



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

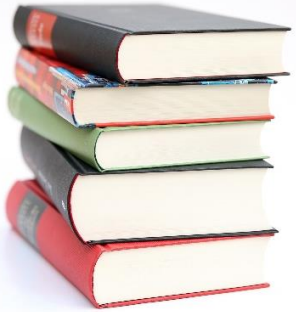
Bezpečná správa zariadení (Blok V)

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

Prečo sú procesy a nástroje pre správu zariadení potrebné?

## 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 zneužitý útočníkom.

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.

Prečo sú procesy a nástroje pre správu zariadení potrebné?

# 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.

Prečo sú procesy a nástroje pre správu zariadení potrebné?

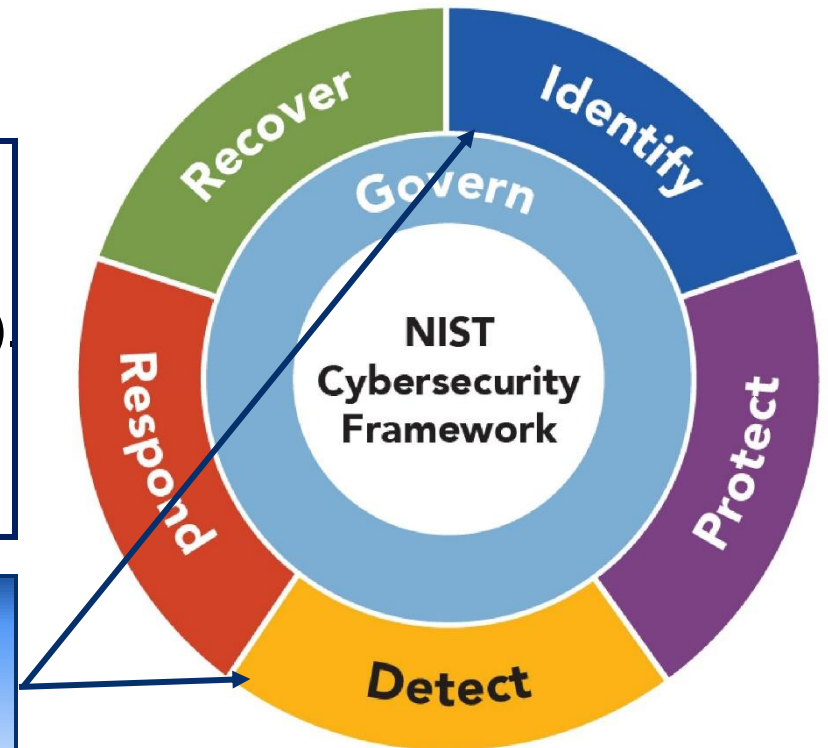
# NIST CSF – prepojenie na správu aktív a monitoring

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.“

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.**

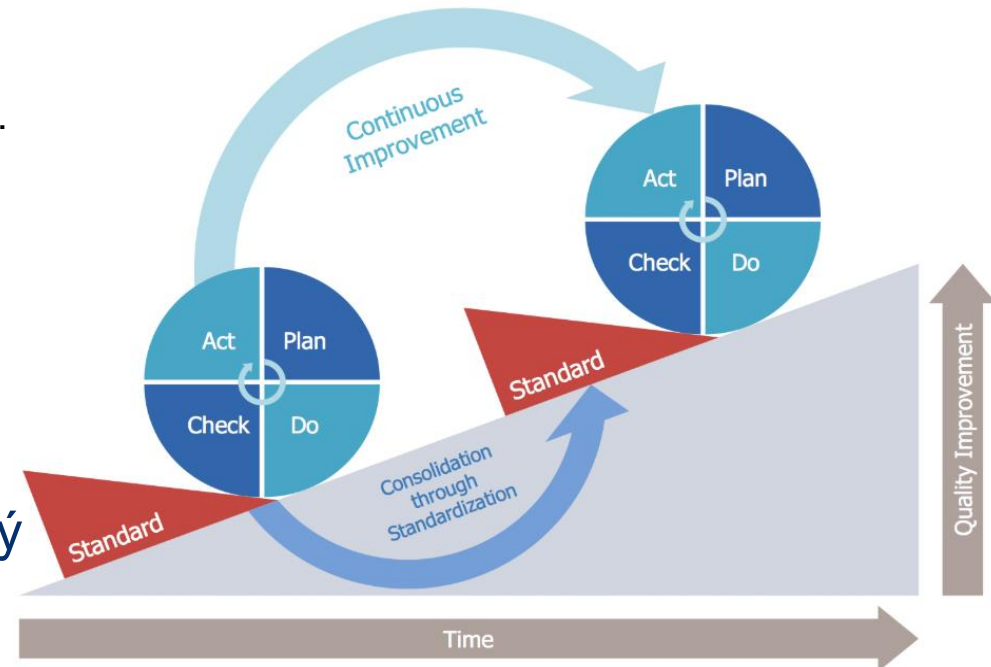


- **Plan** (Naplánuj)– plánovanie: identifikácia aktív, analýza rizík, návrh opatrení.
- **Do** (Vykonaj) – realizácia: implementácia opatrení, monitoring, patching.
- **Check** (Over)– kontrola: audity, skeny, reporting, interné hodnotenie.
- **Act** (Jednaj)– zlepšenie: nápravné opatrenia, aktualizácia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

### Centrálne databáza

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

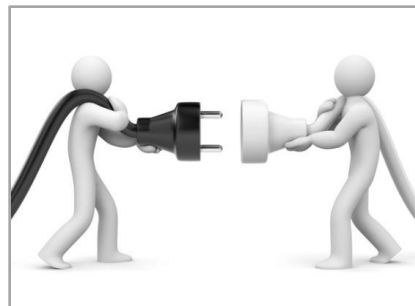
### Riadenie rizík

Identifikácia kritických aktív a určenie priorít pre ich ochranu.

# Primárne vs. sekundárne aktíva

## Primárny proces: Výučba informatiky v učebni

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



## 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...).

**System 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.

Typ aktíva

Podporné informačné aktívum

Podporné fyzické aktívum

Prevádzkové aktívum  
(neinformačné)

Príklad

školský informačný systém, učebné dáta, notebook učiteľa

serverovňa, dvere, zámok, UPS, klimatizácia

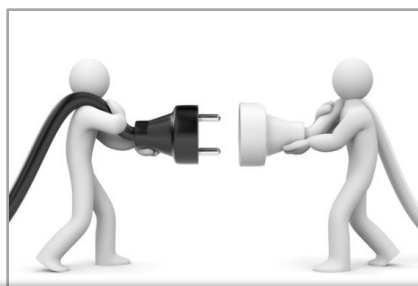
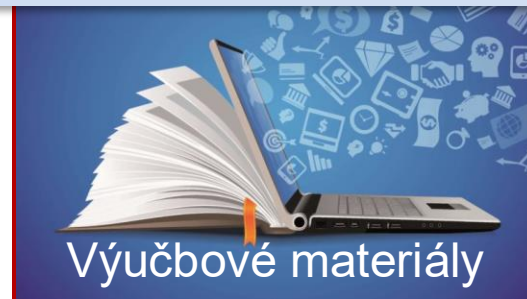
stolička, osvetlenie, kúrenie

Poznámka

priamo spracúva alebo uchováva informácie

umožňuje bezpečné fungovanie IT prostredia

nemá priamy vplyv na bezpečnosť informácií

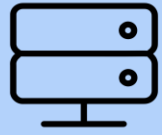


**Fyzická bezpečnosť = súčasť informačnej bezpečnosti, pretože chráni prostredie, v ktorom sú uložené alebo spracúvané informácie.**

# Identifikácia primárnych aktív podľa ISO/IEC 27005

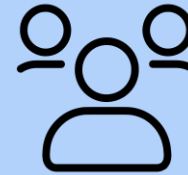
- Primárne aktíva sú 2 typov:
  - **Obchodné procesy (alebo subprocessy) a činnosti, zahrňujúce:**
    - **kritické procesy** – ich strata zastaví misiu/hlavnú činnosť organizácie,
    - **chránené procesy** – obsahujú tajné alebo patentované know-how,
    - **citlivé procesy** – zmena alebo manipulácia môže ohroziť plnenie cieľov,
    - **regulačne viazané procesy** – nevyhnutné pre splnenie zmluvných, právnych a regulačných povinností.
  - **Informácie, kde primárne informácie zahŕňajú najmä**
    - **klúčové 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.

# Identifikácia sekundárnych aktív podľa ISO/IEC 27005



## Hardvér

Fyzické zariadenia a komponenty

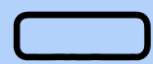


## Personál

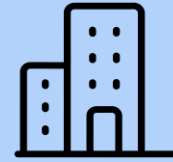
Ľudské zdroje a role



## 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.***

# 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

# 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:

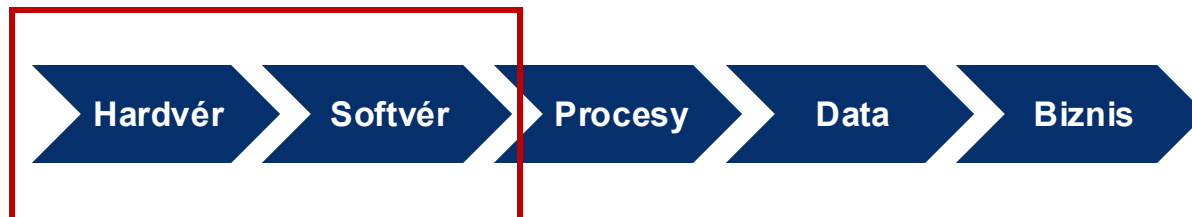
- servisná zmluva – typ podpory, reakčný čas (SLA), rozsah,
- záruka, dátum expirácie, možnosť predĺženia,
- história opráv a servisných zásahov.

### 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, zneužitie?



**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.

# 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 rovnako 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

# 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.

# 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.

# 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	nešifrovaná komunikácia, sniffing paketov

# 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

# 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

# Hodnotenie aktív a analýza vplyvu

### ▪ Ciel' hodnotenia aktív

- stanoviť hodnotu aktív ako vstup do procesu riadenia rizík,
- pripraviť podklad pre určenie úrovne dopadu a priorít ošetrovania 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).

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





## 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.



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



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



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



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



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

Lansweeper

**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...)

# Lansweeper

The screenshot displays the LanSweeper interface for managing IT assets. On the left, a sidebar lists various asset categories and management tools. The main panel shows a table of IT assets, with a detailed view for a specific asset (AUPC-163) overlaid on the right. This view provides technical details such as the asset type (Windows), OS version (Windows 10 Enterprise 64-bit), and IP location (DEMO Subnet).

NAME	TYPE
AP2	Wireless Access
ARUBA - Login Form	Switch
ASM	Webserver
AUMac-190	Apple Mac
AUMac-191	Apple Mac
AUPC-163	Windows
AUPC-189	Windows
AUPC-192	Windows
AUPC-195	Windows
AUPC-198	Windows
C7003D4X	Windows
CONESWFS01	Windows
CONESWWS01	Windows
CONHQAP01	Windows
CONHQFILES01	Windows
CONHQFW01.c	Windows
CONHQFW01.c	Windows
CONHQLESX01.CONTOSO.local	ESX
CONHQLESX02.CONTOSO.local	ESX

Asset type	Windows
OS	Windows 10 Enterprise 64 ...
OS Build	10.0.19044 - 1766
OS Version	21H2
IP Location	DEMO Subnet
Manufacturer	Microsoft Corporation
Model	Surface Laptop 4
System SKU	Surface_Laptop_4_1978:1979

# 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

The screenshot displays the LanSweeper web interface. On the left is a dark sidebar with navigation icons and a menu. The main content area is titled 'IT assets' and shows a table of assets. A modal window is open for the asset 'AUPC-163', showing its details.

NAME	TYPE
AP2	Wireless Access
ARUBA - Login Form	Switch
ASM	Webserver
AUMac-190	Apple Mac
AUMac-191	Apple Mac
AUPC-163	Windows
AUPC-189	Windows
AUPC-192	Windows
AUPC-195	Windows
AUPC-198	Windows
C7003D4X	Microsoft Corporation
CONESWFS01	Surface Laptop 4
CONESWWS01	Surface Laptop 4
CONHQAP01	Surface Laptop 4
CONHQFILES01	Surface Laptop 4
CONHQFW01.c	Surface Laptop 4
CONHQFW01.c	Surface Laptop 4
CONHQLESX01.CONTOSO.local	ESX
CONHQLESX02.CONTOSO.local	ESX

**Asset Details for AUPC-163:**

- Asset type: Windows
- OS: Windows 10 Enterprise 64 ...
- OS Build: 10.0.19044 - 1766
- OS Version: 21H2
- IP Location: DEMO Subnet
- Manufacturer: Microsoft Corporation
- Model: Surface Laptop 4
- System SKU: Surface\_Laptop\_4\_1978:1979

**Relation:** ASSET/USER

**Connected To:** Dell Inc. DEMOSERIAL1

Buttons: CONFIG, SOFTWARE, COMMI

# 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 <sup>?</sup>
- ✓ 1 Installation
- ✓ Service Desk Ticket Enrichment <sup>?</sup>
- ✓ 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 <sup>?</sup>
- ✓ 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 <sup>?</sup>
- ✓ More than 3 installations
- ✓ Full API Access
- ✓ Customer Success Manager
- ✓ Assistance for Global Deployments
- ✓ Concierge Service (Add-on)
- 🛠️ Enterprise Support



## Scanning Target

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



## Asset Radar

automatické zisťovanie nových zariadení odchyťovaním komunikácie v sieti.



## Performance Scanning

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

# 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 siet'ou** - Môže byť blokováné firewallmi alebo vyžadovať prihlasovacie údaje.
- **škálovanie** - Pre veľké siete môže byť potrebné viac skenovacích serverov alebo konfigurácií.

## 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.

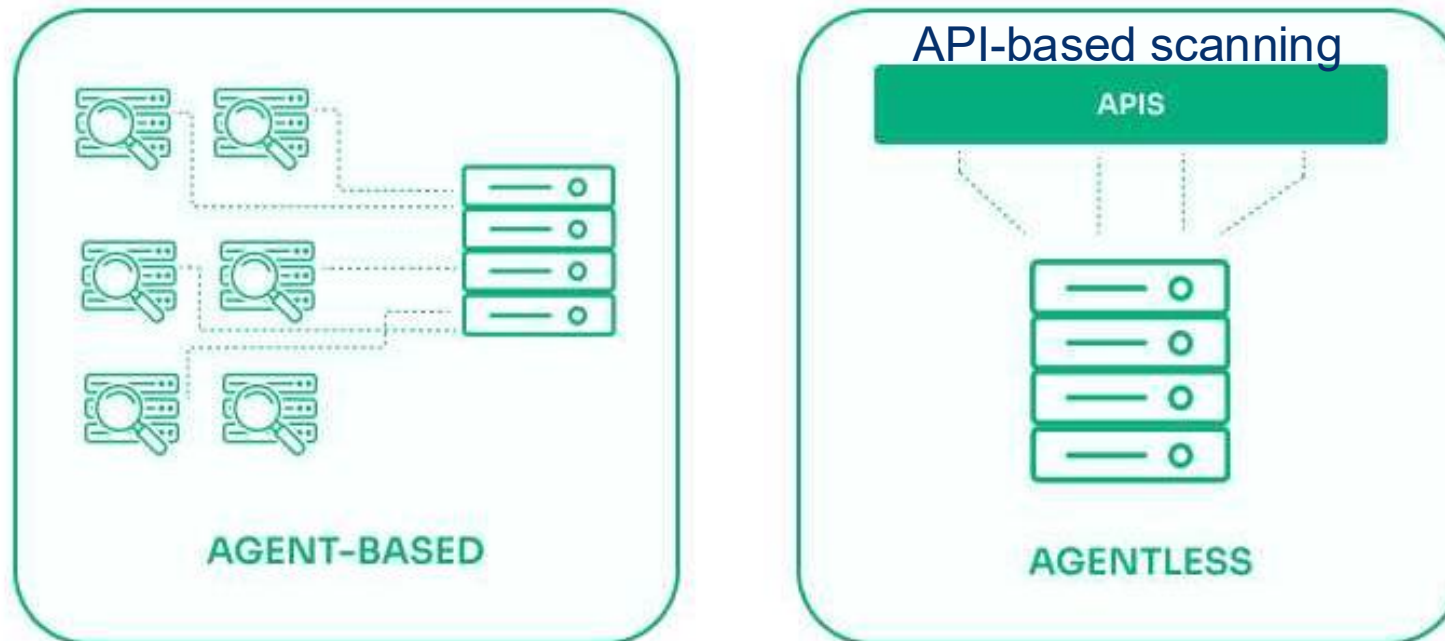
## Nevýhody:

- **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.

## 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**.





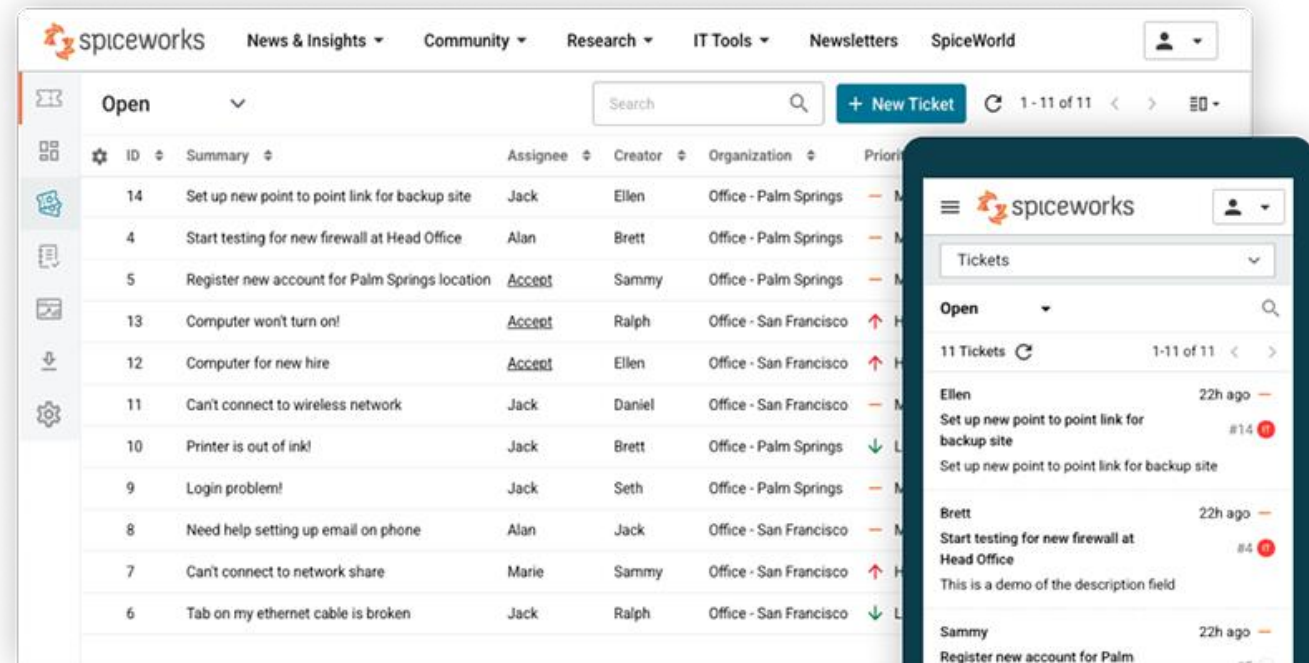
# Inventarizačný nástroj - SpiceWorks

# Nástroje na správu a kategorizáciu aktív

## SpiceWorks



- **Cloudové riešenie** na správu IT požiadaviek a incidentov, určené **pre interné IT tímy**.
- Umožňuje centralizované vytváranie, **priradovanie 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**.



# 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

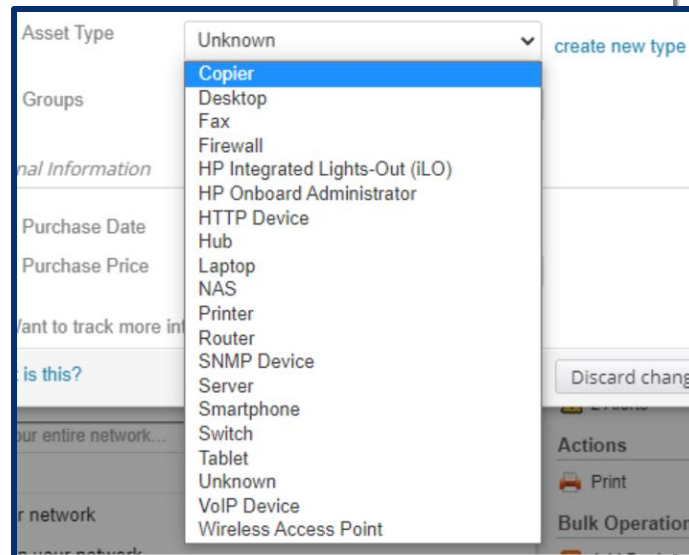
## Premium plán

- 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	✗	✓

# 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.



### Create a new asset

Use this when you want to track an asset that is not on your network. Devices with IP addresses on your network should get discovered on your next scheduled scan.

Name

Serial Number

Mac Address

Asset Type  [create new type](#)

Groups

---

*Optional Information*

Purchase Date

Purchase Price

Tip: Want to track more information? [Customize the optional fields](#)

[What is this?](#)

# 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							
8							

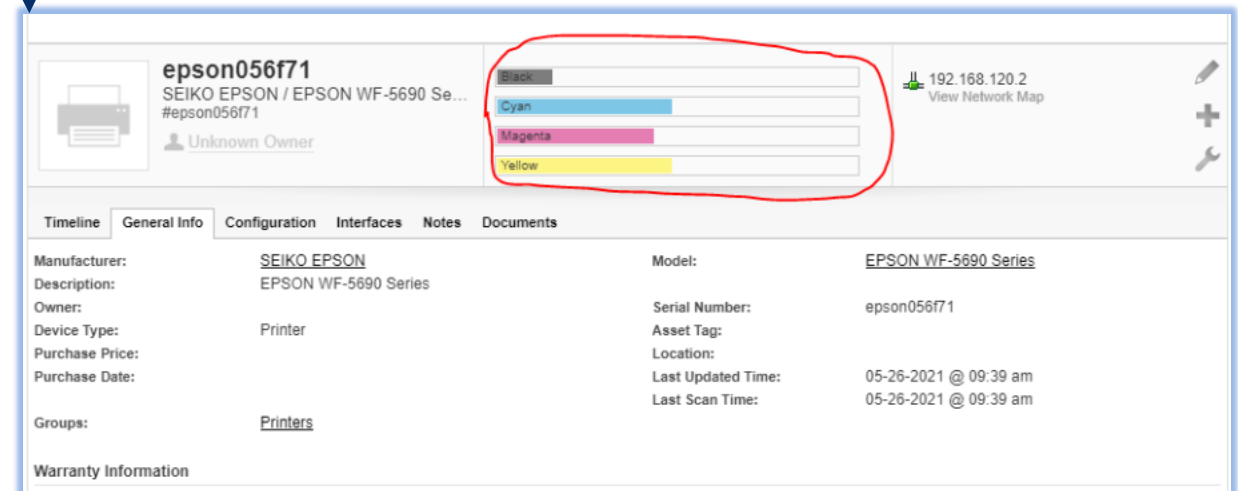
# Skenovanie aktív zo siete

## 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.














The screenshot displays the Spiceworks interface for a printer asset. The asset name is 'epson056f71', identified as a 'SEIKO EPSON / EPSON WF-5690 Series' printer with serial number '#epson056f71'. The owner is listed as 'Unknown Owner'. The IP address is '192.168.120.2'. A red circle highlights the ink level indicators for Black, Cyan, Magenta, and Yellow. Below the asset details, there is a 'General Info' tab with fields for Manufacturer (SEIKO EPSON), Model (EPSON WF-5690 Series), Owner, Device Type (Printer), Purchase Price, and Purchase Date. Other fields include Serial Number (epson056f71), Asset Tag, Location, Last Updated Time (05-26-2021 @ 09:39 am), and Last Scan Time (05-26-2021 @ 09:39 am). The 'Groups' field is set to 'Printers'.

# 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 priradujú sa automaticky pri skenovaní podľa protokolu alebo typu zariadenia.

## Stored Passwords

The credentials for devices on your network

			+ Add Account ...	
	WMI	(0)		
	SSH	(0)		
	SNMP	(0)		
	SNMPv2c	(0)		
	SNMPv3	(0)		
	Enable	(0)		
	ESX/vSphere	(0)		
	HTTP	(0)		
	iLO	(0)		
	Telnet	(0)		
	vPro	(0)		

Username	<input type="text" value="domain\username"/>
Password	<input type="password"/> <input type="button" value="show"/>
Description	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

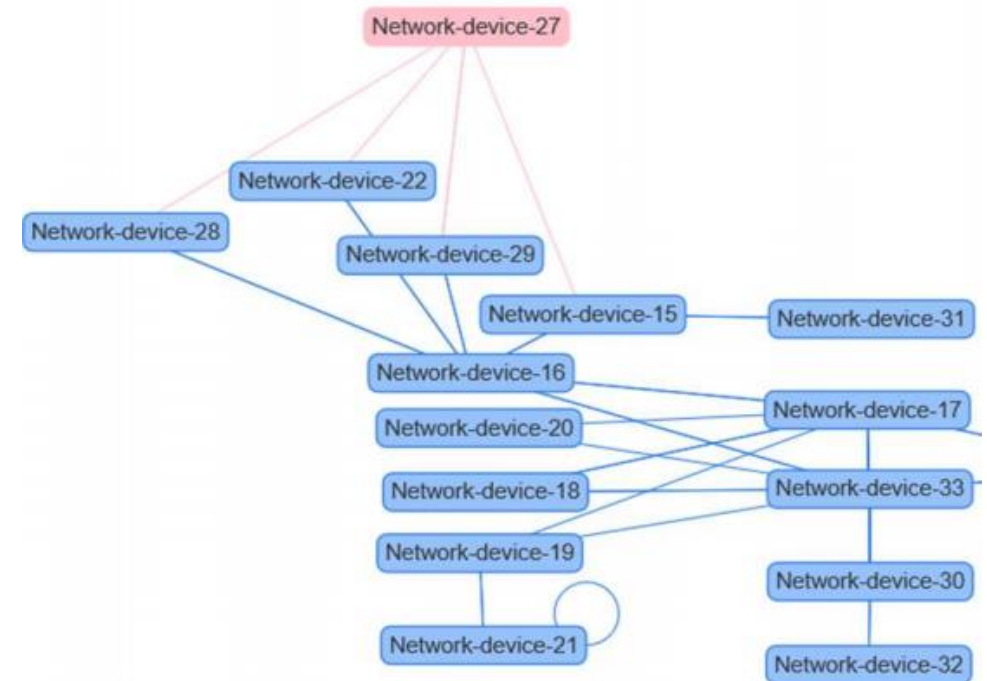


# Inventarizačný nástroj - LibreNMS

# 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

*System 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.

## Výhody

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

## Nevýhody

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

## 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

Please note the minimum supported PHP version is 8.2

Install Required Packages

Ubuntu 24.04

Ubuntu 22.04

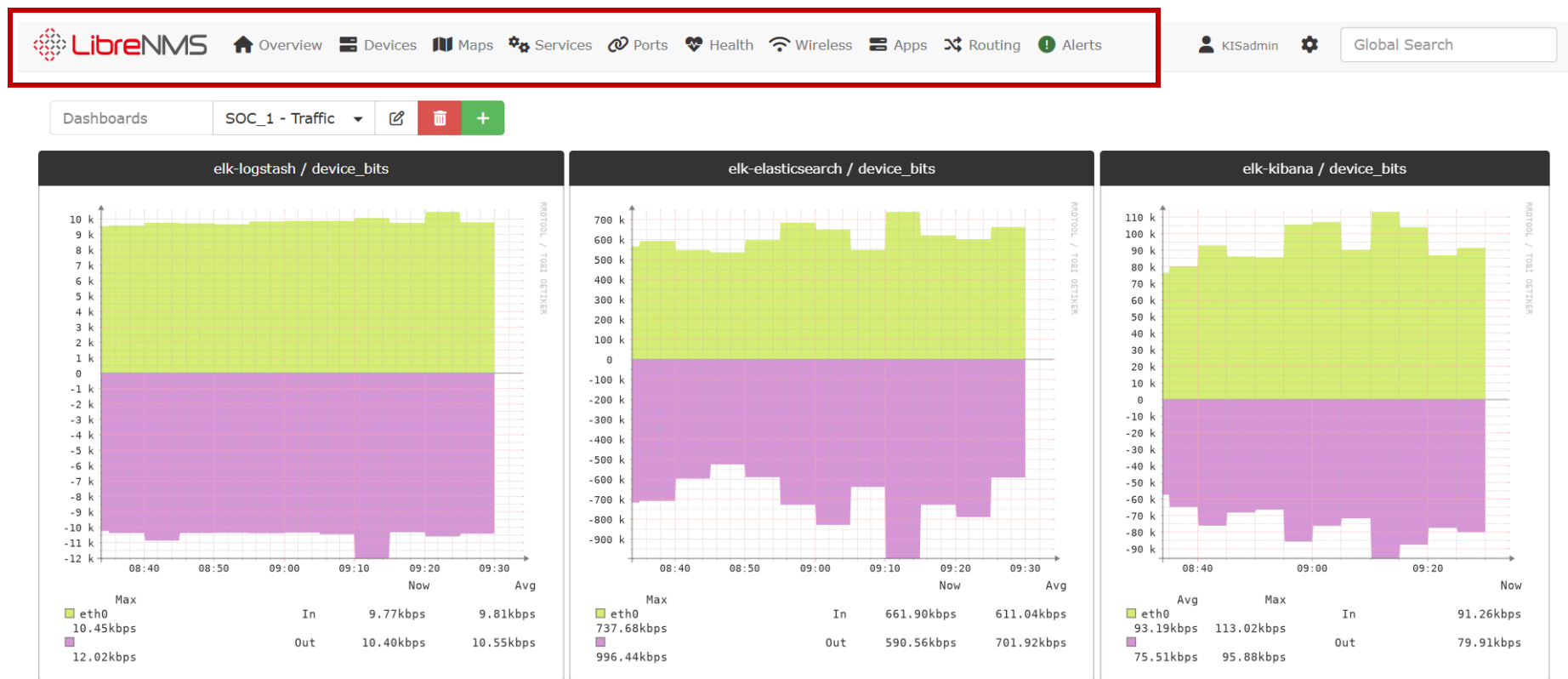
CentOS 8

Debian 12

Debian 13

# Webové používateľské rozhranie

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

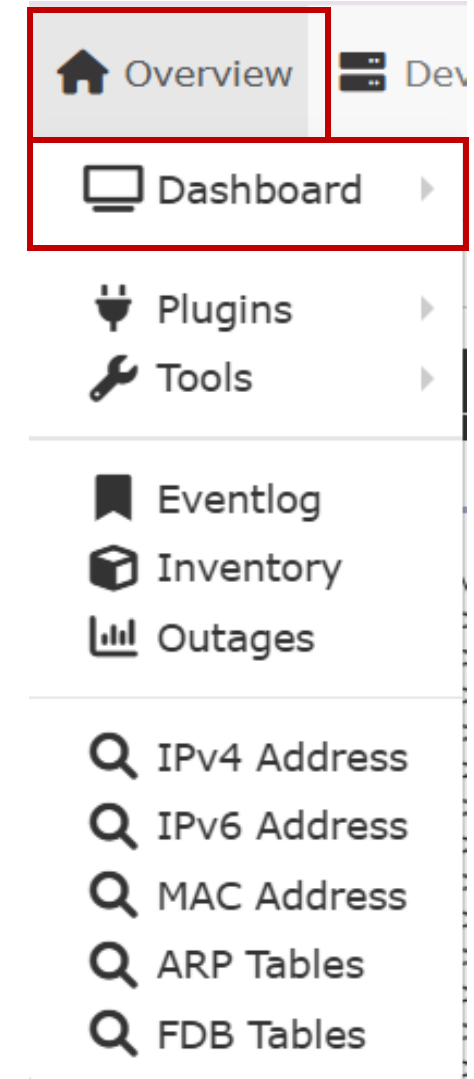


# Hlavné menu - Overview



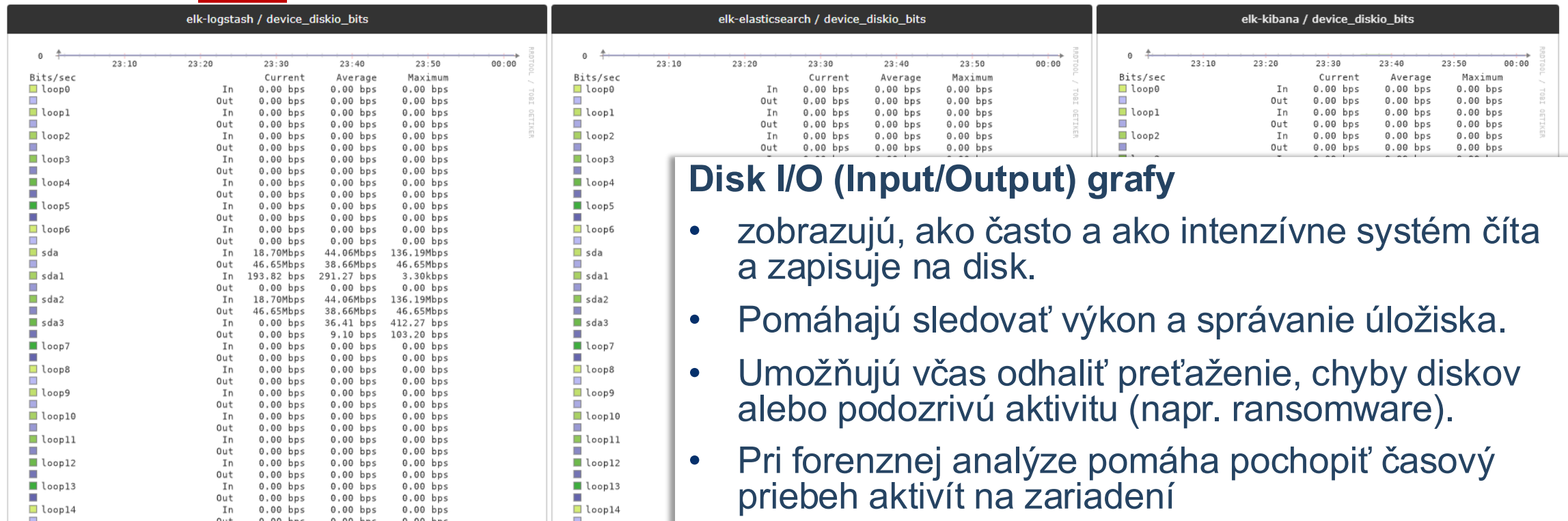
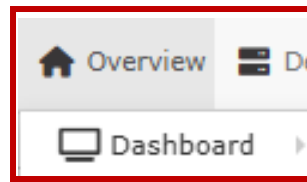
## Overview (prehľad systému):

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



## Bezpečnostný význam:

→ rýchla detekcia prevádzkových problémov - preťaženia, výpadkov alebo podozrivého správania.

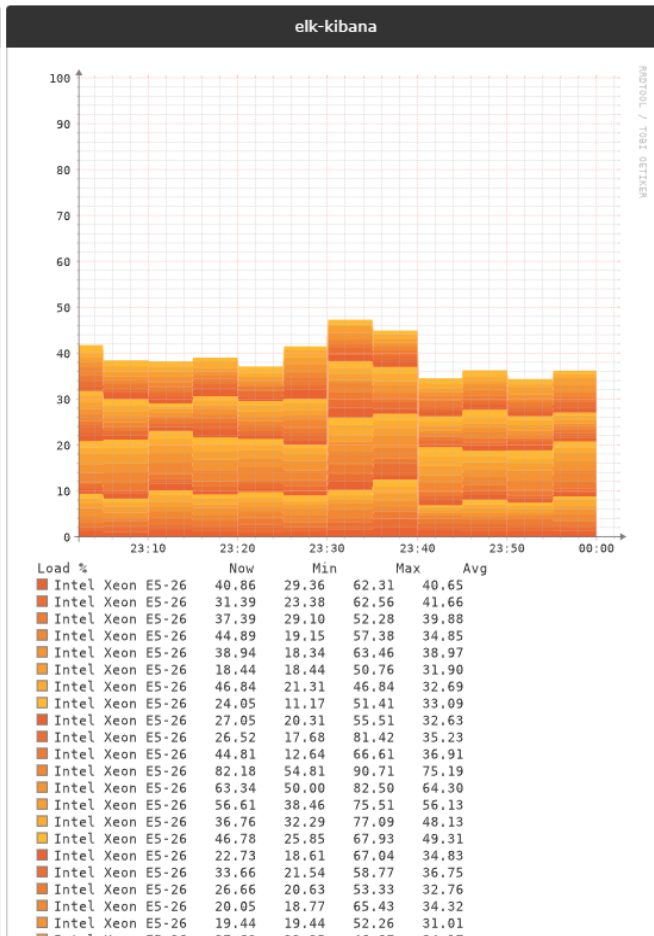
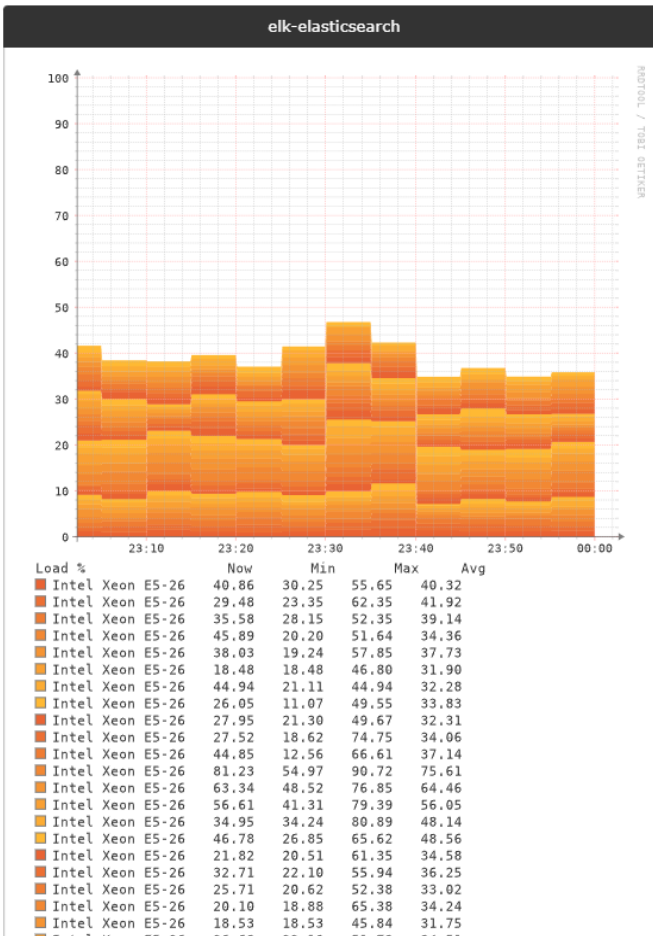
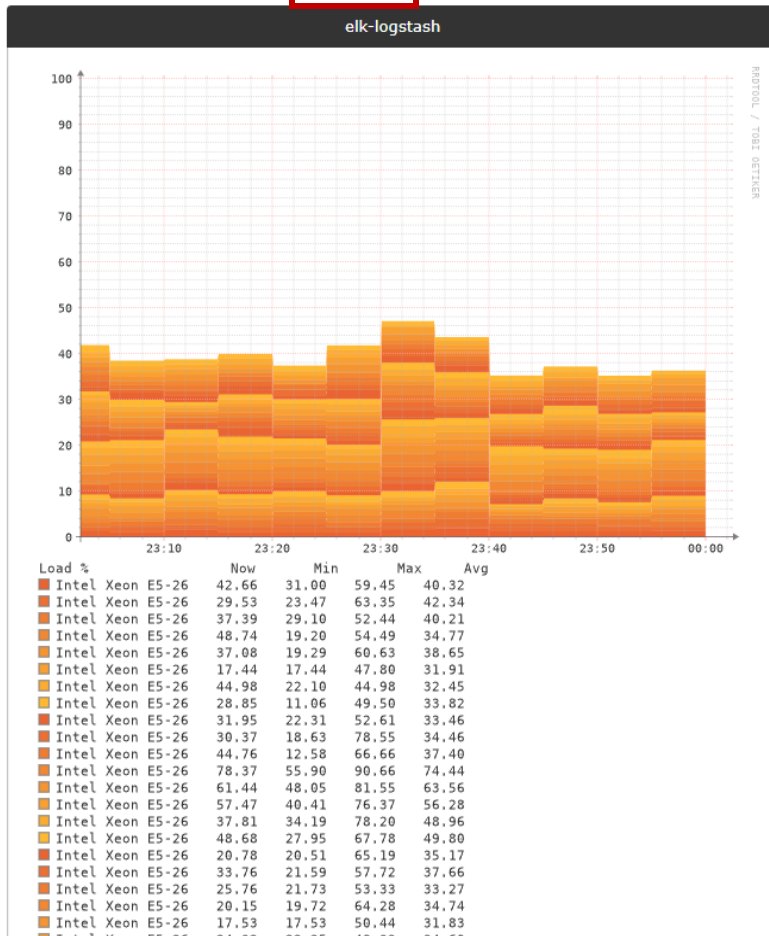
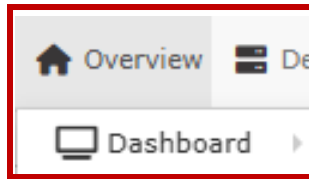


## Disk I/O (Input/Output) grafy

- 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).

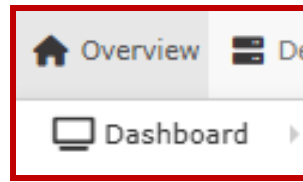
# LibreNMS

## Využitie CPU

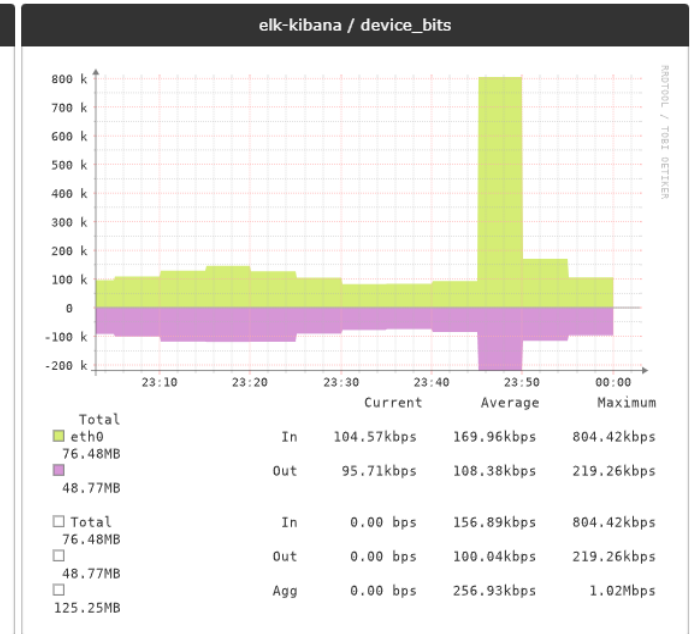
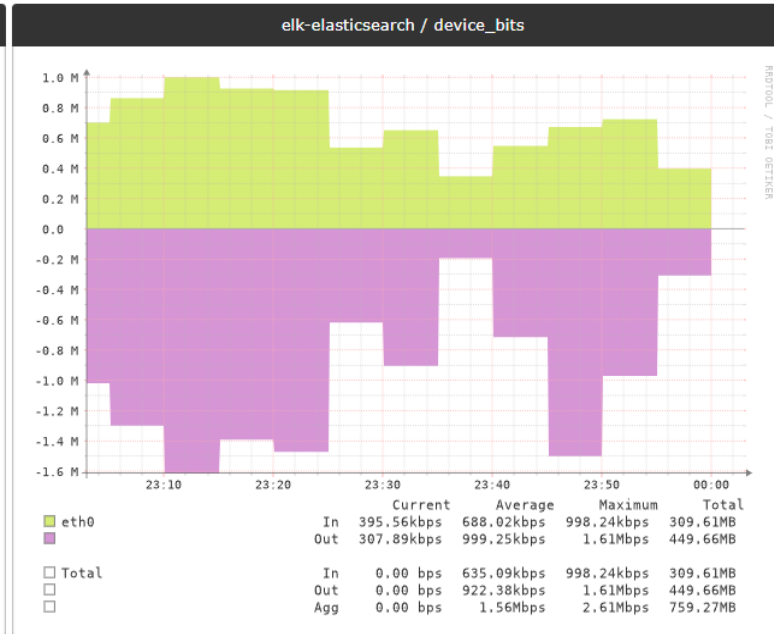
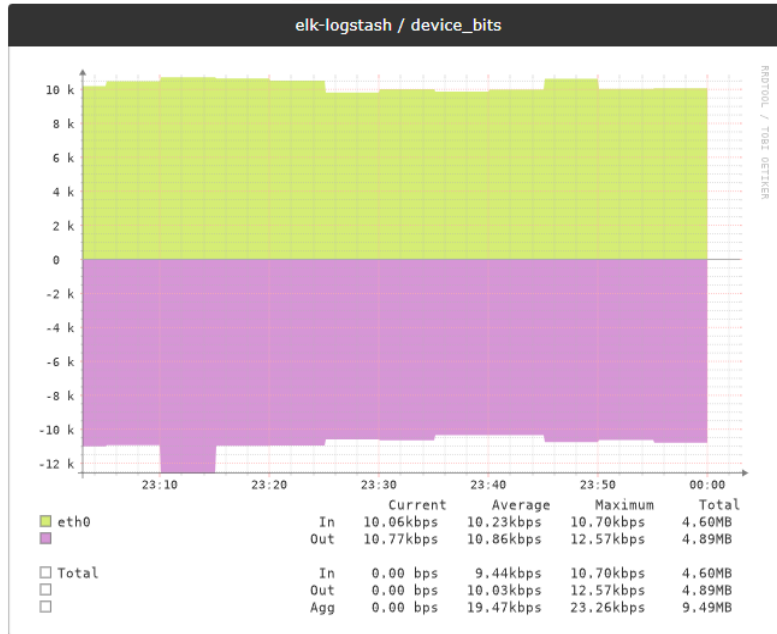


# LibreNMS

## Siet'ová prevádzka



Dashboards SOC\_1 Traffic



# LibreNMS Eventlog



LibreNMS Overview | Devices | Maps | Services | Ports | Health | Wireless | Apps | Routing | Alerts | KISadmin | Global Search

Eventlog | Dashboard | Plugins | Tools | Eventlog | Inventory | Outages | Filter | Search | 50 | [Grid Icon]

Timestamp	Type	Hostname	Message	User
2026-01-28 23:51:53	down	ra212	Device status changed to Down from snmp check.	System
2026-01-28 23:51:53	stp	ra212	STP designated root changed: 001ec9905caa >	System
2026-01-28 23:51:53	Gi0/52	ra212	ifVlan: -> 1	System
2026-01-28 23:51:53	Gi0/51	ra212	ifVlan: -> 1	System
2026-01-28 23:51:53	Gi0/50	ra212	ifVlan: 1 -> NULL	System
2026-01-28 23:51:53	Gi0/49	ra212	ifVlan: -> 1	System
2026-01-28 23:51:53	Gi0/46	ra212	ifVlan: -> 1	System
2026-01-28 23:51:53	Gi0/45	ra212	ifVlan: -> 1	System
2026-01-28 23:51:53	Gi0/44	ra212	ifVlan: 138 -> NULL	System
2026-01-28 23:51:53	Gi0/42	ra212	ifVlan: 138 -> NULL	System
2026-01-28 23:51:53	Gi0/41	ra212	ifVlan: -> 135	System

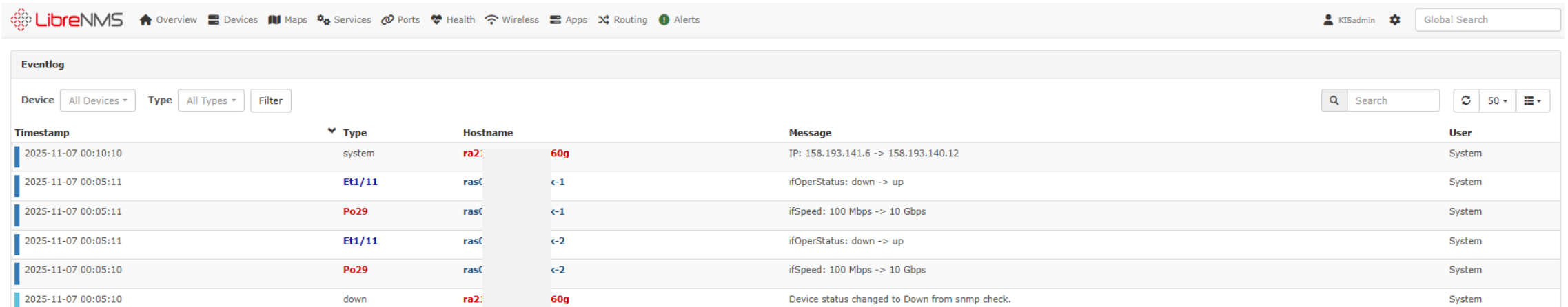
## .Overview - Logs

- 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.

# .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 <code>eventlog</code> )	log súbory alebo databáza syslog servera
Použitie	prehľad o stave zariadení a ich zmien	detailná forenzná analýza, bezpečnostné udalosti



The screenshot shows the LibreNMS Eventlog interface. At the top, there is a navigation bar with the LibreNMS logo and various menu items: Overview, Devices, Maps, Services, Ports, Health, Wireless, Apps, Routing, and Alerts. On the right side of the navigation bar, there is a user profile for 'KISadmin' and a 'Global Search' input field.

The main content area is titled 'Eventlog'. It features a filter section with 'Device' set to 'All Devices', 'Type' set to 'All Types', and a 'Filter' button. To the right of the filter section, there is a search input field, a refresh button, and a dropdown menu set to '50' items.

The event log is displayed as a table with the following columns: Timestamp, Type, Hostname, Message, and User. The table contains several entries:

Timestamp	Type	Hostname	Message	User
2025-11-07 00:10:10	system	ra21	IP: 158.193.141.6 -> 158.193.140.12	System
2025-11-07 00:05:11	Et1/11	rasC	ifOperStatus: down -> up	System
2025-11-07 00:05:11	Po29	rasC	ifSpeed: 100 Mbps -> 10 Gbps	System
2025-11-07 00:05:11	Et1/11	rasC	ifOperStatus: down -> up	System
2025-11-07 00:05:10	Po29	rasC	ifSpeed: 100 Mbps -> 10 Gbps	System
2025-11-07 00:05:10	down	ra21	Device status changed to Down from snmp check.	System

# LibreNMS Inventár



LibreNMS Overview

Maps Services Ports Health Wireless Apps Routing Alerts

KISadmin Global Search

Inventory

Dashboard

Part Description Serial No Device All Devices Search

Plugins

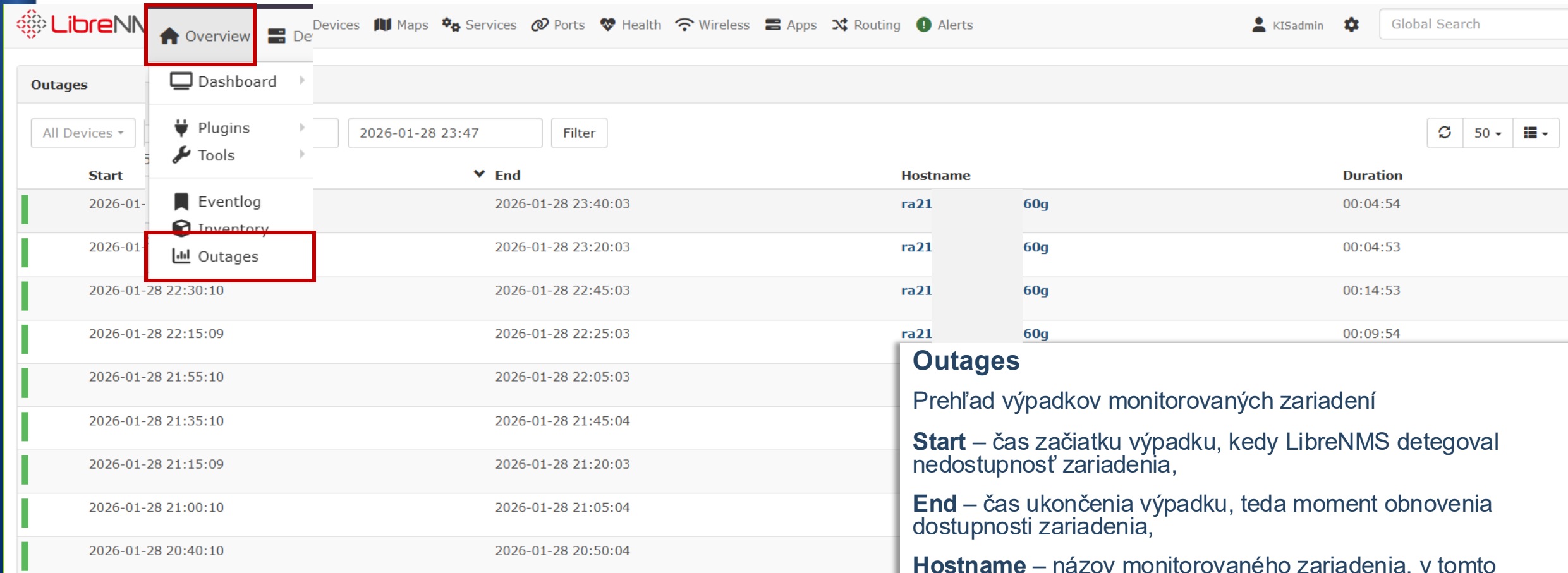
Tools

Eventlog

Inventory

Outages

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 Overview

Devices Maps Services Ports Health Wireless Apps Routing Alerts

KISadmin Global Search

Outages

All Devices

2026-01-28 23:47 Filter

Start	End	Hostname	Duration	
2026-01-28 23:40:03	2026-01-28 23:40:03	ra21	60g	00:04:54
2026-01-28 23:20:03	2026-01-28 23:20:03	ra21	60g	00:04:53
2026-01-28 22:30:10	2026-01-28 22:45:03	ra21	60g	00:14:53
2026-01-28 22:15:09	2026-01-28 22:25:03	ra21	60g	00:09:54
2026-01-28 21:55:10	2026-01-28 22:05:03			
2026-01-28 21:35:10	2026-01-28 21:45:04			
2026-01-28 21:15:09	2026-01-28 21:20:03			
2026-01-28 21:00:10	2026-01-28 21:05:04			
2026-01-28 20:40:10	2026-01-28 20:50:04			

### 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.

# Nájdanie 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
<b>Auto-Discovery</b>	<b>Pridanie do zoznamu</b>	<b>Detail zariadenia</b>
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 zariadení 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

# Nájdanie 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.

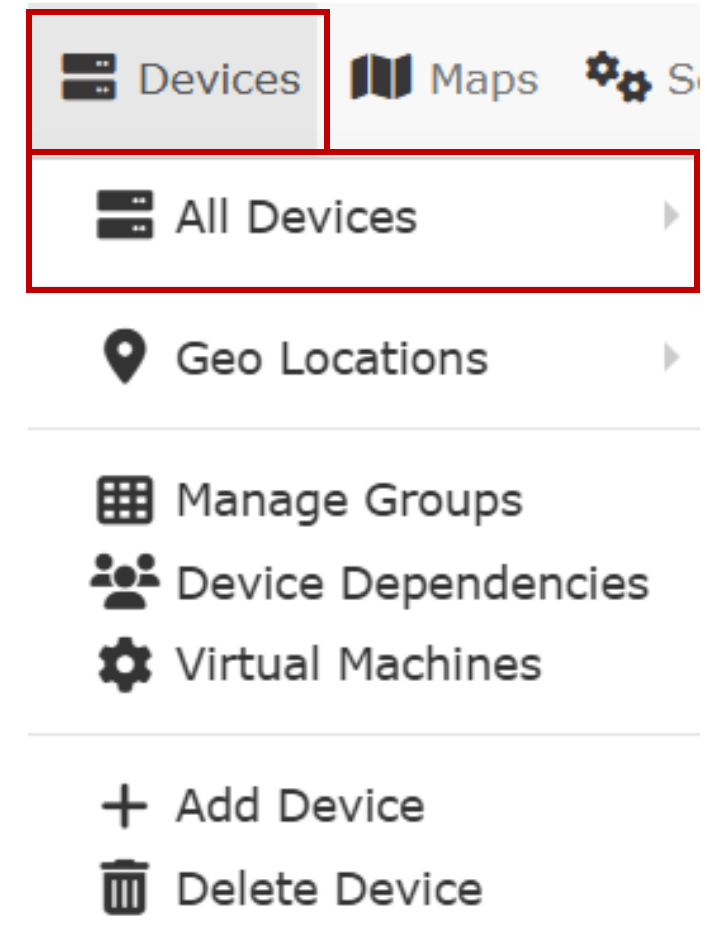
# Hlavné menu - Devices

## 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.

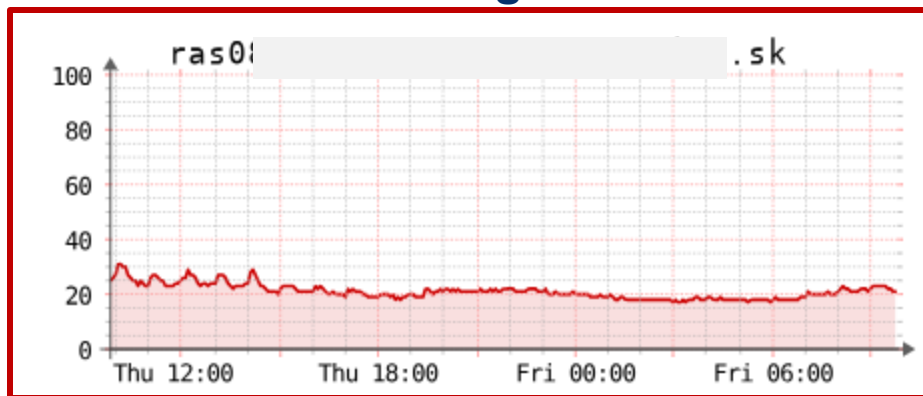


# Hlavné menu - Devices

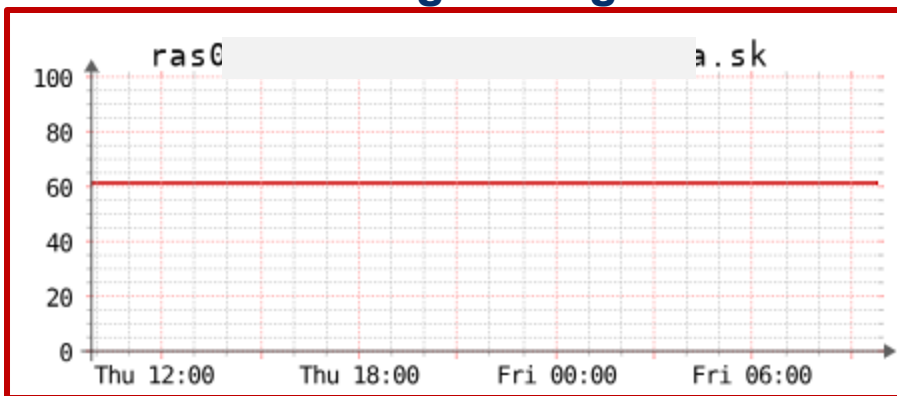
## Zobrazenie podsekcie All devices

S.	Id	M.	Vendor	Device	Metrics	Platform	Operating System	Time	Location	Actions
62				ras0158.	a.sk 57 5	Catalyst 3750G (WS-C3750G-48TS-S)	Cisco IOS 15.0(2)SE11 (IPSERVICESK9)	1mo 2d 22h		
40				rb00158.	a.sk 55 5	Catalyst 3560G (WS-C3560G-48TS-S)	Cisco IOS 12.2(55)SE12 (IPBASEK9)	4mos 3w 6d		
59				rc02158.	a.sk 34 5	Cat37xx Stacking	Cisco IOS 12.2(50)SE5 (IPBASEK9)	10mos 2w 20h		
47				ra32158.	a.sk 35 5	Catalyst 2960X (WS-C2960X-24TS-L)	Cisco IOS 15.2(2)E6 (UNIVERSALK9)	10mos 2w 19h		
60				ras0158.	a.sk 62 5	Cat37xx Stacking	Cisco IOS 15.0(2)SE11 (IPSERVICESK9)	10mos 1w 1h		
63				ras0158.	za.sk 47 17	Catalyst 3750E (WS-C3750E-24TD-E)	Cisco IOS 15.0(2)SE11 (UNIVERSALK9)	10mos 2w 20h		

monitoring CPU



monitoring storage



- ☰ Devices
- ☰ Maps
- ☰ All Devices
- 📍 Geo Locations
- 🗃️ Manage Groups
- 👤 Device Dependencies
- ⚙️ Virtual Machines
- + Add Device
- 🗑️ Delete Device

Lists: Basic | Detail **Graphs: Bits** | CPU | Load | Memory | Uptime | Storage | Disk I/O | Poller | Ping | Temperature

Bits Remove Search | Remove Header

From 2025-11-06 00:04 To 2025-11-07 00:04 Update



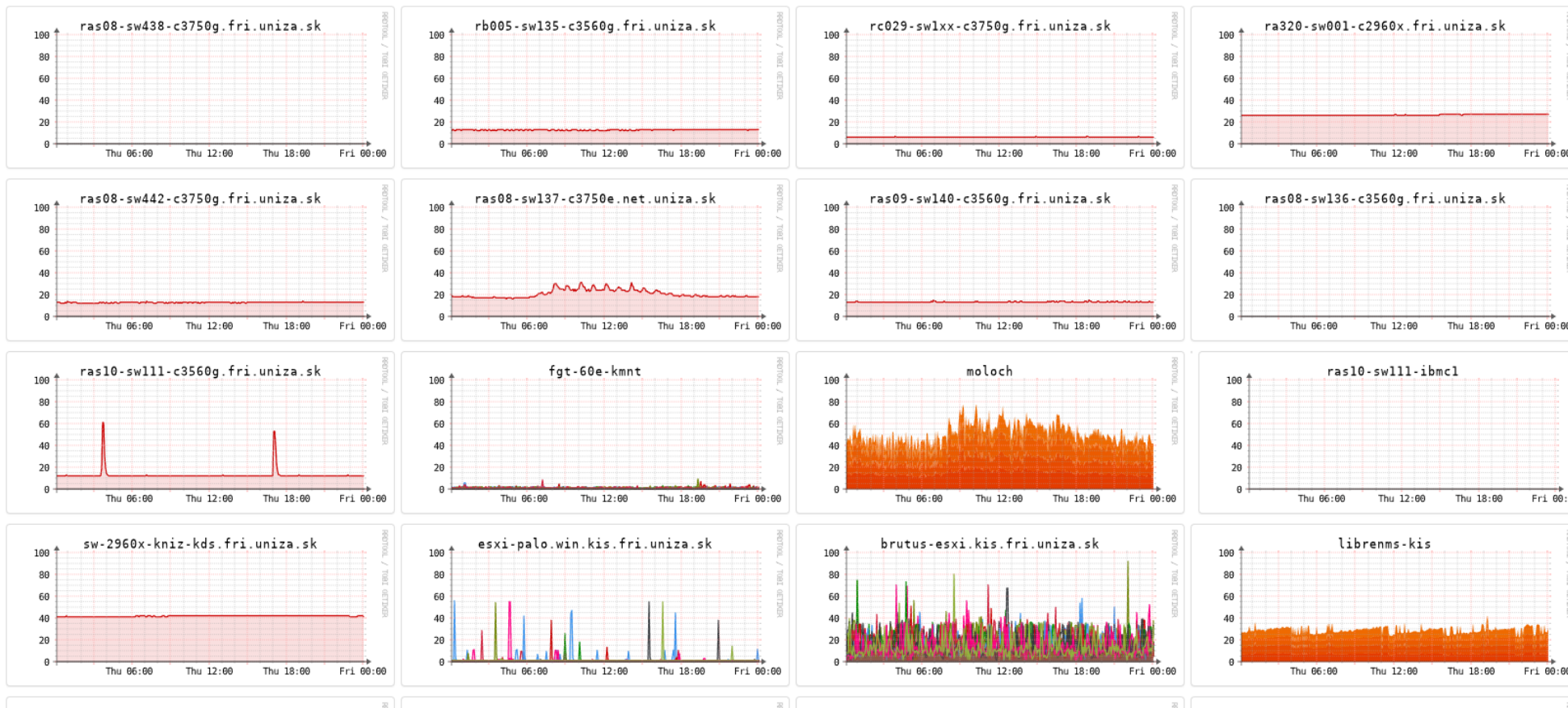
- Devices**  Maps  Services
- All Devices** ▶
- Geo Locations ▶
- Manage Groups
- Device Dependencies
- Virtual Machines
- + Add Device
- Delete Device

# Zariadenia - Zat'azhenie CPU

Lists: Basic | Detail **Graphs: Bits | CPU | Load | Memory | Uptime | Storage | Disk I/O | Poller | Ping | Temperature**

From 2025-11-06 00:05 To 2025-11-07 00:05 Update

Processor Remove Search | Remove Header

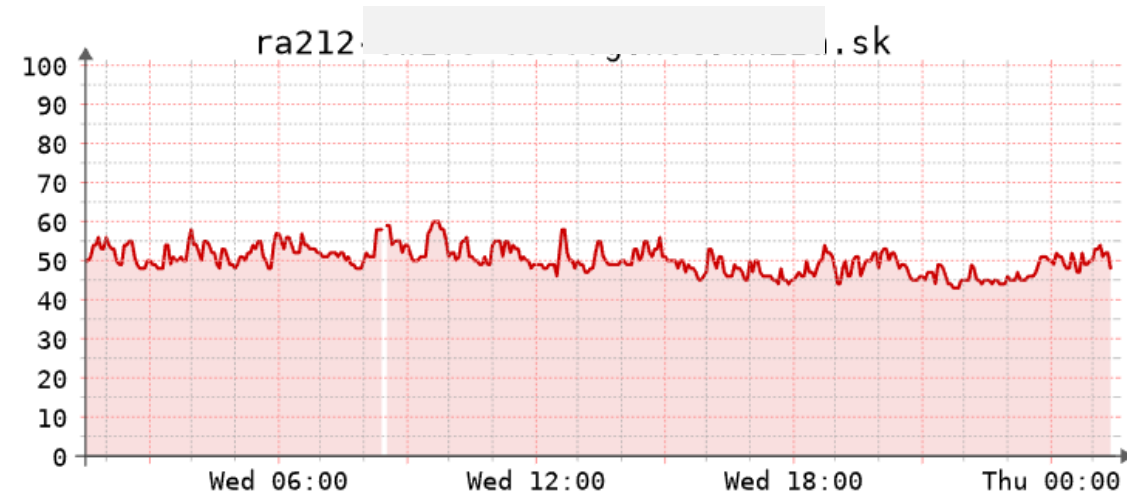
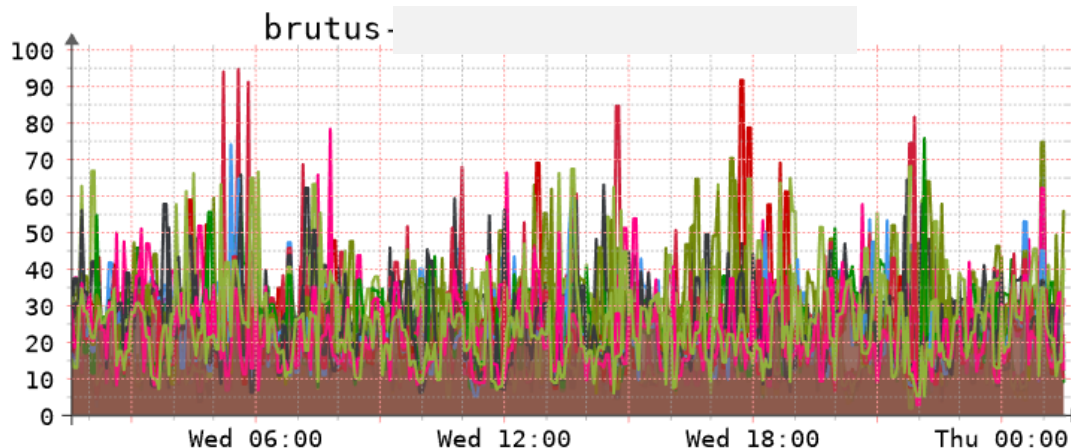


- Devices
- Maps
- All Devices
- Geo Locations
- Manage Groups
- Device Dependencies
- Virtual Machines
- + Add Device
- Delete Device

# Zariadenia - Zat'azenie CPU

Lists: Basic | Detail **Graphs: Bits | CPU | Load | Memory | Uptime | Storage | Disk I/O | Poller | Ping | Temperature**

Processor Remove Search | Remove Header



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

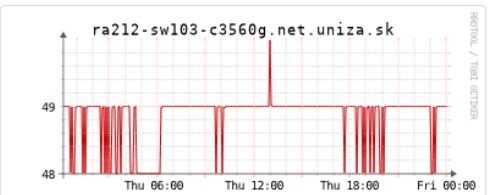
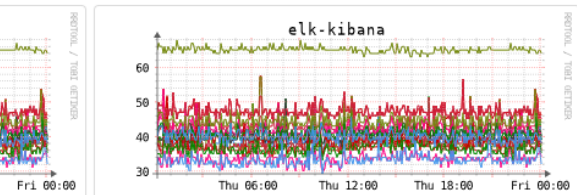
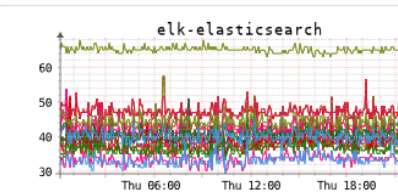
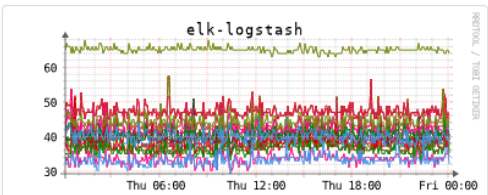
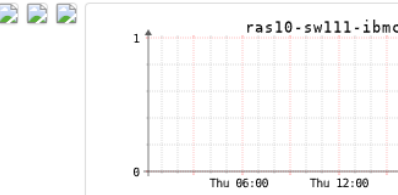
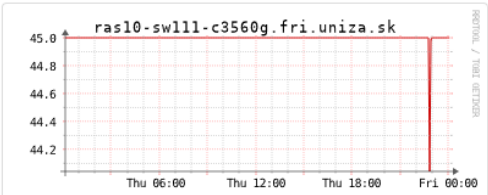
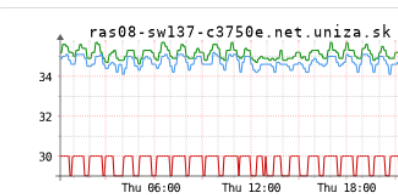
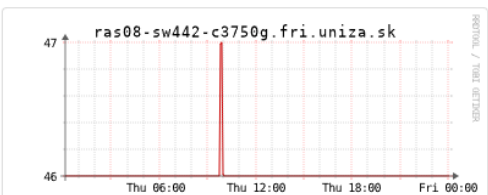
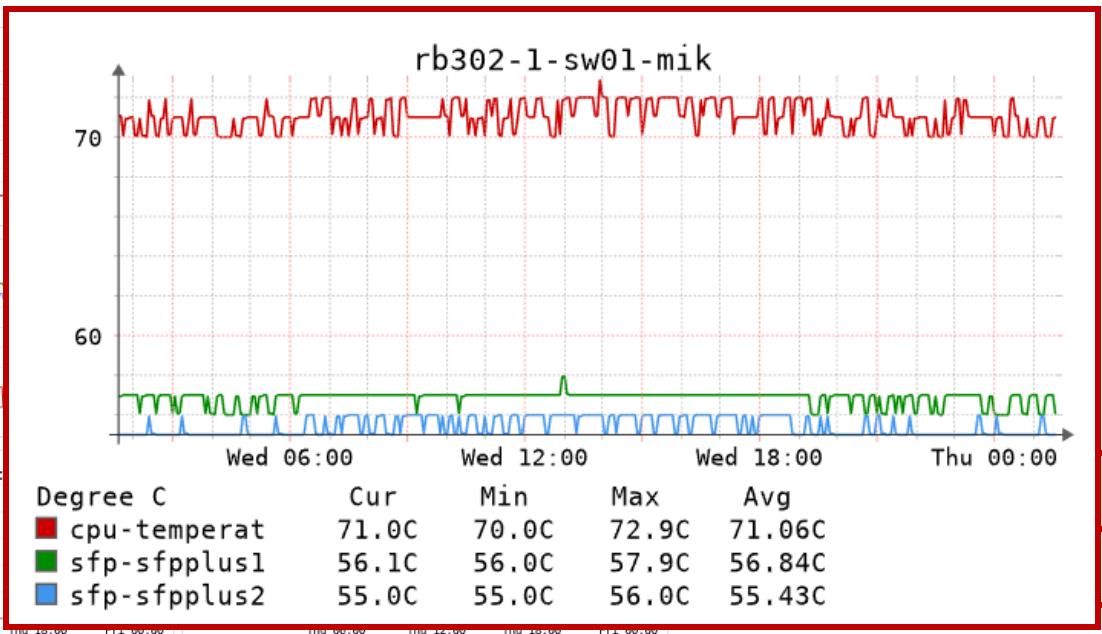
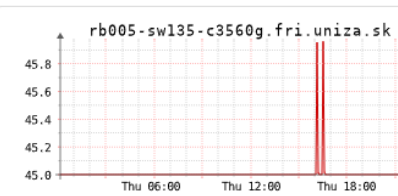
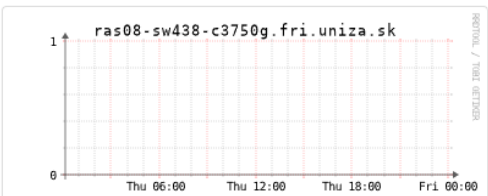
- Devices Maps S
- All Devices**
- Geo Locations
- Manage Groups
- Device Dependencies
- Virtual Machines
- + Add Device
- Delete Device

RRDTOOL / TOBI OETIKER

[Lists: Basic](#) | [Detail](#)
**Graphs: Bits** | [CPU](#) | [Load](#) | [Memory](#) | [Uptime](#) | [Storage](#) | [Disk I/O](#) | [Poller](#) | [Ping](#) | **Temperature**

[Temperature](#)
[Remove Search](#) | [Remove Header](#)

From  To



- [Devices](#)
- [Maps](#)
- [All Devices](#)
- [Geo Locations](#)
- [Manage Groups](#)
- [Device Dependencies](#)
- [Virtual Machines](#)
- [+ Add Device](#)
- [Delete Device](#)

# Zariadenia - Lokácia zariadení

LibreNMS Overview **Devices** Maps Settings Ports Health Wireless Apps Routing Alerts KISAdmin Global Search

Locations **All Devices**

- Geo Locations**
  - All Locations
  - FRI serverovna, CO5
  - FRI serverovna, RAS09
  - KIS FRI serverovna, B355
  - RA212
  - Rack, Room, Building, City, Country [Lat, Lon]
  - RAS08-VM303-Proxmox
  - RAS10
  - RB003
  - RB255
  - RB301
  - RB302
  - RB303
  - Serverovna FRI A
  - Serverovna FRI, CO5
  - Sitting on the Dock of the Bay
  - Unknown
  - xcp-Janka
- Manage Groups
- Device Dependencies
- Virtual Machines
- + Add Device
- Delete Device

Location	Devices	Down	Actions
FRI serverovna, CO5	2	0	Traffic Edit Delete
FRI serverovna, RAS09	0	0	Traffic Edit Delete
KIS FRI serverovna, B355	3	0	Traffic Edit Delete
RA212	1	0	Traffic Edit Delete
Rack, Room, Building, City, Country [Lat, Lon]	1	0	Traffic Edit Delete
RAS08-VM303-Proxmox	1	0	Traffic Edit Delete
RAS10	1	1	Traffic Edit Delete
RB003	1	0	Traffic Edit Delete
RB255	1	0	Traffic Edit Delete
RB301	1	0	Traffic Edit Delete
RB302	3	0	Traffic Edit Delete
RB303	0	0	Traffic Edit Delete
Serverovna FRI A	1	0	Traffic Edit Delete
Serverovna FRI, CO5	0	0	Traffic Edit Delete
Sitting on the Dock of the Bay	1	0	Traffic Edit Delete
Unknown	4	0	Traffic Edit Delete
xcp-Janka	2	0	Traffic Edit Delete
xcp-Janka	2	1	Traffic Edit Delete

Showing 1 to 17 of 17 entries

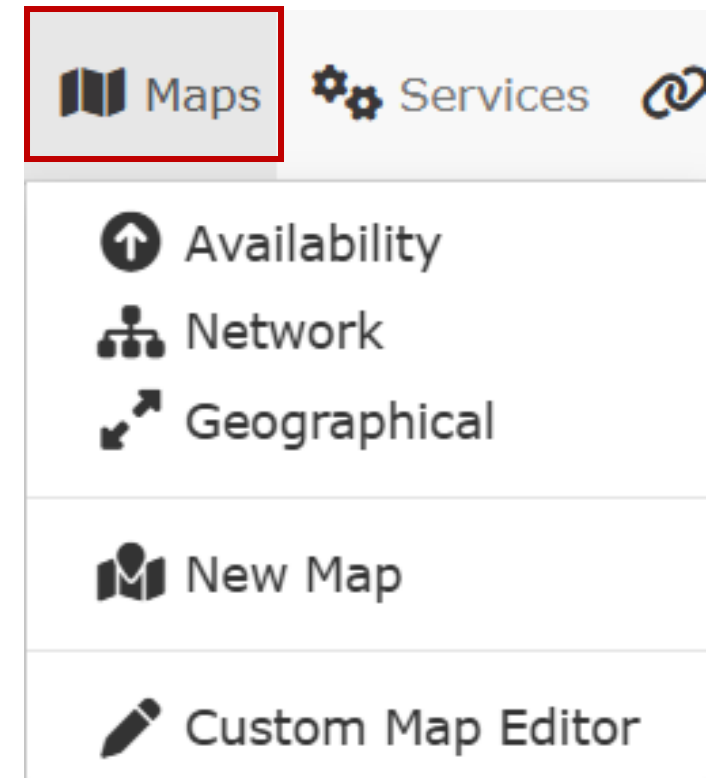
# Hlavné menu - Maps

## 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





# Hlavné menu - Maps

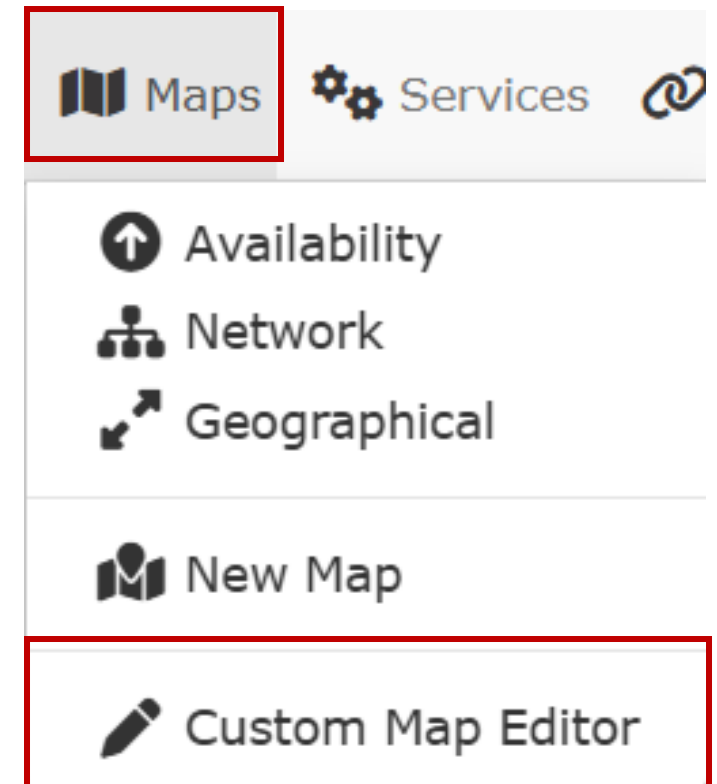
The screenshot displays the LibreNMS 'Maps' menu on the left, with 'Network' selected. The main area shows a network topology map with various devices connected. A red box highlights the 'ras10-sw111-c3' device, which is expanded to show detailed statistics:

- Device Traffic:** Two line graphs showing traffic volume over time. The left graph covers Thursday 12:00 to Friday 00:00, and the right graph covers Saturday 25 Oct to Wednesday 29 Oct. The y-axis ranges from -1.0 M to 1.0 M.
- CPU Usage:** Two line graphs showing CPU usage percentage over time. The left graph covers Thursday 12:00 to Friday 00:00, and the right graph covers Saturday 25 Oct to Wednesday 29 Oct. The y-axis ranges from 0 to 100.
- Memory Usage:** Two line graphs showing memory usage in MB over time. The left graph covers Thursday 12:00 to Friday 00:00, and the right graph covers Saturday 25 Oct to Wednesday 29 Oct. The y-axis ranges from 0 to 70 M.

A text box at the bottom right explains: "Po priložení kurzora na zariadenie, sa nám zobrazia jeho grafické štatistiky ako Device Traffic, CPU Usage a Memory Usage".

# Custom Map Editor

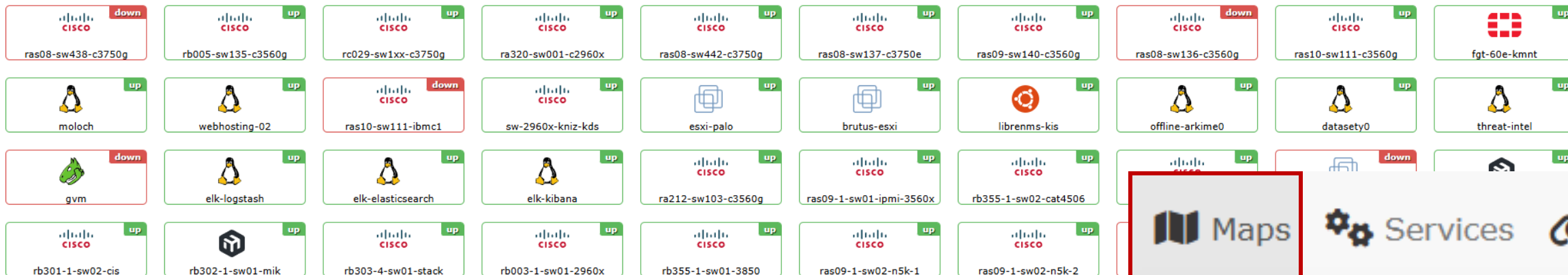
- Možnosť vytvoriť vlastnú mapu
- definujeme:
  - Názov, šírku a výšku mapy v pixeloch, zarovnanie uzlov – po pridaní nových zariadení ich táto funkcia zarovná do neviditeľnej mriežky - vylepší to custom vzhľad mapy
- Pridanie zariadenia:
  - Po pridaní zariadenia nás libreNMS vyzve aby sme si vybrali 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



# .Maps - Dostupné zariadenia

Availability map for only devices

Total hosts up: 32 warn: 0 down: 6



📖 Maps
⚙️ Services
🔗

---

⬆️ Availability

🌐 Network

📍 Geographical

---

🗺️ New Map

---

✍️ Custom Map Editor

# Hlavné menu – ports, health, alerts

## Ports

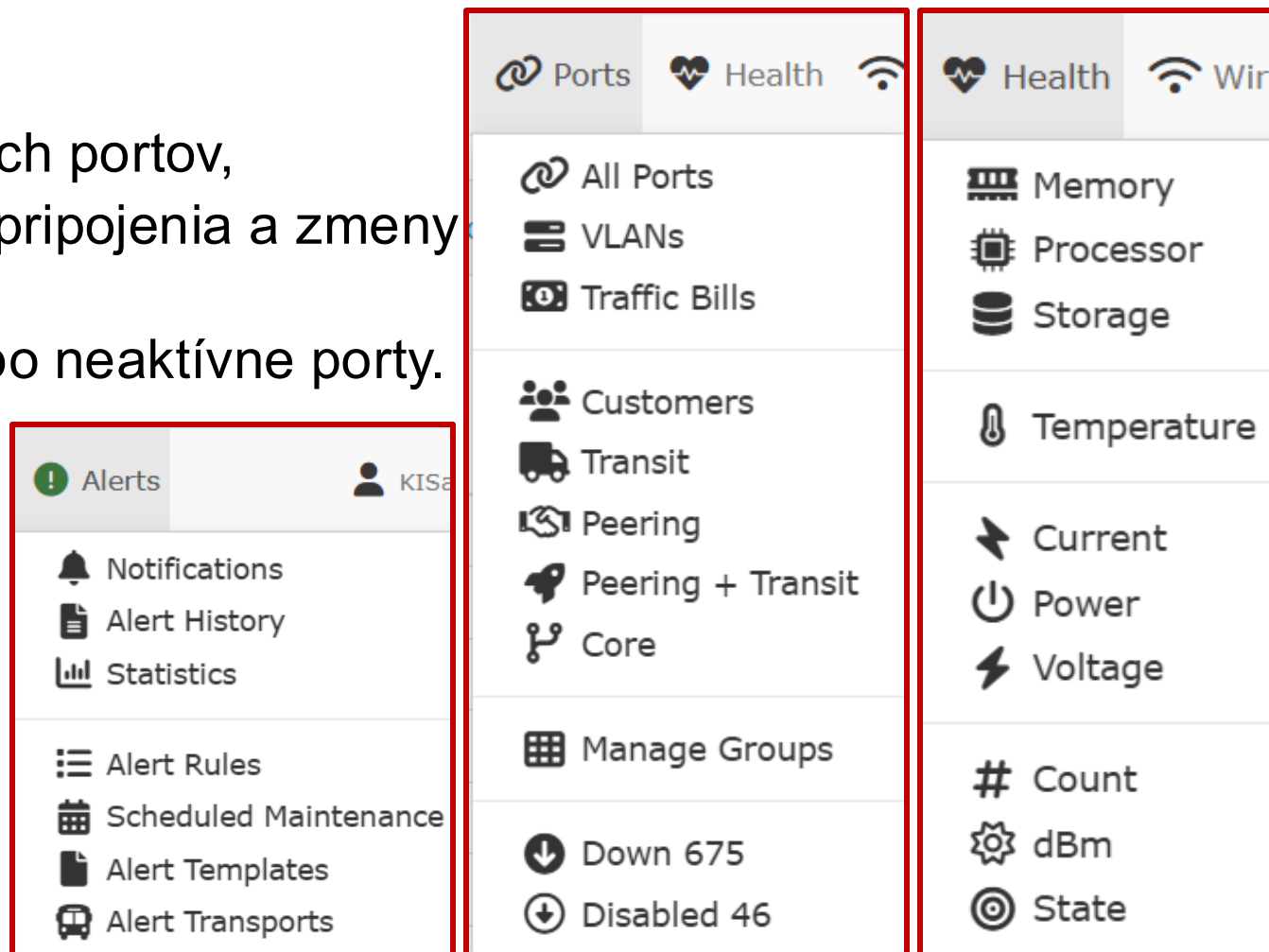
- sleduje stav a priepustnosť sieťových portov,
- deteguje výpadky, neautorizované pripojenia a zmeny konfigurácie,
- umožňuje identifikovať chybné alebo neaktívne porty.

## 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.



The screenshot displays the LibreNMS main menu with three panels highlighted by red boxes:

- Alerts Panel:** Alerts (KISa), Notifications, Alert History, Statistics, Alert Rules, Scheduled Maintenance, Alert Templates, Alert Transports.
- Ports Panel:** Ports, Health, Wi-Fi, All Ports, VLANs, Traffic Bills, Customers, Transit, Peering, Peering + Transit, Core, Manage Groups, Down 675, Disabled 46.
- Health Panel:** Health, Wi-Fi, Memory, Processor, Storage, Temperature, Current, Power, Voltage, Count, dBm, State.

LibreNMS Overview Devices Maps Services **Ports** Health less Apps Routing Alerts KISadmin Global Search

Ports lists » **Basic** | Detail Graphs » Bits | Unicast Packets | Non-Unicast Packets

**All Ports** | [Export CSV](#) | [Update URL](#) | [Search](#) | [Header](#) | [Bulk actions](#) » [Purge all deleted](#)

All Devices Hostname All States All Speeds

Port Description All Locations Ignored Disabled Deleted

VLANs Traffic Bills

Device	Port	Status Changed	Speed	In	Out	Media	Description	Actions	
rb3	bond1	14 days	10Gbps	21.47Kbps	10.13Kbps	ieee8023adLag	bond1	! ✎	
rb3	bond1-sfp	14 days	10Gbps	15.49Kbps	1.14Kbps	ieee8023adLag	bond1-sfp	! ✎	
rb3	bridge1	14 days		3.09Kbps	848bps	bridge	bridge1	! ✎	
rb3	bridge1	14 days		1.31Kbps	888bps	bridge	bridge1	! ✎	
bru	vmnic0	10 months	1Gbps	27.92Kbps	1.94Kbps	Ethernet	01:00.0	! ✎	
vm	za.sk	vmnic0	2 months	100Mbps	26.28Kbps	704bps	Ethernet	01:00.0	! ✎
bru	vmnic1	10 months				Ethernet	01:00.1	! ✎	
esx	vmnic1	10 months	10Gbps	2.45Kbps	608bps	Ethernet	65:00.1	! ✎	
esx	vmnic2	10 months				Ethernet	04:00.0	! ✎	

# LibreNMS

## Virtuálne siete



VLAN 1

Devices Ports

All Ports  
VLANs  
Traffic Bills

Search [ ] [ ] 10 [ ] [ ]

Device	Ports	Local Name	Type	MTU
rb35!	25	default	ethernet	
rb35!	1	default	ethernet	
ras0!	15	default	ethernet	
rb30!	1	default	ethernet	
rb00!	5	default	ethernet	
rb30!	8	default	ethernet	
rb35!	25	default	ethernet	
ras0!	43	VLAN0001	ethernet	
ras0!	49	VLAN0001	ethernet	
rb00!	23	default	ethernet	

Showing 1 to 10 of 22 entries

# LibreNMS Health - Memory



Memory  
Processor  
Storage

Device	Memory	Used	Usage
libre	Physical memory	1.53 GiB / 7.75 GiB 6.22 GiB	20%
libre	Virtual memory	7.47 GiB / 11.75 GiB 4.28 GiB	64%
libre	Memory buffers	370.25 MiB / 7.75 GiB 7.39 GiB	5%
libre	Cached memory	5.33 GiB / 7.75 GiB 2.41 GiB	69%
libre	Shared memory	44.03 MiB / 7.75 GiB 7.7 GiB	1%
libre	Swap space	251.5 MiB / 4 GiB 3.75 GiB	6%
ras0	32 port Modular Universal Port Supervisor in Fixed Module-1 Memory	1.69 GiB / 7.87 GiB 6.18 GiB	21%
ras0	32 port Modular Universal Port Supervisor in Fixed Module-1 Memory	1.69 GiB / 7.87 GiB 6.18 GiB	21%
rb35	Processor	249.82 MiB / 776.06 MiB 526.23 MiB	32%
rb35	reserve Processor	88 B / 100 KiB 99.92 KiB	0%
rb3C	Processor	69.51 MiB / 349.16 MiB 279.65 MiB	20%
rb3C	I/O	11.99 MiB / 32 MiB 20.01 MiB	37%
rb3C	Driver text	40 B / 1 MiB 1023.96 KiB	0%
rb0C	Processor	19.81 MiB / 74.85 MiB 55.04 MiB	26%

# Health - Processor

LibreNMS Overview Devices Maps Services Ports **Health** Wireless Apps Routing Alerts KISadmin Global Search

Health » Memory | **Processor** | Storage | Temperature | Current | Power | Voltage | C

Memory Processor Storage

Search 50

Device	Processor	Usage
rasl	Processor 1	8% 92%
rb0l	Processor 1	13% 87%
rc0:	Processor 1	6% 94%
ra3:	1	26% 74%
rasl	Processor 1	12% 88%
rasl	.sk Processor 1	19% 81%
rasl	.sk Processor 1	13% 87%
rasl	.sk Processor 1	12% 88%
ras:	.sk Processor 1	17% 83%
fgt-	CPU Core 1	0% 100%
fgt-	CPU Core 2	1% 99%
fgt-	CPU Core 3	1% 99%
fgt-	CPU Core 4	1% 99%

# LibreNMS

## Health - storage



LibreNMS Overview Devices Maps Services Ports Health Wireless Apps Routing Alerts KISadmin Global Search

Health » Memory | Processor | **Storage** | Temperature | Current | Power | Voltage | C

Memory Processor Storage

Search 50

Device	Storage	Used	Usage
ras	.sk flash1(flash1):	17.45 MiB / 31.01 MiB 13.56 MiB	56%
rbC	.sk flash(flash):	16.73 MiB / 31.01 MiB 14.28 MiB	54%
rc0	.sk flash3(flash3):	9.88 MiB / 31.01 MiB 21.13 MiB	32%
ra3	.sk flash1(flash1):	103 MiB / 116.53 MiB 13.53 MiB	88%
ras	.sk flash4(flash4):	17.46 MiB / 31.01 MiB 13.55 MiB	56%
ras	a.sk flash1(flash1):	33.72 MiB / 55 MiB 21.28 MiB	61%
ras	.sk flash(flash):	12.18 MiB / 31.01 MiB 18.83 MiB	39%
ras	.sk flash(flash):	12.19 MiB / 31.01 MiB 18.82 MiB	39%
ras	.sk flash(flash):	12.52 MiB / 31.01 MiB 18.49 MiB	40%
mo	/	182.26 GiB / 182.28 GiB 16 MiB	100%
mo	/dev/shm	0 B / 24.51 GiB 24.51 GiB	0%
mo	/mnt/data	11.3 TiB / 11.9 TiB 614.42 GiB	95%
mo	/run	441.82 MiB / 4.9 GiB 4.47 GiB	9%

# LibreNMS

## Wireless - AP



LibreNMS Overview Devices Maps Services Ports Health **Wireless** Apps Routing Alerts

KISadmin Global Search

Wireless > APs | Clients Graphs | No Graphs

Search 50

Device	Sensor	Current	Low Limit	High Limit
fgt-60e-kmnt	Connected APs	0	-	-

Showing 1 to 1 of 1 entries

# LibreNMS

## VRF, OSPF zariadenia



Routing > **VRFs (2)** | OSPF (4) | CEF (11)

VRFs > **Basic** | Graphs: Bits | Unicast Packets | Non-Unicast Packets | Errors | Etherlike

VRF	RD	Interfaces
<b>Mgmt-vrf</b>		rb355-1-sw01-3850.kis.fri.uniza.sk Gi0/0
<b>mgmtVrf</b>		rb355-1-sw02-cat4506.kis.fri.uniza.sk Fa1

LibreNMS [Overview](#) [Devices](#) [Maps](#) [Services](#) [Ports](#) [Health](#) [Wireless](#) [Apps](#) **Routing** [Alerts](#) KISadmin

Routing > VRFs (2) | **OSPF (4)** | CEF (11)

Device	Router ID	Status	ABR	ASBR	Areas	Ports(Enabled)	Neighbours
ras08-s	1! 2	enabled	false	true	1	4(4)	5
ra212-s	1! 1	enabled	false	true	1	29(29)	5
fgt-60e	1! 3.36	enabled	false	false	1	2(2)	3
ra212-s	1! 1	enabled	false	true	1	0(0)	5

# .Routing - Cisco CEF

**Cisco zariadenie** (napr. router alebo L3 switch) s povoleným SNMP, dokáže načítať a zobrazit' 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
<b>FIB entries</b>	počet záznamov vo Forwarding Information Base – t. j. koľko smerovacích ciest má zariadenie predpočítaných
<b>Adjacency entries</b>	počet susedných zariadení alebo rozhraní, pre ktoré sú pripravené cesty
<b>CEF switching statistics</b>	počty prepnutých paketov, chybovosť, CPU využitie pri forwarding operáciách
<b>CEF interface states</b>	stav CEF na jednotlivých sieťových rozhraniach (či je zapnutý/vypnutý, aktívny/neaktívny)

Routing » VRFs (2) | OSPF (4) | **CEF (11)**

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

The logo for GLPI (Gestionnaire Libre de Parc Informatique) features the letters 'GLPI' in a bold, blue, sans-serif font. A stylized blue swoosh or underline is positioned beneath the 'G' and extends slightly to the left.

**Inventarizačný nástroj - GLPI**

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

# 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.

# Prehľad klúčových 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:

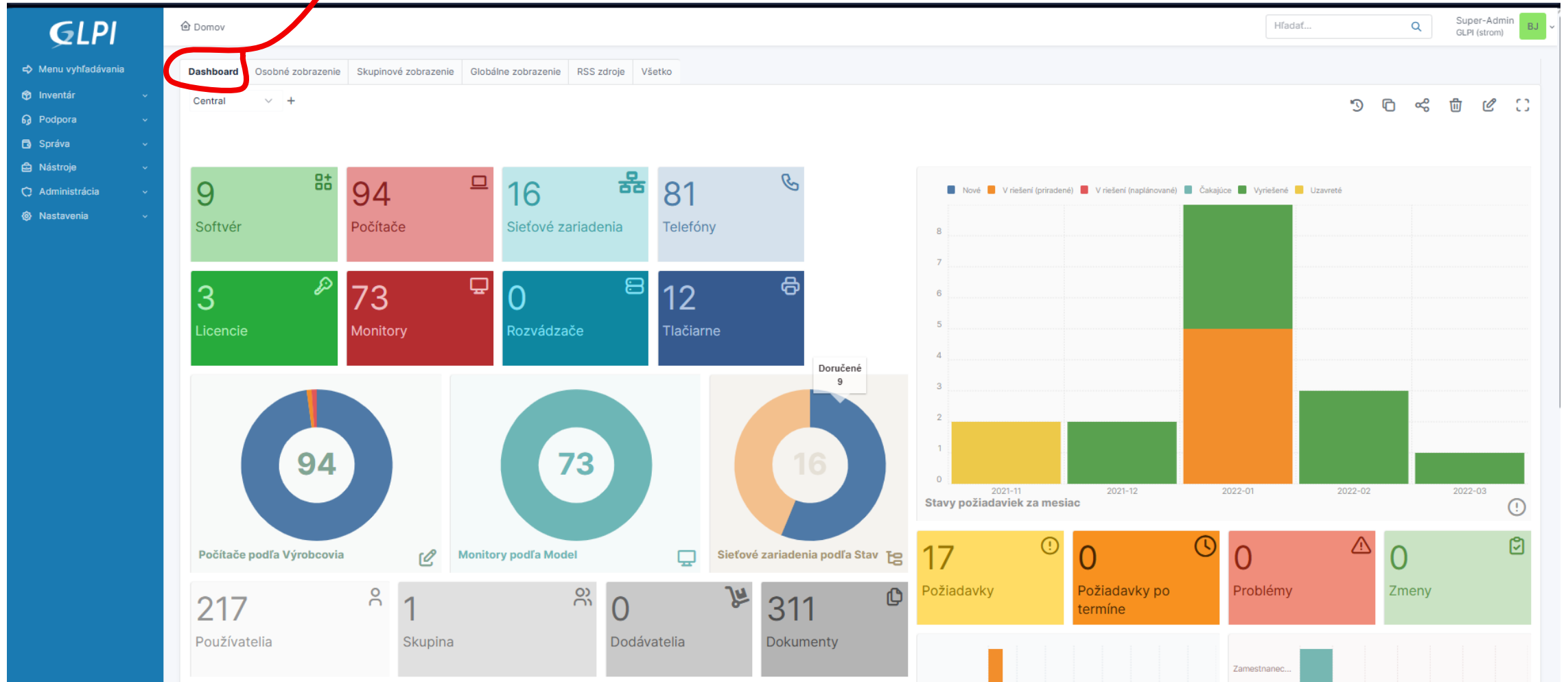
- automaticky zisťuje a zapisuje zariadenia (PC, tlačiarne, servery, sieťové prvky),
- zhromažďuje informácie o hardvéri, softvéri, OS, IP adresách, používateľoch,
- podporuje **agentov** – malé programy inštalované na klientoch, ktoré pravidelne posielajú dáta,
- umožňuje **nasadenie softvéru** alebo skriptov na diaľku,
- dáta sa ukladajú priamo do **GLPI databázy**.

### ▪ Prínosy:

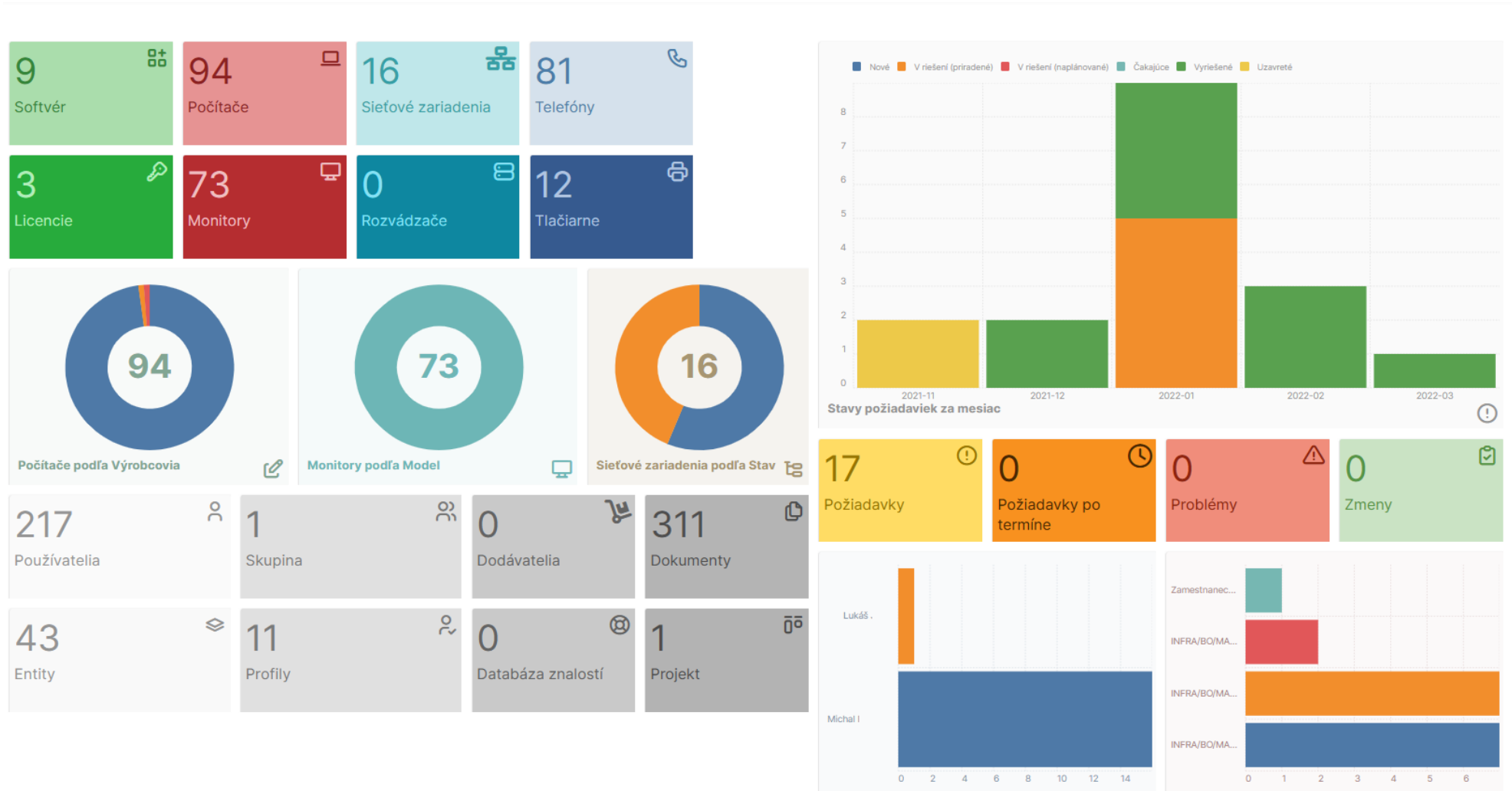
- úplná a automatická inventarizácia,
- integrácia s GLPI (ITSM, Helpdesk, Asset management),
- **open-source alternatíva k drahým komerčným riešeniam ako SCCM.**



# GLPI Dashboard



# GLPI Dashboard



# Dashboard – Inventár (Assets)

Domov / Inventár
Hľadať...
Super-Admin  
GLPI (strom) BJ

Menu vyhľadávania


**Inventár**

- Dashboard
- Počítače
- Monitory
- Softvér
- Sieťové zariadenia
- Zariadenia
- Tlačiarne
- Náplne
- Spotrebný materiál
- Telefóny
- Rozvádzače
- Skrine
- Napájacie PDU lišty
- Pasívne zariadenia
- Nespravované zariadenia
- Káble
- Základná doska položky

Assets

94 Počítače	9 Softvér	16 Sieťové zariadenia	0 Rozvádzače	0 Skrine
73 Monitory	3 Licencie	12 Tlačiarne	0 Napájacie PDU lišty	81 Telefóny

<p>Počítače podľa Stav</p> <p>94</p>	<p>Počítače podľa Výrobcovia</p> <p>Raspberry Pi</p> <p>Apple</p> <p>bez</p> <p>0 40 80</p>	<p>Počítače podľa Typ</p> <p>94</p>	<p>Sieťové zariadenia podľa</p> <p>bez</p> <p>CISCO</p> <p>0 4 8</p>	<p>Monitory podľa Výrobcovia</p> <p>73</p>
--------------------------------------	---	-------------------------------------	--	--



- Menu vyhľadávania
- Inventár
- Podpora
- Správa
  - Licencie**
  - Rozpočty
  - Dodávatelia
  - Kontakty
  - Zmluvy
  - Dokumenty
  - Linky
  - Certifikáty
  - Dátové centrá
  - Klastre
  - Domény
  - Aplikácie
  - Databázy
- Nástroje
- Administrácia
- Nastavenia

Domov / Správa / Licencie
+ Pridať
Hľadať
Uložené hľadania
Sablóny

Super-Admin GLPI (strom) BJ

<< < > >>
Licencia - Microsoft Windows 11 Pro
GLPI Akcie 2/3 >>

**Licencia**

- Licencie
- Súhrn
- Položky
- Správa
- Zmluvy
- Dokumenty
- Databáza znalostí
- Požiadavky
- Problémy
- Zmeny
- Poznámky
- Certifikáty
- História 2
- Všetko

**Softvér** Microsoft Windows 11 Pro

Název Microsoft Windows 11 Pro

Ako potomok ----- i +

Typ licencie ----- i +

Výrobca ----- i +

Sériové číslo

Používateľ ----- i

Komentáre

Používaná verzia -----

Počet 3

Expirácia ?

Stav ----- i +

Umiestnenie ----- i +

Zodpovedný technik ----- i

Zodpovedná skupina ----- i +

Inventárne číslo

Skupina ----- i +

Obrázky


Súbory (15 MB max) i

Pretiahnite súbor sem, alebo ho načítajte

Zakúpená verzia -----

Umožniť prekročenie kvóty Nie

Vytvorené: 23-10-2024 07:40
Posledná aktualizácia: 23-10-2024 07:41



- Menu vyhľadávania
- Inventár
  - Dashboard
  - Počítače**
  - Monitory
  - Softvér
  - Sieťové zariadenia
  - Zariadenia
  - Tlačiarne
  - Náplne
  - Spotrebný materiál
  - Telefóny
  - Rozvádzače
  - Skrine
  - Napájacie PDU lišty
  - Pasívne zariadenia
  - Nespravované zariadenia
  - Káble
  - Základná doska položky
  - Firmvér položky

Domov / Inventár / Počítače


+ Pridať    Hľadať    Uložené hľadania    Šablóny

Hľadať...    Super-Admin GLPI (strom)    BJ

Akcie

NÁZOV	ENTITA	POUŽÍVATEL	TYP	SÉRIOVÉ ČÍSLO
<input type="checkbox"/> ASUS	GLPI ▶ BIT		Notebook	X09H05102B
<input type="checkbox"/> Asus ZenBook	GLPI ▶ BIT		ASUS	N0JX012100059
<input type="checkbox"/> Dell G5 5587	GLPI ▶ BIT		Notebook	R2
<input type="checkbox"/> Dell Inspiron	GLPI ▶ BIT			IG3
<input type="checkbox"/> Dell Inspiron	GLPI ▶ BIT		Dell	G3
<input type="checkbox"/> Dell Latitude	GLPI ▶ BIT		Notebook	F2
<input type="checkbox"/> Dell Latitude 3520	GLPI ▶ BIT		Notebook	:S3
<input type="checkbox"/> Dell latitude 5530	GLPI ▶ BIT		Notebook	S3
<input type="checkbox"/> Dell Latitude 5530	GLPI ▶ BIT			S3
<input type="checkbox"/> Dell Latitude 5540	GLPI ▶ BIT			<3
<input type="checkbox"/> Dell Latitude 5590	GLPI ▶ BIT		Notebook	R2
<input type="checkbox"/> Dell Latitude 7420	GLPI ▶ BIT			K3
<input type="checkbox"/> Dell Latitude E5530	GLPI ▶ BIT		Notebook	V1
<input type="checkbox"/> Dell Latitude E5530	GLPI ▶ BIT		Notebook	Y1
<input type="checkbox"/> Dell Latitude E5540	GLPI ▶ BIT		Notebook	I2

15 riadkov na stránku    Zobrazujem 16 až 30 z 94 riadkov    << < 1 2 3 4 ... > >>



Menu vyhľadávania

**Inventár**

- Dashboard
- Počítače
- Monitory
- Softvér
- Sieťové zariadenia**
- Zariadenia
- Tlačiarne
- Náplne
- Spotrebný materiál
- Telefóny
- Rozvádzače
- Skrine
- Napájacie PDU lišty
- Pasívne zariadenia
- Nespravované zariadenia
- Káble
- Základná doska položky
- Firmvér položky
- Procesor položky
- Pamäť položky
- Pevný disk položky
- Sieťová karta položky
- Mechanika položky
- Batéria položky
- Grafická karta položky

Domov / Inventár / Sieťové zariadenia

+ Pridať    🔍 Hľadať    ☆ Uložené hľadania    📄 Šablóny

Hľadať...    🔍    Super-Admin GLPI (strom)    BJ

Akcie

<input type="checkbox"/> NÁZOV	ENTITA	STAV	VÝROBCA	UMIESTNENIE	TYP	MODEL	FIRMVER	POSLEDNÁ AKTUALIZÁCIA
<input type="checkbox"/> Cisco Catalyst 9100AX	GLPI ▶ BIT	Doručené	CISCO	BIT - ZA	Access Point	Catalyst 9100AX		29-11-2024 09:10
<input type="checkbox"/> Cisco Catalyst 9100AX	GLPI ▶ BIT	Doručené	CISCO	BIT - ZA	Access Point	Catalyst 9100AX		29-11-2024 09:10
<input type="checkbox"/> Cisco Catalyst 9100AX	GLPI ▶ BIT	Doručené	CISCO	BIT - ZA	Access Point	Catalyst 9100AX		29-11-2024 09:10
<input type="checkbox"/> Cisco Catalyst 9100AX	GLPI ▶ BIT	Doručené	CISCO	BIT - ZA	Access Point	Catalyst 9100AX		29-11-2024 09:10
<input type="checkbox"/> Cisco Catalyst 9100AX	GLPI ▶ BIT	Doručené	CISCO	BIT - ZA	Access Point	Catalyst 9100AX		29-11-2024 09:10
<input type="checkbox"/> Cisco Catalyst 9100AX	GLPI ▶ BIT	Doručené	CISCO	BIT - ZA	Access Point	Catalyst 9100AX		29-11-2024 09:10
<input type="checkbox"/> Cisco Catalyst 9100AX	GLPI ▶ BIT	Doručené	CISCO	BIT - ZA	Access Point	Catalyst 9100AX		29-11-2024 09:10
<input type="checkbox"/> Cisco Catalyst 9100AX	GLPI ▶ BIT	Doručené	CISCO	BIT - ZA	Access Point	Catalyst 9100AX		29-11-2024 09:10
<input type="checkbox"/> Cisco Catalyst 9100AX	GLPI ▶ BIT	Doručené	CISCO	BIT - ZA	Access Point	Catalyst 9100AX		29-11-2024 09:10
<input type="checkbox"/> Cisco Catalyst 9100AX	GLPI ▶ BIT	Doručené	CISCO	BIT - ZA	Access Point	Catalyst 9100AX		29-11-2024 09:10
<input type="checkbox"/> Synology DiskStation DS420+	GLPI ▶ Welltis			Welltis > ZA(VUD)				01-07-2021 00:00
<input type="checkbox"/> Synology RackStation RS1219+	GLPI ▶ Welltis			Welltis > ZA(VUD)				01-07-2021 00:00
<input type="checkbox"/> TP-Link Deco	GLPI ▶ Welltis			Welltis > Centrala				17-10-2024 13:39
<input type="checkbox"/> TP-Link switch	GLPI ▶ Welltis			Welltis > Centrala				17-10-2024 13:39
<input type="checkbox"/> Ubiquiti UniFi Security Gateway Pro, router	GLPI ▶ Welltis			Welltis > Centrala				17-10-2024 13:39
<input type="checkbox"/> Ubiquiti UniFi Security Gateway Pro, router	GLPI ▶ Welltis			Welltis > ZA(VUD)				17-10-2024 13:40

15 riadkov na stránku      Zobrazujem 1 až 15 z 16 riadkov      << < 1 2 > >>

GLPI

- Menu vyhľadávania
- Inventár
  - Dashboard
  - Počítače
  - Monitory
  - Softvér
  - Siet'ové zariadenia
  - Zariadenia
  - Tlačiarne
  - Náplne
  - Spotrebný materiál
  - Telefóny
  - Rozvážače
  - Skrine
  - Napájacie PDU lišty
  - Pasívne zariadenia
  - Nespravované zariadenia
  - Káble
  - Základná doska položky
  - Firmvér položky
  - Processor položky
  - Pamäť položky
  - Pevný disk položky
  - Siet'ová karta položky
  - Mechanika položky
  - Batéria položky
  - Grafická karta položky

Domov / Inventár / Siet'ové zariadenia + Pridať Hľadať Uložené hľadania Šablóny

Hľadať... Super-Admin GLPI (strom) BJ

GLPI > BIT Podriadené entity Akcie 1/15 > >

**Siet'ové zariadenie - Cisco Catalyst 9100AX**

<b>Siet'ové zariadenie</b>	<p>Názov <input type="text" value="Cisco Catalyst 9100AX"/></p> <p>Umiestnenie <input type="text" value="BIT - ZA"/> <span style="float: right;">i +</span></p> <p>Zodpovedný technik <input type="text" value="-----"/> <span style="float: right;">i</span></p> <p>Zodpovedná skupina <input type="text" value="-----"/> <span style="float: right;">i +</span></p> <p>Číslo alternatívneho používateľského mena <input type="text"/></p> <p>Alternatívne používateľské meno <input type="text"/></p> <p>Popis systému <input type="text"/></p> <p>Používateľ <input type="text" value="infra"/> <span style="float: right;">i</span></p> <p>Skupina <input type="text" value="-----"/> <span style="float: right;">i +</span></p> <p>Komentáre <input type="text"/></p> <p>Zdroj aktualizácií <input type="text" value="-----"/> <span style="float: right;">i +</span></p>	<p>Stav <input type="text" value="Doručené"/> <span style="float: right;">i +</span></p> <p>Typ siet'ového zariadenia <input type="text" value="Access Point"/> <span style="float: right;">i +</span></p> <p>Výrobca <input type="text" value="CISCO"/> <span style="float: right;">i +</span></p> <p>Model <input type="text" value="Catalyst 9100AX"/> <span style="float: right;">i +</span></p> <p>Sériové číslo <input type="text" value="FC"/></p> <p>Inventárne číslo <input type="text"/></p> <p>SNMP prihlasovacie údaje <input type="text" value="-----"/> <span style="float: right;">i</span></p> <p>Sieť <input type="text" value="-----"/> <span style="float: right;">i +</span></p> <p>UUID <input type="text"/></p> <p>Pamäť (MB) <input type="text" value="0"/></p>
----------------------------	--	--

Presunúť do koša
Uložiť

Vytvorené: 29-11-2024 08:55 Posledná aktualizácia: 29-11-2024 09:10

Akcie

<input type="checkbox"/> NÁZOV	ENTITA	STAV	VÝROBCA	UMIESTNENIE	TYP	MODEL	POSLEDNÁ AKTUALIZÁCIA
<input type="checkbox"/> BROTHER DCP-1623WE	GLPI ▶ EUBA	Doručené	Brother	Centrála			12-08-2024 00:00
<input type="checkbox"/> Canon i-SENSYS MF461dw	GLPI ▶ EUBA	Doručené	Canon	Centrála			12-08-2024 00:00
<input type="checkbox"/> Canon i-SENSYS MF461dw	GLPI ▶ EUBA	Doručené	Canon	Centrála			12-08-2024 00:00
<input type="checkbox"/> Canon i-SENSYS MF461dw	GLPI ▶ EUBA	Doručené	Canon	Centrála			12-08-2024 00:00
<input type="checkbox"/> Canon i-SENSYS MF461dw	GLPI ▶ EUBA	Doručené	Canon	Centrála			12-08-2024 00:00
<input type="checkbox"/> Canon i-SENSYS MF461dw	GLPI ▶ Národné lesnícke centrum	Doručené	Canon	Centrála			19-08-2024 00:00
<input type="checkbox"/> Canon i-SENSYS MF752Cdw	GLPI ▶ EUBA	Doručené	Canon	Centrála			12-08-2024 00:00
<input type="checkbox"/> Canon i-SENSYS X 1440i MFP	GLPI ▶ EUBA	Doručené	Canon	Centrála			12-08-2024 00:00
<input type="checkbox"/> Canon i-SENSYS X C1533IF II	GLPI ▶ Národné lesnícke centrum	Doručené	Canon	Centrála			17-10-2024 14:15
<input type="checkbox"/> EPSON EcoTank L15150	GLPI ▶ EUBA	Doručené	Epson	Centrála			12-08-2024 00:00
<input type="checkbox"/> HP Color LaserJet Pro MFP 3302fdn	GLPI ▶ Správa NP Muránska Planina	Doručené	HP	Centrála			26-09-2024 00:00
<input type="checkbox"/> HP LaserJet Tank 1604w	GLPI ▶ EUBA	Doručené	HP	Centrála			12-08-2024 00:00

15 riadkov na stránku

Zobrazujem 1 až 12 z 12 riadkov

GLPI

- Menu vyhľadávania
- Inventár
  - Dashboard
  - Počítače
  - Monitory
  - Softvér
  - Sieťové zariadenia
  - Zariadenia
  - Tlačiarne**
  - Náplne
  - Spotrebný materiál
  - Telefóny
  - Rozvádzače
  - Skrine
  - Napájacie PDU lišty
  - Pasívne zariadenia
  - Nespravované zariadenia
  - Káble
  - Základná doska položky
  - Firmvér položky
  - Procesor položky
  - Pamäť položky
  - Pevný disk položky
  - Sieťová karta položky
  - Mechanika položky
  - Batéria položky
  - Grafická karta položky

Domov / Inventár / Tlačiarne

+ Pridať Q Hľadať Uložené hľadania Šablóny

Hľadať...

Super-Admin  
GLPI (strom) BJ

Tlačiareň - Canon i-SENSYS MF461dw

GLPI > EUBA Podriadené entity i Akcie v 2/12 > >>


Tlačiareň	
Analýza dopadov	Názov <input type="text" value="Canon i-SENSYS MF461dw"/>
Operačné systémy	Umiestnenie <input type="text" value="Centrála"/> i +
Softvér	Zodpovedný technik <input type="text" value="----"/> i
Náplne	Zodpovedná skupina <input type="text" value="----"/> i +
Počítadlo strán	Číslo alternatívneho používateľského mena <input type="text"/>
Komponenty	Alternatívne používateľské meno <input type="text"/>
Zväzky	Popis systému <input type="text"/>
Pripojenia	Používateľ <input type="text" value="----"/> i
Sieťové porty	Sieť <input type="text" value="----"/> i +
Zásuvky	UUID <input type="text"/>
Správa	Zdroj aktualizácií <input type="text" value="----"/> i +
Zmluvy	Počiatočný počet stránok <input type="text" value="0"/>
Dokumenty	Aktuálny stav počítadla stránok <input type="text" value="0"/>
Databáza znalostí	Porty <input type="checkbox"/> Sériový <input type="checkbox"/> Paralelný <input type="checkbox"/> USB <input type="checkbox"/> Ethernet <input type="checkbox"/> Wifi
Požiadavky	
Problémy	
Zmeny	
Odkazy	
Poznámky	
Rezervácie	
Certifikáty	
Domény	
Aplikácie	
História	
Lifecycle	
Všetko	

Presunúť do koša

Uložiť

Vytvorené: 12-08-2024 00:00

Posledná aktualizácia: 12-08-2024 00:00



- Menu vyhľadávania
- Inventár
- Podpora
- Správa
- Nástroje
- Administrácia
- Používateľia
- Skupiny
- Entity
- Pravidlá
- Číselníky
- Profily
- Fronta oznámení
- Logy
- Inventár
- Item's Lifecycle
- Nastavenia

Domov / Administrácia / Používateľia + Pridať Hľadať Uložené hľadania

Hľadať... Super-Admin GLPI (strom) BJ

7/15

Používateľ: Preberací protokol Vytvoriť

Poznámka

<input checked="" type="checkbox"/>	Typ	Výrobca	Model	Názov	Sériové číslo	Inventárne číslo	Komentáre
<input checked="" type="checkbox"/>	Počítače			Dell latitude 5530	C:		<input type="text"/>
<input checked="" type="checkbox"/>	Monitory			Samsung	LS:		<input type="text"/>
<input checked="" type="checkbox"/>	Zariadenia			Externý disk Kingston XS1000 SSD 1 TB	SXS10		<input type="text"/>
<input checked="" type="checkbox"/>	Telefóny			Huawei P20	AEJ7N1		<input type="text"/>
<input checked="" type="checkbox"/>	Telefóny			Xiaomi Redmi Note 9	2790/		<input type="text"/>
<input checked="" type="checkbox"/>	Telefóny			Samsung Galaxy S23 Ultra	R3CV		<input type="text"/>
<input checked="" type="checkbox"/>	SIM karta položky			34	1800	++	<input type="text"/>
<input checked="" type="checkbox"/>	Dock			Neuvedene	PPID: CN-05FDDV-		<input type="text"/>
<input checked="" type="checkbox"/>	Kluc			ZA305			<input type="text"/>
<input checked="" type="checkbox"/>	Kluc			BA office			<input type="text"/>

Add Custom Fields

<input type="checkbox"/>	Názov	Typ	Dátum	Súbor	Tvorca	Poznámka	Send email
<input type="checkbox"/>	09202024_0828	Preberací protokol	2024-09-20 10:28:07		Branislav		<input type="button" value="Poslať"/>
<input type="checkbox"/>	01272025_0916	Preberací protokol	2025-01-27 09:16:37	Preberací_protokol-2...	Rastislav I		<input type="button" value="Poslať"/>

Domov / Nastavenia / Pluginy / Obchod








Hľadaf Uložené hľadania Obchod Pluginy

Hľadaf...

Super-Admin GLPI (strom) BJ

**Nainštalované** [Objavte viac](#)

Filtrovat zoznam pluginov

 <p><b>Behaviours</b></p> <p>AGPL v3+</p> <p>Infotel, Remi Collet, Nelly Mahu-Lasson</p> <p>2.7.3</p>	 <p><b>Data injection</b></p> <p>GPL v2+</p> <p>Walid Nouh, Dévi Balpe, Remi Collet, Nelly Mahu-L...</p> <p>2.14.1</p>	 <p><b>Escalation</b></p> <p>GPL v2+</p> <p>Alexandre Delaunay, TECLIB'</p> <p>2.9.10</p>	 <p><b>Item's Lifecycle (uninstall)</b></p> <p>GPL v2+</p> <p>Walid Nouh, François Legastelois, Remi Collet</p> <p>2.9.2</p>
 <p><b>OCS Inventory NG</b></p> <p>GPL v2+</p> <p>Remi Collet, Nelly Mahu-Lasson, David Durieux, Xa...</p> <p>2.0.4</p>	 <p><b>Protocols manager</b></p> <p>GPLv3+</p> <p>Mikail</p> <p>1.5.3.7</p>	 <p><b>Správa objektov</b></p> <p>GPL v2+</p> <p>Walid Nouh</p> <p>2.14.11</p>	

Chcete tu vidieť svoj plugin? Kontaktujte nás. [✉](#)

**GLPI**

- Menu vyhľadávania
- Inventár
- Podpora
- Správa
- Nástroje
- Administrácia
- Nastavenia**
- Rozbaľovacie pokusy
- Komponenty
- Oznámenia
- Úrovne služieb
- Všeobecné
- Jedinečnosť polí
- Automatické akcie
- Autentifikácia
- Prijímače
- Externé odkazy
- Pluginy**
- Správa objektov
- Protocols Manager

Domov / Nastavenia / Pluginy / Obchod

Hľadaf... Super-Admin  
GLPI (strom) BJ

Nainštalované **Objavte viac**

- Všetko
- Inventory
- Ticket
- Helpdesk
- Management
- GLPI-Network
- Network
- Data
- Setup
- Export
- Import
- Notification
- Architecture
- Task
- Dashboard
- Reports


Filtrovať zoznam pluginov Vzostupne

<p><b>Accounts Inventory</b></p> <p>Manage accounts (login / password). This plugin enables you to manage the accounts of your network and associate them with elements of the inventory. The accounts are crypted in database with hash and crypting key. A mailing system allow to verify expired accounts.</p> <p>★★★★☆ GPL v2+ Xavier Caillaud, Infotel 3.0.4</p>	<p><b>Activity</b></p> <p>Activity management. This plugin allows you add your activities into planning. Holidays management.</p> <p>★★★★☆ GPL v2+ Xavier Caillaud, Infotel 3.1.5</p>	<p><b>ActualTime</b></p> <p>Adds actual time tracking for GLPI tasks</p> <p>★★★★☆ AGPL v3+ TICgal 3.2.0</p>	<p><b>Additional Alerts</b></p> <p>Sending of additional alerts. This plugin enables you to send email alerts regarding the items with empty buy date and Cartridges whose level is low.</p> <p>★★★★☆ GPL v2+ Xavier Caillaud 2.4.0</p>
<p><b>Advanced Forms</b></p> <p>Advanced Forms GLPI plugin.</p> <p>★★★★★ MIT TECLIB'</p>	<p><b>Advanced GLPI dashboards</b></p> <p>★ GLPI Network Standard</p> <p>SQL queries for GLPI dashboards.</p> <p>★★★★☆ GPL V3+ TECLIB' 1.6.3</p>	<p><b>advancedplanning</b></p> <p>This plugin unlock advanced planning features (Scheduler view) in GLPI (Home &gt; Assistance &gt; Planning)</p> <p>★★★★☆ GPL V3+ TECLIB' 1.1.1</p>	<p><b>Airwatch connector</b></p> <p>Connector to gather inventory information from Airwatch</p> <p>★★★★☆ GPL v2+ Teclib, Walid Nouh</p>
<p><b>anonymize</b></p> <p>★ GLPI Network Basic</p> <p>GLPI data Anonymization</p> <p>★★★★☆ GPL V3+ TECLIB' 2.7.1</p>	<p><b>Appliances Dashboard</b></p> <p>Appliance dashboard. This plugin allows you to display your business applications with all their characteristics in the form of a dashboard.</p> <p>★★★★☆ GPL v2+ Xavier Caillaud, Infotel 5.0.2</p>	<p><b>Appliances Inventory</b></p> <p>Appliances management. This plugin enables you to create appliance (several elements constituting a unit).</p> <p>★★★★☆ AGPLv3 Xavier Caillaud, Remi Collet, Nelly Mahu-Lasson</p>	<p><b>ApprovalByMail</b></p> <p>★ GLPI Network Standard</p> <p>ApprovalByMail GLPI plugin.</p> <p>★★★★☆ GPL V2+ TECLIB' 2.2.6</p>


< 1 2 ... 9 10 > 113 pluginov


Chcete tu vidieť svoj plugin? Kontaktujte nás. [✉](#)

102




Financované  
Európskou úniou  
NextGenerationEU





MINISTERSTVO  
INVESTÍCIE REGIONÁLNEHO ROZVOJA  
A INFORMATIZÁCIE  
SLOVENSKEJ REPUBLIKY



KOMPETENČNÉ CENTRUM  
KYBERNETICKEJ BEZPEČNOSTI  
ŽILNSKEJ UNIVERZITY V ŽILNE

# Dashboard - Podpora (systém pre správu požiadaviek)

**Dashboard - Podpora**

Assistance

17 Požiadavky

0 Požiadavky po termíne

0 Problémy

0 Zmeny

0 Opakujúce sa požiadavky

0 Opakujúce sa zmeny

0 Správa

0 Nástroje

0 Administrácia

0 Nastavenia

Vývoj požiadaviek v uplynulom roku

Stav	Count
Otvorené	17
Vyriešené	0
Vyriešené po termíne	0
Uzavreté	0

Stavy požiadaviek za mesiac

Mesiac	Nové	V riešení (priradené)	V riešení (naplánované)	Čakajúce	Vyriešené	Uzavreté
2021-11	0	0	0	0	0	1
2021-12	0	0	0	0	1	0
2022-01	0	4	0	4	0	0
2022-02	0	0	0	0	2	0
2022-03	0	0	0	0	0	1

Top kategórie požiadaviek

Top zdroje požiadaviek

Top entity požiadaviek

**GLPI**

- Menu vyhľadávania
- Inventár
- Podpora
  - Dashboard
  - Požiadavky**
  - Vytvorí požiadavku
  - Problémy
  - Zmeny
  - Plánovanie
  - Štatistiky
  - Opakujúce sa požiadavky
  - Opakujúce sa zmeny
- Správa
- Nástroje
- Administrácia
- Nastavenia

Domov / Podpora / Požiadavky

+ Pridať Hľadať Uložené hľadania Šablóny Globálny Kanban Požiadavky čakajúce na moje schválenie

Hľadať...

Super-Admin  
GLPI (strom)

**Branislav**

Požiadavka bude pridaná do entity GLPI

Názov

Popis \*

Odstavec

Súbory (15 MB max) *i*

Pretiahnite súbor sem, alebo ho načítajte

Vybrať súbory Nie je vybratý žiadny súbor

Požiadavka

Entita GLPI

Typ Požiadavka

Kategória \* -----

Stav **Nové**

Naliehavosť Stredná

Dopad Stredný

Priorita **Stredná**

Účastníci 0

Žiadateľ

x Branislav 0

Riešiteľ

x tech 5 x tech 5 x Infra 5

Položky 0

Moje zariadenia -----


Alebo kompletne vyhľadavanie Všeobecná

+ Pridať

Úrovne služieb

Prepojené požiadavky

+ Pridať



- Menu vyhľadávania
- Inventár
- Podpora
- Správa
- Nástroje
- Administrácia
- Nastavenia**
- Rozbaňovacie ponuky
- Komponenty
- Oznámenia
- Úrovne služieb
- Všeobecné
- Jedinečnosť polí
- Automatické akcie
- Autentifikácia
- Prijímače
- Externé odkazy
- Plugíny
- Správa objektov**
- Protocols Manager

Domov / Nastavenia / Správa objektov + Pridať Hľadať Uložené hľadania

Hľadať... Super-Admin GLPI (strom) BJ

Akcie

MODEL	POUŽIT HISTÓRIA	PRIRADITEĽNÉ K POZIADAVKE	POUŽIT DOKUMENTY	POUŽIT REZERVÁCIE
<input type="checkbox"/> adapter	Nie	Nie	Nie	Nie
<input type="checkbox"/> dock	Nie	Nie	Nie	Nie
<input type="checkbox"/> klavesnica	Nie	Nie	Nie	Nie
<input type="checkbox"/> kluc	Nie	Nie	Nie	Nie
<input type="checkbox"/> mysky	Nie	Nie	Nie	Nie
<input type="checkbox"/> nabytok	Nie	Nie	Nie	Nie
<input type="checkbox"/> nfqesqscd	Nie	Nie	Nie	Nie
<input type="checkbox"/> simkarty	Áno	Nie	Nie	Nie
<input type="checkbox"/> vpn	Nie	Nie	Nie	Nie

15 riadkov na stránku Zobrazujem 1 až 9 z 9 riadkov

GLPI

- Menu vyhľadávania
- Inventár
- Podpora
- Správa
- Nástroje
  - Projekty**
  - Pripomienky
  - RSS zdroje
  - Databáza znalostí
  - Rezervácie
  - Reporty
  - Uložené hľadania
  - Import dát
  - OCS Inventory NG
- Administrácia
- Nastavenia

Domov / Nástroje / Projekty

+ Pridať Hľadať Uložené hľadania Šablóny Moje úlohy Globálny Kanban

Hľadať...

Super-Admin  
GLPI (strom) BJ

Projekt - 4001\_F

GLPI > PUSR Podriadené entity 1 Akcie 1/1

<b>Projekt</b>	Dátum vytvorenia	01-10-2024 14:11:38	Posledná aktualizácia	16-10-2024 10:26
Projektové úlohy	Názov	4001_F	Kód	
Projektový tím 1	Priorita	Stredná	Ako potomok	----- i
Projekty	Stav	----- i +	Hotovo percent	0% i
Kanban	Typ	----- i +		
Náklady				
Itil položky				
Položky 1	Používateľ	Jaroslav i	Skupina	----- i +
Dokumenty				
Zmluvy	Plánovaný dátum začatia		Reálny dátum začatia	
Poznámky	Plánovaný dátum ukončenia		Reálny dátum ukončenia	
Databáza znalostí	Plánované trvanie i	0 sekúnd	Skutočné trvanie i	0 sekúnd
História 6				
Všetko				
	Popis			
	Komentáre			

MANAŽER

PLÁNOVANIE

Presunúť do koša Uložiť

Templates settings
Email settings

### Vytvoriť šablónu

Názov šablony\*

Nadpis dokumentu\*

Môžete tu použiť premennú (owner)

Font:

Font size:

Word breaking:  On

Mesto:

Upper Content:

Môžete tu použiť premennú (owner) alebo (admin)

Obsah:

Môžete tu použiť premennú (owner) alebo (admin)

Footer:

Orientácia:

Sériové číslo:  serial and inventory number in separate columns

Logo:  Nie je vybratý žiadny súbor

Enable email autosending:  ON

Email template:

Vyberte, kto má vytvoriť PDF:  Používateľ, ktorý vytvára tento dokument

serial or inventory number if serial doesn't exists

OFF

- 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.).
  - služi na generovanie „protokolov o odovzdaní“ alebo „prevzatí“ aktív.

#### Šablóny

Názov	Akcia
Preberací protokol	<input type="button" value="Upraviť"/> <input type="button" value="Zmazať"/>
Odovzdávací protokol	<input type="button" value="Upraviť"/> <input type="button" value="Zmazať"/>

# GLPI

## Správa dokumentov



GLPI

Domov / Správa / Dokumenty + Pridať Hľadať Uložené hľadania Hľadať... Super-Admin GLPI (strom) BJ

Akcie

<input type="checkbox"/>	NÁZOV	ENTITA	HLAVIČKA	KOMENTÁRE	SÚBOR
<input type="checkbox"/>	01092023_0916	GLPI			86-01092023.pdf
<input type="checkbox"/>	01092023_1456	GLPI			87-01092023.pdf
<input type="checkbox"/>	01092023_1629	GLPI			88-01092023.pdf
<input type="checkbox"/>	01092025_1025	GLPI			Preberaci_protokol-0...
<input type="checkbox"/>	01132025_0854	GLPI			Preberaci_protokol-1...
<input type="checkbox"/>	01162025_1333	GLPI			Preberaci_protokol-1...
<input type="checkbox"/>	01162025_1334	GLPI			Preberaci_protokol-1...
<input type="checkbox"/>	01162025_1335	GLPI			Preberaci_protokol-1...
<input type="checkbox"/>	01172023_1124	GLPI			89-01172023.pdf
<input type="checkbox"/>	01222025_1505	GLPI			Preberaci_protokol-2...
<input type="checkbox"/>	01242024_1412	GLPI			228-01242024.pdf
<input type="checkbox"/>	01262024_1427	GLPI			230-01262024.pdf
<input type="checkbox"/>	01272025_0905	GLPI			Preberaci_protokol-2...
<input type="checkbox"/>	01272025_0916	GLPI			Preberaci_protokol-2...
<input type="checkbox"/>	02052024_0739	GLPI			231-02052024.pdf

15 riadkov na stránku Zobrazujem 1 až 15 z 311 riadkov << < 1 2 3 ... > >>

# 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



netbox

**Inventarizačný nástroj - Netbox**

# Nástroje na správu a kategorizáciu aktív

## Netbox

- 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.



PONUKA DEMO NÁSTROJA

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.

A screenshot of the Netbox Community login page. At the top is the Netbox logo and the word "Community". Below that, it says "This is a demo instance of NetBox for public use." and "Click here to create a new user account, or log in with your existing credentials below." There is a note "Data is reset nightly at 04:00 UTC." The main section is titled "Log In" and contains two input fields: "Username" and "Password". Below the fields is a green "Sign In" button.

Link: [Home | NetBox](#)

# Nástroje na správu a kategorizáciu aktív Netbox



The screenshot shows the Netbox web interface. On the left is a navigation sidebar with categories like Organization, Racks, Devices, Connections, Wireless, IPAM, VPN, Virtualization, Circuits, Power, Provisioning, Customization, Operations, and Admin. The main content area is a dashboard with several widgets:

- Bookmarks:** Butler Communications, 172.16.0.1/24, dmi01-binghamton-rtr01, PP:B117
- Organization:** Sites (24), Tenants (11), Contacts (3)
- IPAM:** VRFs (6), Aggregates (4), Prefixes (90), IP Ranges (4), IP Addresses (180), VLANs (63)
- Circuits:** Providers (9), Circuits (29), Provider Networks (1), Provider Accounts (0)
- DCIM:** Sites (24), Racks (42), Device Types (14), Devices (81), Cables (118)
- Virtualization:** Clusters (32), Virtual Machines (180)
- Welcome!** This is your personal dashboard. Feel free to customize it by rearranging, resizing, or removing widgets. You can also add new widgets using the "add widget" button below. Any changes affect only your dashboard, so feel free to experiment!
- NetBox News:** Announcing the Diode Go SDK, NetBox Branching is Now Available in Public Beta, A New Look For NetBox and NetBox Labs



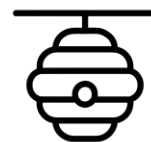
### **Centralizovaná dokumentácia**

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



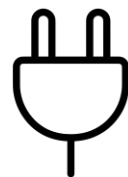
### **Open-source riešenie**

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,
  - rozdávače (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

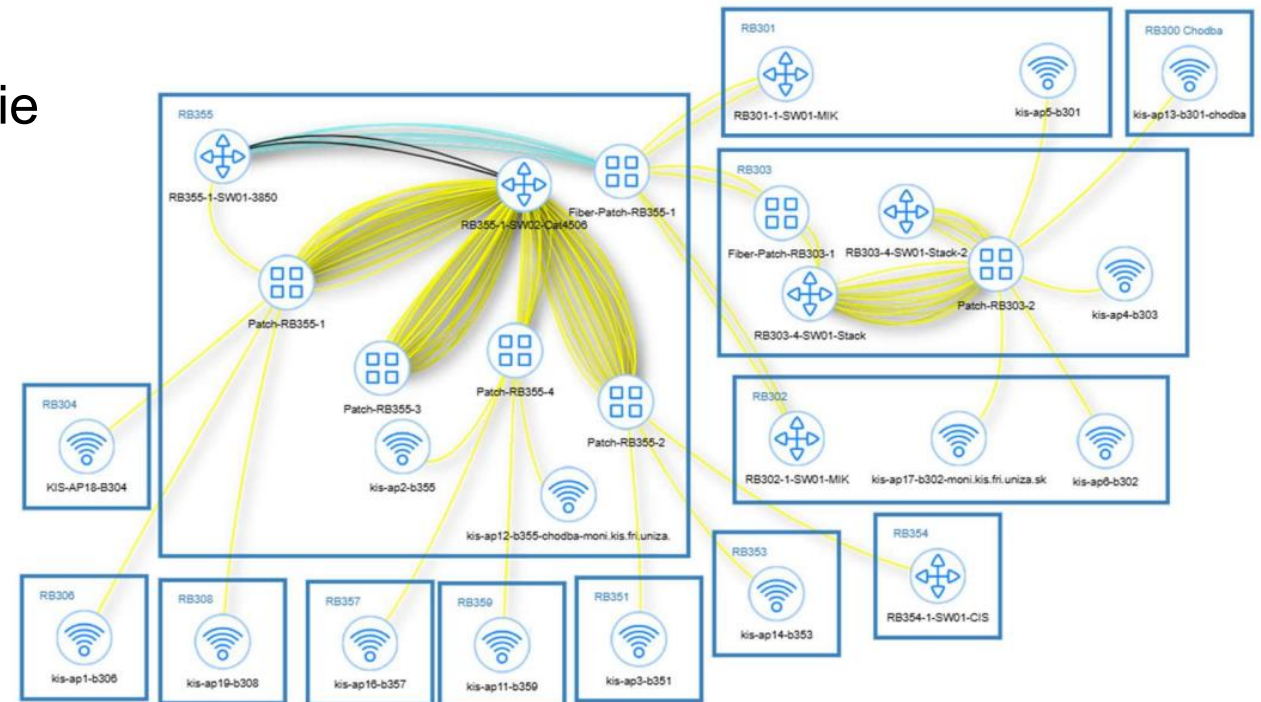
- Druhý spôsob je import dát.
- Definujeme si, aké parametre budú mať nové objekty (aktíva).
  - Ak súbor, ktorý nahrávame obsahuje ID čísla objektov, NetBox sa snaží upraviť existujúce objekty.
  - Ak objekt s daným ID neexistuje nahratie zmien sa nevykoná a nič sa nezmení.
- Podporované formáty sú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

```
- 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





Search...

Staff

## Sites

+ Add   ↑ Import   ↓ Export

Results **1**   Filters

Quick search

<input type="checkbox"/>	NAME	STATUS	FACILITY	REGION	GROUP	TENANT	DESCRIPTION	
<input type="checkbox"/>	FRI	Active	—	—	—	FRI	Fakulta riadenia a informatiky	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Showing 1-1 of 1

# Netbox

## Locations



netbox Community

Organization

SITES

Sites

Locations

TENANCY

Tenants

CONTACTS

Contacts

Contact Groups

Contact Roles

Contact Assignments

Racks

Devices

Connections

Wireless

IPAM

VPN

Virtualization

Search...

Locations

+ Add Import Export

Results 16 Filters

Quick search

Configure Table

<input type="checkbox"/>	NAME	SITE	STATUS	FACILITY	TENANT	RACKS	DEVICES	VLAN GROUPS	DESCRIPTION		
<input type="checkbox"/>	RAS09	FRI	Active	—	KIS	4	5	0	RAS09		
<input type="checkbox"/>	RB003	FRI	Active	—	KIS	0	0	0	RB003		
<input type="checkbox"/>	RB300 Chodba	FRI	Active	—	KIS	0	1	0	Chodba na RB300		
<input type="checkbox"/>	RB301	FRI	Active	—	KIS	1	5	0	RB301		
<input type="checkbox"/>	RB302	FRI	Active	—	KIS	1	6	0	RB302		
<input type="checkbox"/>	RB303	FRI	Active	—	KIS	1	6	0	RB303		
<input type="checkbox"/>	RB304	FRI	Active	—	KIS	0	1	0	RB304		
<input type="checkbox"/>	RB306	FRI	Active	—	KIS	0	1	0	RB306		
<input type="checkbox"/>	RB308	FRI	Active	—	KIS	0	1	0	RB308		
<input type="checkbox"/>	RB351	FRI	Active	—	KIS	0	1	0	RB351		

# Tenants (Vlastníci)



Organization

SITES

Sites

Locations

TENANCY

Tenants + ↑

CONTACTS

Contacts

Contact Groups

Contact Roles

Contact Assignments

Racks

Devices

Connections

Wireless

IPAM

VPN

🔔 📧 Staff

## Tenants

+ Add
↑ Import
↓ Export

Results 3

Filters

Quick search

⌵


⚙️ Configure Table



<input type="checkbox"/>	NAME <span style="font-size: small;">▼</span>	GROUP	DESCRIPTION	✎️
<input type="checkbox"/>	FRI	—	Fakulta riadenia a informatiky	✎️
<input type="checkbox"/>	Iný vlastník	—	Iný vlastník	✎️
<input type="checkbox"/>	KIS	—	Katedra informačných sietí	✎️

Showing 1-3 of 3

Per Page ▼

✎️ Edit Selected
🗑️ Delete Selected





















Staff

**Racks**

Results 8 Filters

Quick search

View Elevations Add Import Export

<input type="checkbox"/>	NAME	SITE	LOCATION	STATUS	FACILITY ID	TENANT	ROLE	TYPE	HEIGHT	DEVICES	SPACE	
<input type="checkbox"/>	RAS09-1-čierny	FRI	RAS09	Active	—	KIS	—	—	42U	1	<div style="width: 2.4%; background-color: #27ae60; height: 10px;"></div> 2.4%	 
<input type="checkbox"/>	RAS09-2-biely	FRI	RAS09	Active	—	KIS	—	—	42U	4	<div style="width: 9.5%; background-color: #27ae60; height: 10px;"></div> 9.5%	 
<input type="checkbox"/>	RAS09-3-biely	FRI	RAS09	Active	—	KIS	—	—	15U	0	<div style="width: 0%; background-color: #27ae60; height: 10px;"></div> 0.0%	 
<input type="checkbox"/>	stolík	FRI	RAS09	Active	—	KIS	—	—	42U	0	<div style="width: 0%; background-color: #27ae60; height: 10px;"></div> 0.0%	 
<input type="checkbox"/>	RB301-1	FRI	RB301	Active	—	KIS	—	—	4U	4	<div style="width: 100%; background-color: #34495e; height: 10px;"></div> 100.0%	 
<input type="checkbox"/>	RB302-1	FRI	RB302	Active	—	KIS	—	—	9U	4	<div style="width: 44.4%; background-color: #27ae60; height: 10px;"></div> 44.4%	 
<input type="checkbox"/>	RB303-1	FRI	RB303	Active	—	KIS	—	—	38U	5	<div style="width: 13.2%; background-color: #27ae60; height: 10px;"></div> 13.2%	 
<input type="checkbox"/>	RB355-1	FRI	RB355	Active	—	KIS	—	—	42U	8	<div style="width: 40.5%; background-color: #27ae60; height: 10px;"></div> 40.5%	 


Showing 1-8 of 8
Per Page

- Organization
- Racks
- RACKS**
- Racks + ↑
- Reservations
- Elevations
- Devices
- Connections
- Wireless
- IPAM
- VPN
- Virtualization
- Provisioning
- Customization
- Operations
- Topology Views



# Vizualizácia rack-ov (osadenie zariadení)



The screenshot displays the Netbox web interface for rack visualization. On the left is a navigation sidebar with categories: Organization, Racks, RACKS (Racks, Reservations, Elevations), Devices, DEVICES (Devices, Modules, Device Roles, Platforms, Virtual Chassis), DEVICE TYPES (Device Types, Module Types, Manufacturers), and DEVICE COMPONENTS. The main area features a search bar, a lightbulb icon, a bell icon, and a 'Staff' link. The rack visualization shows three racks: RB301-1, RB302-1, and RB303-1. Each rack is represented as a vertical column of 20 slots. RB301-1 has devices at slots 1-4: RB301-1-SW02-CIS (slot 1), RB301-1-SW01-MIK (slot 2), Patch-RB301-2 (slot 3), and Patch-RB301-1 (slot 4). RB302-1 has devices at slots 3-4: RB302-1-SW01-MIK (slot 3) and RB302-1-SW02-CIS (slot 4). RB303-1 is currently empty. Below each rack visualization is a 'Download SVG' button. At the bottom, it shows 'Showing 1-8 of 8' and a 'Per Page' dropdown menu.



netbox  
Community



Staff

## Devices

+ Add
↑ Import
↓ Export

Results 42 Filters

▼

⚙️ Configure Table

<input type="checkbox"/>	NAME	STATUS	TENANT	SITE	LOCATION	RACK	ROLE	MANUFACTURER	TYPE	IP
<input type="checkbox"/>	Fiber-Patch-RB303-1	Active	KIS	FRI	RB303	RB303-1	Patch Panel	Generic	SC-24-port Fiber Patch Panel	—
<input type="checkbox"/>	Fiber-Patch-RB355-1	Active	KIS	FRI	RB355	RB355-1	Patch Panel	Generic	SC-24-port Fiber Patch Panel	—
<input type="checkbox"/>	kis-ap1-b306	Active	KIS	FRI	RB306	—	Access Point	Cisco	Aironet 2702I-E-K9	192.168.1.1
<input type="checkbox"/>	kis-ap2-b355	Active	KIS	FRI	RB355	—	Access Point	Cisco	Aironet 2702I-E-K9	192.168.1.2
<input type="checkbox"/>	kis-ap3-b351	Active	KIS	FRI	RB351	—	Access Point	Cisco	Aironet 2702I-E-K9	192.168.1.3
<input type="checkbox"/>	kis-ap4-b303	Active	KIS	FRI	RB303	—	Access Point	Cisco	Aironet 2702I-E-K9	192.168.1.4
<input type="checkbox"/>	kis-ap5-b301	Active	KIS	FRI	RB301	—	Access Point	Cisco	Aironet 2702I-E-K9	192.168.1.5
<input type="checkbox"/>	kis-ap6-b302	Active	KIS	FRI	RB302	—	Access Point	Cisco	Aironet 2702I-E-K9	192.168.1.6
<input type="checkbox"/>	kis-ap11-b359	Active	KIS	FRI	RB359	—	Access Point	Cisco	Aironet 2702I-E-K9	192.168.1.7
<input type="checkbox"/>	kis-ap10-b355	Active	KIS	FRI	RB355	—	Access Point	Cisco	Aironet 2702I-E-K9	192.168.1.8

netbox
Community

- Organization
- Racks
- Devices

**DEVICES**

- Devices + ↑
- Modules
- Device Roles
- Platforms
- Virtual Chassis

**DEVICE TYPES**

- Device Types
- Module Types
- Manufacturers

**DEVICE COMPONENTS**

- Interfaces
- Front Ports
- Rear Ports
- Console Ports
- Console Server Ports
- Module Bays

# Devices - Hardvérové moduly (karty)



netbox  
Community

Staff

## Modules

+ Add
↑ Import
↓ Export

Results 6
Filters

▼

▼

⚙️ Configure Table

<input type="checkbox"/>	ID	DEVICE	MODULE BAY <span style="color: red;">✕</span>	MANUFACTURER	MODULE TYPE	STATUS	SERIAL NUMBER	ASSET TAG	
<input type="checkbox"/>	25	RAS09-1-SW02-N5K-1	Slot 3	Cisco	Nexus 5548 Layer 2 Daughter Card	Active	—	—	
<input type="checkbox"/>	26	RAS09-1-SW02-N5K-2	Slot 3	Cisco	Nexus 5548 Layer 2 Daughter Card	Active	—	—	
<input type="checkbox"/>	21	RB355-1-SW02-Cat4506	Slot 1	Cisco	WS-X45-SUP6-E	Active	—	—	
<input type="checkbox"/>	22	RB355-1-SW02-Cat4506	Slot 3	Cisco	WS-X4648-RJ45V+E	Active	—	—	
<input type="checkbox"/>	23	RB355-1-SW02-Cat4506	Slot 5	Cisco	WS-X4648-RJ45V+E	Active	—	—	
<input type="checkbox"/>	24	RB355-1-SW02-Cat4506	Slot 6	Cisco	WS-X4424-GB-RJ45	Active	—	—	

Showing 1-6 of 6

Per Page
▼

DEVICES

Devices

Modules + ↑

Device Roles

Platforms

Virtual Chassis

DEVICE TYPES

Device Types

Module Types

Manufacturers

DEVICE COMPONENTS

Interfaces

Front Ports

Rear Ports

Console Ports

Console Server Ports

# Devices - Typy zariadení



netbox  
Community

Staff

## Device Roles

+ Add
↑ Import
↓ Export

Results 8
Filters

⚙️ Configure Table

	NAME	DEVICES	VMS	COLOR	VM ROLE	DESCRIPTION	
<input type="checkbox"/>	Access Point	14	0	<div style="width: 20px; height: 10px; background-color: #008080;"></div>	—	—	<span style="color: orange;">✎</span> <span style="color: orange;">⌵</span>
<input type="checkbox"/>	Console Server	0	0	<div style="width: 20px; height: 10px; background-color: #008000;"></div>	—	—	<span style="color: orange;">✎</span> <span style="color: orange;">⌵</span>
<input type="checkbox"/>	Firewall	2	0	<div style="width: 20px; height: 10px; background-color: #ff0000;"></div>	—	—	<span style="color: orange;">✎</span> <span style="color: orange;">⌵</span>
<input type="checkbox"/>	PDU	0	0	<div style="width: 20px; height: 10px; background-color: #000000;"></div>	—	—	<span style="color: orange;">✎</span> <span style="color: orange;">⌵</span>
<input type="checkbox"/>	Patch Panel	12	0	<div style="width: 20px; height: 10px; border: 1px solid #ccc;"></div>	—	—	<span style="color: orange;">✎</span> <span style="color: orange;">⌵</span>
<input type="checkbox"/>	Router	0	0	<div style="width: 20px; height: 10px; background-color: #0000ff;"></div>	—	—	<span style="color: orange;">✎</span> <span style="color: orange;">⌵</span>
<input type="checkbox"/>	Server	0	0	<div style="width: 20px; height: 10px; background-color: #ffa500;"></div>	✓	—	<span style="color: orange;">✎</span> <span style="color: orange;">⌵</span>
<input type="checkbox"/>	Switch	14	0	<div style="width: 20px; height: 10px; background-color: #6495ed;"></div>	—	—	<span style="color: orange;">✎</span> <span style="color: orange;">⌵</span>

Showing 1-8 of 8

Per Page

✎ Edit Selected
🗑 Delete Selected

Organization

Racks

Devices

**DEVICES**

Devices

Modules

Device Roles + ↑

Platforms

Virtual Chassis

**DEVICE TYPES**

Device Types

Module Types

Manufacturers

**DEVICE COMPONENTS**

Interfaces

Front Ports

Rear Ports

Console Ports

Console Server Ports

Module Bays

# Netbox OS platformy



netbox Community

Organization Racks Devices

DEVICES

Devices Modules Device Roles Platforms + - Virtual Chassis

DEVICE TYPES

Device Types Module Types Manufacturers

DEVICE COMPONENTS

Interfaces Front Ports Rear Ports Console Ports Console Server Ports Module Bays

Search... Staff

## Platforms

+ Add Import Export

Results 10 Filters

Quick search [ ] [ ] Configure Table

<input type="checkbox"/>	NAME	MANUFACTURER	DEVICES	VMS	DESCRIPTION	
<input type="checkbox"/>	Cisco AIR-CAP27	Cisco	14	0	—	
<input type="checkbox"/>	Cisco IOS	Cisco	7	0	—	
<input type="checkbox"/>	Cisco IOS XE	Cisco	2	0	—	
<input type="checkbox"/>	Cisco NX-OS	Cisco	2	0	—	
<input type="checkbox"/>	FortiOS v7.2	Fortinet	2	0	—	
<input type="checkbox"/>	JunOS 15	Juniper	1	0	—	
<input type="checkbox"/>	RouterOS v7	MikroTik	2	0	—	
<input type="checkbox"/>	Ubuntu 20.04	Canonical	0	0	—	
<input type="checkbox"/>	Ubuntu 22.04	Canonical	0	0	—	
<input type="checkbox"/>	Ubuntu 24.04	Canonical	0	0	—	

# Netbox

## Virtual chassis



netbox Community

- Organization
- Racks
- Devices

**DEVICES**

- Devices
- Modules
- Device Roles
- Platforms
- Virtual Chassis**

**DEVICE TYPES**

- Device Types
- Module Types
- Manufacturers

**DEVICE COMPONENTS**

- Interfaces
- Front Ports
- Rear Ports
- Console Ports
- Console Server Ports

Search...

Virtual Chassis

+ Add   ↑ Import   ↓ Export


Results 2   Filters

Quick search   Filter   Configure Table

<input type="checkbox"/>	NAME	DOMAIN	MASTER	MEMBERS	
<input type="checkbox"/>	RB303-4-SW01-Stack	—	RB303-4-SW01-Stack	2	
<input type="checkbox"/>	RB355-1-SW01-3850	—	RB355-1-SW01-3850	2	

Showing 1-2 of 2   Per Page

Edit Selected   Delete Selected



netbox  
Community

Staff

## Device Types

+ Add
↑ Import
↓ Export

Results 17
Filters

▼


⚙️ Configure Table

<input type="checkbox"/>	DEVICE TYPE <span style="font-size: 0.8em;">▼</span>	<span style="color: red;">×</span> MANUFACTURER <span style="font-size: 0.8em;">▼</span>	<span style="color: red;">×</span> PART NUMBER	U HEIGHT	FULL DEPTH	INSTANCES	<span style="color: orange;">✎</span> <span style="color: orange;">▼</span>
<input type="checkbox"/>	Aironet 2702I-E-K9	Cisco	AIR-CAP2702I-E-K9	0	—	14	<span style="color: orange;">✎</span> <span style="color: orange;">▼</span>
<input type="checkbox"/>	Catalyst 2960-8TC-L	Cisco	WS-C2960-8TC-L	1	—	1	<span style="color: orange;">✎</span> <span style="color: orange;">▼</span>
<input type="checkbox"/>	Catalyst 2960X-24PD-L	Cisco	WS-C2960X-24PD-L	1	—	1	<span style="color: orange;">✎</span> <span style="color: orange;">▼</span>
<input type="checkbox"/>	Catalyst 2960X-48LPS-L	Cisco	WS-C2960X-48LPS-L	1	—	1	<span style="color: orange;">✎</span> <span style="color: orange;">▼</span>
<input type="checkbox"/>	Catalyst 2960X-48TS-L	Cisco	WS-C2960X-48TS-L	1	—	1	<span style="color: orange;">✎</span> <span style="color: orange;">▼</span>
<input type="checkbox"/>	Catalyst 2960XR-48FPS-I	Cisco	WS-C2960XR-48FPS-I	1	—	0	<span style="color: orange;">✎</span> <span style="color: orange;">▼</span>
<input type="checkbox"/>	Catalyst 3560-8PC-S	Cisco	WS-C3560-8PC-S	1	—	2	<span style="color: orange;">✎</span> <span style="color: orange;">▼</span>
<input type="checkbox"/>	Catalyst 3850-12XS	Cisco	WS-C3850-12XS	1	—	2	<span style="color: orange;">✎</span> <span style="color: orange;">▼</span>
<input type="checkbox"/>	Catalyst 4506-E	Cisco	WS-C4506-E	10	✓	1	<span style="color: orange;">✎</span> <span style="color: orange;">▼</span>
<input type="checkbox"/>	Nexus 5548UP	Cisco	N5K-C5548UP	1	—	2	<span style="color: orange;">✎</span> <span style="color: orange;">▼</span>

- Organization
- Racks
- Devices
- DEVICES**
- Devices
- Modules
- Device Roles
- Platforms
- Virtual Chassis
- DEVICE TYPES**
- Device Types + ↑
- Module Types
- Manufacturers
- DEVICE COMPONENTS**
- Interfaces
- Front Ports
- Rear Ports
- Console Ports
- Console Server Ports
- Module Bays

# Typy modulov (kariet)





🔦 🔔 Staff

## Module Types

+ Add
↑ Import
↓ Export

Results 4
Filters

▼


⚙️ Configure Table

<input type="checkbox"/> MODULE TYPE ▼	<input checked="" type="checkbox"/> MANUFACTURER ▼	<input checked="" type="checkbox"/> PART NUMBER	
<input type="checkbox"/> Nexus 5548 Layer 2 Daughter Card	Cisco	N55-DL2	<span style="background-color: #fd7e14; color: white; padding: 2px 5px; border-radius: 3px;">✎</span> <span style="background-color: #6c757d; color: white; padding: 2px 5px; border-radius: 3px;">▼</span>
<input type="checkbox"/> WS-X4424-GB-RJ45	Cisco	WS-X4424-GB-RJ45	<span style="background-color: #fd7e14; color: white; padding: 2px 5px; border-radius: 3px;">✎</span> <span style="background-color: #6c757d; color: white; padding: 2px 5px; border-radius: 3px;">▼</span>
<input type="checkbox"/> WS-X45-SUP6-E	Cisco	WS-X45-SUP6-E	<span style="background-color: #fd7e14; color: white; padding: 2px 5px; border-radius: 3px;">✎</span> <span style="background-color: #6c757d; color: white; padding: 2px 5px; border-radius: 3px;">▼</span>
<input type="checkbox"/> WS-X4648-RJ45V+E	Cisco	WS-X4648-RJ45V+E	<span style="background-color: #fd7e14; color: white; padding: 2px 5px; border-radius: 3px;">✎</span> <span style="background-color: #6c757d; color: white; padding: 2px 5px; border-radius: 3px;">▼</span>


Showing 1-4 of 4

Per Page ▼


✎ Edit Selected
🗑 Delete Selected



Organization



Racks



Devices

**DEVICES**

Devices

Modules

Device Roles

Platforms

Virtual Chassis

**DEVICE TYPES**

Device Types

Module Types + ↑

Manufacturers

**DEVICE COMPONENTS**

Interfaces

Front Ports

Rear Ports

Console Ports

Console Server Ports

# Netbox

## Výrobcovia



netbox Community

Organization Racks Devices

DEVICES

Devices Modules Device Roles Platforms Virtual Chassis

DEVICE TYPES

Device Types Module Types

Manufacturers + ↕

DEVICE COMPONENTS

Interfaces Front Ports Rear Ports Console Ports Console Server Ports Module Bays

Search...

Staff

### Manufacturers

+ Add ↕ Import ↕ Export ↕

Results 8 Filters

Quick search [ ] [ ] [ Configure Table ]

<input type="checkbox"/>	NAME	RACK TYPES	DEVICE TYPES	MODULE TYPES	INVENTORY ITEMS	PLATFORMS	DESCRIPTION	SLUG	
<input type="checkbox"/>	Canonical	0	0	0	0	3	Canonical Ltd. je softvérová spoločnosť vyvíjajúca a podporujúca slobodný softvér.	canonical	
<input type="checkbox"/>	Cisco	0	10	4	0	4	Cisco Systems, Inc., bežne známa ako Cisco, je americká nadnárodná spoločnosť konglomerátu digitálnych komunikačných technológií.	cisco	
<input type="checkbox"/>	Fortinet	0	2	0	0	1	Fortinet, Inc. je spoločnosť zaoberajúca sa kybernetickou bezpečnosťou.	fortinet	



netbox  
Community

Staff

Organization

Racks

Devices

+ Add

↑ Import

↓ Export

Results 740

Filters

Quick search

<input type="checkbox"/>	NAME	DEVICE	LABEL	ENABLED	TYPE	DESCRIPTION	
<input type="checkbox"/>	Dot11Radio0	kis-ap1-b306	—	✓	IEEE 802.11n	—	
<input type="checkbox"/>	Dot11Radio1	kis-ap1-b306	—	✓	IEEE 802.11ac	—	
<input type="checkbox"/>	GigabitEthernet0	kis-ap1-b306	—	✓	1000BASE-T (1GE)	—	
<input type="checkbox"/>	GigabitEthernet1	kis-ap1-b306	—	✓	1000BASE-T (1GE)	—	
<input type="checkbox"/>	Dot11Radio0	kis-ap2-b355	—	✓	IEEE 802.11n	—	
<input type="checkbox"/>	Dot11Radio1	kis-ap2-b355	—	✓	IEEE 802.11ac	—	
<input type="checkbox"/>	GigabitEthernet0	kis-ap2-b355	—	✓	1000BASE-T (1GE)	—	
<input type="checkbox"/>	GigabitEthernet1	kis-ap2-b355	—	✓	1000BASE-T (1GE)	—	
<input type="checkbox"/>	Dot11Radio0	kis-ap3-b351	—	✓	IEEE 802.11n	—	
<input type="checkbox"/>	Dot11Radio1	kis-ap3-b351	—	✓	IEEE 802.11ac	—	

DEVICES

Devices

Modules

Device Roles

Platforms

Virtual Chassis

DEVICE TYPES

Device Types

Module Types

Manufacturers

DEVICE COMPONENTS

Interfaces

+
↑

Front Ports

Rear Ports

Console Ports

Console Server Ports

# Connections - Káble



netbox  
Community

- Organization
- Racks
- Devices
- Connections

**CONNECTIONS**

- Cables
- Wireless Links
- Interface Connections
- Console Connections
- Wireless
- IPAM
- VPN
- Virtualization
- Provisioning
- Customization
- Operations
- Topology Views

🔦 🔔 Staff

## Cables

+ Add
↑ Import
↓ Export

Results 217

Filters

▼

⚙️ Configure Table

	ID	LABEL	TERMINATION A	TERMINATION B	STATUS	TYPE	
<input type="checkbox"/>	295	—	e01-tabula1 (1)	Port 1	Connected	CAT5e	<span>✎</span> <span>▼</span>
<input type="checkbox"/>	296	—	e02-pc1 (2)	Port 1	Connected	CAT5e	<span>✎</span> <span>▼</span>
<input type="checkbox"/>	297	—	e03-tabula2 (3)	Port 2	Connected	CAT5e	<span>✎</span> <span>▼</span>
<input type="checkbox"/>	298	—	e04-pc2 (4)	Port 2	Connected	CAT5e	<span>✎</span> <span>▼</span>
<input type="checkbox"/>	299	—	e05-rack1 (5)	Port 3	Connected	CAT5e	<span>✎</span> <span>▼</span>
<input type="checkbox"/>	300	—	e06-pc3 (6)	Port 3	Connected	CAT5e	<span>✎</span> <span>▼</span>
<input type="checkbox"/>	301	—	e07-rack2 (7)	Port 4	Connected	CAT5e	<span>✎</span> <span>▼</span>
<input type="checkbox"/>	302	—	e08-pc4 (8)	Port 4	Connected	CAT5e	<span>✎</span> <span>▼</span>
<input type="checkbox"/>	303	—	e09-projektor (9)	Port 5	Connected	CAT5e	<span>✎</span> <span>▼</span>
<input type="checkbox"/>	304	—	e10-pc5 (10)	Port 5	Connected	CAT5e	<span>✎</span> <span>▼</span>

133



netbox  
Community

Staff

## Interface Connections Export

Results 74
Filters

DEVICE	INTERFACE	CONNECTION	REACHABLE	
kis-ap1-b306	GigabitEthernet0	RB355-1-SW02-Cat4506 > GigabitEthernet3/23	✓	
kis-ap2-b355	GigabitEthernet0	RB355-1-SW02-Cat4506 > GigabitEthernet5/14	✓	
kis-ap3-b351	GigabitEthernet0	RB355-1-SW02-Cat4506 > GigabitEthernet3/6	✓	
kis-ap4-b303	GigabitEthernet0	RB303-4-SW01-Stack > GigabitEthernet2/0/14	✓	
kis-ap5-b301	GigabitEthernet0	RB303-4-SW01-Stack > GigabitEthernet2/0/22	✓	
kis-ap6-b302	GigabitEthernet0	RB303-4-SW01-Stack > GigabitEthernet2/0/18	✓	
kis-ap11-b359	GigabitEthernet0	RB355-1-SW02-Cat4506 > GigabitEthernet5/18	✓	
kis-ap12-b355	GigabitEthernet0	RB355-1-SW02-Cat4506 > GigabitEthernet5/18	✓	

- Organization
- Racks
- Devices
- Connections
- CONNECTIONS**
- Cables
- Wireless Links
- Interface Connections
- Console Connections
- Wireless
- IPAM
- VPN
- Virtualization
- Provisioning
- Customization
- Operations
- Topology Views



netbox  
Community

🔦
🔔
Staff

Devices / FRI dcim.device:81

## kis-ap1-b306

Created 2025-03-10 18:40 · Updated 2025-03-20 08:30

📎 Add Attachment
+ Add Components
🔖 Bookmark
🔔 Subscribe
📄 Clone

✎ Edit
🗑 Delete

Device
Interfaces 4
Console Ports 1
Attachments
Config Context
Render Config
Contacts
Journal


Changelog



Device	
Region	—
Site	FRI
Location	RB306
Rack	—
Position	—
GPS Coordinates	—
Tenant	KIS
Device Type	Cisco Aironet 2702I-E-K9 (OU)
Description	—
Airflow	—

Management	
Status	<span style="background-color: #008080; color: white; padding: 2px 5px; border-radius: 3px;">Active</span>
Role	Access Point
Platform	Cisco AIR-CAP27
Primary IPv4	192.168.255.201 <span style="background-color: #444; color: white; padding: 0 2px;">📄</span>
Primary IPv6	—
Out-of-band IP	—

**Services** + Add a service

NAME	PARENT	PROTOCOL	PORTS	DESCRIPTION
— No services found —				





Staff

- Organization
- Racks
- Devices
- DEVICES**
- Devices
- Modules
- Device Roles
- Platforms
- Virtual Chassis
- DEVICE TYPES**
- Device Types
- Module Types
- Manufacturers
- DEVICE COMPONENTS**
- Interfaces + -
- Front Ports
- Rear Ports
- Console Ports
- Console Server Ports
- Module Bays
- Device Bays
- ADDRESSING**
- MAC Addresses
- Connections
- Wireless
- IPAM

### Cable Trace for Interface GigabitEthernet0

**kis-ap1-b306**  
Cisco Aironet 2702I-E-K9  
FRI / RB306

**GigabitEthernet0**

Cable #496  
Connected

**Port 12**

**Patch-RB355-1**  
Generic 24-port Copper Patch Panel  
FRI / RB355 / RB355-1 / Front / U39.0

**Port 12**

Cable #412  
Connected

**GigabitEthernet3/23**

**RB355-1-SW02-Cat4506**  
Cisco Catalyst 4506-E  
FRI / RB355 / RB355-1 / Front / U15.0

[Download SVG](#)

#### Related Paths

ORIGIN	DESTINATION	SEGMENTS
None found		

# Netbox IP adresy



netbox Community

- Organization
- Racks
- Devices
- Connections
- Wireless
- IPAM
  - IP ADDRESSES**
  - IP Addresses
  - IP Ranges
  - PREFIXES
    - Prefixes
    - Prefix & VLAN Roles
  - AGGREGATES
    - Aggregates
    - RIRs
  - VLANS
    - VLANS
  - OTHER
    - FUPD Groups

Search...

IP Addresses + Add Import Export

Results **383** Filters

Quick search

<input type="checkbox"/>	IP ADDRESS	VRF	STATUS	ROLE	TENANT	ASSIGNED	DNS NAME	DESCRIPTION	<input type="button" value="Copy"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/>	10.11.0.1/24	Global	Active	—	KIS	—	—	Serverovna c5   Fortigate	<input type="button" value="Copy"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/>	10.11.0.2/24	Global	Active	—	KIS	—	—	VM na Ctrl2	<input type="button" value="Copy"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/>	10.11.0.3/24	Global	Active	—	KIS	—	—	VM na Ctrl2	<input type="button" value="Copy"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/>	10.11.0.4/24	Global	Active	—	KIS	—	—	VM na Ctrl2	<input type="button" value="Copy"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/>	10.11.0.5/24	Global	Active	—	KIS	—	—	VM na Ctrl2	<input type="button" value="Copy"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/>	10.254.0.1/24	Global	Active	—	KIS	—	—	Serverovna c5   Fortigate	<input type="button" value="Copy"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/>	10.254.0.5/24	Global	Active	—	KIS	—	—	Serverovna c5   VM na Ctrl2	<input type="button" value="Copy"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/>	10.254.0.11/24	Global	Active	—	KIS	—	—	Serverovna c5   Cisco UCS 220 M3 CIMC	<input type="button" value="Copy"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/>	10.254.0.12/24	Global	Active	—	KIS	—	—	Serverovna c5   Cisco UCS 220 M3 ESXi	<input type="button" value="Copy"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/>	10.254.0.13/24	Global	Active	—	KIS	—	—	Serverovna c5   Cisco UCS 220 M3	<input type="button" value="Copy"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>




 Community	Search...	Staff								
<ul style="list-style-type: none"> <li>Organization</li> <li>Racks</li> <li>Devices</li> <li>Connections</li> <li>Wireless</li> <li>IPAM</li> </ul>	<input type="checkbox"/> 172.23.0.0/24	Active	0	Global	0.0%	KIS	FRI	KIS-CCTest-external (1023)	Cloud	—
	<input type="checkbox"/> 192.168.10.0/24	Active	0	Global	43.7%	KIS	FRI	Internal (10)	Data	—
	<input type="checkbox"/> 192.168.20.0/24	Active	0	Global	0.0%	KIS	FRI	SAN (20)	Data	—
	<input type="checkbox"/> 192.168.30.0/24	Active	0	Global	1.6%	KIS	FRI	ECDL (30)	Data	—
	<input type="checkbox"/> 192.168.31.0/24	Active	0	Global	6.7%	KIS	FRI	B301 (31)	Data	—
	<input type="checkbox"/> 192.168.32.0/24	Active	0	Global	1.6%	KIS	FRI	B302 (32)	Data	—
	<input type="checkbox"/> 192.168.33.0/24	Active	0	Global	2.8%	KIS	FRI	B303 (33)	Data	—
	<input type="checkbox"/> 192.168.34.0/24	Active	0	Global	2.8%	KIS	FRI	B03 (34)	Data	—
	<input type="checkbox"/> 192.168.40.0/24	Active	0	Global	11.4%	KIS	FRI	VoIP (40)	VoIP	—
	<input type="checkbox"/> 192.168.50.0/24	Active	0	Global	0.4%	KIS	FRI	IOT (50)	IoT	—
	<input type="checkbox"/> 192.168.60.0/24	Active	0	Global	0.8%	KIS	FRI	SOC (60)	Management	—
	<input type="checkbox"/> 192.168.110.0/24	Active	0	Global	0.8%	KIS	FRI	IntWIFI (110)	Wireless	—
	<input type="checkbox"/> 192.168.120.0/24	Active	0	Global	0.8%	KIS	FRI	WiFi_KIS_students (120)	Wireless	—
	<input type="checkbox"/> 192.168.130.0/24	Active	0	Global	0.8%	KIS	FRI	WiFi_eduroam (130)	Wireless	—

# Netbox

## Virtuálne siete





Search...

Staff

### VLANS

[+ Add](#) [↑ Import](#) [↓ Export](#)

Results **34** Filters

Quick search   [Configure Table](#)

<input type="checkbox"/>	VID	NAME	SITE	GROUP	PREFIXES	TENANT	STATUS	ROLE	DESCRIPTION	<input type="button" value="✎"/>	<input type="button" value="▼"/>
<input type="checkbox"/>	1	default	FRI	—	—	KIS	Active	Other	Default vlan	<input type="button" value="✎"/>	<input type="button" value="▼"/>
<input type="checkbox"/>	10	Internal	FRI	—	192.168.10.0/24	KIS	Active	Data	Dátová pevná sieť KIS	<input type="button" value="✎"/>	<input type="button" value="▼"/>
<input type="checkbox"/>	11	KIS-Cloud-internal	FRI	—	10.11.0.0/16	KIS	Active	Cloud	Katedrový Cloud	<input type="button" value="✎"/>	<input type="button" value="▼"/>
<input type="checkbox"/>	20	SAN	FRI	—	192.168.20.0/24	KIS	Active	Data	Dátová/SAN sieť	<input type="button" value="✎"/>	<input type="button" value="▼"/>
<input type="checkbox"/>	30	ECDL	FRI	—	192.168.30.0/24	KIS	Active	Data	ECDL sieť	<input type="button" value="✎"/>	<input type="button" value="▼"/>
<input type="checkbox"/>	31	B301	FRI	—	192.168.31.0/24	KIS	Active	Data	RB301 sieť	<input type="button" value="✎"/>	<input type="button" value="▼"/>
<input type="checkbox"/>	32	B302	FRI	—	192.168.32.0/24	KIS	Active	Data	RB302 sieť	<input type="button" value="✎"/>	<input type="button" value="▼"/>
<input type="checkbox"/>	33	B303	FRI	—	192.168.33.0/24	KIS	Active	Data	RB303 sieť	<input type="button" value="✎"/>	<input type="button" value="▼"/>
<input type="checkbox"/>	34	B03	FRI	—	192.168.34.0/24	KIS	Active	Data	RB03 sieť	<input type="button" value="✎"/>	<input type="button" value="▼"/>



- 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; 5 = Plná CRUD funkcionálna 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; 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; 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; 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; 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; 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; 5 = Viacúrovňová bidirekčná integrácia s relevantnými systémami.

# 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; 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; 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; 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; 5 = Automatizované discovery s plánovaním a API vstupmi.
12 Webové rozhranie s možnosťou úprav a prehľadnou správou	Používateľsky prívetivé GUI pre správu assetov.	1 = Neintuitívne alebo len CLI; 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; 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; 5 = Komplexné sledovanie s upozomeniami a stavmi.
15 Upozomenia na zmenu stavu, expirácie, servisné intervaly	Automatické notifikácie pri zmene stavu alebo potrebe servisného zásahu.	1 = Bez upozomení; 5 = Konfigurovateľné upozomenia podľa podmienok alebo kalendára.



# Reálna implementácia procesu riadenia rizík (MONARC)

# 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



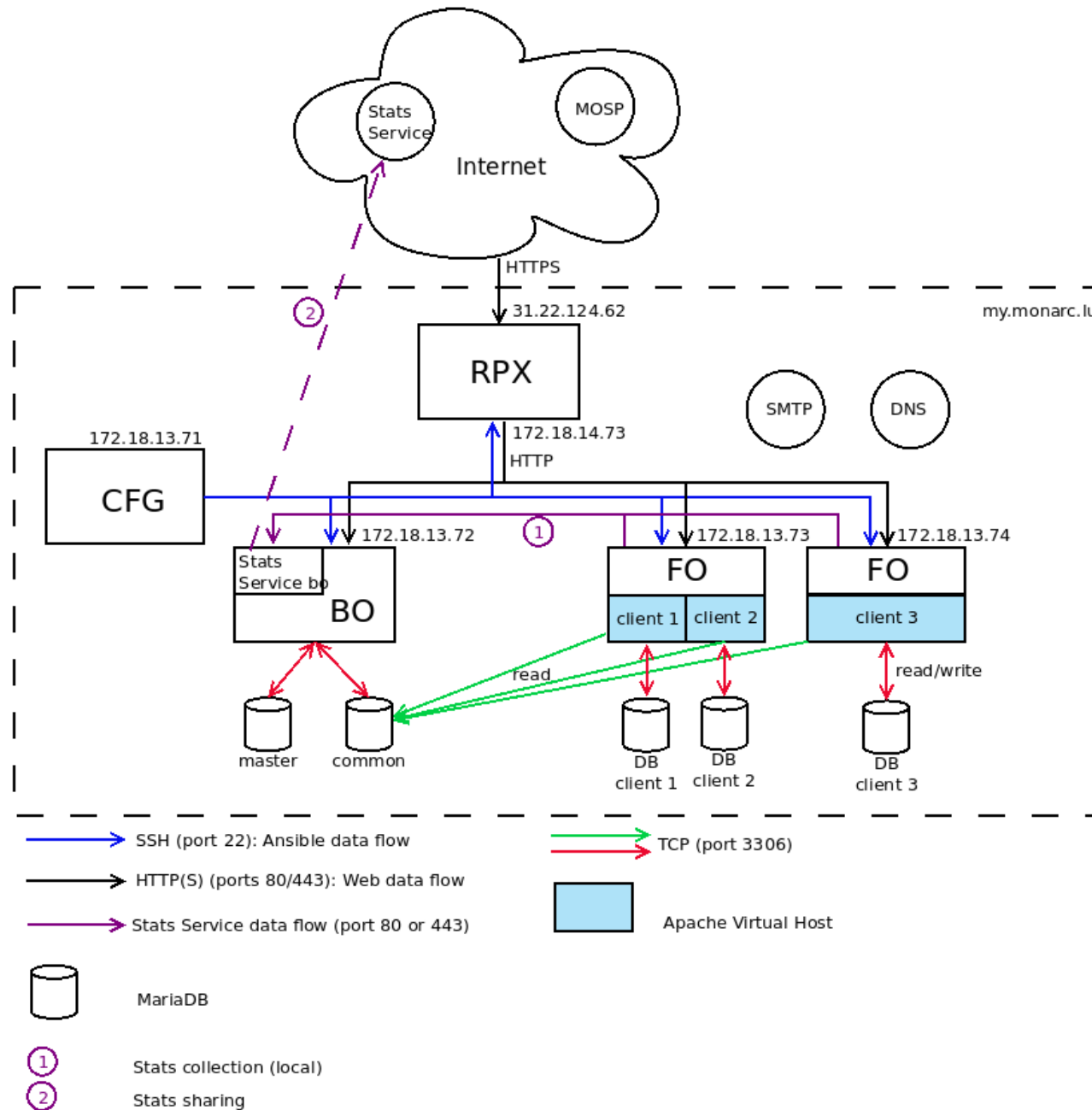
- MONARC sa skladá z 2 hlavných častí:
  - **Back office (BO)** – správa bezpečnostných modelov, FO serverov a klientov inštalácií MONARC
  - **Front office (FO)** – riadenie analýzy rizík, FO nepotrebuje využívať BO
- Celá architektúra obsahuje dodatočný reverzný proxy (RPX) a konfiguračný server (CFG). 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)

# 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 ošetrovanie rizík:

- posúdenie hrozieb, zraniteľností a úrovne rizík
- návrh opatrení na zníženie významných rizík

## 4. implementácia a monitorovanie:

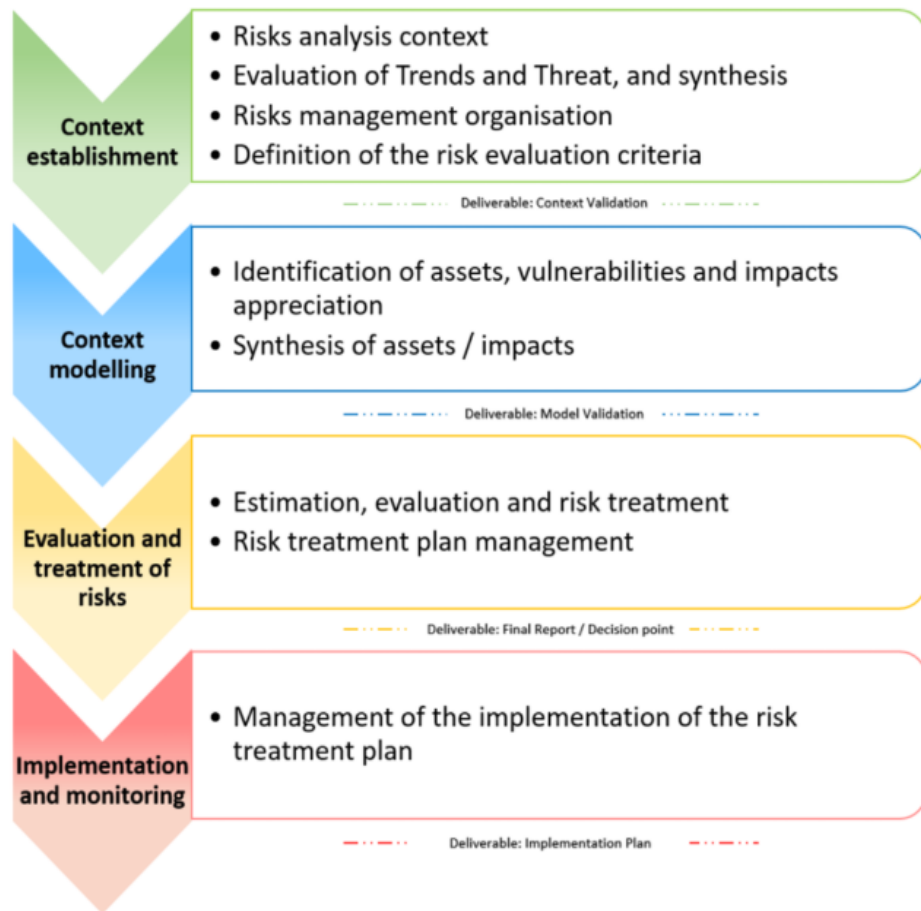
- realizácia odporúčaných bezpečnostných opatrení
- priebežné sledovanie zmien a aktualizácia analýzy



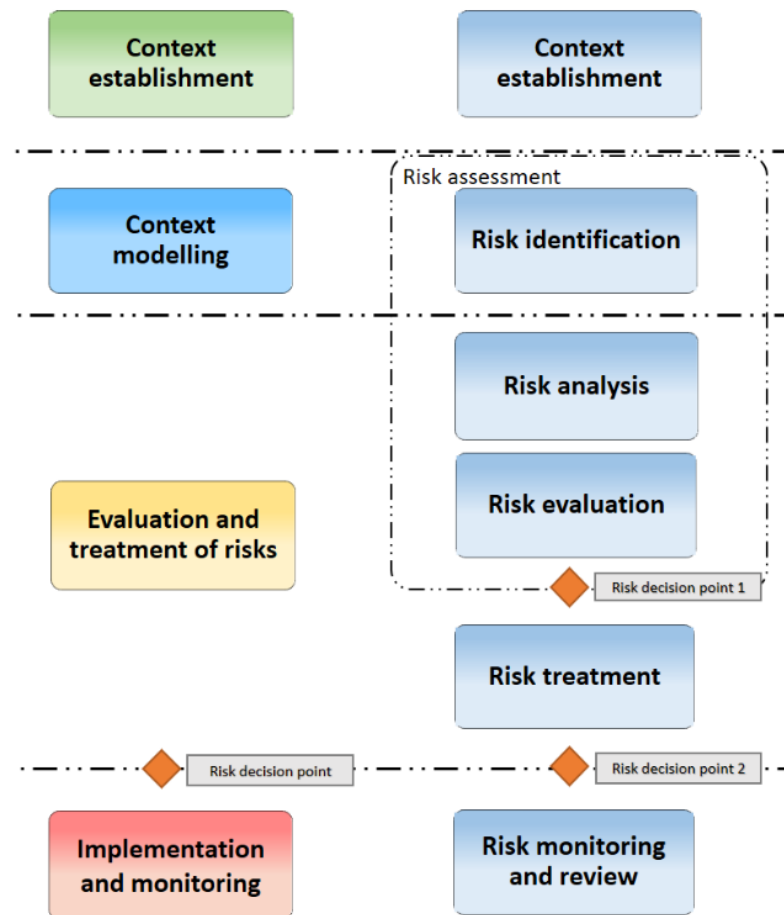
# Analýza rizík v 4 fázach



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 analýzám 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

Risk analysis label	Permissions
Test	No access
Testv2	No access
KIS FRI UNIZA	No access
	Read
	Read and write

# Nastavenie pri vytváraní projektu



Create a risk analysis ✕


Source

List of risks models  Existing risk analysis

Select a risks model \*

Modelling CASES

Description

 Language \*

 Name \*

 Description

 + Add referential

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

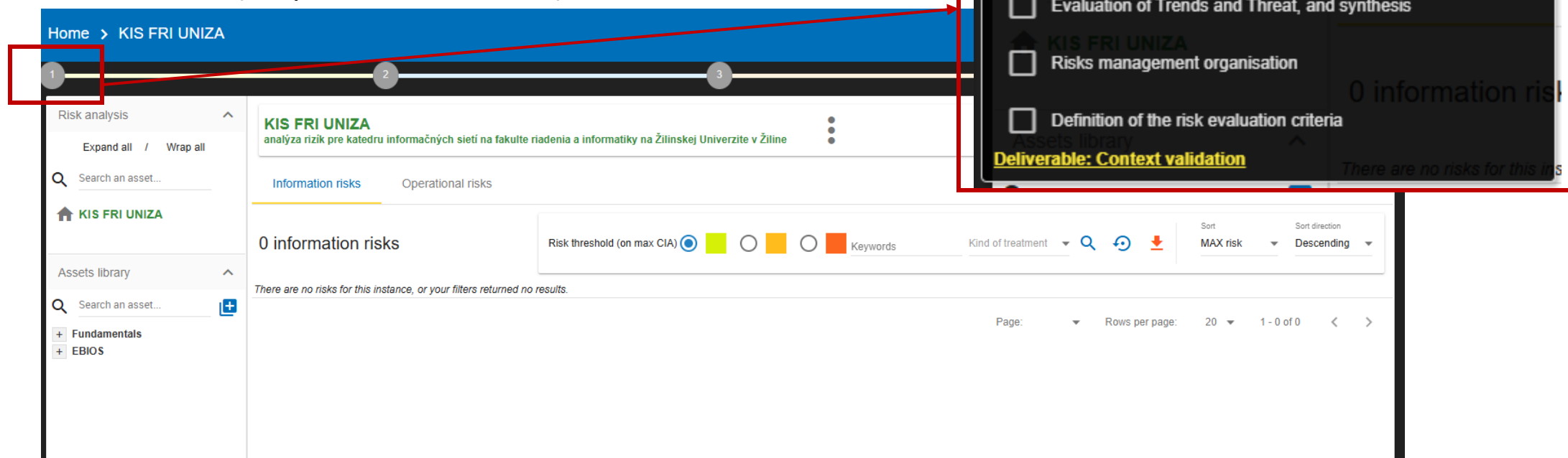
Výber bezpečnostného štandardu, ktorý chceme pridať / podľa akej normy alebo rámca chceme hodnotiť a riadiť riziká

Cancel

Create

# 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).



Home > KIS FRI UNIZA

1

Risk analysis

Expand all / Wrap all

Search an asset...

KIS FRI UNIZA

Assets library

Search an asset...

Fundamentals

EBIOS

KIS FRI UNIZA  
analýza rizík pre katedru informačných sietí na fakulte riadenia a informatiky na Žilinskej Univerzite v Žiline

Information risks Operational risks

0 information risks

Risk threshold (on max CIA)       Keywords

Kind of treatment

Sort MAX risk Sort direction Descending

Page: Rows per page: 20 1 - 0 of 0

Context Establishment

Expand all / Wrap all

Risks analysis context 1.A

Evaluation of Trends and Threat, and synthesis

Risks management organisation

Definition of the risk evaluation criteria

Assets library

Deliverable: Context validation

There are no risks for this instance, or your filters returned no results.

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



Hlavné časti, ktoré sa v tomto kroku vyplňajú:

- **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...)

Risks analysis context

**General consideration:**

The purpose of this risk analysis is to support the implementation of information security risk management in accordance with the ISO/IEC 27005 standard and to improve the overall security level of the Department of Information Networks (KIS) at the Faculty of Management Science and Informatics, University of Žilina (UNIZA).

The analysis aims to identify, assess and treat risks related to the

- operation of educational,
- research and laboratory information systems, with a focus on protecting student data,
- research results,
- the availability of internal network services.

The results of this risk analysis are intended for internal use only and serve as a basis for the future development of an Information Security Management System (ISMS) and for alignment with applicable legal requirements, including GDPR.

**Risk Management Approach:**

The risk management process follows the ISO/IEC 27005 methodology and is based on an iterative cycle of risk identification, assessment, treatment and monitoring.

The risk analysis will be reviewed at least once per year or whenever relevant changes occur in the infrastructure, processes, systems or security requirements.

The risk owner is the Head of the Department of Information Networks (KIS) at FRI UNIZA, or a delegated network/security responsible person. A Risk Treatment Plan will be created for unacceptable risks, specifying responsible persons, deadlines and mitigation measures. The default risk evaluation model (impact and likelihood scoring) provided by MONARC will be used for the assessment.

**Basic Criteria:**

**Impact Criteria:**  
The impact of risks is evaluated based on the following dimensions:

- impact on the availability of network services and laboratory infrastructure,
- impact on teaching and education continuity,
- impact on research activities and scientific results,
- reputational impact on the department, faculty or university.

**Risk evaluation criteria:**  
The default MONARC scale (1–5 for likelihood and 1–5 for impact) is used to calculate the risk score (1–25).

**Additional information**

General considerations: What is the purpose of the information security risk management? ISMS Management, preparation of a business continuity plan or incident response plan, legal compliance.

Risk management approach: ongoing iteration, provision of resources.

Basic Criteria:  
- Risk evaluation criteria: The process strategic value or information, legal obligations, regulatory requirements or contractuals.  
- Impact criteria: Consequences on business, image, legal, ...  
- Risk acceptance criteria: ROSI (Return On Security Investment), legal and regulatory aspects, future security risk management, company strategy.

Scope and boundaries: Activity, business processes, organization's objectives, limits and exclusion of the analysis (geographical, logical ...), legal requirements, socio-cultural environment, other requirements.

General Considerations

Risk management approach

Basic criteria

Scope and boundaries

Cancel Save

1

## Context Establishment

1.A

- Risks analysis context
- Evaluation of Trends and Threat, and synthesis
- Risks management organisation
- Definition of the risk evaluation criteria

Deliverable: Context validation

There are no risks for this...

# 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:

Evaluation of Trends and Threat, and synthesis
×

Trends assessment

Threats assessment

Summary

What is the purpose of your organization?

---

What is the progression of your business in recent years?

---

What is the evolution of the external environment (competition, market evolution, laws, etc.)?

---

What might be the attack reasons on your structure?

---

What are your most important business processes?

---

# 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 obsluhu, 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

# 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 káblach 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

# 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

# 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

# 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

Evaluation of Trends and Threat, and synthesis ×

Trends assessment
Threats assessment
Summary

Threats analysis - 1 / 30 Error in use ▾

**Theme:** Compromise of functions

**Description:** A person commits an operating error, input error or utilisation error on hardware or software.

**Comments:** Osoba sa dopustí chyby pri obsluhu, chyby pri zadávaní vstupov alebo chyby pri používaní hardvéru alebo softvéru.

**Impacted criteria:**  C  I  A

**Trend:**  -  n  +  ++

< Previous
Save
Next >

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



Sekcia II: **Threats assessment**

Evaluation of Trends and Threat, and synthesis



Trends assessment

**Threats assessment**

Summary

Threats analysis - 30 / 30

Environmental disaster (fire, flood, dust, dirt, etc.)

Theme: Physical damage

Description: Any event that can physically ruin the premises

Comments

Závažná prírodná udalosť môže poškodiť zariadenia alebo prerušiť napájanie.

Impacted criteria

C  I  A

Trend

☉ - ○ n ○ + ○ ++

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

< Previous

Save

Next >

# 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

### Evaluation of Trends and Threat, and synthesis

Trends assessment

Threats assessment

**Summary****B****I**

↺

↑

☰

☰

↶

↷

i

Na základe vyhodnotenia trendov a analýzy hrozieb možno konštatovať, že najvýznamnejšie riziká pre Katedru informačných sietí (KIS) FRI UNIZA sú spojené najmä s dostupnosťou a bezpečnosťou interných IT služieb, sieťovej a serverovej infraštruktúry. Výraznú úlohu pritom zohráva rastúca závislosť na digitálnych prostriedkoch výučby, správe študijných dát a výskumných projektov.

Medzi kľúčové hrozby patria najmä:

- Poruchy hardvéru a softvéru, ktoré môžu viesť k výpadkom služieb
- Chyby používateľov pri konfigurácii alebo správe systémov
- Kybernetické útoky ako malware a DoS útoky, ktoré ohrozujú dostupnosť a bezpečnosť systémov
- Výpadky elektrickej energie alebo telekomunikačných služieb, ktoré môžu narušiť výučbu aj výskumné činnosti

Hrozby spojené s fyzickými katastrofami (požiar, povodeň) alebo sofistikovanou špionážou sú hodnotené ako málo pravdepodobné v aktuálnom kontexte.

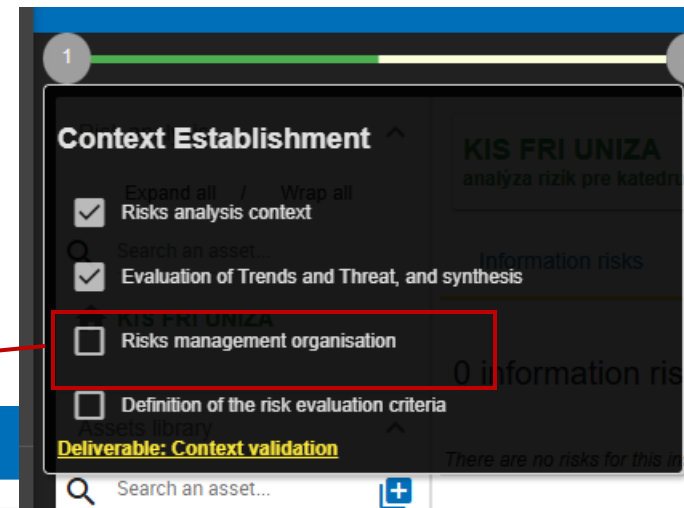
Opakujúce sa incidenty (napr. používateľské chyby, výpadky zariadení alebo výskyt malware) a rastúci počet kybernetických hrozieb naznačujú potrebu zlepšenia procesov riadenia rizík, posilnenia ochrany IT infraštruktúry a pravidelného školenia používateľov. Výstupy z tejto fázy tvoria základ pre ďalší krok – modelovanie rizík a priradenie hrozieb ku konkrétnym aktívam organizácie.

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

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

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

## Risks management organisation



**Context Establishment**

- Risks analysis context
- Evaluation of Trends and Threat, and synthesis
- Risks management organisation
- Definition of the risk evaluation criteria

**Deliverable: Context validation**

Search an asset...

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 ošetrovaní 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 úrovni 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**

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

Typ rizika	Čo znamená	Ako sa hodnotí	Príklady
<b>Informačné riziká</b>	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
<b>Operačné riziká</b>	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

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

**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 informácií
- 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

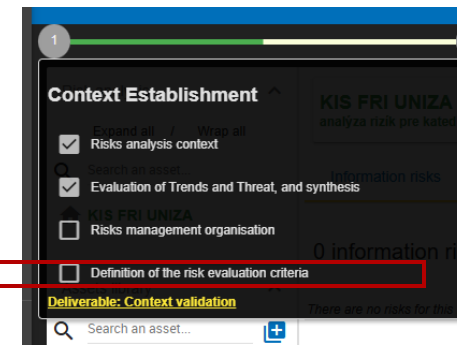
Typ rizika	Čo znamená	Ako sa hodnotí	Príklady
Informačné riziká	Riziká, ktoré ohrozujú konkrétne aktívum (napr. server, dáta, proces, aplikáciu)	Kombináciou CIA triády + ROLPF a vždy sa berie najhoršia (max) hodnota	únik dát, strata integrity databázy, nedostupnosť servera
Operačné riziká	Riziká, ktoré 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. The confidentiality criterion is not important.	Nonexistent impact. The integrity criterion is not important.	Nonexistent impact. The availability criterion is not important.	No consequences
1	Weak Impact, Insignificant. Information leaks are negative to the organization's interests. Examples: - Internal information leaks which shouldn't be outside the company. - Memorandum - Internal phone directory	Weak Impact, Insignificant. Corruption easy to rectify without any consequences. Example: - Internal mail or letter.	Weak impact, insignificant. Unavailability which is inconvenient, but not really harmful for the stakeholders.	Sporadic media criticism
2	Average impact, acceptable. Information leaks harm organization's interests. Examples: - Moderately sensitive information leaks which are only for a group of people. - Internal networking scheme. - Documentation or source code which is non-critical.	Average impact, acceptable. Corruption which brings an inconvenience to the stakeholders. Recovery is easy. Example: - Informational web site.	Average impact, acceptable. Unavailability which brings an inconvenience to the stakeholders. Example: - Maximum time periods consider as unbearable are not reached.	Temporary degradation or staff reputation. Occasional media criticism
3	Strong impact, hardly bearable. Information leaks seriously harm organization's interest. Example: - Confidential information leaks. - Bank secrecy - Sensitive personal data - Security incident	Strong impact, hardly bearable. Corruption which brings a considerable inconvenience to the stakeholders. Example: - Confusion between stakeholders.	Strong impact, hardly bearable. Unavailability which bring a considerable inconvenience to the stakeholders. Example: - Maximum time periods consider as unbearable are reached.	Strong degradation of staff reputation. Serious and repeated
4	Really strong impact, unbearable. Information leaks almost deadly harm organization's interest. Example: - Secret or really sensitive information leaks. - Classified information by the law (the EU, NATO, national...)	Really strong impact, unbearable. Corruption which can't be recovered or bring a permanent downtime.	Really strong impact, unbearable. Unavailability which asks some drastic efforts to recover, or even final. Example: - Important maximums time periods consider as unbearable.	Death of someone. Definitive degradation staff reputation. International media criticism
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					
<input type="checkbox"/> 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. 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. 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).	Significant 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. 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).	Significant consequences which could be topped, but with some serious difficulties (funds embezzlement, bank ban, deterioration of goods, job loss.).
4	Death of someone. Definitive degradation of the company or staff reputation. International media coverage.	Complete stop of all services	Heavy sentence for the company.	Brings some deadly fees almost insurmountable (more or less 20% of the sales revenue).	Significant 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 stíženie 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 revenue).	Some inconvenience which will be topped without difficulty (Time waste, procedure reiteration, irritation, etc.).	
non-marginal fees (more or less 5% of 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.).	
heavy fees which can affect the 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.).	
deadly fees almost insurmountable (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

**Likelihood scale: [ 0 - 4 ]**

0. Vieme si tu nastaviť svoju škálu

1. Very unlikely: never happened, requires a high level of expert knowledge, or it is very expensive to execute.
2. Unlikely: might have happened, rare phenomenon which requires a good level of expert knowledge, or it is expensive to execute.
3. Could happen occasionally
4. Very likely: easy to execute, no mentionable investment or knowledge necessary

**Vulnerabilities scale: [ 0 - 5 ]**

0. No vulnerabilities.
1. Very weak vulnerability: Some efficient measures have been already taken, and their effectiveness is controlled.  
Very high maturity: Good practices are implemented and frequently verified.
2. Weak vulnerability: Some efficient measures have been already taken.  
High maturity: Good practices are implemented.
3. Average vulnerability: Some measures have been already taken, even though they could be better.  
Average maturity: Good practices are implemented without searching a better way.
4. Strong vulnerability: Some measures have been already taken, even though they are ineffective or unadapted.  
Low maturity: Good practices aren't implemented, but there are some positive reactions without any thoughts.
5. Very strong vulnerability: No measures have been implemented.  
Very low maturity or no maturity at all.

**Likelihood scale: [ 0 - 4 ]**

0. Impossible
1. Very unlikely: never happened, requires a high level of expert knowledge, or it is very expensive to execute.
2. Unlikely: might have happened, rare phenomenon which requires a good level of expert knowledge, or it is expensive to execute.
3. Could happen occasionally
4. Very likely: easy to execute, no mentionable investment or knowledge necessary

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



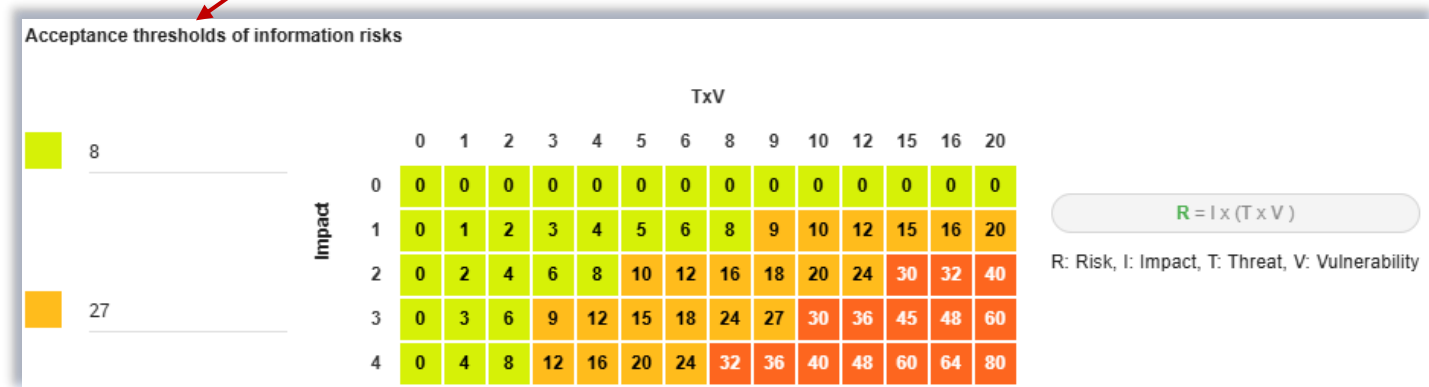
**Definition 4: Acceptance thresholds of information risks** (Prahové hodnoty pre prijatie informačných rizík)

- **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**  
**> 27 = neprijateľné, nutné riešenie**

Farba	Význam	Stav
<span style="color: green;">■</span> zelená	prijateľné riziko	nie je potrebná akcia
<span style="color: orange;">■</span> oranžová	treda sledovať / podmiennečne akceptovať	môže vyžadovať opatrenie
<span style="color: red;">■</span> 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)

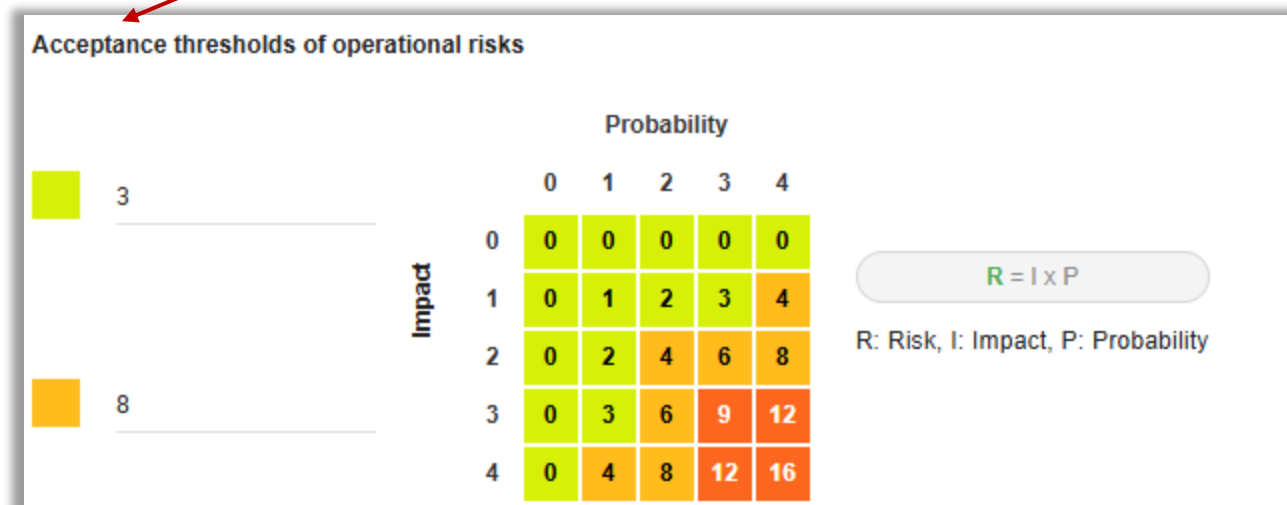
Definition 5

- **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**



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
$R = \text{Impact} \times (\text{Threat} \times \text{Vulnerability})$	$R = \text{Impact} \times \text{Probability}$
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

# 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)

Acceptance thresholds of information risks

8

24

TxV

	0	1	2	3	4	5	6	8	9	10	12	15	16	18	20	24	25	30
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	8	9	10	12	15	16	18	20	24	25	30
2	0	2	4	6	8	10	12	16	18	20	24	30	32	36	40	48	50	60
3	0	3	6	9	12	15	18	24	27	30	36	45	48	54	60	72	75	90
4	0	4	8	12	16	20	24	32	36	40	48	60	64	72	80	96	100	120
5	0	5	10	15	20	25	30	40	45	50	60	75	80	90	100	120	125	150

$R = I \times (T \times V)$

R: Risk, I: Impact, T: Threat, V: Vulnerability

Acceptance thresholds of operational risks

3

8

Probability

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	6	8	10
3	0	3	6	9	12	15
4	0	4	8	12	16	20
5	0	5	10	15	20	25







$R = I \times P$

R: Risk, I: Impact, P: Probability

Úprava akceptačného prahu

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

- úroveň zhody (súlady 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 priradzuje farby k úrovniam zhody – ako pri semaforovej metóde

Information risks		Operational risks		Compliance	
Compliance scale: 6 Levels					
	Level of compliance	Colour			
0	Non-existent				
1	Initial				
2	Managed				
3	Defined				
4	Quantitatively managed				
5	Optimized				

Úroveň	Názov	Význam
0 – Non-existent	Neexistujúca	Neexistujú žiadne pravidlá, procesy ani evidencia.
1 – Initial	Počiatková	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)

1
2

## Context Establishment

- Risks analysis context
- Evaluation of Trends and Threat, and synthesis
- Risks management organisation
- Definition of the risk evaluation criteria

**Deliverable: Context validation**

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

Integrity

Nonexistent impact.  
The integrity criterion is not important.

## 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:

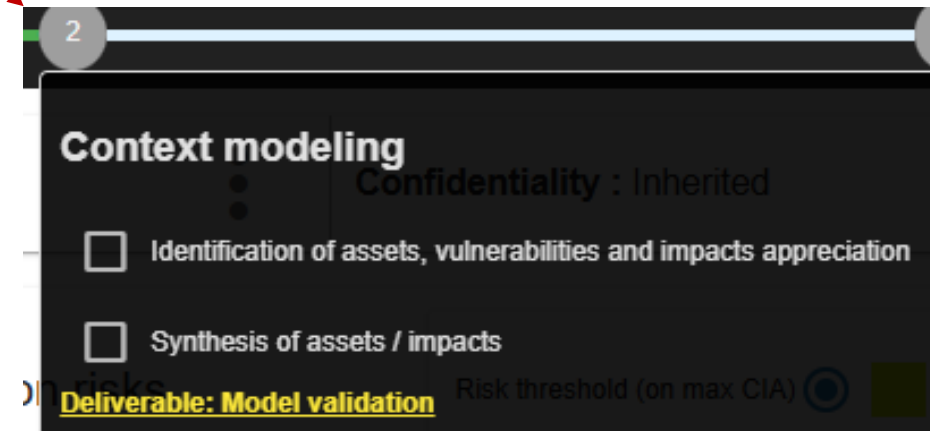
- identifikácia aktív a ich rozdelenie podľa priority
- vytvorenie rizikového modelu pomocou databázy MONARC

### 3. hodnotenie a ošetrovanie 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



2




**Context modeling**




















- Confidentiality : Inherited
- Identification of assets, vulnerabilities and impacts appreciation
- Synthesis of assets / impacts

**Deliverable: Model validation** Risk threshold (on max CIA)

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

- Preddefinovaný zoznam **aktív**

Asset types   Show active only  

<input type="checkbox"/>	Status	Label 	Code	Type	Description	Actions
<input type="checkbox"/>	✓	Backup	OV_BACKUP	Secondary	Backup	 
<input type="checkbox"/>	✓	Building, office or premises	OV_BATI	Secondary	Building, office or premises	 
<input type="checkbox"/>	✓	Business application	LOG_APP	Secondary	Custom business application or standard	 
<input type="checkbox"/>	✓	Company directory	SYS_ANU	Secondary	Company directory	 
<input type="checkbox"/>	✓	Container	CONT	Primary	Asset container	 
<input type="checkbox"/>	✓	Decision maker	PER_DEC	Secondary	Decision maker	 
<input type="checkbox"/>	✓	Desktop computer	OV_POSTE_FIXE	Secondary	Desktop computer	 
<input type="checkbox"/>	✓	Developer	PER_DEV	Secondary	Developer	 
<input type="checkbox"/>	✓	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

### Add an asset type ×

↓ Import from file ☁ Import from MOSP

Manual creation

#### Labels and descriptions

Label \*

Description

#### General information

Cancel Create Create and continue

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

- 3 spôsoby pre vloženie aktív do analýzy:

**Add an asset** ✕

↓ Asset import center
☁ Import from MOSP

Labels and descriptions

Name \*  
Router

Label \*  
network

General information

Scope  
Global

Asset type \*  
Network

Category \*  
Fundamentals >> Network

Cancel
Create
Create and continue

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:

**Add an asset** ✕

↓ Asset import center
↑ Import from MOSP

Labels and descriptions

Name \*

Router

Label \*

network

General information

Scope

Global

Asset type \*

Network

Category \*

Fundamentals >> Network

Cancel Create Create and continue

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

Add an asset



Asset import center

Import from MOSP

Labels and descriptions

Asset import center

CSV file

MONARC export file

MONARC library

Cancel

File import center

Vybrať súbor Nie je vybratý žiadny súbor

0 Assets library

Import file

name	label	asset type code	scope	operational risk tag	category
------	-------	-----------------	-------	----------------------	----------

Cancel

Cancel

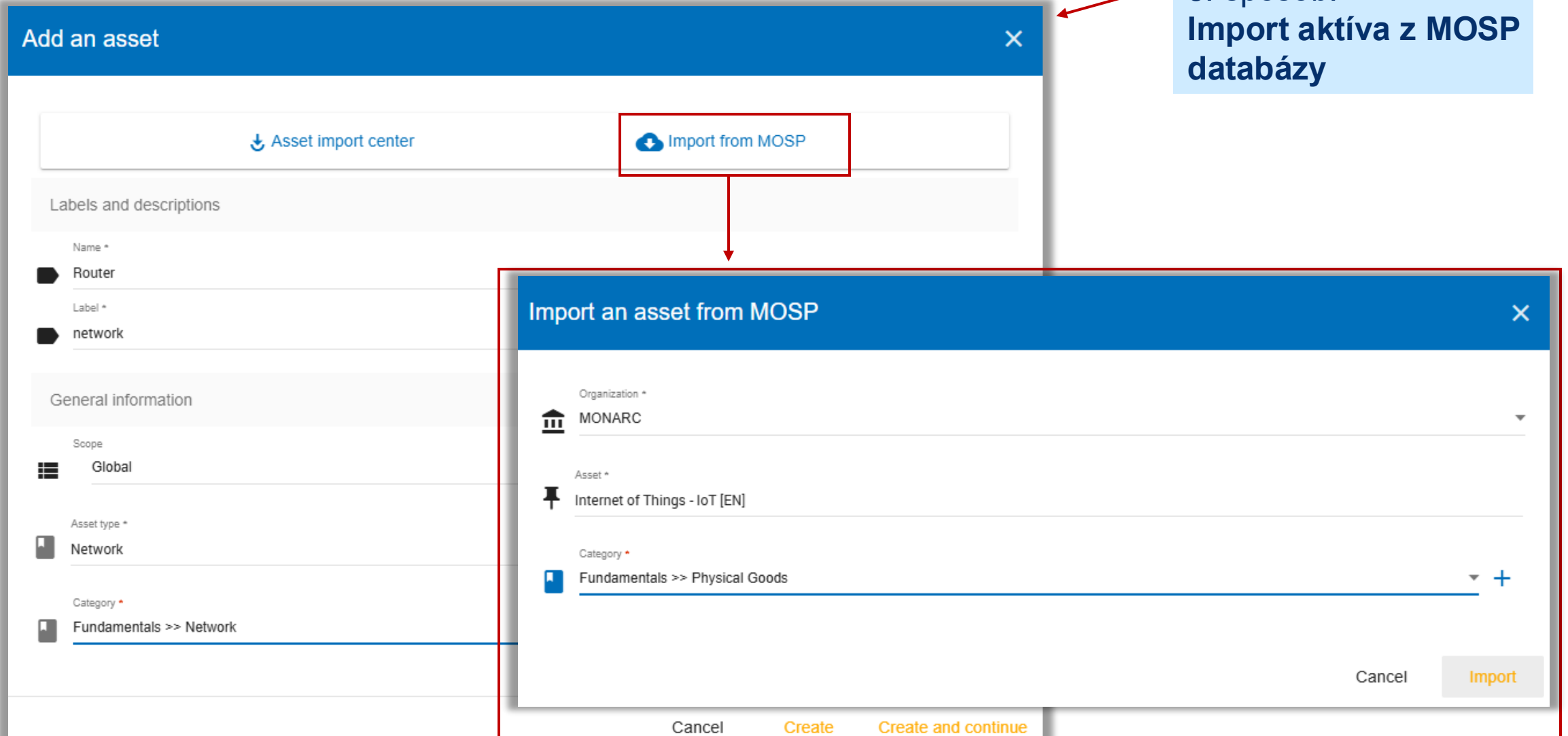
Create

Create and continue

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

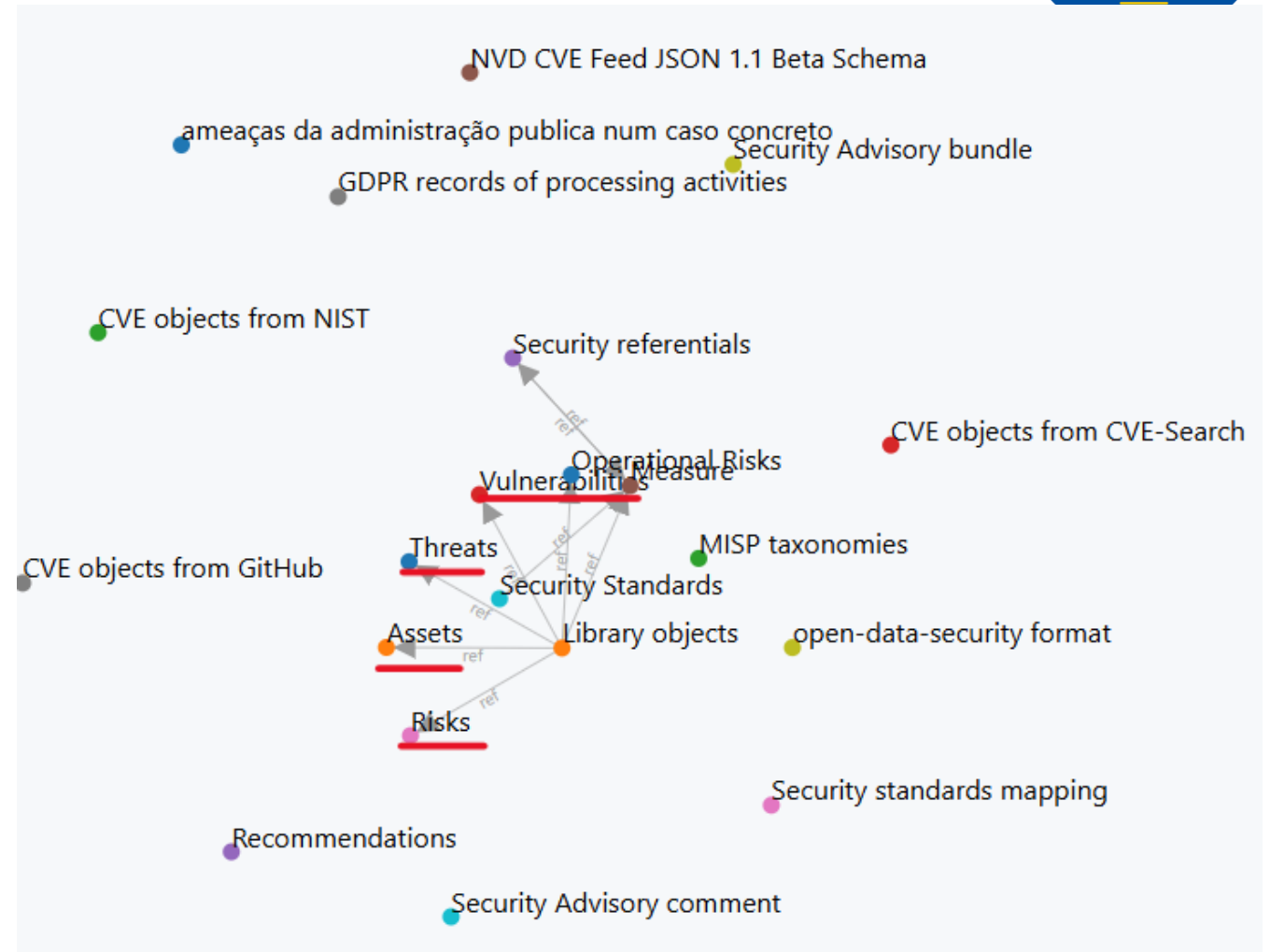
- 3 spôsoby pre vloženie aktív do analýzy:

3. spôsob:  
Import aktíva z MOSP  
databázy



The screenshot displays the 'Add an asset' interface in the MONARC system. The main window has a blue header with the title 'Add an asset' and a close button. Below the header, there is a white bar with a blue arrow icon and the text 'Asset import center'. A red box highlights the 'Import from MOSP' button, which has a blue plus icon. A red arrow points from this button to a dialog box titled 'Import an asset from MOSP'. The dialog box has a blue header and a close button. It contains several fields: 'Organization' with a dropdown menu showing 'MONARC'; 'Asset' with a dropdown menu showing 'Internet of Things - IoT [EN]'; and 'Category' with a dropdown menu showing 'Fundamentals >> Physical Goods'. At the bottom of the dialog box, there are three buttons: 'Cancel', 'Create', and 'Create and continue'. The 'Import' button is highlighted in yellow.

- 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)



## List of schemas

Create a new schema

### Vulnerabilities

Validator for vulnerabilities used in MONARC  
provided by MONARC.

validates 2834 objects

### Risks

Risks used in MONARC. A risk is composed of an Asset, a Threat and a Vulnerability.  
provided by MONARC.

validates 1938 objects

### Assets

Validator for assets used in MONARC  
provided by MONARC.

validates 168 objects

### Threats

Validator for threats used in MONARC  
provided by MONARC.

validates 123 objects

### Security referentials

Schema for the validation of security referentials aimed to be used in MONARC.  
provided by Various contributors.

validates 20 objects

### Recommendations

Recommendations sets used in MONARC.  
provided by MONARC.

validates 11 objects

## Aktíva v MOSP databáze:



## Assets

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

Search on the properties of the objects  
 code

« 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	Multifunton 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



<b>Description</b>	Any network hardware (router, switch, firewall, etc.)
<b>Owning organization</b>	<a href="#">MONARC</a>
<b>Validating JSON schema</b>	<a href="#">Assets</a> (provided by <a href="#">MONARC</a> )
<b>Creator</b>	<a href="#">Cedric</a>
<b>License</b>	Creative Commons Zero v1.0 Universal

### Related objects

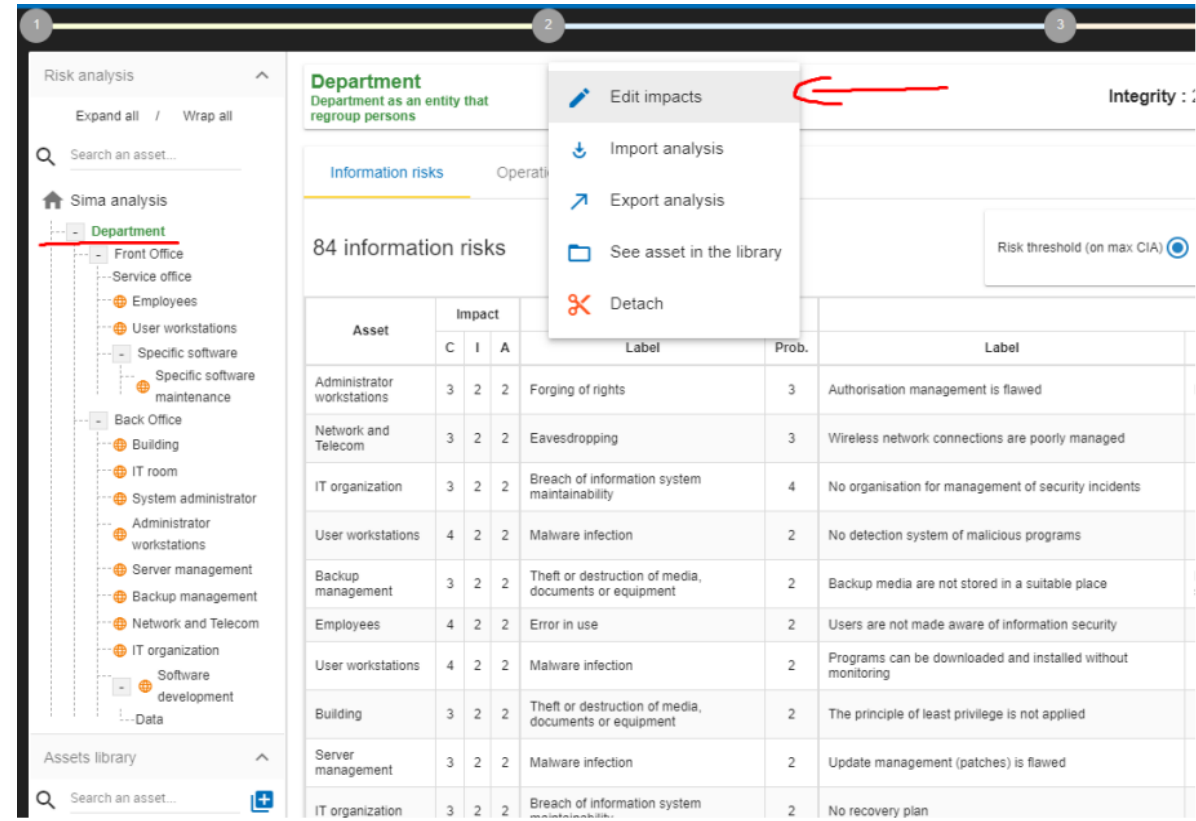
Refers to 0 object(s)   Referred to by 4 object(s)   Part of 0 collection(s)

### 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

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

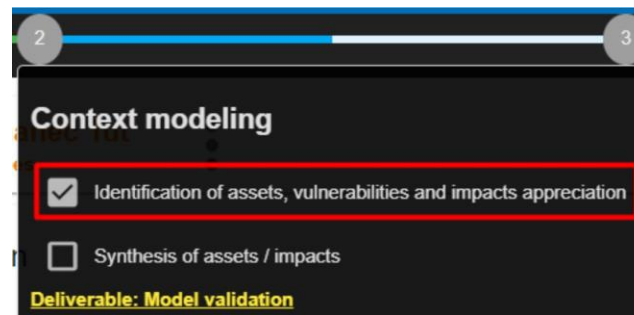
The screenshot displays the MONARC Risk analysis interface. On the left, a tree view shows the asset hierarchy under 'Sima analysis' > 'Department'. The 'Department' node is highlighted with a red line. The main area shows '84 information risks' with a table of details. A context menu is open over the table, with 'Edit impacts' highlighted by a red arrow.

Asset	Impact			Label	Prob.	Label
	C	I	A			
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 maintainability	2	No recovery plan

## 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




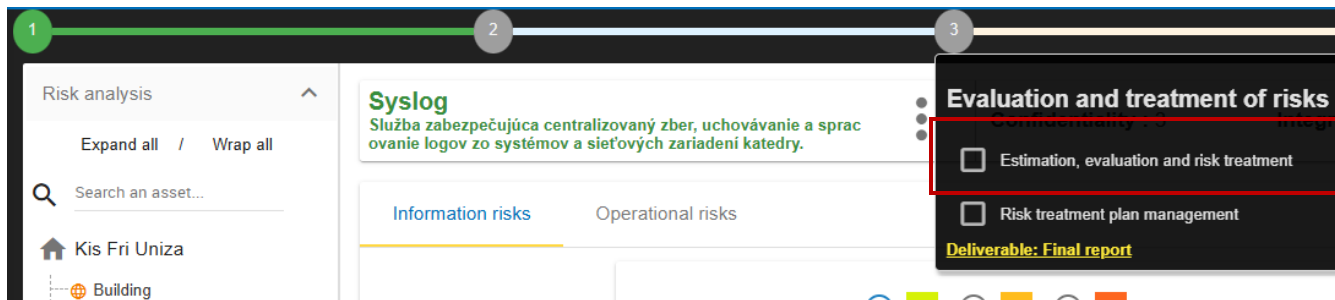
Výsledná hodnota dopadu je **maximálna hodnota v riadku**

	Consequences					Max
	Reputation	Operational	Legal	Financial	Personal	
Confidentiality	2	0	1	Unknown	3	3
Integrity	2	0	2	Unknown	2	2
Availability	2	0	2	Unknown	2	2

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

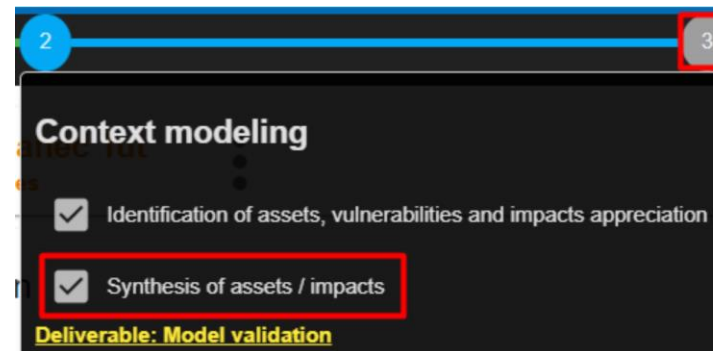
- Zraniteľnosť sa v MONARC neurčuje samostatne ako objekt
- Vyplývajú z bodu - aké bezpečnostné opatrenia existujú prípadne neexistujú
- Po kliknutí na riziko sa nám zobrazia detailné informácie o riziku, kde môžeme dodatočne vypísať **existujúce opatrenia**.
- Ďalej v kroku 3, budeme existujúce opatrenia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

Syslog		Confidentiality : 3
Služba zabezpečujúca centralizovaný zber, uchovávanie a spracovanie logov zo systémov a sieťových zariadení katedry.		
Information risks		Operational risks
Current risk	-	C
Residual risk	-	
Asset	Syslog > Administration software (+)	
Threat	Error in use	
Threat probability	-	
Vulnerability	No accessible user support	
Vulnerability qualification	-	
Risk owner		
Risk context		
Existing controls		
Recommendations		
Search a recommendation 		
Kind of treatment	Not treated	
Vulnerability reduction		



## 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).




Cancel

Save

## 3. Hodnotenie a ošetrovanie 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 ošetrovanie 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

The screenshot shows the MONARC web application interface. A progress bar at the top indicates four steps: 1 (green), 2 (blue), 3 (grey), and 4 (grey). Step 3, 'Evaluation and treatment of risks', is highlighted with a red box. A dropdown menu for step 3 is open, showing two options: 'Estimation, evaluation and risk treatment' (checked) and 'Risk treatment plan management'. Below the menu, a table displays two information risks.

Asset	Impact			Threat Label	Prob.	Vulnerability	
	C	I	A			Label	Existing controls
Tutorial	-	-	-	Equipment malfunction or failure	-	Backups are not carried out in accordance with the state of the art	
Tutorial	-	-	-	Theft or destruction of media, documents or equipment	-	Backup media are not stored in a suitable place	

## 3. Hodnotenie a ošetrovanie 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	2 Impact			Threat Label	3 Prob.	Vulnerability Label	4 Existing controls	5 Qualif.	6 Current risk			7 Treatment	8 Residual risk
	C	I	A						C	I	A		
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 ošetrovanie 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 Asset	2 Risk description	3 Net risk						4 Current risk	5 Existing controls	6 Treatment	7 Residual risk
		Prob.	Impact								
			Rep.	Op.	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



Typ rizika	Výpočet	Používa
Informačné riziká	$R = \text{Impact} \times (\text{Threat} \times \text{Vulnerability})$	CIA
Operačné riziká	$R = \text{Impact} \times \text{Probability}$	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 ošetrovanie 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
↓ ↑	<b>Authorisation</b> Implement a procedure for the authorisation management	***	Administrator workstations	No procedure	36	9
↓ ↑	<b>Monitoring</b> Implement a monitoring of the workstation	***	Administrator workstations	The workstations are not monitored	45	18
↓ ↑	<b>Program management</b> Implement a white list of the program which have been approved by the IT department	***	Administrator workstations	No measure	30	0
↓ ↑	<b>Administrator right</b> Remove the administrator right from the workstations of the users	**	Administrator workstations	There is no procedures	15	9
↓ ↑	<b>Patch management</b> Check if the patch are really applied	**	Administrator workstations	The patch are normally done in automatic	12	6

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



1. **Accept** – Residual risk  $\approx$  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
↓ ↑	<b>Authorisation</b> Implement a procedure for the authorisation management	***	Administrator workstations	No procedure	36	9
↓ ↑	<b>Monitoring</b> Implement e a monitoring of the workstation	***	Administrator workstations	The workstations are not monitored	45	18
↓ ↑	<b>Program management</b> Implement a white list of the program which have been approved by the IT department	***	Administrator workstations	No measure	30	0
↓ ↑	<b>Administrator right</b> Remove the administrator right from the workstations of the users	**	Administrator workstations	There is no procedures	15	9
↓ ↑	<b>Patch management</b> 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 ošetrovanie 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**

	Recommendation	Imp.	Comment	Manager	Deadline	Status	Actions
	My rec Moje odporúčanie	..			15/07/2022  	Coming	

# 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 topológia
  - 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)  $\text{Risk} = \text{Likelihood} \times \text{Number of assets}$
  - b)  $\text{Risk} = \text{Impact} \times (\text{Threat} \times \text{Vulnerability})$
  - c)  $\text{Risk} = \text{Impact} \div \text{Probability}$
  - d) Risk sa vždy prideluje 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](mailto:Jana.Uramova@fri.uniza.sk)