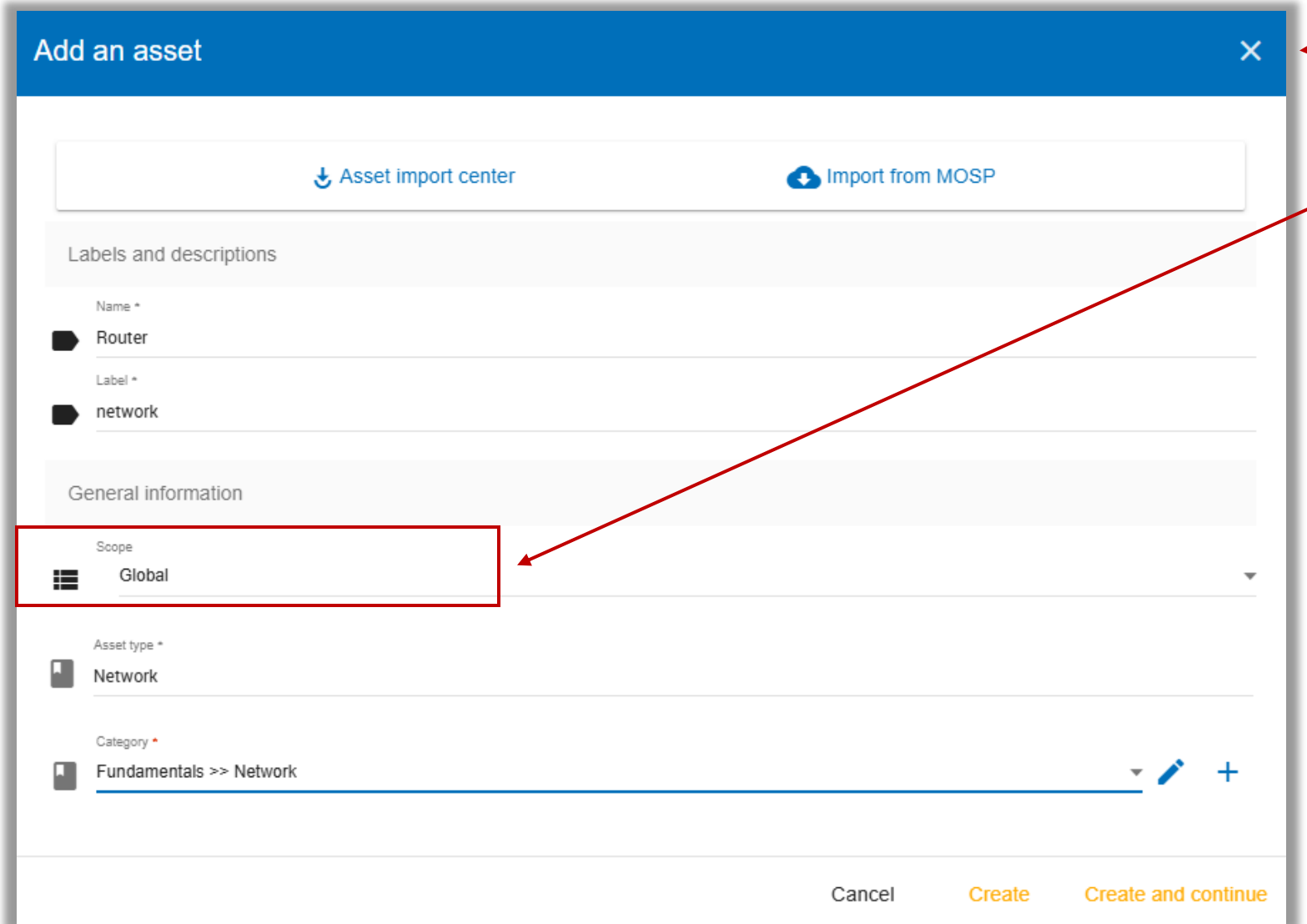
Ako často hodnotíme riziko

Typ určuje o aký druh aktíva ide

Umiestnenie v knižnici, kde bude aktívum vytvorené

# 2. Modelovanie kontextu – 2.A Identification of assets, vulnerabilities and impacts appreciation

- 3 spôsoby pre vloženie aktív do analýzy:




1. spôsob:
**Manuálne vkladanie aktíva**

LOCAL vs GLOBAL

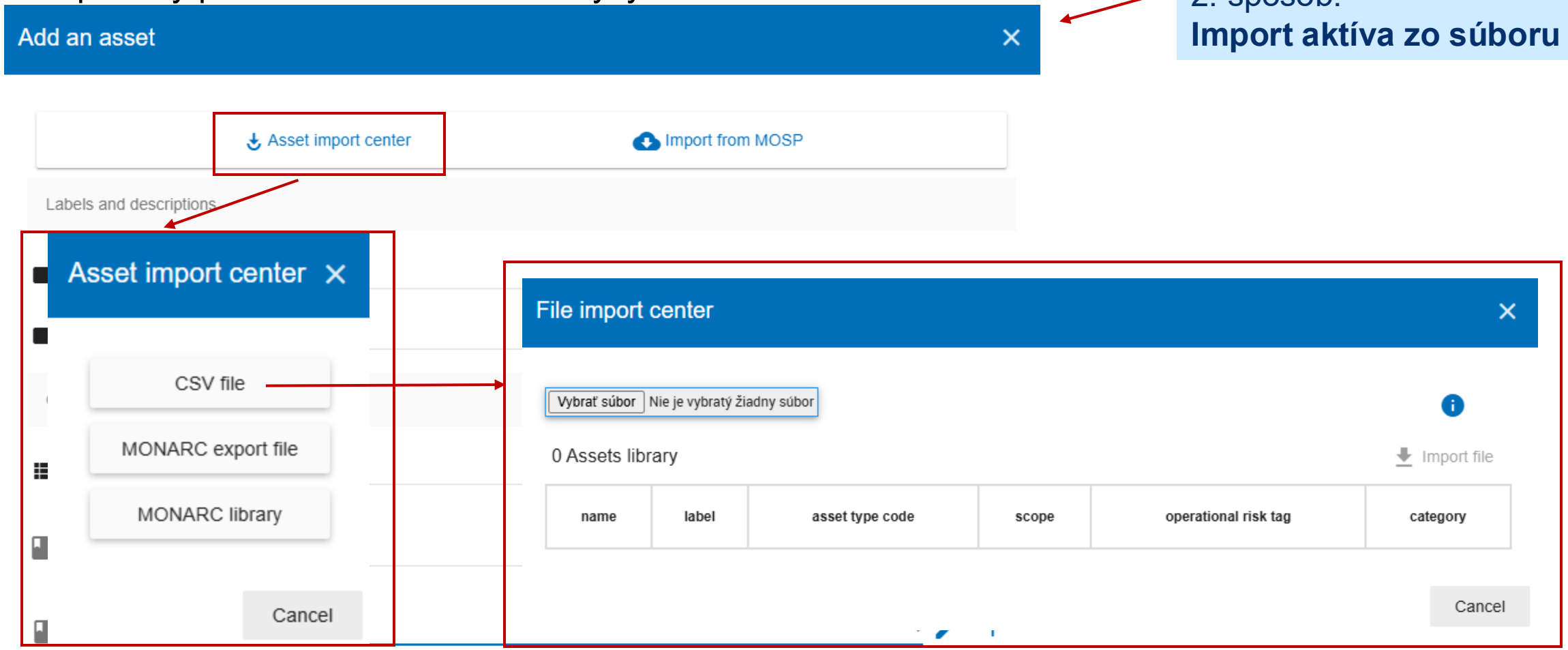
Local: lokálne aktívum existuje iba v konkrétnej analýze rizík, v ktorej bolo vytvorené

Global: globálne aktívum je spoločné aktívum, ktoré môže byť znova použité vo viacerých analýzach alebo projektoch vytvorených v rámci 1 inštancie MONARC

# 2. Modelovanie kontextu – 2.A Identification of assets, vulnerabilities and impacts appreciation

- 3 spôsoby pre vloženie aktív do analýzy:

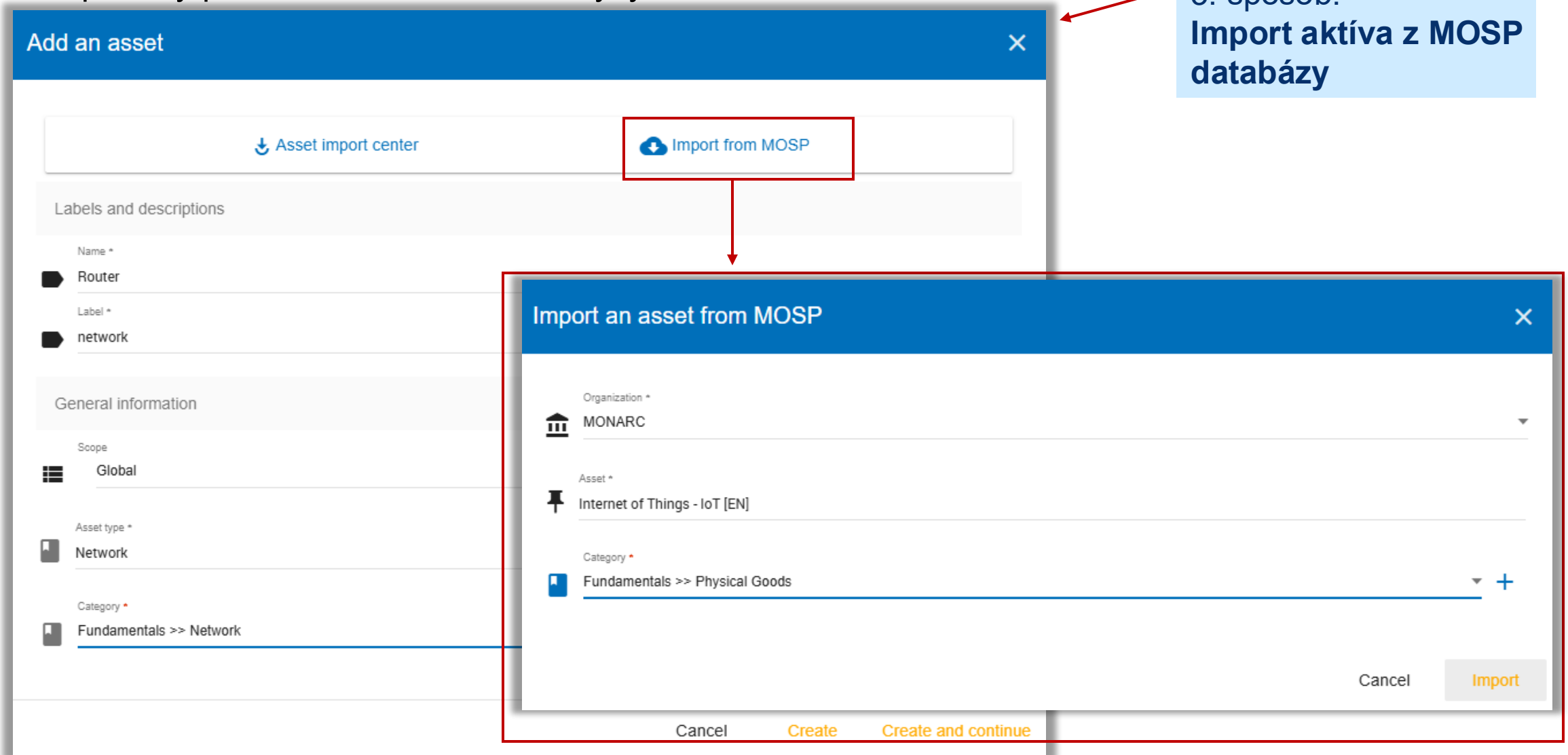
2. spôsob:
**Import aktíva zo súboru**



# 2. Modelovanie kontextu – 2.A Identification of assets, vulnerabilities and impacts appreciation

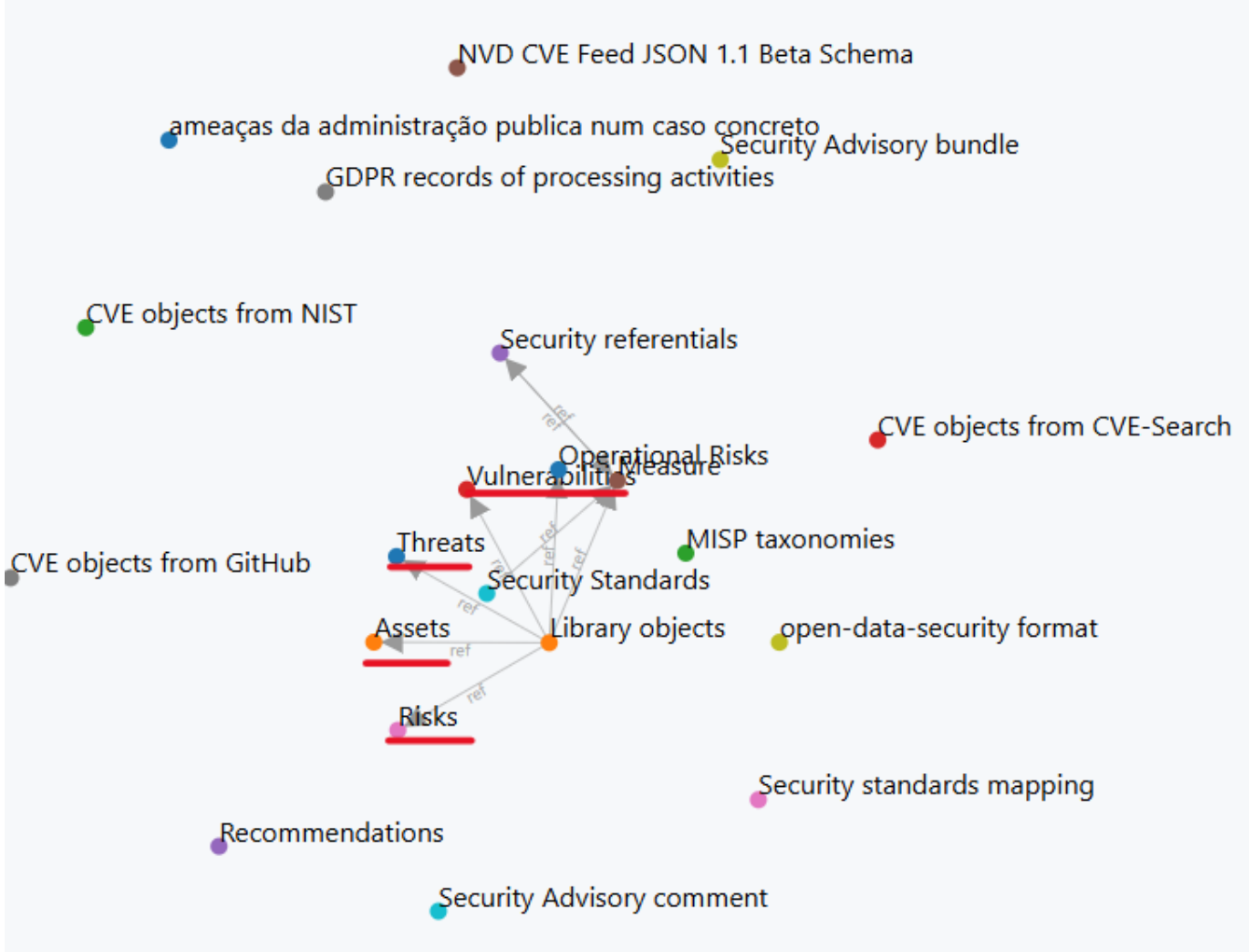
- 3 spôsoby pre vloženie aktív do analýzy:

3. spôsob:
**Import aktíva z MOSP databázy**



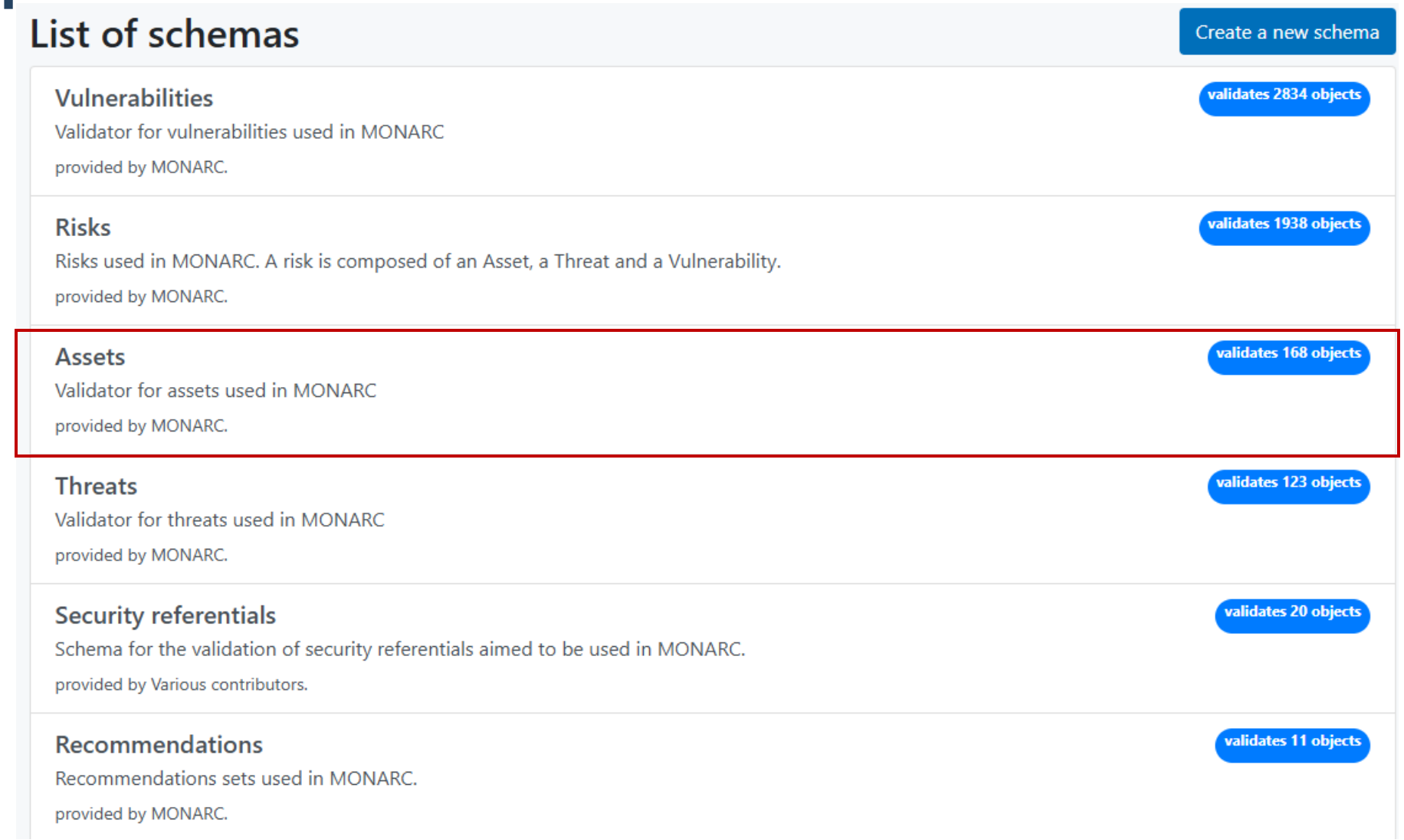
# MOSP databáza

- MOSP - otvorená databáza objektov používaných v nástroji MONARC
- Poskytuje štandardizované definície aktív, hrozieb, zraniteľností a ďalších prvkov analýzy rizík vo forme znovu-použiteľných objektov
- (objects.monarc.lu) obsahuje viac typov objektov, nie len aktíva.
- MOSP typy objektov:
  - Assets (aktíva)
  - Threats (hrozby)
  - Vulnerabilities (zraniteľnosti)
  - Risks (rizikové scenáre)
  - Controls / Measures (bezpečnostné opatrenia)



# MONARC

# MOSP


List of schemas
Create a new schema
Vulnerabilities
validates 2834 objects
Validator for vulnerabilities used in MONARC
provided by MONARC.
Risks
validates 1938 objects
Risks used in MONARC. A risk is composed of an Asset, a Threat and a Vulnerability.
provided by MONARC.
Assets
validates 168 objects
Validator for assets used in MONARC
provided by MONARC.
Threats
validates 123 objects
Validator for threats used in MONARC
provided by MONARC.
Security referentials
validates 20 objects
Schema for the validation of security referentials aimed to be used in MONARC.
provided by Various contributors.
Recommendations
validates 11 objects
Recommendations sets used in MONARC.
provided by MONARC.

# Aktíva v MOSP databáze:

## Assets

**Description** Validator for assets used in MONARC
**Provided by** MONARC

Search on the properties of the objects
code Submit

« 1 2 ... 5 6 7 8 9 »

displaying **121 - 140** objects in total **168**

Search:

| id | Name | Organization | Last updated | Edit | Definition | Object | Delete |
|---|---|---|---|---|---|---|---|
| 3140 | Multifuntion Printer | MONARC | May 6, 2019, 12:29:59 PM | | | | |
| 3135 | Software development | MONARC | May 6, 2019, 12:29:58 PM | | | | |
| 3143 | Network | MONARC | May 6, 2019, 12:29:56 PM | | | | |
| 3138 | Software maintenance | MONARC | May 6, 2019, 12:29:34 PM | | | | |
| 3153 | Network and Communication | MONARC | May 6, 2019, 12:28:35 PM | | | | |
| 3155 | Essential service | MONARC | May 6, 2019, 12:28:14 PM | | | | |
| 3150 | Operator / Maintenance | MONARC | May 6, 2019, 12:27:30 PM | | | | |

# Aktíva v MOSP sú definované:

## Network

| | |
|---|---|
| **Description** | Any network hardware (router, switch, firewall, etc.) |
| **Owning organization** | MONARC |
| **Validating JSON schema** | Assets (provided by MONARC) |
| **Creator** | Cedric |
| **License** | Creative Commons Zero v1.0 Universal |

**Related objects**

Refers to 0 object(s) | Referred to by 4 object(s) | Part of 0 collection(s)

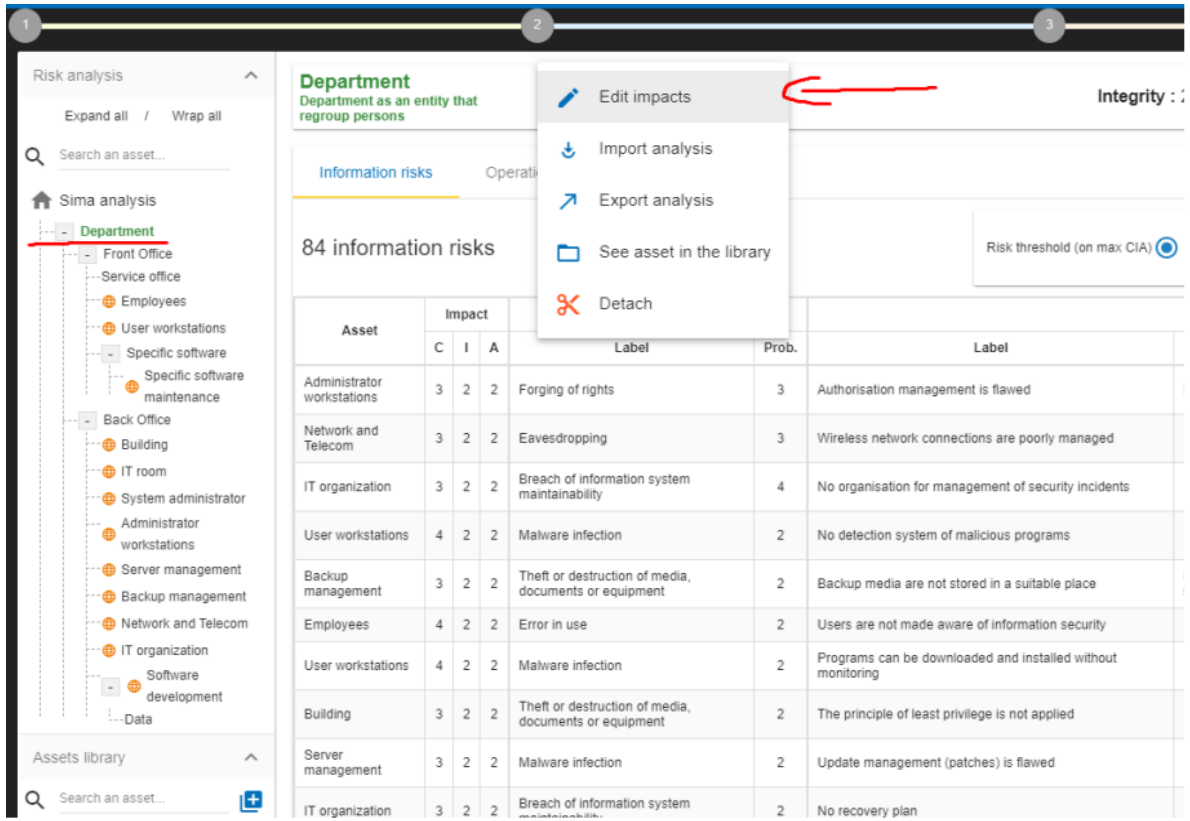
**Definition of the object**


```
{
    "code": "OV_RESEAU",
    "description": "Any network hardware (router, switch, firewall, etc.)",
    "label": "Network",
    "language": "EN",
    "type": "Secondary",
    "uuid": "d2023e4b-44d1-11e9-a78c-0800277f0571",
    "version": 1
}
```

# 2. Modelovanie kontextu – 2.A Identification of assets, vulnerabilities and impacts appreciation

- Po otvorení analýzy sa zobrazí **hlavná pracovná plocha** s knižnicou aktív a stromovou štruktúrou
- Cieľom je vytvoriť **model rizík** umiestnením aktív do hierarchie
- Hodnotenie dopadov (Impact)
  - Každé **primárne aktívum** musí mať definovaný dopad pri vzniku rizika
  - Dopady sa hodnotia podľa CIA + ROLPF
  - Sekundárne aktíva **automaticky zdedia hodnoty**, ale je možné ich upraviť manuálne

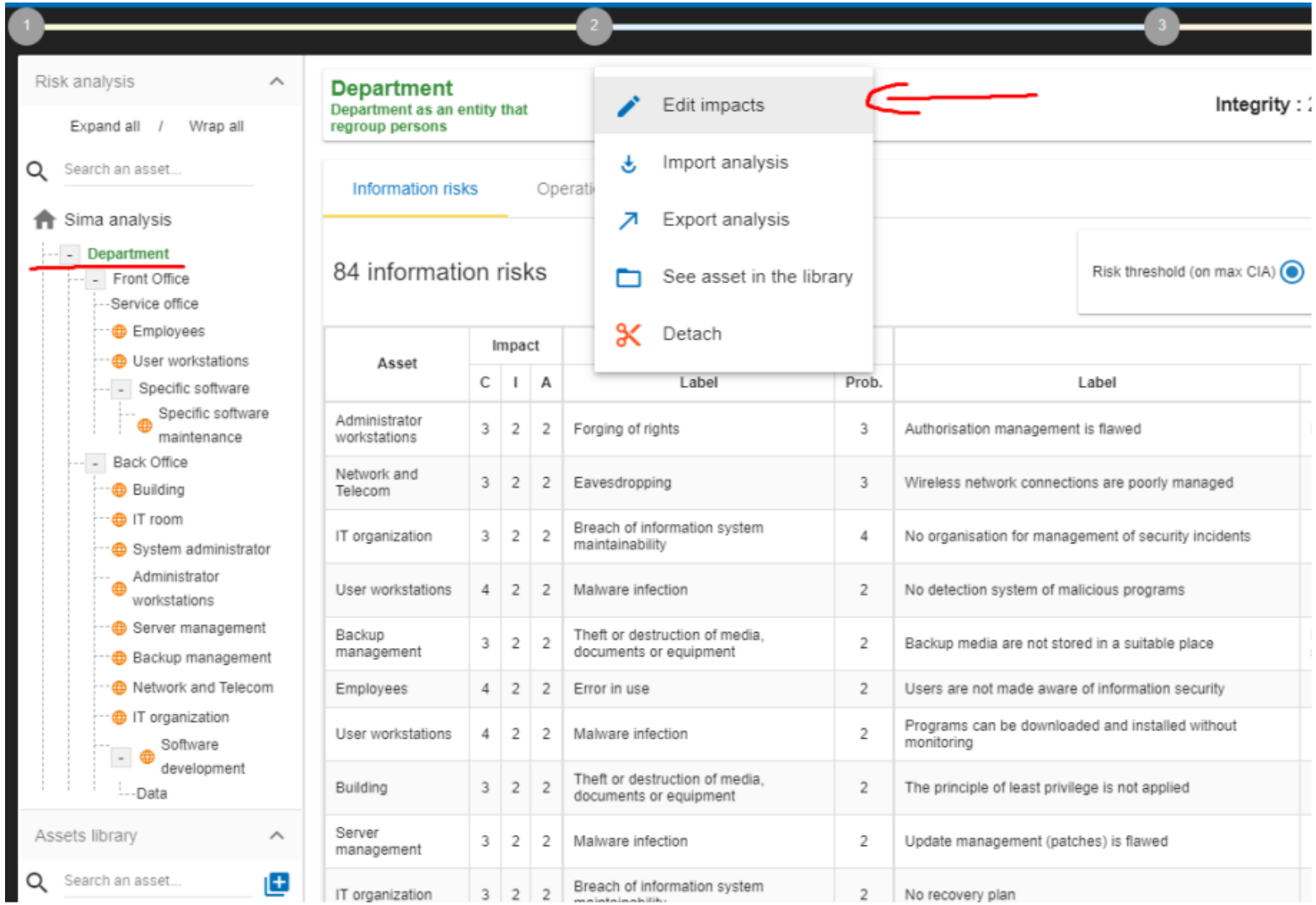
| Typ aktíva | Úloha v modeli | Poznámka |
|---|---|---|
| Primárne aktíva | to, čo chceme chrániť (výučba, dáta, systémy…) | sú „koreňom“ analýzy |
| Sekundárne aktíva | podporné prostriedky (HW, SW, sieť, ľudia…) | dedia hodnoty dopadu z primárnych |






Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# 2. Modelovanie kontextu – 2.A Identification of assets, vulnerabilities and impacts appreciation




| Asset | Impact C | I | A | Label | Prob. | Label |
|---|---|---|---|---|---|---|
| Administrator workstations | 3 | 2 | 2 | Forging of rights | 3 | Authorisation management is flawed |
| Network and Telecom | 3 | 2 | 2 | Eavesdropping | 3 | Wireless network connections are poorly managed |
| IT organization | 3 | 2 | 2 | Breach of information system maintainability | 4 | No organisation for management of security incidents |
| User workstations | 4 | 2 | 2 | Malware infection | 2 | No detection system of malicious programs |
| Backup management | 3 | 2 | 2 | Theft or destruction of media, documents or equipment | 2 | Backup media are not stored in a suitable place |
| Employees | 4 | 2 | 2 | Error in use | 2 | Users are not made aware of information security |
| User workstations | 4 | 2 | 2 | Malware infection | 2 | Programs can be downloaded and installed without monitoring |
| Building | 3 | 2 | 2 | Theft or destruction of media, documents or equipment | 2 | The principle of least privilege is not applied |
| Server management | 3 | 2 | 2 | Malware infection | 2 | Update management (patches) is flawed |
| IT organization | 3 | 2 | 2 | Breach of information system | 2 | No recovery plan |

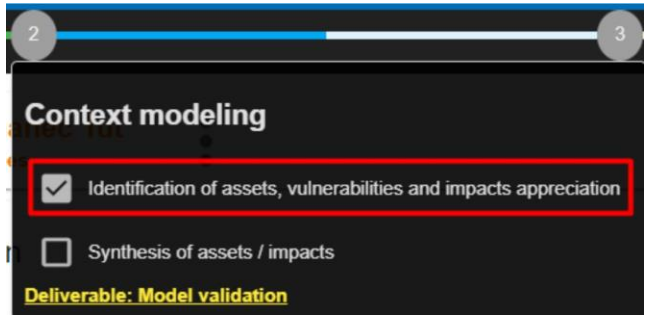


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

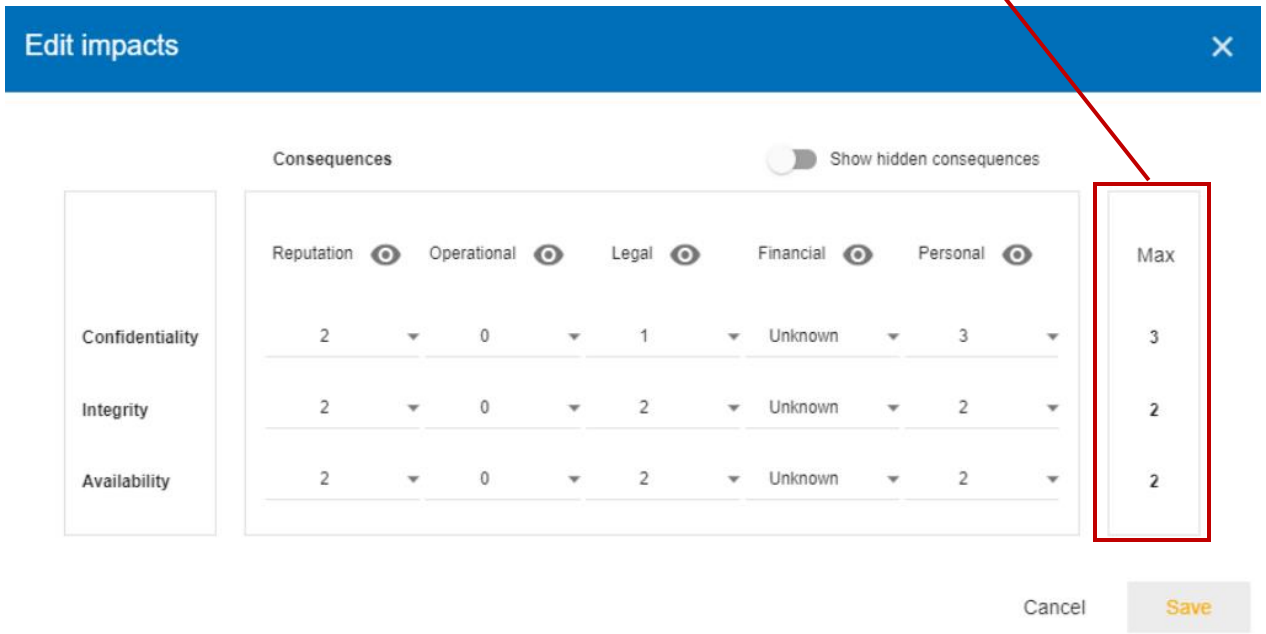
# 2. Modelovanie kontextu – 2.A Identification of assets, vulnerabilities and impacts appreciation

- V tomto okne (Edit Impacts) sa hodnotia (appreciation) **dopady rizika na aktívum** podľa **CIA triády**:
  - Confidentiality – Dôvernosť
  - Integrity – Integrita
  - Availability – Dostupnosť
- Pre každú hodnotu CIA sa hodnotí **dôsledok na organizáciu** podľa ROLFP kategórií:

| ROLFP | Význam |
|---|---|
| Reputation | vplyv na povesť organizácie |
| Operational | narušenie prevádzky, výučby, výskumu |
| Legal | porušenie zákonov, noriem, GDPR |
| Financial | finančné straty, sankcie, náklady |
| Personal | dopad na zamestnancov / študentov |




Výsledná hodnota dopadu je **maximálna hodnota v riadku**

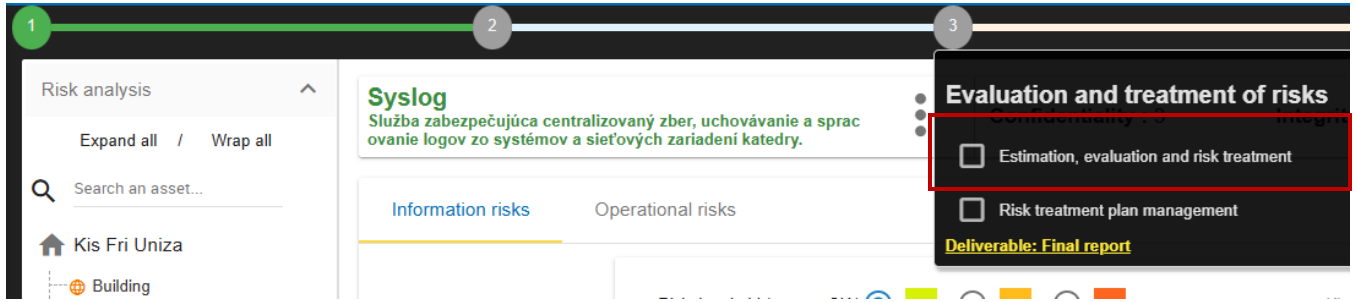


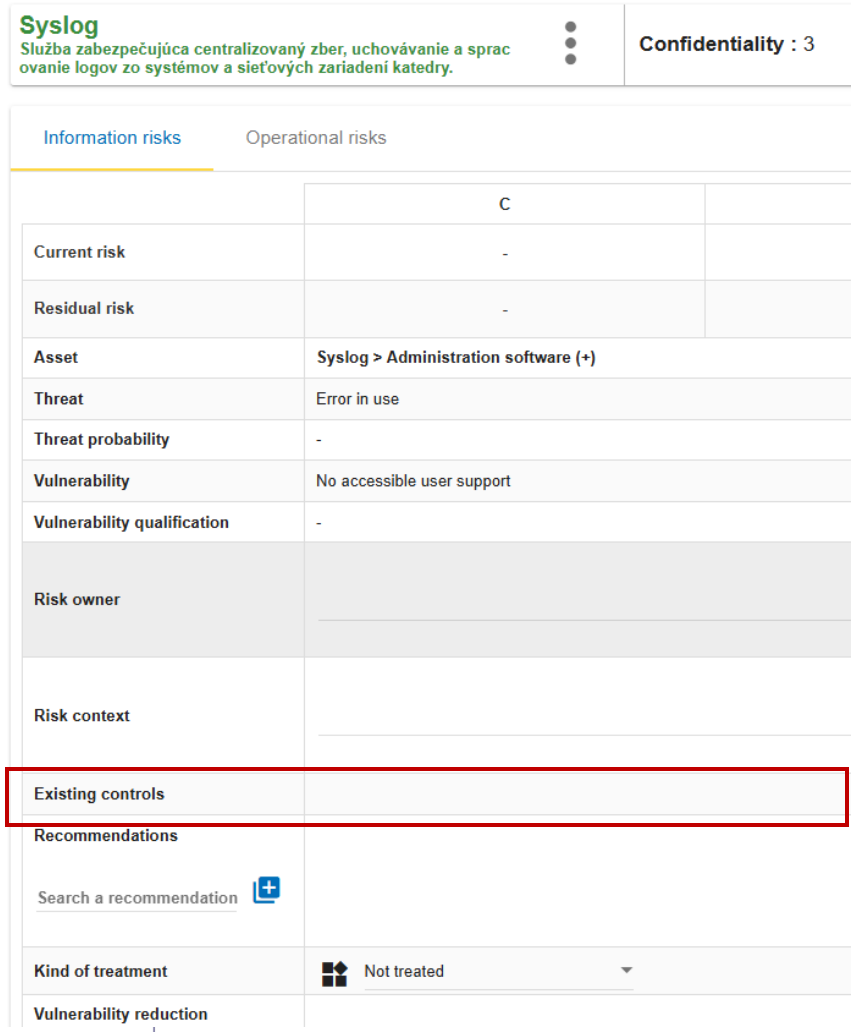



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# 2. Modelovanie kontextu – 2.A Identification of assets, vulnerabilities and impacts appreciation

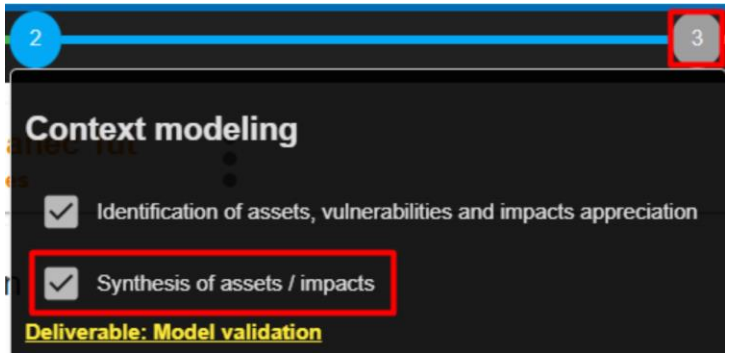
- Zraniteľnosť sa v MONARC neurčuje samostatne ako objekt
- Vyplývajú z bodu - aké bezpečnostné opatrenia existujú prípadne neexistujú
- Po kliknutí na riziko sa nám zobrazia detailné informácie o riziku, kde môžeme dodatočne vypísať **existujúce opatrenia**.
- Ďalej v kroku 3, budeme existujúce opatrenia prevádzať na číselnú hodnotu, do časti Qualification

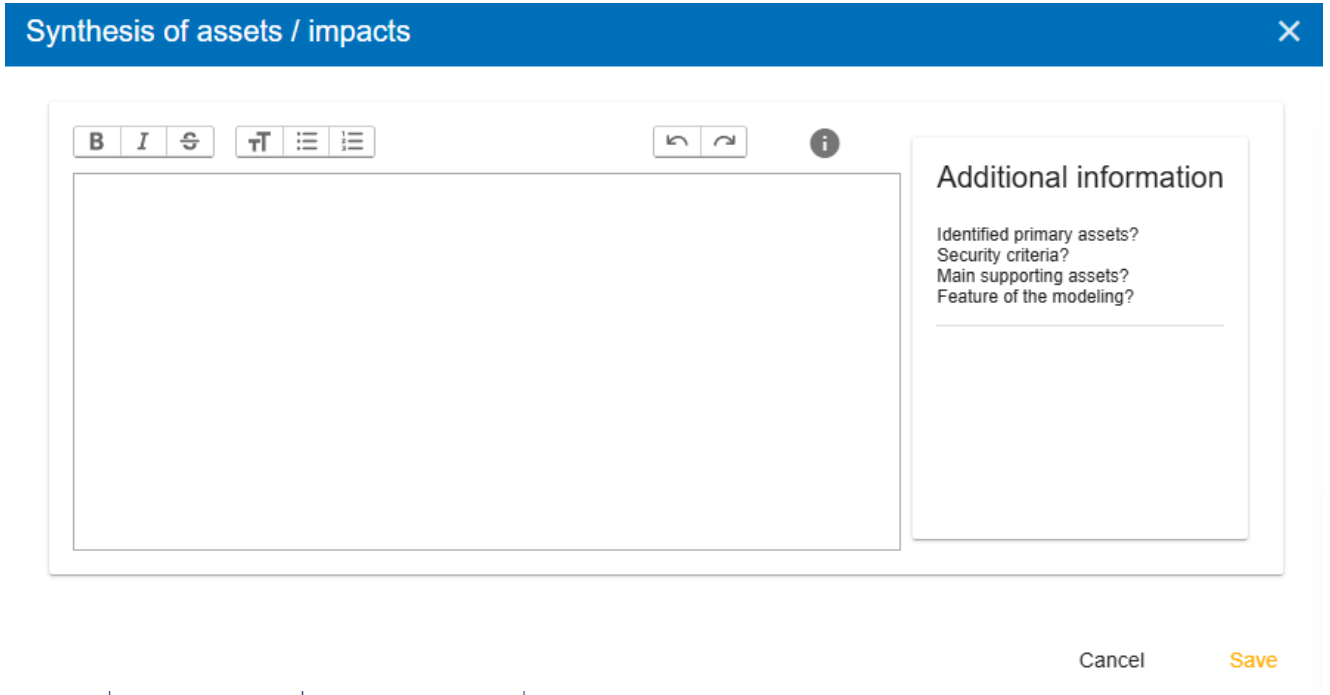


# 2. Modelovanie kontextu – 2.B Synthesis of assets / impacts

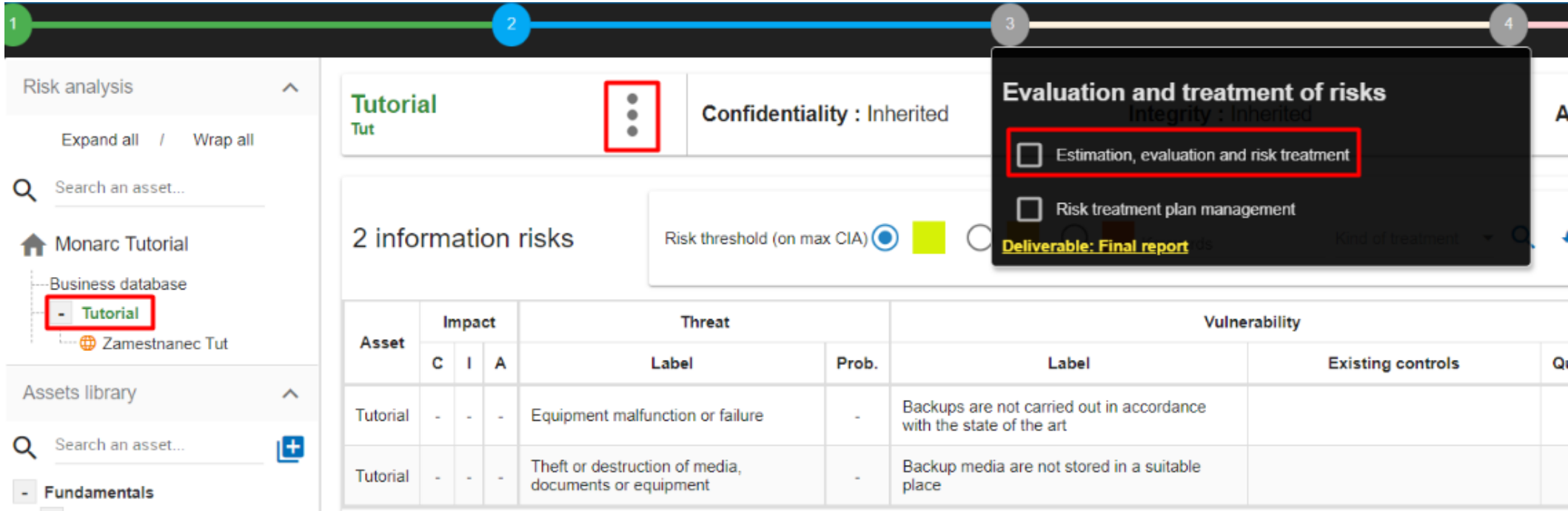
- Ide o textový súhrn modelu aktív a hodnotenia dopadov
- Obsah slúži ako odôvodnenie výberu aktív a spôsobu, akým boli ohodnotené dopady (CIA + ROLFP)
- Text sa automaticky zobrazí vo finálnom risk reporte (správe z analýzy)
- Mal by obsahovať:
  - Aké **primárne aktíva** boli identifikované.
  - Podľa čoho boli hodnotené **bezpečnostné kritériá** (CIA).
  - Aké **podporné aktíva** boli priradené (HW, SW, sieť, personál…).
  - Špecifiká modelovania (napr. dedenie hodnôt, zoskupovanie systémov, rozsah analýzy).



# 3. Hodnotenie a ošetrenie rizík – 3.A Estimation, evaluation and risk treatment

1. **stanovenie kontextu:**
   - určenie cieľa analýzy a definovanie prostredia
   - stanovenie kritérií a metodiky hodnotenia rizík
2. **modelovanie kontextu:**
   - identifikácia aktív a ich rozdelenie podľa priority
   - vytvorenie rizikového modelu pomocou databázy MONARC
3. **hodnotenie a ošetrenie rizík:**
   - posúdenie hrozieb, zraniteľností a úrovne rizík
   - návrh opatrení na zníženie významných rizík
4. **implementácia a monitorovanie:**
   - realizácia odporúčaných bezpečnostných opatrení
   - priebežné sledovanie zmien a aktualizácia analýzy



# 3. Hodnotenie a ošetrenie rizík – 3.A Estimation, evaluation and risk treatment

- V tejto fáze sa pre aktíva [1] **kvantifikujú riziká** [6] pomocou:
  - Impact (dopad) [2] – podľa CIA alebo ROLFP
  - Probability [3] (pravdepodobnosť hrozby)
  - Vulnerability [5] (zraniteľnosť aktíva)
- MONARC automaticky vypočíta aktuálne riziko (Current risk) [6] a zvyškové riziko (Residual risk) [8]

- Postup v tejto fáze:
  - Ohodnotenie **pravdepodobnosti hrozieb** pre každé aktívum [3]
  - Priradenie **zraniteľností** (ak sú známe) [5]
  - Výpočet **rizikového skóre** – informačné aj operačné riziká [6]
  - Porovnanie so **stanovenou prijateľnou úrovňou rizika (thresholds)**
  - Ak je riziko neprijateľné → definovanie **risk treatment** (mitigácia, akceptácia, prevod, odstránenie) [7]

| 1 Asset | Impact 2 C | I | A | Threat Label | 3 Prob. | Vulnerability Label | 4 Existing controls | 5 Qualif. | Current risk 6 C | I | A | 7 Treatment | 8 Residual risk |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Administrator workstations | 2 | 1 | 4 | Forging of rights | 2 | Authorisation management is flawed | Nothing | 4 | 16 | 8 | 32 | Not treated | 32 |

Zvyškové riziko

# 3. Hodnotenie a ošetrenie rizík – 3.A Estimation, evaluation and risk treatment

- V tejto fáze sa pre aktíva [1] **kvantifikujú operačné riziká** pomocou:
  - Impact (dopad) – hodnotený výhradne podľa ROLFP(Regulatory, Organizational, Legal, Financial, Privacy/Personal)
  - Probability (pravdepodobnosť) – pravdepodobnosť hrozby
  - Vulnerability / Existing controls – zohľadnenie existujúcich opatrení
- Výsledný dopad sa určuje ako najhoršia (maximálna) hodnota z ROLFP dimenzií (worst-case princíp).

**MONARC automaticky vypočíta:**

- **Current risk** – aktuálne riziko
- **Residual risk** – zvyškové riziko po navrhnutých opatreniach

- Postup v tejto fáze:
  - Výber primárneho aktíva/oblasti (dodávateľské vzťahy, prevádzka IT, GDPR povinnosti) [1]
  - Identifikácia operačných rizík [2]
  - Ohodnotenie **pravdepodobnosti hrozieb**[Prob] a dopadov cez ROLFP [3]
  - Výpočet: Net [3] (Current risk pri existujúcich opatreniach)
  - Porovnanie s prahovými hodnotami prijateľnosti
  - Ak je riziko neprijateľné -> risk treatment [5] v našom prípade redukcia

| 1 | 2 | 3 | | | | | | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|---|---|---|
| Asset | Risk description | Net risk | | | | | | | Treatment | Residual risk |
| | | Prob. | Impact | | | | | Current risk | Existing controls | |
| | | | Rep. | Ope. | Leg. | Fin. | Per. | | | |
| DPO | Low communication between DPO and the commission | 4 | 1 | 3 | 3 | 2 | 3 | 12 | Absence of DPO | Reduction | 3 |

Zvyškové riziko

# CIA vs. ROLFP

| Typ rizika | Výpočet | Používa |
|---|---|---|
| Informačné riziká | R = Impact × (Threat × Vulnerability) | CIA |
| Operačné riziká | R = Impact × Probability | ROLFP |

| Skratka | Význam |
|---|---|
| C – Confidentiality | Ochrana pred neoprávneným prístupom k dátam |
| I – Integrity | Ochrana pred zmenou, poškodením alebo manipuláciou s dátami |
| A – Availability | Zabezpečenie, aby boli systémy a údaje dostupné, keď sú potrebné |

| Skratka | Význam dopadu |
|---|---|
| R – Reputation | poškodenie mena organizácie |
| O – Operational | narušenie činnosti, procesov, výučby, výskumu |
| L – Legal | porušenie zákonov, noriem, GDPR |
| F – Financial | sankcie, pokuty, výpadky príjmov, náklady na obnovu |
| P – Personal | vplyv na zamestnancov, študentov, zdravie, údaje osôb |

# 3. Hodnotenie a ošetrenie rizík – 3.A Risk treatment plan management

- V MONARC-u sa riziká riešia pomocou **4 typov reakcie:**
  1. **Accept** – riziko je prijaté, nerobia sa ďalšie kroky
  2. **Modify / Reduce** – zavádzajú sa opatrenia na zníženie rizika
  3. **Share** – riziko sa prenáša na tretiu stranu (napr. poistenie, outsourcing)
  4. **Deny / Avoid** – odstráni sa príčina rizika, riziko ďalej neexistuje
- Každé riziko v analýze je priradené k jednému z týchto postupov.

Výsledné odporúčania sa zobrazujú v **pláne riadenia rizík** (Risk treatment plan).

Risk treatment plan management

Reset positions

| | Recommendation | Imp. | Asset | Existing controls | Current risk | Residual risk |
|---|---|---|---|---|---|---|
| | **Authorisation**<br>Implement a procedure for the authorisation management | ••• | Administrator workstations | No procedure | 36 | 9 |
| | **Monitoring**<br>Implement e a monitoring of the workstation | ••• | Administrator workstations | The workstations are not monitored | 45 | 18 |
| | **Program management**<br>Implement a white list of the program which have been approved by the IT department | ••• | Administrator workstations | No measure | 30 | 0 |
| | **Administrator right**<br>Remove the administrator right from the workstations of the users | •• | Administrator workstations | There is no procedures | 15 | 9 |
| | **Patch management**<br>Check if the patch are really applied | •• | Administrator workstations | The patch are normally done in automatic | 12 | 6 |

# 3. Hodnotenie a ošetrenie rizík – 3.A Risk treatment plan management

1. **Accept** – Residual risk ≈ Current risk, riziko je na prijateľnej úrovni
2. **Modify / Reduce** – Residual risk < Current risk - zavádzame opatrenia, riziko je neprijateľné ale tolerovateľné
3. **Share** – prenášame ho na 3. stranu, poistenie, SLA s dodávateľom, ...
4. **Deny / Avoid** – Residual risk = 0 - ruším činnosť, systém, prestanem robiť to, čo ho spôsobovalo

- Každé riziko v analýze je priradené k jednému z týchto postupov.

Risk treatment plan management

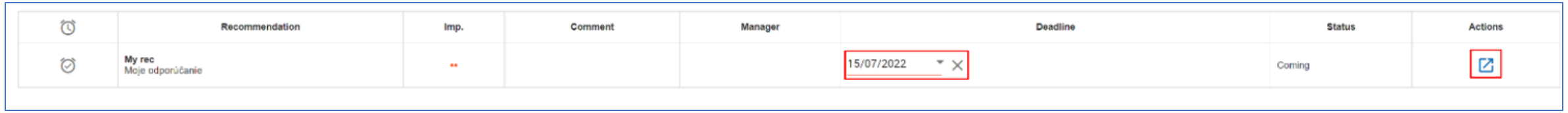
Reset positions

| | Recommendation | Imp. | Asset | Existing controls | Current risk | Residual risk |
|---|---|---|---|---|---|---|
| | **Authorisation**<br>Implement a procedure for the authorisation management | ••• | Administrator workstations | No procedure | 36 | 9 |
| | **Monitoring**<br>Implement e a monitoring of the workstation | ••• | Administrator workstations | The workstations are not monitored | 45 | 18 |
| | **Program management**<br>Implement a white list of the program which have been approved by the IT department | ••• | Administrator workstations | No measure | 30 | 0 |
| | **Administrator right**<br>Remove the administrator right from the workstations of the users | •• | Administrator workstations | There is no procedures | 15 | 9 |
| | **Patch management**<br>Check if the patch are really applied | •• | Administrator workstations | The patch are normally done in automatic | 12 | 6 |

# 4. Implementácia a monitorovanie – Management of the implementation of the risk treatment plan

1. **stanovenie kontextu:**
   - určenie cieľa analýzy a definovanie prostredia
   - stanovenie kritérií a metodiky hodnotenia rizík
2. **modelovanie kontextu:**
   - identifikácia aktív a ich rozdelenie podľa priority
   - vytvorenie rizikového modelu pomocou databázy MONARC
3. **hodnotenie a ošetrenie rizík:**
   - posúdenie hrozieb, zraniteľností a úrovne rizík
   - návrh opatrení na zníženie významných rizík
4. **implementácia a monitorovanie:**
   - realizácia odporúčaných bezpečnostných opatrení
   - priebežné sledovanie zmien a aktualizácia analýzy

- Po vykonaní prvých 3 fáz nasleduje fáza riadenia s **bezpečnostným monitorovaním** a opakovanou kontrolou bezpečnostných opatrení.
- Táto fáza slúži na opakované a **nepretržité zlepšovanie** a **udržiavanie bezpečnostných opatrení**



MONARC

# Export Aktív

Aktíva je možné exportovať do .csv súboru,
ktorý je štruktúrovaný nasledovne:

| uuid | code | label (Typ aktíva) | description | type |
|---|---|---|---|---|
| d2023c5d-44d1-11e9-a78c-0800277f0571 | BAT_LOC | Premises, building | Establishment, buildings, offices, reserved access zone, etc. | 2 |
| d2023c8f-44d1-11e9-a78c-0800277f0571 | CONT | Container | Asset container | 1 |
| d2023ca5-44d1-11e9-a78c-0800277f0571 | INFO | Information | Sensitive or essential information | 1 |
| d2023cb8-44d1-11e9-a78c-0800277f0571 | LOG_APP | Business application | Custom business application or standard | 2 |
| d2023ceb-44d1-11e9-a78c-0800277f0571 | LOG_OS | Operating system | Windows 7, MAC OX 10, Linux | 2 |
| d2023cfb-44d1-11e9-a78c-0800277f0571 | LOG_SRV | Service, maintenance or administration software | All administrative tools | 2 |
| d2023d0a-44d1-11e9-a78c-0800277f0571 | LOG_STD | Package software or standard software | Microsoft office, MySQL, SAP, Photoshop, etc. | 2 |
| d2023d19-44d1-11e9-a78c-0800277f0571 | MAT_FIX | **Fixed equipment** | Server, microcomputer used as a workstation | 2 |
| d2023d29-44d1-11e9-a78c-0800277f0571 | MAT_MOB | **Transportable equipment** | Laptop, PDA, etc. | 2 |
| d2023d38-44d1-11e9-a78c-0800277f0571 | MAT_NELE | Other media | Paper, slide, transparency, documentation, fax. | 2 |
| d2023d46-44d1-11e9-a78c-0800277f0571 | MAT_PERI | **Processing peripheral** | Printer, removable disc drive | 2 |
| d2023d57-44d1-11e9-a78c-0800277f0571 | MAT_SUPP | **Electronic medium** | CD ROM, back-up cartridge, removable hard disc, memory key, ta | 2 |
| d2023d64-44d1-11e9-a78c-0800277f0571 | ORG_EXT | Subcontractors, suppliers, manufacturers | Third-party service companies | 2 |
| d2023d89-44d1-11e9-a78c-0800277f0571 | ORG_GEN | Structure of the organisation | Structure of the organisation | 2 |
| d2023d98-44d1-11e9-a78c-0800277f0571 | OV_BACKUP | **Backup** | Backup | 2 |
| d2023da7-44d1-11e9-a78c-0800277f0571 | OV_BATI | Building, office or premises | Building, office or premises | 2 |
| d2023db5-44d1-11e9-a78c-0800277f0571 | V_DEVELOPPEMEN | Software development | Software development | 2 |
| d2023dc4-44d1-11e9-a78c-0800277f0571 | OV_INFOPHY | Paper document | Information in physical form | 2 |
| d2023dd3-44d1-11e9-a78c-0800277f0571 | OV_LOGICIEL | Software | Business application | 2 |

# Otvorená reflexia

- **Ktorá z kategórií patrí medzi primárne aktíva podľa normy ISO/IEC 27005?** (1 správna)
  - a) Tlačiarne a skenery
    b) Firemná sieťová topológie
    c) Obchodné procesy a informácie
    d) Zamestnanecké prístupové karty
- **Čo vyjadruje cyklus PDCA v oblasti riadenia bezpečnosti?** (1 správna)
  - a) Jednorazový projektový plán
    b) Metódu na správu hardvéru
    c) Iteratívny proces neustáleho zlepšovania
    d) Postup používaný iba pri auditoch
- **Ktorý z nasledujúcich prvkov NEPATRÍ medzi základné atribúty CIA triády?** (1 správna)
  - a) Dôvernosť (Confidentiality)
    b) Integrita (Integrity)
    c) Dostupnosť (Availability)
    d) Pravosť (Authenticity)
- **Ktorý z uvedených cieľov patrí medzi hlavné dôvody správy softvérových aktív?** (1 správna)
  - a) Zvyšovať výkon hardvéru
    b) Zabezpečiť aktualizácie, licencie a kompatibilitu softvéru
    c) Automatizovať bezpečnostné monitorovanie siete
    d) Tvorba šifrovacích kľúčov
- **Ktorý z nasledujúcich prvkov je nevyhnutnou súčasťou hodnotenia aktív podľa ISO/IEC 27005?** (1 správna)
  - a) Automatická záloha bez definovania rizík
    b) Identifikácia aktív, kritérií hodnotenia a určenie dopadov
    c) Výpočet sieťovej priepustnosti
    d) Analýza kybernetických útokov pomocou SIEM systému

# Otvorená reflexia

- **Aký je hlavný účel nástroja MONARC?** (1 správna)
  - a) Automatizovať antivírusové skenovanie
    b) Vytvárať a spravovať modely rizík organizácie
    c) Zálohovať firemné dáta
    d) Monitorovať sieťovú prevádzku
- **Čo predstavuje „Residual risk“ v MONARC?** (1 správna)
  - a) Pôvodné riziko pred analýzou
    b) Riziko po odstránení hrozby
    c) Zvyškové riziko po aplikovaní opatrení
    d) Riziko, ktoré je úplne eliminované
- **Ako sa líši Front Office (FO) od Back Office (BO) v architektúre MONARC?** (1 správna)
  - a) FO je určený na správu viacerých organizácií, BO sa používa iba lokálne
    b) FO slúži na vykonávanie analýzy rizík, BO riadi správu modelov a viacerých FO
    c) BO je cloudová verzia MONARC, FO je desktopová verzia
    d) Rozdiel neexistuje, ide o rovnaké moduly
- **Ako MONARC počíta aktuálne riziko?** (1 správna)
  - a) Risk = Likelihood × Number of assets
    b) Risk = Impact × (Threat × Vulnerability)
    c) Risk = Impact ÷ Probability
    d) Risk sa vždy prideľuje manuálne administrátorom
- **Ktorý prvok sa v MONARC-u používa na posúdenie výskytu hrozby v minulosti?** (1 správna)
  - a) CIA scoring
    b) Vulnerability index
    c) Trend (− / n / + / ++) indikátor
    d) Compliance level

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

# Ďakujem za pozornosť

## Procesy a nástroje pre bezpečnú správu zariadení

Bezpečná správa zariadení (Blok V)

**Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe**

Mgr. Jana Uramová, PhD.

**KC KYB UNIZA, https://kc.uniza.sk/**

Jana.Uramova@fri.uniza.sk