Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Monitoring sítě ve firmě

Bc. Adam Freja

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Adam Freja

Informatika

Název práce

Monitoring sítě ve firmě

Název anglicky

Network monitoring in the company

Cíle práce

Hlavním cílem diplomové práce bude na základě studia teoretických podkladů vybrání monitorovacího softwaru, jeho porovnání a stanovení výhod a nevýhod a následná implementace do firmy Aerosol-Service a.s. Dalším cílem bude objasnění tématu monitoringu sítě a význam monitorování síťového toku ve firemních podmínkách.

Metodika

Bude provedeno podrobné studium teoretických základů monitorování sítě. To bude zahrnovat posouzení různých typů softwaru, jejich funkcí a výhod. Na základě výsledků výzkumu bude vybrán monitorovací software, který nejlépe vyhovuje potřebám společnosti Aerosol-Service a.s. Tento proces zahrnuje zhodnocení funkcí, nákladů a kompatibility softwaru s existující infrastrukturou sítě společnosti.

Praktická část bude obsahovat implementaci vybraného monitorovacího softwaru do stávající infrastruktury sítě společnosti, tedy instalaci softwaru a jeho konfiguraci. Tento postup bude v práci detailně popsán v krocích. Po implementaci monitorovacího softwaru by dalším krokem bylo zhodnocení účinnosti monitorování sítě v operacích společnosti.

Doporučený rozsah práce

60-80s.

Klíčová slova

monitoring, infrastruktura, implementace, konfigurace, síť, server, síťový provoz, software

---

Doporučené zdroje informací

COLLINS, Robert. Network Security Monitoring: Basics for Beginners. A Practical Guide. Jižní Karolína: CreateSpace Publishing, 2017. ISBN 1978309236.

LUCAS, M W. Networking for Systems Administrators (It Mastery). Gross Pointe Woods: Tilted Windmill Press, 2015. ISBN 978-1642350340.

SANDERS, Chris a Jason SMITH. Applied network security monitoring: collection, detection, and analysis. Boston: Syngress, an imprint of Elsevier, [2014]. ISBN 9780124172081.

SCOTT, Russell. Networking for Beginners: An Easy Guide to Learning Computer Network Basics. Take Your First Step, Master Wireless Technology, the OSI Model, IP. ISBN 1704314100.

STALLINGS, William a William STALLINGS. SNMP, SNMPv2, SNMPv3, and RMON 1 and 2. 3rd ed. Reading, Mass.: Addison-Wesley, c1999. ISBN 0201485346.

WILSON, E. Networking monitoring and analysis. New Jersey: Upper Saddle River, 2000. ISBN 0-13-026495-4.

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Martin Havránek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 4. 9. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 26. 03. 2024

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Monitoring sítě ve firmě" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31.03.2024 _____

Poděkování

Rád bych touto cestou poděkoval vedoucímu práce panu Ing. Martinu Havránkovi, Ph.D., za cenné a odborné rady. Také bych velice rád poděkoval společnosti Aerosol-Service a.s., za poskytnuté možnosti a materiály.

Monitoring sítě ve firmě

Abstrakt

Diplomová práce se soustředí na implementaci monitorovacího softwaru do firemní sítě společnosti Aerosol-Service a.s. Teoretická část poskytuje důkladný přehled o monitorování sítě, zahrnující definice, význam, typy a bezpečnostní aspekty. Na základě analýzy teoretických základů je pečlivě vybrán optimální monitorovací software, jehož implementace do existující infrastruktury je podrobně dokumentována. Výsledky práce poskytují konkrétní doporučení pro efektivní monitorování sítě v konkrétních podmínkách společnosti Aerosol-Service a.s. Tímto způsobem práce přispívá k optimalizaci IT infrastruktury a rozšiřuje znalosti v oblasti síťového monitorování.

Klíčová slova: monitorovací software, firemní síť, monitorování, implementace, server, síťový provoz

Network monitoring in the company

Abstract

The thesis focuses on the implementation of monitoring software in the corporate network of Aerosol-Service a.s. The theoretical part provides a thorough overview of network monitoring, including definitions, meaning, types and security aspects. Based on the analysis of the theoretical foundations, the optimal monitoring software is carefully selected and its implementation into the existing infrastructure is documented in detail. The results of the work provide specific recommendations for effective network monitoring in the specific conditions of Aerosol-Service a.s. In this way, the work contributes to the optimization of IT infrastructure and expands the knowledge in the field of network monitoring.

Keywords: monitoring software, corporate network, monitoring, implementation, server, network traffic

Obsah

1 Úvod 10

2 Cíl práce a metodika 11

2.1 Cíl práce 11

2.2 Metodika 11

3 Teoretická východiska 13

3.1 Úvod do monitoringu sítě a jeho význam 13

3.1.1 Důvody pro implementaci monitorovacího systému 14

3.2 Počítačová síť a protokoly 15

3.3 Typy síťového monitorování a jejich cíle 19

3.3.1 Monitorování dostupnosti, výkonu, bezpečnosti a dalších aspektů sítě 19

3.3.2 Pasivní vs. aktivní monitorování 20

3.4 Metody a nástroje pro síťové monitorování 21

3.4.1 Paketová analýza a telemetrie 32

3.5 Kritické metriky a ukazatele pro monitorování sítě 33

3.5.1 Latence, odezva a ztráta paketů: měření kvality komunikace 34

3.5.2 Šířka pásma, propustnost sítě 35

3.5.3 Aktivita a chování uživatele 37

3.6 Bezpečnostní aspekty síťového monitorování 38

3.6.1 Ochrana dat a soukromí při sběru a analýze monitorovacích dat 38

3.6.2 Identifikace hrozeb a anomálií v síťovém provozu 39

3.7 Síťový monitoring a cloudová infrastruktura 40

3.7.1 Monitorování v rámci virtuálních a cloudových prostředí 41

3.7.2 Specifika monitorování v kontejnerových architekturách 42

3.8 Budoucnost síťového monitorování a trendy 43

3.8.1 Vývoj technologií a směřování budoucnosti v oblasti monitorování sítě. 43

3.8.2 Vliv technologických trendů na monitorování sítě 44

4 Vlastní práce 47

4.1 Výběr vhodného monitorovacího softwaru pro Aerosol-Service a.s. 47

4.1.1 Představení zkoumané společnosti 47

4.1.2 Topologie sítě 49

4.1.3 Segmentace sítě 49

4.1.4 Informace o serverech 49

4.1.5 Aktuální stav monitorování sítě 50

4.1.6 Analýza požadavků společnosti na monitorovací software 50

4.1.7 Porovnání dostupných monitorovacích nástrojů s ohledem na funkce a náklady 51

4.1.8 Výběr optimálního monitorovacího softwaru na základě kritérií a potřeb společnosti. ... 54
4.1.9 Příprava serveru ... 56
4.2 Implementace monitorovacího softwaru ... 58
4.2.1 Postup instalace zvoleného monitorovacího softwaru do infrastruktury sítě Aerosol-Service a.s ... 58
4.2.2 Konfigurace monitorování ... 60
4.2.3 Nastavení triggerů a senzorů ... 62
4.2.4 Nastavení upozornění ... 63
4.2.5 Mapa topologie sítě ... 63
4.2.6 Řídící panel ... 64
4.2.7 Reportovací panel ... 65
4.3 Zhodnocení účinnosti monitorování sítě v praxi ... 66
4.3.1 Sběr dat a informací o provozu sítě před a po implementaci monitorovacího softwaru ... 66
4.3.2 Analyzování získaných dat a hodnocení účinnosti monitorovacího softwaru ... 67
4.3.3 Diskuse o přínosech a případných vylepšeních v praxi. ... 70
5 Závěr ... 71
6 Seznam použitých zdrojů ... 73
7 Seznam obrázků, tabulek, grafů a zkratek ... 79
7.1 Seznam obrázků ... 79
7.2 Seznam tabulek ... 79

1 Úvod

V rámci neustálého technologického pokroku a rostoucí komplexity firemních informačních technologií se stává síťový monitoring klíčovým prvkem pro zajištění bezpečnosti a efektivity firemních sítí. Diplomová práce se zabývá konkrétním případem implementace monitorovacího softwaru do síťové infrastruktury společnosti Aerosol-Service a.s. Záměrem této práce je nejen posoudit současná teoretická východiska síťového monitorování, ale též navrhnout a implementovat řešení, které bude odpovídat specifickým potřebám a požadavkům dané společnosti.

První část práce se zaměřuje na teoretický úvod do monitorování sítě, kde jsou analyzovány klíčové pojmy, jako je síťová bezpečnost, typy monitorovacích metod a důvody pro implementaci monitorovacího systému v podnikovém prostředí. Důraz je kladen na současný vývoj technologií a trendy v oblasti síťového monitorování, aby bylo možné vybrat optimální a perspektivní monitorovací software pro konkrétní případ společnosti Aerosol-Service a.s.

Druhá část práce se detailně zabývá metodikou výběru monitorovacího softwaru, analýzou požadavků společnosti a porovnáním dostupných nástrojů s ohledem na jejich funkce, náklady a kompatibilitu s existující infrastrukturou sítě. Tato fáze je klíčová pro následnou úspěšnou implementaci monitorovacího softwaru, který bude plně odpovídat potřebám a specifikům společnosti.

Celkovým cílem této diplomové práce je tedy nejen teoretická analýza síťového monitorování, ale také konkrétní aplikace těchto poznatků ve prospěch efektivity, bezpečnosti a funkčnosti síťové infrastruktury společnosti Aerosol-Service a.s.

2 Cíl práce a metodika

2.1 Cíl práce

Diplomová práce se bude zaměřovat na několik klíčových cílů. Prvním z nich je provést důkladné studium teoretických základů v oblasti monitorovacího softwaru. Tímto způsobem budou identifikovány klíčové faktory a kritéria, která budou sloužit k výběru optimálního monitorovacího řešení pro společnost Aerosol-Service a.s.

Následný krok spočívá v důkladném porovnání dostupných monitorovacích softwarových produktů na trhu. Toto srovnání bude zahrnovat jak technické parametry a funkcionality, tak i ekonomické aspekty včetně nákladů na licencování a provoz. Důraz bude kladen na schopnost softwaru plnit specifické požadavky a potřeby společnosti Aerosol-Service a.s.

Dalším důležitým aspektem práce bude stanovení výhod a nevýhod vybraného monitorovacího softwaru. Tato analýza bude zahrnovat mimo jiné jeho schopnost integrovat se s existujícími systémy a procesy ve firmě, uživatelskou přívětivost, škálovatelnost a možnosti rozšíření v budoucnosti.

Po důkladné analýze bude následovat fáze implementace vybraného monitorovacího softwaru do společnosti Aerosol-Service a.s. Tato etapa zahrnuje technickou instalaci, konfiguraci a přizpůsobení softwaru specifickým potřebám a prostředí firmy.

Kromě technických hledisek se diplomová práce bude věnovat i teoretickému objasnění tématu monitoringu sítě a jeho významu v rámci firemních podmínek. Bude se zabývat klíčovými koncepty, principy a metodami monitorování síťového toku a analyzovat, jak mohou tyto informace přispět k efektivnějšímu a bezpečnějšímu provozu sítě ve společnosti Aerosol-Service a.s.

2.2 Metodika

Diplomová práce se zaměří na důkladné studium teoretických aspektů monitorování sítě. Bude provedeno podrobné zhodnocení různých typů monitorovacího softwaru, včetně jejich funkcionalit a předností. Cílem této analýzy je identifikovat ten software, který nejlépe vyhovuje specifickým potřebám a prostředí společnosti Aerosol-Service a.s. Důraz bude kladen na faktory jako kompatibilita s existující infrastrukturou sítě a náklady spojené s provozem.

Následná část práce se bude věnovat implementaci vybraného monitorovacího softwaru do stávající infrastruktury sítě společnosti. Tento proces zahrnuje technickou instalaci softwaru a jeho následnou konfiguraci tak, aby plně odpovídal specifickým potřebám a prostředí firmy Aerosol-Service a.s. Každý krok tohoto postupu bude detailně popsán.

Po úspěšné implementaci monitorovacího softwaru bude následovat fáze zhodnocení jeho účinnosti v reálném provozu společnosti. To zahrnuje monitorování síťových operací a analýzu získaných dat. Cílem tohoto kroku je ověřit, zda zvolený monitorovací software plně splňuje očekávání a přináší významný přínos pro výkon a bezpečnost sítě společnosti Aerosol-Service a.s.

Celkovým výsledkem této diplomové práce bude poskytnutí společnosti Aerosol-Service a.s. konkrétního a prakticky ověřeného řešení pro efektivní monitorování sítě, které bude podporovat růst a spolehlivost firemní infrastruktury.

3 Teoretická východiska

V úvodní sekci diplomové práce jsou představena teoretická východiska, jež poskytují základ pro zpracování vlastní práce.

3.1 Úvod do monitoringu sítě a jeho význam

Proces sledování informačních technologií zahrnuje sběr metrik týkajících se provozu IT prostředí. Organizace využívají tohoto sledování k získávání metrik o výkonu svého hardwaru a softwaru, což jim umožňuje udržet správný chod v souladu s očekáváním a zároveň odhalit a řešit potenciální IT problémy. (Gillis, 2023)

Základní sledování zahrnuje dohled nad během zařízení, zatímco pokročilejší forma sledování poskytuje podrobné přehledy o stavu provozu, jako jsou průměrné časy odezvy, počet instancí aplikací, míra výskytu chyb a požadavků, vytížení procesoru a dostupnost softwarových aplikací. Sledování může být prováděno kontinuálně nebo v pravidelných intervalech, ať už denních, týdenních či měsíčních. (Gillis, 2023)

Proces monitorování začíná sběrem dat pomocí sběrných agentů, specializovaných softwarových programů spuštěných na sledovaných entitách, jako jsou hostitelé, databáze nebo síťová zařízení. Agenti zachycují smysluplné systémové informace, zapouzdřují je do kvantitativních datových vstupů a poté tyto datové vstupy v pravidelných intervalech hlásí monitorovacímu systému. Tyto vstupy jsou pak shrnuty a agregovány do metrik, které jsou později prezentovány jako datové body v časové řadě. (Ligus, 2012)

Činitele sběru dat lze rozdělit do následujících skupin: (Ligus, 2012)

- **White-box**
    - Parsery protokolů

Ty získávají specifické informace ze záznamů protokolu, například stavové kódy a časy odezvy požadavků z protokolu webového serveru.

    - Skenery protokolů

Počítají výskyty řetězců v souborech protokolu definovaných regulárními výrazy. Chcete-li například vyhledat regulární chyby i kritické chyby, můžete zkontrolovat počet výskytů regexu "ERROR|CRITICAL" v souboru protokolu.

    - Čtečky rozhraní

Ty čtou a interpretují systémová rozhraní a rozhraní zařízení. Příkladem je čtení vytížení procesoru z pseudosystému /proc systému Linux a čtení teploty nebo vlhkosti ze specializovaných zařízení.

- **Black-box**
    - Probery

Ty běží mimo monitorovaný systém a odesílají do systému požadavky na ověření jeho odezvy, například požadavky ping nebo volání HTTP na webové stránky pro ověření dostupnosti.

    - Sniffery

Sledují síťová rozhraní a analyzují statistiky provozu, například počet přenesených paketů rozdělených podle protokolů.

3.1.1 Důvody pro implementaci monitorovacího systému

Monitorování výkonu sítě hraje klíčovou roli pro úspěch podniků, které se spoléhají na počítačové sítě. Některé benefity sledování se projevují okamžitě, jako například promptní identifikace, základní rozhodování podložené důkazy a automatizace. Avšak jeho komplexní hodnota zasahuje mnohem dále. Sledování zastává klíčovou úlohu při integrování pracovních poznatků a podporování inovací. Nelze řídit to, co není měřeno. (Wilson, 2000)

V dnešní době rostoucího technologického pokroku a komplexity podnikatelského prostředí se stává implementace monitorovacího systému pro organizace nejen klíčovou potřebou, ale i strategickým rozhodnutím s mnoha důležitými důvody a výhodami, jako jsou například: (Charbonneau, 2023)

- **Optimální výkon**

Monitorování výkonu sítě umožňuje podnikům zajistit, aby jejich sítě fungovaly s maximální efektivitou. (MCS, 2023)

- **Detekce a řešení problémů**

Proaktivní přístup minimalizuje prostoje, zabraňuje přerušení provozu a zajišťuje nepřerušený přístup ke kritickým aplikacím a službám. (MCS, 2023)

- **Vylepšená uživatelská zkušenost**

Rychlejší a spolehlivější přístup k aplikacím, webovým stránkám a službám, což vede ke zvýšení spokojenosti a loajality zákazníků. (MCS, 2023)

- **Plánování a škálovatelnost kapacity**

Analýzou historických údajů o výkonu a trendů mohou podniky přesně předpovídat budoucí požadavky na síť a přijímat informovaná rozhodnutí týkající se modernizace sítě, přidělování šířky pásma a investic do infrastruktury. Tento proaktivní přístup zajišťuje, že síť dokáže vyhovět rostoucím požadavkům a efektivně se přizpůsobit měnícím se potřebám podniku. (MCS, 2023)

- **Zabezpečení a dodržování předpisů**

Sledováním vzorců síťového provozu a anomálií mohou podniky odhalit potenciální narušení bezpečnosti, pokusy o neoprávněný přístup nebo neobvyklé chování. To umožňuje včas reagovat a zmírnit bezpečnostní hrozby, chránit citlivá data a zachovat soulad s předpisy. (MCS, 2023)

- **Zvýšená návratnost investic (ROI)**

Monitorování IT infrastruktury je pro mnoho organizací finančně značně užitečné, protože přináší úsporu nákladů. Může však také zvýšit návratnost investic. (MCS, 2023)

3.2 Počítačová síť a protokoly

Počítačová síť se skládá z propojených výpočetních zařízení, jako jsou počítače, servery, směrovače, přepínače a další hardware. Tato zařízení jsou vzájemně propojena, aby usnadnila komunikaci, sdílení dat a sdílení zdrojů. (Larry L. Peterson, 2011)

Síťování je pojem, který popisuje procesy spojené s návrhem, implementací, modernizací, správou a další prací se sítěmi a síťovými technologiemi. Sítě se používají k neuvěřitelnému množství různých účelů. (Kozierok, 2005)

Počítačové sítě mohou mít různý rozsah, od malých lokálních sítí (LAN) v rámci jednotlivých budov až po rozsáhlé globální sítě, jako je internet. Umožňují komunikaci zařízení pomocí různých komunikačních kanálů, například kabelových (Ethernet) nebo bezdrátových (Wi-Fi), a spoléhají se na definovanou sadu protokolů a standardů, které určují, jak jsou data v síti vysílána, přijímána a chápána. (Larry L. Peterson, 2011)

Mezi hlavní cíle počítačových sítí patří efektivní přenos dat, spolehlivá komunikace, škálovatelnost pro zvládnutí rostoucího počtu zařízení a bezpečná výměna dat. Sítě hrají

zásadní roli v moderních technologiích a umožňují provádět různé úlohy, od základního procházení internetu až po složité cloudové výpočty a vzdálenou spolupráci. (Mohanakrishnan, 2023)

Fungování počítačových sítí lze jednoduše definovat jako pravidla nebo protokoly, které pomáhají při odesílání a přijímání dat prostřednictvím spojů, které umožňují komunikaci počítačových sítí. Každé zařízení má IP adresu, která pomáhá identifikovat zařízení. (GeeksforGeeks, 2023)

Protokoly

V reálném světě protokol často označuje kodex chování nebo formu etikety. V případě technického prostředí síťové protokoly definují jazyk a soubor pravidel a postupů, které umožňují zařízením a systémům komunikovat. Počítače samozřejmě nemají "místní zvyklosti" a sotva se musí obávat, že se dopustí "faux pas", které by mohlo jiný počítač urazit. Síťové protokoly se starají o to, aby všechna zařízení v síti nebo internetové síti souhlasila s tím, jak je třeba provádět různé akce v celkovém procesu komunikace. (Kozierok, 2005)

V kontextu referenčního modelu OSI je protokol formálně definován jako soubor pravidel, jimiž se řídí komunikace mezi entitami na stejné vrstvě referenčního modelu. Například protokol TCP odpovídá za specifickou sadu funkcí v sítích TCP/IP. Každý hostitel v síti TCP/IP má implementaci TCP a všichni spolu logicky komunikují na čtvrté vrstvě modelu OSI. (Kozierok, 2005)

Protokoly se dělí do dvou kategorií podle toho, jak využívají připojení:

- **Protokoly zaměřené na spojení**:

Tyto protokoly vyžadují, aby bylo mezi dvěma zařízeními před přenosem dat vytvořeno logické spojení. Toho se obvykle dosahuje dodržováním specifického souboru pravidel, která určují, jak má být spojení zahájeno, vyjednáno, spravováno a případně ukončeno. Obvykle jedno zařízení začíná odesláním požadavku na otevření spojení a druhé odpovídá. Předávají si řídicí informace, které určují, zda a jak má být spojení navázáno. Pokud se to podaří, jsou mezi zařízeními odeslána data. Když skončí, spojení se přeruší. (Scott, 2019)

- **Protokoly bez spojení**:

Tyto protokoly nenavazují spojení mezi zařízeními. Jakmile má zařízení odeslat data jinému zařízení, prostě je odešle. (Scott, 2019)

OSI

Ve standardním modelu známém jako model OSI (Open Systems Interconnection), řídí činnosti na každé vrstvě telekomunikační výměny jeden nebo více síťových protokolů. Nižší vrstvy se zabývají přenosem dat, zatímco vyšší vrstvy modelu OSI se zabývají softwarem a aplikacemi. (Yasar, 2023)

OSI model se skládá z následujících sedmi vrstev: (Imperva, 2023)

- Vrstva 1:

Fyzická vrstva, stejně jako u TCP/IP, zajišťuje fyzické připojení k síti a definuje elektrické a fyzické vlastnosti.

- Vrstva 2:

Datová vrstva koncepčně vytváří spojení bod-bod mezi koncovými body sítě a přijímá a odesílá data do a ze síťové vrstvy.

- Vrstva 3:

Síťová vrstva je zodpovědná za směrování dat mezi koncovými body sítě.

- Vrstva 4:

Transportní vrstva zajišťuje funkce doručování a kvality služby.

- Vrstva 5:

Relace vytváří, udržuje a ukončuje relace mezi koncovými body sítě.

- Vrstva 6:

Prezentační vrstva převádí datové toky do formátů, které mohou zpracovávat nižší vrstvy, a může také data komprimovat/dekomprimovat a šifrovat/dešifrovat.

- Vrstva 7:

Aplikační vrstva poskytuje přístup ke službám poskytovaným nižšími vrstvami.

TCP/IP

Protokol TCP/IP pečlivě definuje způsob, jakým se informace přesouvají od odesílatele k příjemci. Nejprve aplikační programy posílají zprávy nebo proudy dat jednomu z protokolů transportní vrstvy internetu, buď protokolu UDP (User Datagram Protocol), nebo protokolu TCP (Transmission Control Protocol). Tyto protokoly přijmou data od

aplikace, rozdělí je na menší části zvané pakety, přidají cílovou adresu a pak je předají další vrstvě protokolu, vrstvě internetové sítě. (IBM, 2023)

Čtyři vrstvy modelu TCP/IP jsou následující: (Yasar, 2023)

- Vrstva 1:

Aplikační vrstva. Jedná se o nejvyšší vrstvu modelu TCP/IP, která je zodpovědná za poskytování přístupu uživatelů k síťovým zdrojům. Mezi protokoly, které jsou součástí této vrstvy, patří HTTP, SMTP a FTP.

- Vrstva 2:

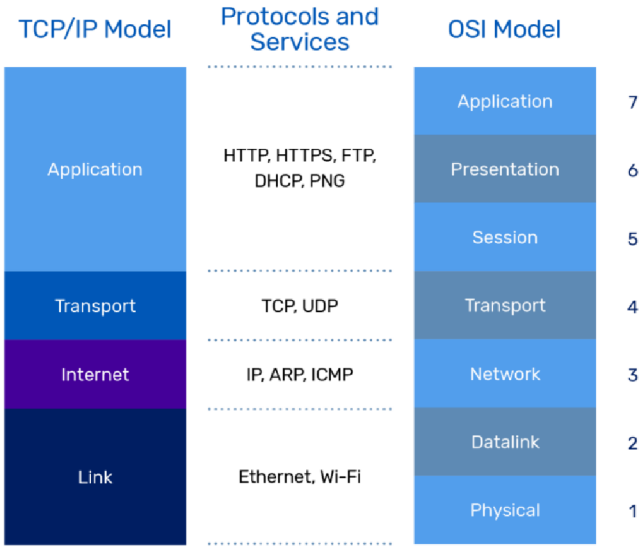
Transportní vrstva. Tato vrstva zajišťuje správný přenos segmentů komunikačním kanálem. Na této vrstvě se také vytváří síťové spojení mezi zdrojovým a cílovým systémem.

- Vrstva 3:

Internetová vrstva. Známá také jako síťová vrstva, přijímá a odesílá pakety pro síť. Tato vrstva zahrnuje protokol IP, protokol ARP (Address Resolution Protocol) a protokol ICMP (Internet Control Message Protocol).

- Vrstva 4:

Přístupová vrstva sítě. Síťová přístupová vrstva protokolu TCP/IP kombinuje fyzickou a datovou linkovou vrstvu modelu OSI.



Obrázek 1 - TCP/IP a OSI modely, zdroj: (A10, 2023)

3.3 Typy síťového monitorování a jejich cíle

Monitorování sítě lze rozdělit do různých typů podle toho, co přesně je třeba monitorovat, včetně monitorování poruch, monitorování protokolů, monitorování výkonu, monitorování konfigurace a monitorování dostupnosti. (Wilson, 2000)

3.3.1 Monitorování dostupnosti, výkonu, bezpečnosti a dalších aspektů sítě

Monitorování poruch

Monitorování poruch sítě zahrnuje vyhledávání a hlášení poruch v počítačové síti. Má zásadní význam pro udržení nepřetržité provozuschopnosti a bezproblémového provozu sítě, což je nezbytné pro hladký chod všech programů a služeb. (TRIPATHY, 2023)

Monitorování protokolů

Monitorování protokolů zahrnuje analýzu protokolů generovaných síťovými prostředky, jako jsou servery, aplikace nebo webové stránky. Tyto protokoly poskytují cenné informace o činnosti uživatelů a pomáhají podnikům při dodržování předpisů, rychlém řešení incidentů a zvyšování bezpečnosti sítě. (TRIPATHY, 2023)

Monitorování výkonu sítě

Monitorování výkonu sítě (NPM) sleduje monitorovací parametry, jako je latence, síťový provoz, využití šířky pásma a propustnost, a optimalizuje tak služby koncovým uživatelům. Nástroje NPM poskytují cenné informace, které lze využít k minimalizaci výpadků a řešení problémů se sítí. (Froehlich, 2021)

Monitorování konfigurace

Monitorování konfigurace sítě zahrnuje sledování softwaru a firmwaru používaného v síti. Tím je zajištěno, že jsou nesrovnalosti identifikovány a okamžitě řešeny, aby se předešlo mezerám ve viditelnosti nebo zabezpečení. (Froehlich, 2021)

Monitorování dostupnosti sítě

Monitorování dostupnosti je sledování celé IT infrastruktury za účelem zjištění provozuschopnosti zařízení. Díky důslednému monitorování IT zařízení a serverů mohou organizace dostávat upozornění na výpadky sítě nebo na jejich nedostupnost. Nejčastěji používanými technikami pro monitorování dostupnosti jsou ICMP, SNMP a Syslog. (TRIPATHY, 2023)

3.3.2 Pasivní vs. aktivní monitorování

Aktivní monitorování

Aktivní monitorování sítě se také označuje jako syntetické monitorování a má více prediktivní a proaktivní přístup. Syntetické se mu říká proto, že tento přístup nepoužívá skutečná data uživatelů. Místo toho se nástroje používané při tomto typu monitorování zaměřují na předvídání potenciálního výkonu sítě pomocí simulací aktuálního chování sítě. (Stephen F. Bush, 2013)

Cílem aktivního monitorování značky je získat kompletní přehled o výkonu sítě v reálném čase. Tato metoda umožňuje proaktivně identifikovat potenciální problémová místa a problémy, které se mohou v síti vyskytnout, a tím předcházet problémům v síti. (Renata Teixeira, 2009)

Aktivní analýza navíc umožňuje měřit výkonnost sítě pomocí různých metrik a klíčových ukazatelů výkonnosti. Pomocí aktivního monitorování se může měřit latence, doba odezvy HTTP, jitter a ztráty paketů. (Red Sift, 2022)

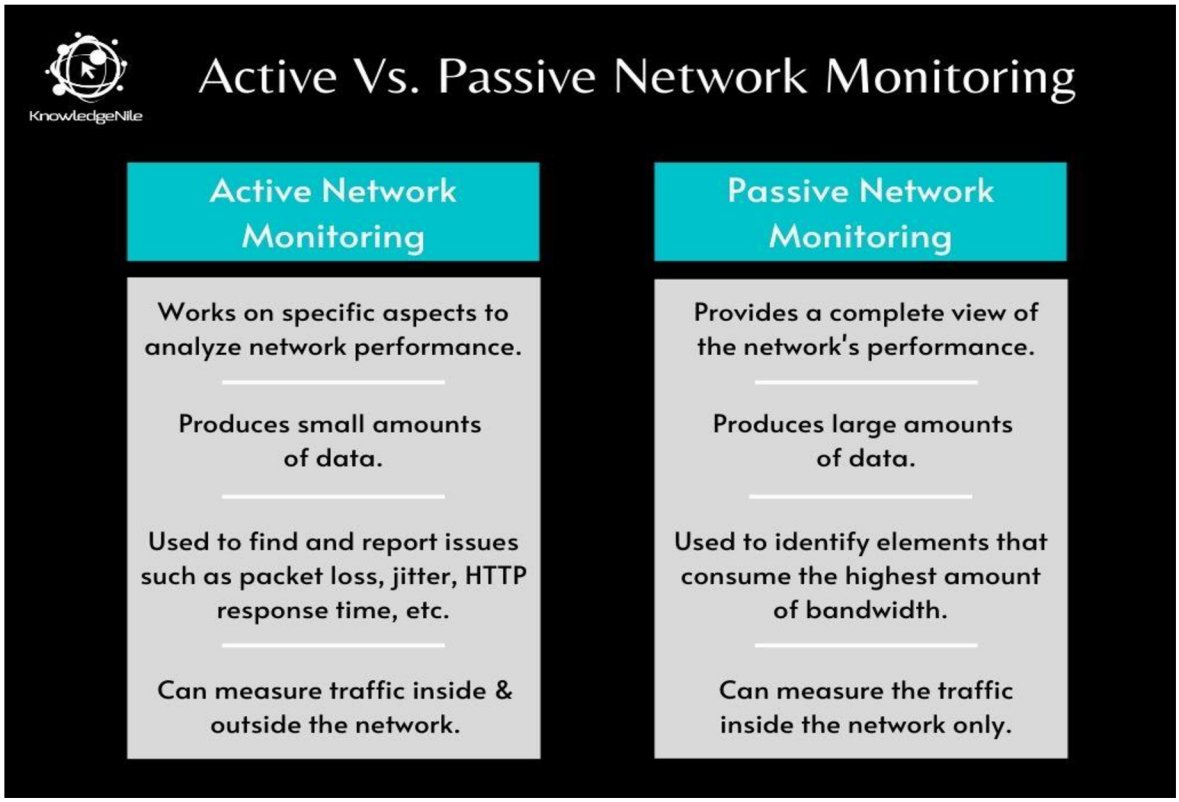
Vzhledem k tomu, že aktivní monitorování bude poskytovat výsledky na základě prediktivních dat, nemusí vždy vykazovat přesné výsledky, protože místo skutečných uživatelských dat používá simulace. Další nevýhodou tohoto přístupu je, že zatěžuje síťové zdroje, protože nepřetržitě produkuje data v reálném čase. (Red Sift, 2022)

Pasivní monitorování

Pasivní síťové monitorování operuje na principu zachytávání a analýzy reálných uživatelských dat, jež jsou shromažďována kontinuálně z konkrétních síťových připojení v určených časových úsecích. Tato technologie disponuje kapacitou generovat a akumulovat rozsáhlejší množství výkonnostních dat v porovnání s metodou aktivního monitorování, neboť nemusí být aktivně spouštěna v krátkých intervalech. Tato data dále umožňují komplexnější analýzu výkonnosti sítě a mohou zahrnovat různé metriky, což přináší užitečnější perspektivu na stav a efektivitu dané sítě. (The Progress team, 2020)

Vzhledem k tomu, že pasivní monitorování shromažďuje údaje o skutečných uživatelích, jsou správci sítě informováni o problémech, které mají přímý dopad na koncové uživatele. Namísto provádění změn na základě předpovědí dostávají správci upozornění na problémy, které je třeba okamžitě řešit. (The Progress team, 2020)

Pasivní monitorování se v porovnání s aktivním monitorováním vyznačuje nižší zátěží na síťové zdroje, neboť mezi jednotlivými testy probíhají větší časové intervaly. Pasivní monitory se nicméně obvykle specializují na analýzu toku dat směřujícího do a z konkrétního síťového zařízení, což vyžaduje nasazení specializovaného hardwaru. (The Progress team, 2020)



Obrázek 2 - Aktivní vs Pasivní monitoring, zdroj: (KnowledgeNile, 2023)

3.4 Metody a nástroje pro síťové monitorování

Síťové monitorovací nástroje poskytují konsolidovaný přehled o stavu a zdravotním stavu celé sítě, a to prostřednictvím jednotného uživatelského rozhraní. Tento integrální pohled umožňuje správcům sítí identifikovat aktuální i potenciální problémy v infrastruktuře a přijmout adekvátní kroky pro nápravu, s cílem obnovit normální provoz. (IBM, 2023)

Metodologie mohou být základního charakteru, například využití pingování pro ověření dostupnosti konkrétního hostitele v síti. Avšak tyto postupy mohou také zahrnovat komplexnější techniky, jako je sledování přístupu k firewallu, analýzu využití šířky pásma, monitorování spotřeby zdrojů, dobu trvání síťového provozu a odhalování nepředvídaných změn v charakteru síťové komunikace. (Lucas, 2015)

Takové metody monitorování rovněž zahrnují ověření, a to přepínače, směrovače, servery, brány firewall a další koncové body sítě, které udržují přijatelnou úroveň propustnosti. Kromě toho se využívá vyrovnávání zátěže pro optimalizaci výkonu a monitoruje se výskyt vysoké chybovosti, což přispívá k celkové bezpečnosti a efektivitě síťové infrastruktury. (Lucas, 2015)

Ping monitoring

Síťové pingy představují jednu z nejstarších metod monitorování, která však zůstává v oblasti správy výkonnosti sítí (NPM) stále relevantní. Monitorovací nástroj vysílá paket (nebo soubor paketů) směrem k cílovému uzlu či zařízení a očekává návratovou odezvu. Pokud přijde od cílového uzlu potvrzující zpráva "vše v pořádku", monitor ví, že dané zařízení je v provozu. Avšak v případě, že neobdrží žádnou odpověď, pokračuje ve vysílání dalších pingů s cílem získat pozornost uzlu. V situaci, kdy ani tyto pokusy nevedou k úspěchu, upozorní monitorovací nástroj uživatele na možnou anomálii. Pingy, ač relativně jednoduchá monitorovací technika, se ukazují jako výtečný nástroj pro firmy, umožňující prověřit aktuální stav zařízení. (Lanesskog, 2019)

Log file monitoring

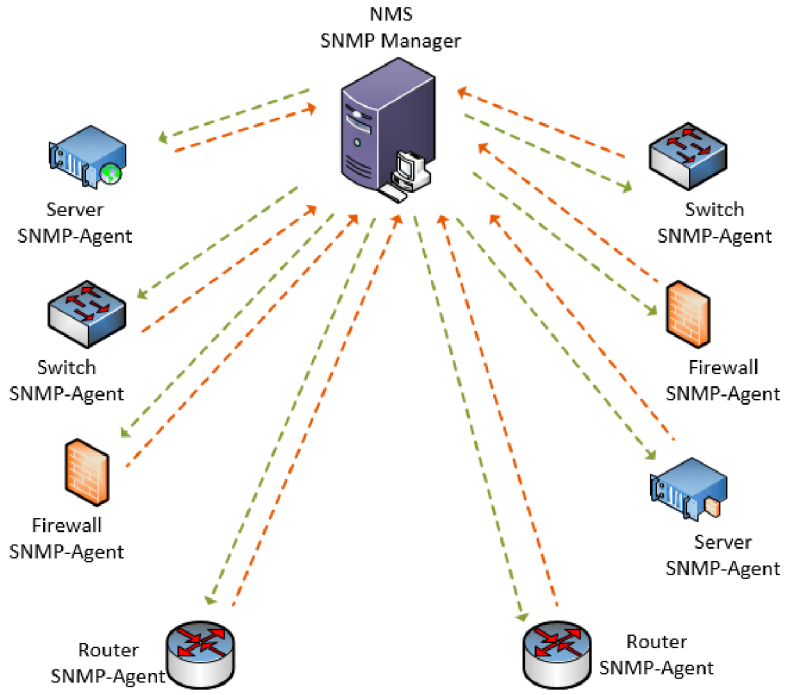
Monitorování síťových protokolů představuje systematický proces využívaný IT správci k organizaci, analýze a komplexnímu zhodnocení výkonu sítě. Každé síťové zařízení, včetně aplikací a hardware, generuje protokoly při vykonávání svých operací. Tyto protokoly fungují jako záznamový deník zařízení, dokumentující každou událost a získávající klíčové informace, jako jsou IP adresy uživatelů, data a časy událostí, časové značky požadavků a další relevantní údaje. Analyzování těchto protokolů umožňuje odhalení a řešení potenciálních problémů, porozumění běžným aktivitám v infrastruktuře a optimalizaci provozu napříč různými platformami. (Clinton, 2018)

Vzhledem k tomu, že každé síťové zařízení může vytvářet vlastní typy protokolů, často se využívají standardizované protokoly pro unifikaci záznamů. Syslog, zkráceně System Logging Protocol, představuje takový standardizovaný protokol, který slouží k odesílání událostních protokolů na specifický server označovaný jako syslog server. Tento syslog server je navržen tak, aby centralizoval všechny síťové protokoly na jednom místě, což zjednodušuje správu cenných dat syslogu a přidává jim srozumitelný kontext. (Griffin, 2021)

SNMP monitoring

Monitorování pomocí protokolu SNMP umožňuje centralizované získávání informací z rozsáhlé sítě síťových zařízení. Protokol SNMP (Simple Network Management Protocol) je založen na aplikačním modelu klient-server a využívá porty 161 a 162. Dotazování probíhá na portu 161 (jde o příchozí komunikaci směrem k zařízení), zatímco informace o událostech jsou přenášeny na portu 162 (jde o odchozí komunikaci směrem ze zařízení). (Julian, 2017)

Pro účely komunikace prostřednictvím protokolu SNMP jsou klíčové dva termíny: agent a manažer. Agent představuje zařízení, ze kterého je záměrem získat informace, zatímco manažer je zařízení, které tyto informace přijímá. Agent funguje jako aktivní proces v operačním systému síťového zařízení, ke kterému směřuje dotazování (v terminologii SNMP se nazývá "poll"). V rámci kontextu můžeme za pojmem "agent" považovat dané síťové zařízení. Správce, tedy zařízení, které přijímá informace od agenta, může představovat jakékoli zařízení, jehož prostřednictvím se provádí dotazy pomocí SNMP, může se jednat o server v datovém centru, notebook či jiný přístroj. (Julian, 2017)



Obrázek 3 - SNMP, zdroj: (Sidheeq, 2023)

Agenta SNMP lze též nakonfigurovat tak, aby automaticky odesílal informace správci bez předchozího dotazování. Agent SNMP je standardně přítomný v drtivé většině síťových zařízení. Pro započetí sběru informací o konkrétním zařízení je nutné aktivovat

protokol SNMP na daném zařízení a nakonfigurovat SNMP Managera tak, aby navázal komunikaci s tímto zařízením. (ManageEngine, 2023)

NetFlow monitoring

Sledování toku představuje metodu, která kvantifikuje pohyb dat mezi dvěma entitami nebo aplikacemi v síťovém prostředí. Jeho cílem je poskytnout IT týmům důkladné informace o toku provozu, který proudí skrz jejich síť a získat pochopení o každodenním provozu sítě. (LiveAction, 2023)

Síťový tok prezentuje záznam o tom, kdo odesílá data, jakým způsobem jsou přenášena a kdy dochází k jejich přenosu. Moderní technologie sledování toku disponují rozšířenými schopnostmi, jako je zachycení celého datového paketu a provádění hluboké analýzy jeho obsahu, což umožňuje získání komplexnějšího pohledu na výkonnost sítě a aplikací. IT týmy mohou přistupovat k datovým tokům z různých zdrojů, včetně směrovačů, firewallů a přepínačů. (LiveAction, 2023)

V rámci monitorování síťových toků se uplatňují různé standardy a formáty, jako jsou NetFlow, sFlow a Internet Protocol Flow Information Export (IPFIX). Tyto protokoly fungují s mírnými odlišnostmi, avšak všechny se odlišují od běžných postupů, jako je zrcadlení portů a hloubková analýza paketů, tím, že nezaznamenávají obsah každého paketu procházejícího daným portem nebo přepínačem. Oproti tomu SNMP nabízí omezené informace, typicky zahrnující obecné statistiky, jako je celkový počet přenesených paketů a využití šířky pásma. (Grimmick, 2023)

SQL query monitoring

Pro monitorování databází připojených k síti využívají monitory dotazy SQL. Tyto dotazy žádají databázi o poskytnutí informací o počtu datových požadavků, přenosů a dalších metrik. Na základě těchto dat může monitor určit, zda databáze pracuje v souladu s očekáváním nebo zda vznikly nějaké problémy. Ideální situací je, když databáze efektivně zpracovává a odesílá data po síti tak, aby splnila všechny příchozí požadavky. V případě pomalého fungování databáze dokáže monitorovací nástroj identifikovat tuto anomálii a upozornit na ní správce sítě. (Hein, 2019)

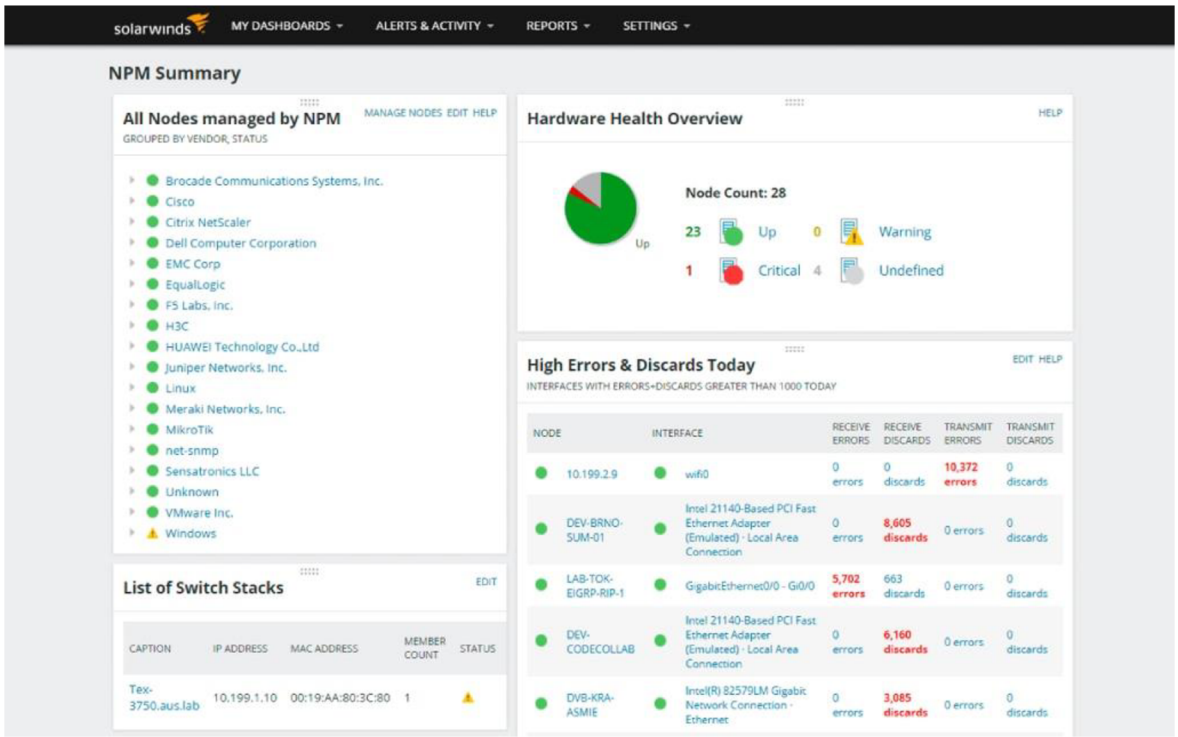
Komerční nástroje na monitorování sítě:

SolarWinds Network Performance Monitor

SolarWinds Network Performance Monitor (NPM) je softwarové řešení vyvinuté společností SolarWinds, předním výrobcem softwaru pro správu IT. NPM je navržen tak, aby poskytoval komplexní monitorování sítě a umožňoval uživatelům nepřetržitě sledovat poruchy, výkon a dostupnost v celé síti. (COOPER, 2023)

Jednou z klíčových atributů nástroje NPM spočívá v jeho schopnosti poskytovat komplexní přehled o stavu a výkonnosti celého síťového prostředí včetně zařízení Cisco ASA. To uživatelům usnadňuje monitorování stavu VPN tunelů a zajištění konektivity mezi lokalitami. (SolarWinds, 2023)

NPM (Network Performance Monitor) disponuje funkcionalitou síťového skeneru, který automaticky identifikuje zařízení v síti, což uživatelům usnadňuje udržení přehledu o monitorování. Tato schopnost přispívá k dosažení komplexního monitorování tím, že iniciováním procesu identifikace zařízení vytváří základ pro sledování. (SolarWinds, 2023)



Obrázek 4 - SolarWinds GUI, zdroj: (SolarWinds, 2023)

Ceník:

Název balíčku	Cena (za měsíc)	Cena (za rok)	Omezení
SL100	€237,08	€2,845	100 elementů
SL250	€554,08	€6,649	250 elementů
SL500	€872,08	€10,465	500 elementů
SL 2000	€1614,08	€19,369	2000 elementů
SLX	€2706,75	€32,481	Neomezeně elementů

Tabulka 1 - Ceník SolarWinds, zdroj: (FirstLight, 2023)

NPM je licencován podle největšího počtu následujících typů sledovaných elementů: (SolarWinds, 2023)

- **Uzly:** jakákoli sledovaná zařízení, například směrovače, přepínače, virtuální a fyzické servery, přístupové body a modemy.
- **Rozhraní:** jakékoli jednotlivé body síťového provozu, například porty přepínačů, fyzická rozhraní, virtuální rozhraní, dílčí rozhraní a sítě VLAN.
- **Svazky:** všechny sledované logické disky.

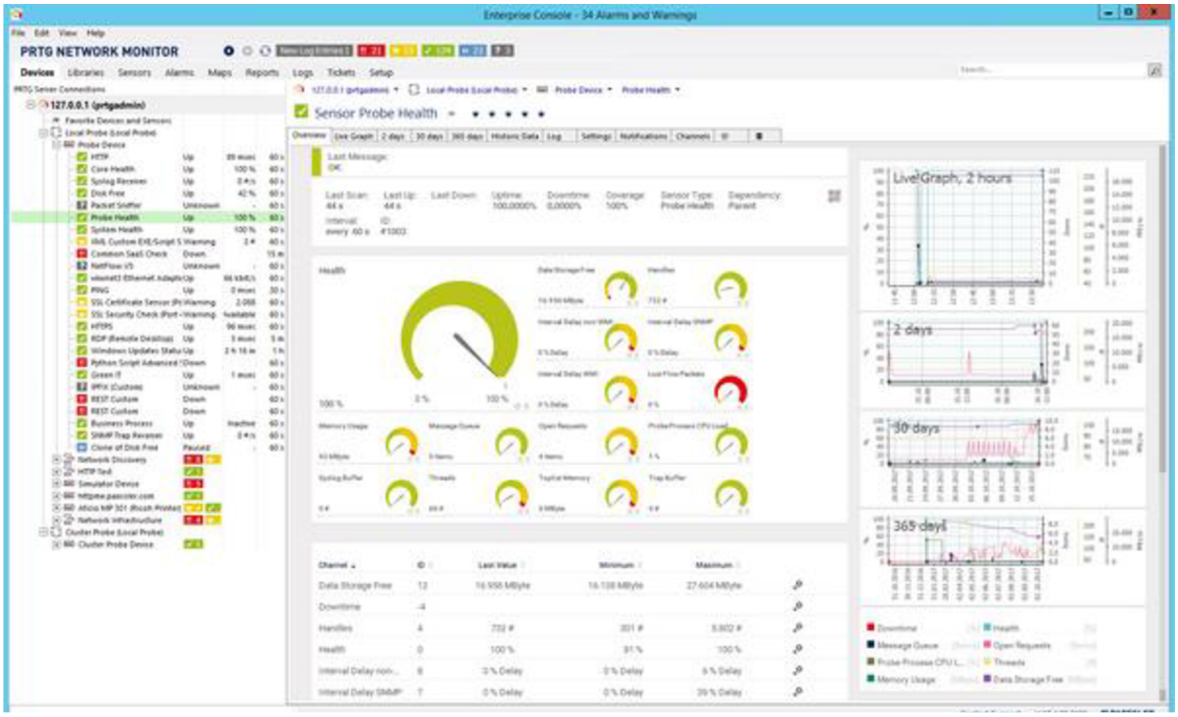
PRTG Network Monitor

PRTG Network Monitor představuje výkonný a snadno ovladatelný software, který asistuje v monitorování a správě počítačových systémů v síťovém prostředí. Zajišťuje bezchybný provoz sítě a minimalizuje výpadky. Svépomocí síťového monitoringu přináší možnost zvýšit efektivitu prostřednictvím poskytování důležitých informací o šířce pásma a využití zdrojů. (Bhardwaj, 2023)

V architektuře PRTG je stěžejními prvky monitorovací senzory. Každý senzor obvykle sleduje konkrétní hodnotu v síti, jako je provoz na portu přepínače, zatížení procesoru serveru nebo dostupné místo na diskové jednotce. Standardně se doporučuje využívat kolem 5 až 10 čidel na jednotlivé zařízení nebo jedno čidlo na každý port přepínače. Aplikace PRTG disponuje variabilními senzory včetně Ping, Cloud Ping a Common SaaS, jež umožňují monitorování síťové konektivity a dostupnosti cloudových služeb. (Paessler, 2023)

V rámci funkcionalit nabízí PRTG rozmanité senzory pro monitorování e-mailového provozu, jež monitorují proces doručení e-mailu od odeslání až po jeho doručení a vyzvednutí. Dále disponuje senzory HTTP Push pro monitorování dat automaticky odesílaných do zařízení PRTG pomocí protokolu HTTP. (Accyotta, 2023)

PRTG je ideální pro nasazení v prostředích malého a středního podniku a disponuje bezplatným lokálním řešením pro snadný start monitoringu sítě. Je koncipován s ohledem na intuitivní ovládání a snadnou přístupnost. Denně se užívá více než 500 000 uživateli. (Paessler, 2023)



Obrázek 5 - PRTG Network monitor GUI, zdroj: (Paessler, 2023)

Ceník:

Název balíčku	Cena (za měsíc)	Cena (za rok)	Omezení
PRTG 500	€137,41	€1,649	500 sensorů = 50 zařízení
PRTG1000	€220,75	€2,649	1000 sensorů = 100 zařízení
PRTG2500	€466,58	€5,599	2500 sensorů = 250 zařízení
PRTG5000	€833,25	€9,999	5000 sensorů = 500 zařízení
PRTG XL	€1149,91	€13,799	10 000 sensorů = 1 000 zařízení

Tabulka 2 - Ceník PRTG, zdroj: (Paessler, 2023)

V PRTG jsou "senzory" základními monitorovacími prvky. Jeden senzor obvykle sleduje jednu měřenou hodnotu v síti, například provoz portu přepínače, zatížení procesoru serveru nebo volné místo na disku. V průměru je potřeba asi 5 až 10 senzorů na jedno zařízení nebo jeden senzor na jeden přepínací port. (Paessler, 2023)

ManageEngine OpManager

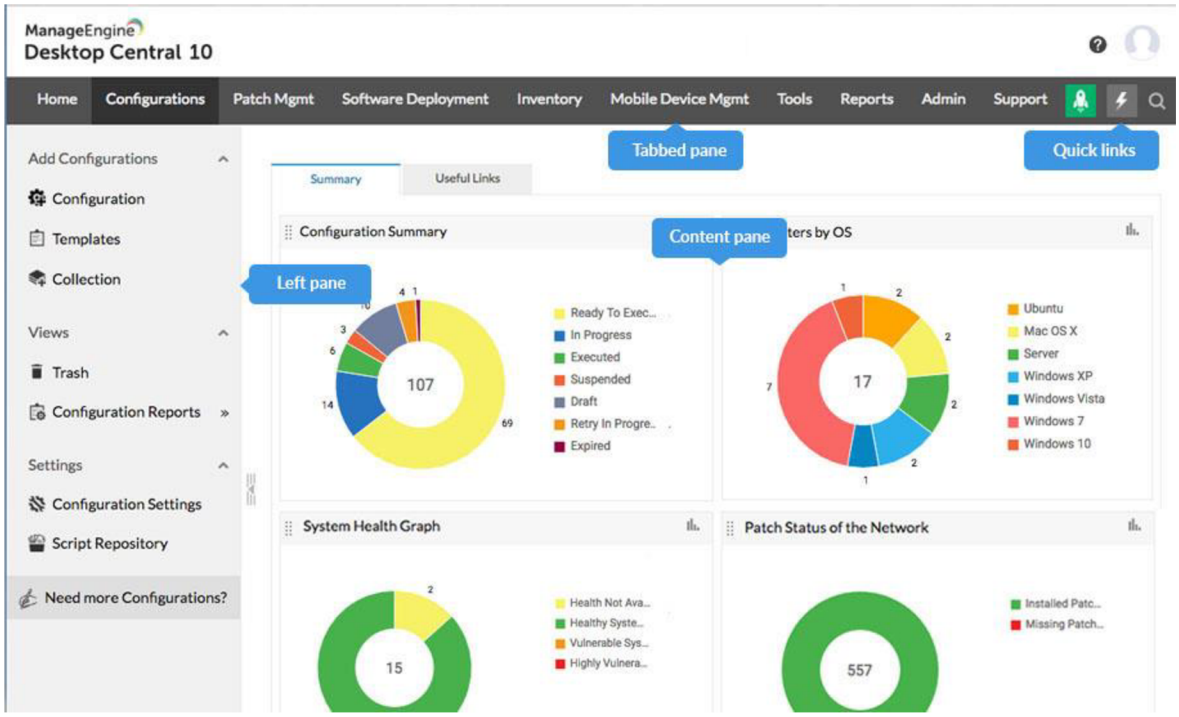
ManageEngine OpManager představuje komplexní software pro monitorování sítě vyvinutý společností ManageEngine, divizí Zoho Corporation. Jeho konstrukce je zaměřena na poskytnutí pomoci IT profesionálům při správě a monitorování rozličných aspektů jejich síťové infrastruktury. (ManageEngine, 2023)

OpManager disponuje integrovanou konzolí, která umožňuje správcům centralizovaně řídit směrovače, brány firewall, servery, přepínače a tiskárny z jediného uživatelského rozhraní. Dále nabízí rozsáhlé funkcionality pro řízení poruch a monitorování výkonu, což výrazně usnadňuje rychlou diagnózu a odstraňování potíží v síti, a zároveň zajistí optimální provoz celé sítě. (Acharya, 2023)

Cílem aplikace OpManager je zjednodušit správu sítě tím, že integruje více funkcí do jediné aplikace, což eliminuje potřebu využívat několik menších aplikací specializujících se pouze na omezené úlohy. Tímto způsobem lze výrazně efektivizovat správu sítě a zvýšit celkovou produktivitu. (ManageEngine, 2023)

V případě výskytu jakýchkoli problémů společnost ManageEngine poskytuje užitečné nápovědné zdroje, včetně poznámek k vydání, seznamu nových funkcí a aktualizačních změn, které usnadňují řešení problémů a zajišťují bezproblémové užívání aplikace OpManager. (Anderson, 2018)

Celkově lze konstatovat, že ManageEngine OpManager je robustní softwarové řešení pro monitorování sítě, které poskytuje IT profesionálům nástroje nezbytné k efektivní správě a sledování jejich sítí, zajistí optimální výkonnost a minimalizuje výpadky. (ManageEngine OpManager, 2023)



Obrázek 6 - ManageEngine GUI, zdroj: (GetApp, 2023)

Ceník:

Název balíčku	Cena (za měsíc)	Cena (za rok)	Omezení
Standard Edition	€20,41	€245	25 zařízení
Professional Edition	€28,75	€345	25 zařízení
Enterprise Edition	€962,08	€11545	250 zařízení

Tabulka 3 - Ceník ManageEngine, zdroj: (ManageEngine OpManager, 2023)

Možnosti licence OpManageru závisí na počtu sledovaných zařízení. Licence zahrnuje všechna rozhraní, uzly nebo senzory v zařízení. Zařízení může mít na rozdíl od konkurence libovolný počet rozhraní, prvků nebo snímačů. (ManageEngine OpManager, 2023)

Bezplatné nástroje na monitorování sítě:

Nagios

Nagios je open-source nástroj pro kontinuální monitorování, který sleduje síť, aplikace a servery. (TutorialsPoint, 2023)

Poskytuje funkce, jako monitorování Windows a Linuxu, monitorování serverů, monitorování aplikací, SNMP monitorování a monitorování logů. Nagios nabízí viditelnost a škálovatelnost pro více sítí a geografické oddělení prostřednictvím své funkce Fusion. Dále

poskytuje řešení jako Nagios Network Analyzer pro monitorování a analýzu síťového provozu, Nagios Log Server pro správu a analýzu logů a Nagios Fusion pro centralizovaný management sítí. (Gillis, 2023)

Zabbix

Zabbix je open-source softwarový nástroj pro monitorování využívaný k sledování různých IT komponentů, jako jsou sítě, servery, virtuální stroje a cloudové služby. Podporuje monitorování s využitím agentů i bez agentů, poskytující metriky a upozornění na výkon a sběr dat. (Zabbix, 2023)

Zabbix nabízí webové GUI s možností přizpůsobení ovládacích panelů a umožňuje distribuované monitorování v různých lokalitách. Dále poskytuje možnosti bez agentů, včetně jednoduchých kontrol, JMX a monitorování webových služeb. Zabbix API umožňuje uživatelům vytvářet nové aplikace a integrovat se s softwarem třetích stran. Šablony rozšiřují funkcionalitu Zabbixu pro monitorování síťových zařízení, serverů, aplikací a dalších prvků. Zabbix je zdarma a může být využíván organizacemi libovolné velikosti s možností získání komerční podpory. (KUMAR, 2022)

Cacti

Cacti představuje open-source webový nástroj pro monitorování sítí a grafické zobrazování dat, který je koncipován jako aplikační rozhraní pro RRDtool, standardní nástroj pro ukládání dat v průmyslu. Uživatelům umožňuje pravidelně dotazovat služby a graficky zobrazovat výsledná data. Cacti poskytuje robustní a rozšiřitelný operační monitoring a rámec pro správu chyb. (Cacti, 2023)

Wireshark

Wireshark představuje široce využívaný open-source program pro analýzu síťových protokolů, který umožňuje uživatelům zachytávat a zkoumat síťový provoz. Je považován za průmyslový standard a využívají ho síťoví správci, bezpečnostní inženýři, inženýři pro zajištění kvality, vývojáři a uživatelé sítí pro účely ladění, výuky a odstraňování chyb. (Kinzie, 2022)

Wireshark zachytává síťový provoz z různých připojení a ukládá data pro následnou offline analýzu. Software nabízí funkce, jako filtry pro zúžení zachycených paketů, volby pro barevné zvýraznění a promiskuitní režim. Wireshark je k dispozici ke stažení pro operační systémy Windows, Mac a Linux. Uživatelé by měli mít oprávnění ke kontrole

síťových paketů a základní pochopení síťových protokolů před použitím Wiresharku. (WireShark, 2023)

Všechny tyto nástroje by měly obsahovat následující funkce:

Název funkce	Popis funkce
Síťová detekce a inventarizace	Automatická identifikace všech síťových zařízení na základě uživatelsky definovaných podmínek výrazně redukuje pracovní zátěž a umožňuje věnovat pozornost prioritním úkolům.
Správa zařízení	Udržování aktuálního soupisu všech síťových zařízení včetně detailů, jako jsou DNS názvy, IP adresy a dodavatelské informace, umožňuje uživatelům udržet přehled o síti a prevenci nepovolených přístupů.
Monitorování SNMP/WMI	S ohledem na to, že většina sítí se skládá z hardware podporujícího protokol SNMP, tato funkce umožňuje monitorování dostupnosti a výkonu rozsáhlé škály síťového hardwaru.
Monitorování rozhraní	Fyzická i virtuální rozhraní tvoří jádro každé sítě. Proto je klíčové sledovat provoz, chyby, zahození datových přenosů, využití, velikost paketů a další metriky, aby bylo možné identifikovat přetížení sítě dříve, než se promítne do uživatelského zážitku.
Mapování topologie sítě	Vizualizace topologie sítě pomáhá uživatelům lépe porozumět struktuře sítě a rychleji identifikovat možné problémy.
Vlastní monitorování	Každé IT prostředí má své vlastní specifické potřeby a žádný standardní nástroj pro monitorování sítě nemůže poskytnout vše, co je potřeba. Proto týmy IT často vytvářejí vlastní monitorovací scénáře a postupy, které jsou přesně přizpůsobeny jejich jedinečným požadavkům.
Upozorňování	Reálný časový monitoring a okamžitá notifikace o síťových poruchách přispívají ke snížení doby, která je potřebná k odstranění problémů na minimum. Barevné kódování upozornění, které reflektuje kritičnost události, umožňuje okamžitou identifikaci a řešení problémů, které mají zásadní vliv na chod podnikového prostředí.
Nástroje pro řešení problémů	Hledání příčin problémů je důležitou součástí práce správce IT. Nástroje pro řešení problémů, jako jsou Ping, Traceroute, SNMP Ping, Vzdálená plocha, Trap Viewer a další, pomáhají efektivně sledovat, analyzovat a řešit problémy s výkonem sítě.
Zprávy	Reporty o různých segmentech sítě pomohou pravidelně kontrolovat výkon sítě a identifikovat oblasti, které je třeba zlepšit.
Převzetí služeb při selhání nebo vysoká dostupnost	Nástroje pro monitorování sítě v reálném čase jsou pro správce IT důležité. Poskytují nepřetržitý přehled o síti. Co se stane, když nástroj pro monitorování sítě selže? Vše se stane chaotickým, proto je ideální mít k dispozici redundantní mechanismus. Přesně to dělá záložní systém, který převezme činnost monitorování sítě, když primární systém selže.
Technická podpora	Žádný nástroj není nikdy dokonalý a správci IT často narážejí na technické problémy v souvislosti s nástroji pro monitorování sítě. Může jít o problém s konfigurací nebo o konkrétní funkci, která nefunguje podle očekávání. To lze překonat s pomocí odborníků na produkty a techniků zákaznické podpory prostřednictvím chatu, hovorů nebo vzdálených relací.
Dokumentace	Dokumentace k produktu je něco, co se často přehlíží. Většinu pochybností o funkčnosti produktu, jeho mechanismu a konfiguraci lze snadno odstranit prostřednictvím dokumentace nápovědy k produktu od dodavatele. To šetří čas a úsilí.

Tabulka 4 - Nástroje pro monitorování sítě, zdroj: (ManageEngine Blog, 2021)

3.4.1 Paketová analýza a telemetrie

Paketová analýza

Paketové zachytávání, často označované též jako pasivní odposlech paketů nebo analýza síťového provozu, představuje technický proces, během něhož jsou zachycovány a analyzovány datové jednotky, známé jako datové pakety, které putují přes komunikační infrastrukturu počítačové sítě. Tyto datové pakety slouží jako základní stavební jednotky informačního přenosu v rámci dané sítě. (Sanders, 2011)

Při přenosu dat v síti jsou informace, které mají být předány z jednoho místa na druhé, rozděleny na menší části, což jsou právě tyto datové pakety. Každý z těchto paketů obsahuje metadata, jako jsou zdrojová a cílová IP adresa, portové identifikátory a samotný užitečný datový obsah. (Sanders, 2011)

Pro účely zachytávání paketů se využívají specializované software, nebo hardware, které umožňují zachytit a zaznamenat tyto datové pakety během jejich průchodu sítí. Tato zachycená data následně mohou být podrobena analýze, což poskytuje uživatelům přehled o výkonnosti sítě, umožňuje detekci problémů, odhalení potenciálních bezpečnostních hrozeb a umožňuje lepší pochopení chování síťových zařízení a aplikací. (Solarwinds, 2022)

Streaming telemetry

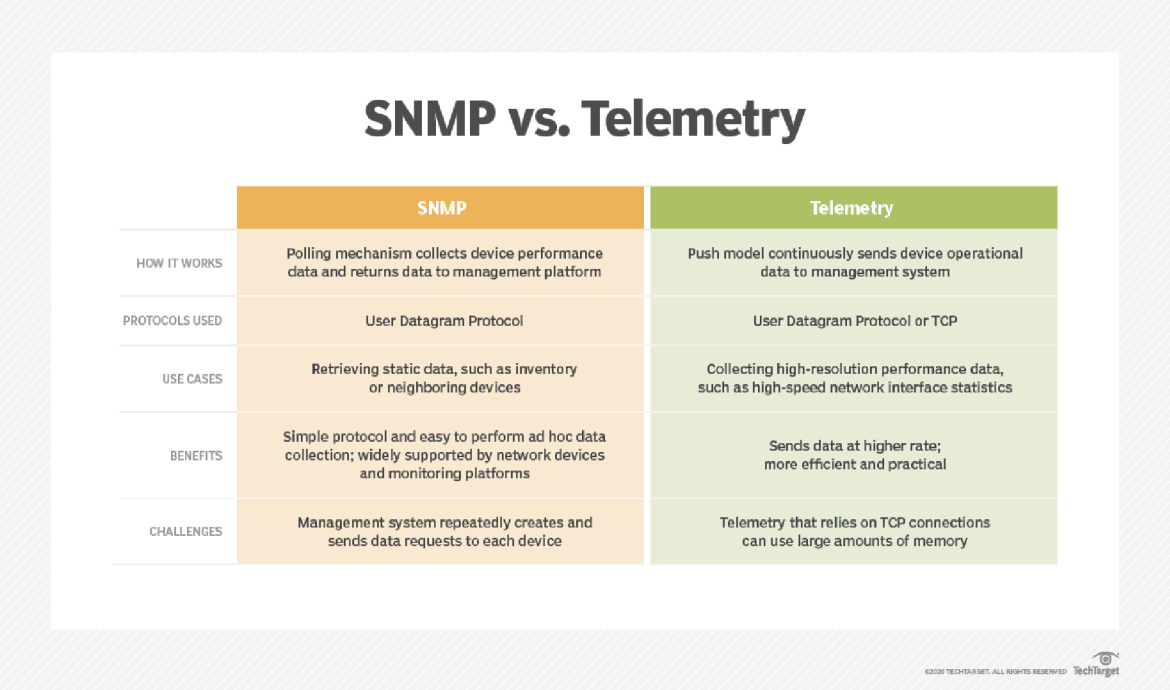
Streamovaná síťová telemetrie představuje reálný časový sběr dat, během kterého síťová zařízení, jako jsou směrovače, přepínače a brány firewall, kontinuálně vysílají aktuální informace o stavu sítě do centralizovaného úložiště. Telemetrie obecně zahrnuje metody a postupy pro přenos měření z vzdáleného zdroje k přijímací stanici, kde jsou data uchovávána a analyzována. (Benoît Claise, 2019)

Síťová telemetrie založená na datových tocích pracuje na principu tzv. "push" a umožňuje automatický a nepřetržitý přenos dat.

Komunikační relace mohou být navázány buď síťovým zařízením, které se přihlásilo k shromažďovateli, nebo shromažďovatelem, který se přihlásil k síťovému zařízení. (Benoît Claise, 2019)

Streamování síťové telemetrie může notifikovat síťové odborníky o výrazném nárůstu nebo poklesu provozu. Data získaná prostřednictvím proudové telemetrie jsou podrobena příslušnému modelu a představují ideální vstup pro analýzu velkých dat za účelem optimalizace toku provozu. (Froehlich, 2023)

Z hlediska implementace mají správci kontrolu nad několika aspekty procesu odběru a streamování. Dále může správce selektivně určit, jaké typy informací budou sbírány. (Froehlich, 2023)



Obrázek 7 - SNMP vs Telemetry, zdroj: (Froehlich, 2023)

3.5 Kritické metriky a ukazatele pro monitorování sítě

Kompletní monitorování by mělo zahrnovat tři hlavní skupiny metrik: dostupnost prostředků, výkonnost softwaru a případně chování uživatelů. Metriky pro všechny skupiny by měly být získatelné jako časové řady prostřednictvím společného rozhraní, které umožňuje efektivní identifikaci zdrojů problémů pomocí korelace časových řad. (Ligus, 2012)

Monitorovací metriky jsou soubory číselných datových vstupů uspořádaných do skupin po sobě jdoucích, chronologicky seřazených seznamů. Každý datový vstup se skládá ze zaznamenané hodnoty měření, časového razítka, kdy měření proběhlo, a souboru vlastností, které ho popisují. (Ligus, 2012)

Jsou-li datové vstupy z metriky rozčleněny do pevných časových intervalů a shrnuty matematickou transformací nějakým smysluplným způsobem, lze je prezentovat jako časové řady a interpretovat na dvourozměrných grafech. (Subramanian, 2012)

Délka intervalů datových bodů, označovaná také jako časová granularita, závisí na typech měření a druhu informací, které mají být získány. Mezi běžné intervaly patří 1, 5, 15 a 60 minut, ale je možné vykreslovat i intervaly s granularitou jedné sekundy a hrubé jednoho dne. (Ligus, 2012)

3.5.1 Latence, odezva a ztráta paketů: měření kvality komunikace

Měření kvality komunikace se týká hodnocení a analýzy různých aspektů komunikace v telekomunikačních a síťových systémech. Tři klíčové faktory, které jsou často zohledněny při měření kvality komunikace, jsou latence, odezva a ztráta paketů. (Andrew Tanenbaum, 2010)

Latence

Latence představuje časový interval, který uplyne, než datový paket projde konkrétní síťovou linkou. Nižší hodnoty latence jsou preferovány, nicméně stále zde existují fyzikální omezení, která jsou dány rychlostí, jakou se může šířit elektrický signál (či světlo v případě optických vláken). (Julian, 2017)

V některých aplikacích, které nesnášejí vysoké hodnoty latence, může zpoždění významně ovlivnit uživatelský zážitek. Jeden z preferovaných přístupů k monitorování latence mezi dvěma body spočívá v pravidelném měření a dokumentování latence za použití specializovaných nástrojů (Julian, 2017)

Existuje několik různých typů latence: (Burke, 2003)

1. **Přenosová latence**: Jedná se o časový úsek, během něhož dochází k přenosu dat z jednoho bodu do druhého, přičemž je měřena od okamžiku, kdy jsou data zcela odeslána, po okamžik, kdy jsou zcela přijata na cílovém zařízení.
2. **Zpracovací latence**: Tato latence reprezentuje čas, který uplyne mezi momentem příchodu dat na síťové zařízení, jako jsou směrovače či přepínače, a okamžikem, kdy jsou tato data plně zpracována a připravena k dalšímu přenosu či zpracování.
3. **Front-end latence**: Tato latence se měří jako interval mezi odesláním požadavku a zahájením přijímání odpovědi či dat. Je to časový úsek, během něhož dochází k iniciačnímu přenosu dat mezi zařízením odesílatele a přijímatele, a je klíčový pro celkový uživatelský zážitek při interakci s aplikacemi či systémy v síťovém prostředí.

Odezva

Doba odezvy je definována jako interval času, který uplyne od odeslání dotazu do systému až po okamžik, kdy systém reaguje poskytnutím odpovědi.
Tato doba se skládá z čekací doby, kdy dotaz čeká ve frontě na vyřízení, a doby obsluhy, což představuje časový úsek věnovaný zpracování daného požadavku. (Comer, 2014)

Nižší doba odezvy obvykle signalizuje optimální výkonnost systému, zatímco zvýšení doby odezvy může naznačovat možný problém s výkonem systému. Je třeba zdůraznit, že doba čekání na vyřízení dotazů tenduje k nelineárnímu nárůstu se zvyšující se zátěží zařízení či systému. Jakmile je systém silně vytížen, může dojít k dramatickému prodloužení doby odezvy. (SolarWinds, 2023)

Ztráta paketů

Ztráta paketů nastává v situacích, kdy je paket zasažen tak významným počtem bitových chyb, že je nemožné jeho korektní obnovení, nebo kdy dochází k nedostupnosti doručení paketu z důvodu přetížení sítě a pakety nejsou schopny dorazit k cíli. Přetížení může způsobit přeplnění fronty, což vede k zahození paketů, nebo může dojít k tak výraznému zpoždění přenosu, že se pakety stávají efektivně nepoužitelnými a jsou tudíž klasifikovány jako "ztracené" (Bäckström, 2018)

Jitter

Jitter lze definovat jako časové zpoždění nebo časový rozdíl mezi odesláním každého datového paketu po síti. V kontextu sítí je jitter často využíván k hodnocení variability latence. Například oscilace latence z 1 ms na 150 ms s rozptylem až 30 ms by představovaly výrazný projev vysokého jitteru, zatímco konstantní latence 3 ms by nebyla provázena žádným výkyvem. (Nicola Da Dalt, 2018)

Jitter má význačný vliv zejména v interaktivních hlasových a zvukových sítích, neboť může způsobit neplynulost či trhání v reprodukovaném zvuku. Monitoringem a kontrolou latence lze efektivně řídit vliv jitteru na kvalitu komunikace. (Julian, 2017)

3.5.2 Šířka pásma, propustnost sítě

Šířka pásma

Šířka pásma reprezentuje teoretické maximální množství informací, které může být simultánně přeneseno přes určité připojení. Obvykle se vyjadřuje v bitech za sekundu (bps),

megabitech za sekundu (Mbps) a gigabitech za sekundu (Gbps). Důležité je si uvědomit, že vysoká šířka pásma samo o sobě nezajišťuje vysoký výkon sítě.

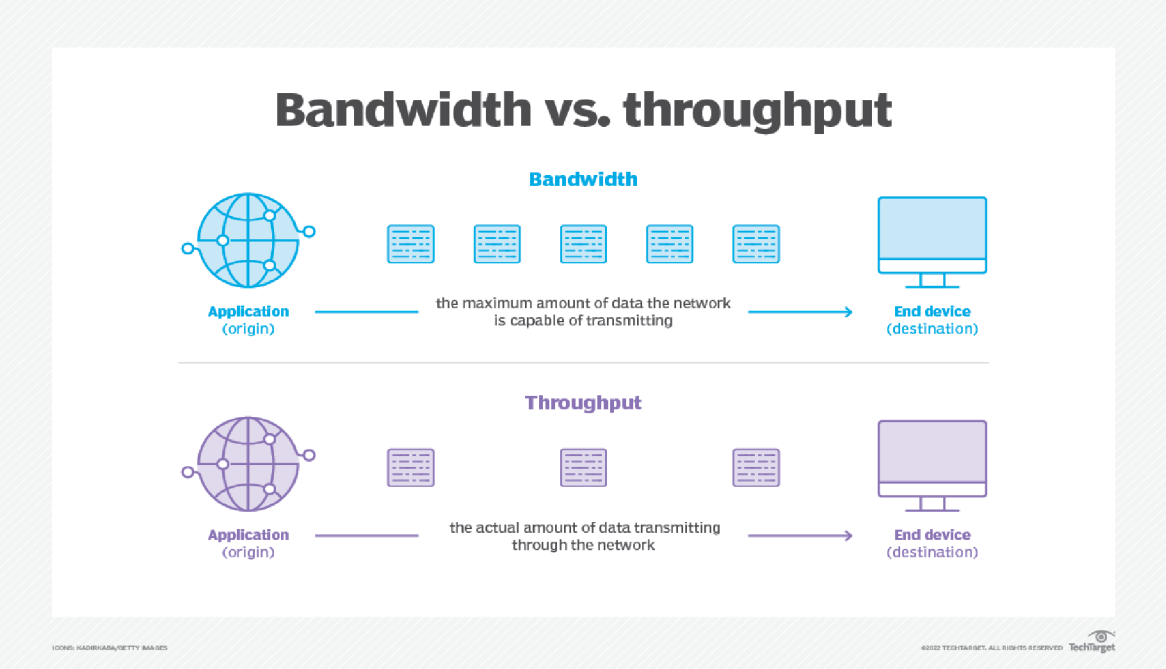
Pokud je propustnost sítě ovlivněna faktory jako jsou zpoždění, ztráta paketů a jitter, může docházet k zpožďování služeb, i když je k dispozici vysoká šířka pásma. Čím větší je šířka pásma sítě, tím více dat může posílat tam a zpět. Termín šířka pásma se nepoužívá k měření rychlosti, ale spíše k měření kapacity. (Verizon, 2023)

Propustnost:

Propustnost, v odborné terminologii též nazývaná jako datový přenosový tok, představuje skutečné množství dat, která jsou úspěšně přenesena přes síťové připojení za definovaný časový úsek. Tento parametr se vyjadřuje v jednotkách bitů za sekundu (bps) či bajtů za sekundu (Bps). Měření propustnosti je zásadní pro zhodnocení výkonnosti sítě a poskytuje klíčové informace o schopnosti sítě přenášet data efektivně a spolehlivě. (Wilson, 2023)

Ovlivnění propustnosti síťového připojení může být podmíněno celou řadou faktorů. Přetížení sítě, vyjádřené nárůstem počtu datových toků přesahujících kapacitní limity zařízení či linky, může výrazně snížit úroveň propustnosti. Ztráta paketů, což představuje situaci, kdy některé datové pakety nejsou úspěšně doručeny k cílovému zařízení, také negativně ovlivňuje efektivitu síťového připojení. Zpoždění sítě, které se projevuje časovou prodlevou mezi odesláním dat a jejich příjmem na cílovém koncovém bodě, je dalším významným faktorem, který může omezit propustnost. (Burke, 2022)

Přesná a spolehlivá analýza propustnosti je klíčovým krokem pro správné dimenzování a optimalizaci síťové infrastruktury. Získané informace o propustnosti umožňují správcům sítí reagovat na aktuální provozní podmínky a případně provádět potřebné úpravy s cílem zajistit plynulý a spolehlivý přenos dat v síti. (Lamberti, 2023)



Obrázek 8 - Propustnost vs Šířka pásma, zdroj: (Burke, 2022)

3.5.3 Aktivita a chování uživatele

Monitorování uživatelské aktivity (UAM) představuje systematický proces, jenž se zaměřuje na sledování a dokumentaci chování koncových uživatelů v rámci informační technologie podnikového prostředí. Jeho hlavním cílem je detekce a prevence potenciálních vnitřních hrozeb, a to prostřednictvím monitorování různorodých aktivit uživatelů, včetně jejich interakcí s webovým prostředím či neoprávněným přístupem k souborovým zdrojům a dalším datovým entitám. (Lord, 2023)

Nástroje pro monitorování uživatelské aktivity přinášejí významný přínos v identifikaci podezřelých vzorců chování, snižují riziko úniku důvěrných dat a zajišťují dodržování předpisů týkajících se ochrany osobních údajů. Je nezbytné, aby data, jež jsou shromažďována prostřednictvím UAM řešení, byla podrobně analyzována s ohledem na související rizika, stanovené směrnice, časová okna a kontext identity uživatele. (Aston, 2023)

K dispozici jsou rozličné technologické prostředky pro sledování aktivity uživatelů, včetně mechanismů umožňujících včasné upozornění na události v reálném čase. Mezi osvědčené postupy v oblasti UAM zahrnujeme zásady transparentnosti v monitorování,

praktikování principu nejmenších oprávnění, důraz na zavedení robustních autentizačních procesů a efektivní správu vzdáleného přístupu. (Bhargava, 2022)

Organizace by měly rovněž ustanovit politiky pro ochranu dat a aktivně podporovat vzdělávání uživatelů v oblasti kybernetické bezpečnosti. Monitorování aktivity uživatelů tvoří nepostradatelnou součást celkového bezpečnostního rámce podniku, zejména co se týče ochrany důvěrných dat. (Loshin, 2022)

3.6 Bezpečnostní aspekty síťového monitorování

S postupným vývojem řešení pro monitorování sítí dochází k inkorporaci bezpečnostních prvků s cílem zmírnit pokles výkonu způsobený bezpečnostními hrozbami. Mezi klíčové bezpečnostní charakteristiky řešení pro monitorování sítí patří okamžité a inteligentní oznamování událostí, komplexní sledování bezpečnostního stavu celé sítě, důkladná analýza provozu, pozorná kontrola využití šířky pásma, automatizované nápravy anomálií a vytvoření centralizovaného rámce pro monitorování zabezpečení. (Chris Sanders, 2013)

Tyto průkopnické technologie zajišťují promptní detekci a oznámení o bezpečnostních incidentech, poskytují pohled na celou síťovou infrastrukturu, proaktivně identifikují potenciální bezpečnostní zranitelnosti, monitorují nesrovnalosti ve využívání šířky pásma, automatizují proces řešení problémů a udržují centralizované řízení nad prostředky pro monitorování zabezpečení. (Hein, 2019)

3.6.1 Ochrana dat a soukromí při sběru a analýze monitorovacích dat

Ochrana dat a zachování soukromí v procesu sběru a analýzy monitorovacích údajů představují v současné digitální éře kritické aspekty. Organizace jsou vyzvány k implementaci opatření zajišťujících bezpečnost a integritu dat, která podléhají shromažďování a následné analýze. (CloudFlare, 2023)

Tato ochrana zahrnuje implementaci strategií a postupů, jež směřují k zajištění soukromí, dostupnosti a integrity dat. Tato opatření jsou klíčová pro jakoukoli organizaci, která manipuluje s citlivými informacemi. (Klosowski, 2021)

V rámci Evropské unie (EU) se ochrana osobních údajů řídí obecným nařízením o ochraně osobních údajů (GDPR). Toto nařízení vyžaduje, aby společnosti získaly

informovaný souhlas a umožnily jednotlivcům práva jako je přístup k vlastním osobním údajům, jejich smazání a kontrola nad nimi. (CloudFlare, 2023)

Při provádění sledování sběru a analýzy dat by měly organizace provádět posouzení vlivu na ochranu osobních údajů (DPIA). Tato posouzení pomáhají identifikovat a minimalizovat rizika, která jsou spojena s činnostmi zpracování údajů. (Posey, 2021)

Důležité je také zavést odpovídající technická a organizační opatření k ochraně dat. To může zahrnovat využívání šifrování, řízení přístupu, pravidelné zálohování dat a školení zaměstnanců v oblasti postupů ochrany dat a zachování soukromí. (CloudFlare, 2023)

Organizace musí rovněž zajistit, že jsou opatřeny právním základem pro sběr a analýzu údajů. To zahrnuje získání informovaného souhlasu, plnění smluvních závazků nebo dodržování právních předpisů. (Posey, 2021)

Při vývoji monitorovacích systémů je esenciální dodržovat principy ochrany soukromí již v etapě návrhu a implementovat opatření na ochranu soukromí a dat v základním nastavení. Tímto způsobem se zaručí, že ochrana soukromí bude preferována od samého počátku návrhového procesu. (Cloudian, 2023)

Pro ochranu individuálního soukromí, při sběru a analýze dat mohou být využity techniky anonymizace a pseudonymizace dat. Tyto strategie zahrnují postupy, které buď úplně odstraňují nebo zjemňují identifikovatelné prvky osobních dat. (Klosowski, 2021)

Důležité je si uvědomit, že konkrétní požadavky a předpisy v oblasti ochrany údajů a soukromí mohou variabilně diferovat v závislosti na příslušné jurisdikci a specifičnostech daného odvětví. (CloudFlare, 2023)

3.6.2 Identifikace hrozeb a anomálií v síťovém provozu

Systémy detekce narušení (IDS) a technologie detekce anomálií v chování sítě (NBAD) zastávají klíčovou úlohu v oblasti zabezpečení sítě. Jejich hlavním úkolem je identifikovat latentní hrozby a zranitelnosti v síťové infrastruktuře, jež jsou po detekci předány odborníkům na bezpečnost sítě. (Lin, 2023)

Detekce anomálií v síťovém chování provádí analýzu vzorců provozních toků, signatur paketů, údajů o výkonnosti sítě a dalších faktorů s cílem odhalit skryté hrozby a podezřelé chování v síti. Pro minimalizaci dopadu kompromitujících situací, jako jsou infekce, úniky dat, narušení sítě a další formy kybernetických útoků, je zásadní, aby monitoring sítě probíhal kontinuálně. (Huy Nguyen, 2008)

Důležitým úkolem řešení pro monitorování sítě je ověření funkčnosti existujících bezpečnostních systémů, včetně firewallů a antivirových skenerů. Například monitoringové řešení průběžně akumuluje detailní výkonnostní a stavové informace o bráně firewall. V případě nefunkčnosti brány firewall se zvyšuje riziko útoku škodlivým softwarem na síť. (Security Scorecard, 2021)

Takové škodlivé útoky mohou mít různorodé důsledky, jako je náhodné spouštění programů procesorem nebo otevírání portů, které by měly zůstat uzavřeny. Pro předejití těmto situacím jsou správci okamžitě informováni o jakýchkoli anomáliích v bráně firewall. Monitoringový software může také dohlížet na antivirové skenery běžící na centrálním poštovním serveru. Tím pomáhá firemním subjektům zajistit nepřetržitou aktivitu skeneru. Monitoringové řešení, s využitím specializovaných senzorů, monitoruje Centrum zabezpečení systému Windows a ověřuje, zda jsou antivirové skenery a antimalwarové programy na individuálních počítačích ve firmě aktuální a bezproblémově fungují. Tím je garantována nepřetržitá ochrana klientských počítačů před škodlivým softwarem. (Paessler AG, 2022)

Detailní sledování využití šířky pásma může rovněž nepřímo signalizovat přítomnost malwaru. Indikátorem útoku může být například pomalá odezva aplikací a webových stránek, způsobená malwarem, jenž zatěžuje značnou část dostupné šířky pásma. Pro detekci těchto odchylek sleduje monitoringový software různé parametry, jako jsou IP adresy, čísla portů, protokoly a další. (Paessler AG, 2022)

3.7 Síťový monitoring a cloudová infrastruktura

Monitorování cloudu je systematický proces sledování, analýzy a správy stavu, výkonu a dostupnosti cloudových aplikací, architektury a služeb. Tento proces využívá jak automatizované, tak manuální techniky a nástroje s cílem zajistit optimální fungování cloudové infrastruktury v souladu s očekáváními. (John Arundel, 2019)

Cloudová infrastruktura představuje komplexní soubor hardwarových a softwarových prvků, jako jsou výpočetní kapacity, síťová infrastruktura, úložná média a virtualizační technologie, nezbytných pro provoz cloudových služeb. Kromě toho zahrnuje i uživatelské rozhraní (UI) pro správu těchto virtuálních prostředků. (VMWare, 2023)

3.7.1 Monitorování v rámci virtuálních a cloudových prostředí

Monitorování cloudu představuje klíčový proces v identifikaci potenciálních problémů před tím, než ovlivní dostupnost služeb. Poskytuje holistický pohled na interakce mezi uživateli, daty a aplikacemi, současně přispívá k optimalizaci výkonnosti aplikací, snižování bezpečnostních rizik a efektivnímu řízení nákladů. Nedílnou součástí tohoto postupu je monitorování rozličných aspektů cloudu, zahrnující webové stránky, virtuální sítě, databáze, virtuální stroje a cloudové úložiště. (NetApp, 2023)

V optimálním scénáři probíhá monitorování cloudu v reálném čase společně s jeho lokálními a hybridními variantami. To výrazně rozšiřuje povědomí o celkovém prostředí, zahrnujícím úložiště, sítě a aplikace. Mezi klíčové funkce nástrojů pro monitorování cloudu patří sledování spotřeby a provozu zdrojů hostovaných v cloudu. (Cisco, 2023)

Neméně podstatnou součástí monitorování cloudu je schopnost měřit a vizualizovat výkon aplikací a síťové infrastruktury mezi hybridním cloudem, privátním cloudem a veřejnými cloudovými službami. Tyto nástroje jsou nezbytné pro konsolidaci rozsáhlých objemů dat v distribuovaných lokalitách, identifikaci anomálií a jejich původů a proaktivní předvídání potenciálních rizik či výpadků v provozu. (Cisco, 2023)

Veřejný cloud

Monitorování veřejného cloudu zahrnuje dohled nad provozem služeb hostovaných u třetích stran, jako jsou DigitalOcean, AWS nebo Google Cloud. Tyto poskytovatele nabízejí vlastní monitorovací nástroje (např. DigitalOcean Monitoring, AWS CloudWatch, Google Cloud Operations), avšak externí nástroje mohou rozšířit pokrytí a hloubku analýzy. Klíčové aspekty monitorování veřejného cloudu zahrnují efektivní alokaci zdrojů, schopnost škálovat v reálném čase, optimalizaci nákladů a udržení vysoké úrovně bezpečnosti. (DigitalOcean, 2023)

Privátní cloud

Monitorování privátního cloudu se zaměřuje na sledování infrastruktury vlastněné a provozované organizací. Kromě monitorování výkonu a efektivity využití zdrojů je nutné klást důraz na správný stav hardwaru, plánování kapacity a případně také na udržování přísných standardů zabezpečení a souladu s regulačními požadavky. Pro efektivní monitorování privátního cloudu je nezbytné důkladné pochopení infrastruktury této privátní cloudové platformy, včetně provozních charakteristik, možných bodů selhání a strategie analýzy a reakce na data shromážděná z monitorovacích systémů. (DigitalOcean, 2023)

Hybridní cloud

Monitorování hybridního cloudu zahrnuje sledování operací v prostředí, které kombinuje jak veřejné, tak privátní cloudu. Klíčovou výzvou je integrace monitorování mezi těmito rozmanitými prostředími a udržení celkového přehledu o provozních procesech. Monitorování hybridního cloudu vyžaduje pozornost věnovanou propojením, přenosu dat a zabezpečení mezi rozhraními veřejného a privátního cloudu. (SolarWinds, 2023)

3.7.2 Specifika monitorování v kontejnerových architekturách

Kontejnerová architektura představuje prostředek izolovaných jednotek, které obsahují kompletní balíček softwaru a jeho závislostí, což zajišťuje konzistentní provoz v různých prostředích. Každý kontejner typicky obsahuje obraz, souborový systémový strom, nainstalované knihovny a jádro operačního systému. (John Arundel, 2019)

Monitorování kontejnerů vyžaduje rozsáhlejší instrumentaci napříč celým technologickým stackem, která shromažďuje metriky o jednotlivých kontejnerech a příslušné infrastruktuře, analogicky k monitorování aplikací. Nástroje pro monitorování kontejnerů musí zaručit, že dokáží sledovat správce klastru, uzly klastru, démona, konkrétní kontejnery a původní mikroslužbu, což jim poskytne komplexní přehled o stavu kontejneru. (Lulka, 203)

Pro efektivní monitorování je nezbytné vytvořit propojení mezi mikroslužbami, které běží v kontejnerech. Monitorování poskytuje perspektivu na škálovatelnost a alokaci zdrojů kontejnerů. Pomáhá optimalizovat využití tím, že identifikuje případy přetížení či nedostatečného využívání kontejnerů, čímž umožňuje správcům zaujmout informovaná rozhodnutí o vertikálním nebo horizontálním škálování prostředků. (Aquasec, 2023)

V implementaci monitorování v kontejnerových architekturách je k dispozici široká škála nástrojů a platforem, které nabízejí funkce jako sběr metrik, agregace logů, vizualizace a upozornění. Tyto nástroje lze integrovat s orchestračními systémy kontejnerů, jako je Kubernetes nebo Docker Swarm, a poskytnout tak komplexní možnosti monitorování. (Snyk, 2023)

Oblíbené open source nástroje v oblasti sledování zahrnují Jaeger pro trasování, Prometheus pro sběr metrik, Logstash pro zpracování logů a Grafana pro vizualizaci a analýzu dat. Existuje také široká škála dodavatelů v oblasti pozorovatelnosti. (Snyk, 2023)

3.8 Budoucnost síťového monitorování a trendy

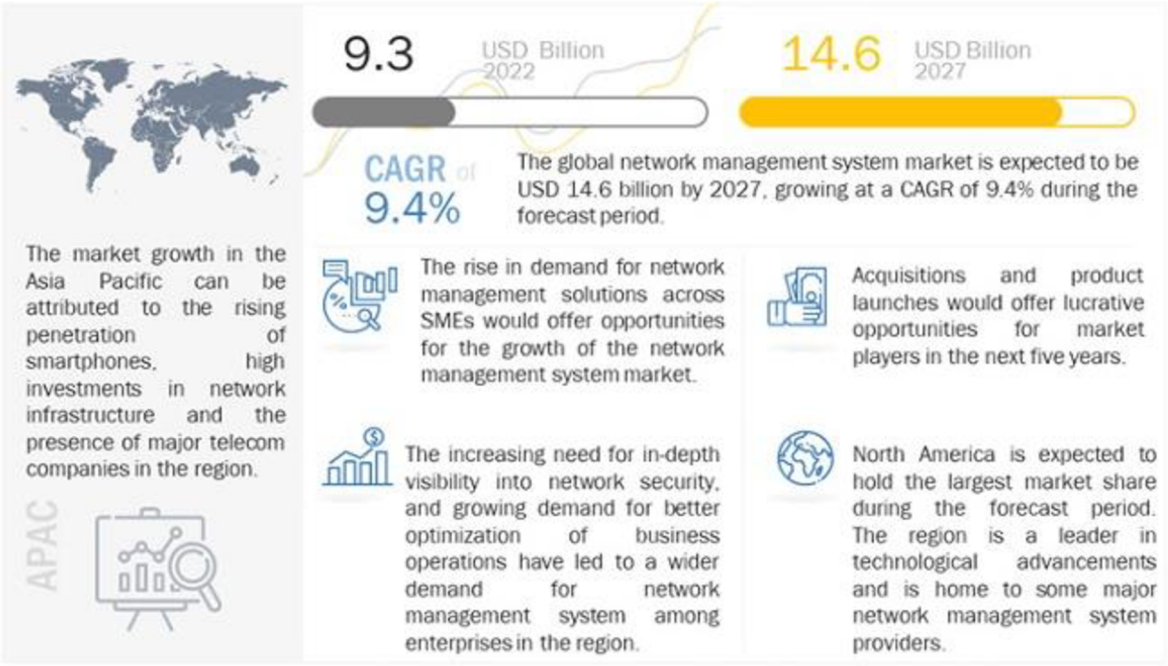
Perspektivy správy a monitorování sítí budou vyžadovat rychlou adaptaci k narůstající složitosti a virtualizaci sítí, včetně vzestupu kontejnerizace a mikroslužeb. S digitálním ekosystémem, jehož vývoj probíhá nevídaným tempem, musí korelovat i nástroje a metodiky, které zajistí jeho neustálou životaschopnost. Od implementace umělé inteligence (AI) a algoritmů strojového učení (ML) po rozšiřování edge computingu, tento disertační příspěvek si klade za cíl osvětlit cestu vpřed, v níž se monitorování sítí stává transformačním prvkem, pohánějícím budoucnost konektivity. (DeCarlo, 2020)

3.8.1 Vývoj technologií a směřování budoucnosti v oblasti monitorování sítě

S nástupem řady pokročilých technologických průlomů dochází k revoluci v oblasti správy sítí. Od implementace sofistikované analytiky a strojového učení, přes rozšíření cloudových řešení až po rostoucí důraz na kybernetickou bezpečnost. (ManageEngine, 2023)

Podle průzkumu společnosti Markets and Markets se předpokládá, že trh s řešeními pro správu sítí (NMS) bude růst složenou roční mírou 9,4 % a dosáhne přes 14,6 miliardy USD do konce roku 2027. Tento významný růst je způsoben přechodem k paradigmám umělé inteligence, strojového učení a softwarově definovaných sítí (SDN). (ManageEngine, 2023)

Tyto průlomové inovace formují cestu pro samokonfigurovatelné, samooptimalizující a samoopravující se sítě, které mohou zcela přetvořit paradigma správy sítí, jak ho známe dnes. Automatizace síťové infrastruktury povede k dosažení bezprecedentního zlepšení rychlosti, spolehlivosti a bezpečnosti sítě, zatímco výrazně sníží provozní náklady. Schopnost předvídat chování sítě a nepřetržitá optimalizace přinese nadstandardní uživatelské zkušenosti, což se promítne do vyšší spokojenosti a loajality zákazníků. Z tohoto důvodu se umělá inteligence, strojové učení a SDN stávají nezbytnými nástroji pro odborníky v oblasti IT, kteří se snaží udržet krok s konkurencí. (ManageEngine, 2023)



Obrázek 9 - Předpokládaná hodnota trhu s monitoringem, zdroj: (MarketsandMarkets, 2022)

3.8.2 Vliv technologických trendů na monitorování sítě

Budoucnost monitorování sítí je ovlivněna dynamickým vývojem v oblasti informačních technologií. Zahrnuje nové trendy a technologie, které neustále posouvají hranice toho, co je možné v oblasti správy a optimalizace sítí. Mezi tyto novinky patří:

Virtualizace:

S postupem virtualizačních technologií, jako je serverová virtualizace, se objevují některé výzvy v oblasti monitorování sítí.

První z nich se týká narůstající složitosti síťové infrastruktury. Virtualizovaná prostředí, zejména virtuální počítače (VM) a přepínače, vytvářejí rozsáhlou virtuální infrastrukturu, vyžadující plynulou komunikaci mezi různými entitami. To zahrnuje komunikaci mezi uživatelem a virtuálním počítačem, virtuálními počítači, virtuálním počítačem a daty, virtuálním počítačem a partnerskými entitami s odolností proti poruchám a také mobilitu virtuálních počítačů. Tato komplexita komunikace představuje výzvu pro monitorovací nástroje, pokud jde o přesné zachycení a analýzu síťového provozu. (Zeoss, 2011)

Druhým problémem je nedostatek adekvátních zdrojů a odborných znalostí. Dynamická povaha virtualizovaných prostředí rovněž představuje výzvu pro monitorování

sítí. Virtuální počítače mohou být vytvářeny, přesunovány nebo odstraňovány na vyžádání, což vede k neustálým změnám v topologii sítě. Tradiční monitorovací nástroje se mohou potýkat s obtížemi při udržování kroku s těmito dynamickými změnami a nemusí poskytovat v reálném čase aktuální přehled o virtualizované síti. (Williams, 2018)

Automatizace a AI:

Integrace umělé inteligence s monitorovacími systémy výrazně zvyšuje jejich efektivitu a přesnost. Díky algoritmům umělé inteligence lze provádět analýzu rozsáhlých datových souborů, která jsou zachycena monitorovacími zařízeními, a identifikovat vzorce, anomálie a potenciální problémy v reálném čase. To umožňuje proaktivní monitorování, prediktivní údržbu a celkové zlepšení výkonnosti systému. (Yulei Wu, 2022)

Zavedení automatizace a technologií umělé inteligence přináší výrazné vylepšení pracovních postupů správců a inženýrů sítě. Redukuje manuální chyby a zvyšuje výkon a bezpečnost sítě. Automatizace a umělá inteligence mohou efektivně pomoci s úkoly jako je konfigurace sítě, řešení problémů, detekce anomálií, analýza příčin a následná náprava. (Israr Ullah, 2019)

Cloud:

Jedním z klíčových trendů v oblasti monitorování sítí je přechod k cloudovým a hybridním prostředím, kde jsou síťové zdroje distribuovány na různých lokalitách a platformách. Tento vývoj přináší nové výzvy v oblasti monitorování sítě, jako je zajištění dostatečné viditelnosti, zvládání rozsahu, integrace a dodržování předpisů. Pro přizpůsobení se tomuto trendu je nezbytné využívat nástroje pro monitorování sítě, které jsou kompatibilní s cloudovými a hybridními prostředími, včetně těch, které nabízejí bez agentní monitorování nebo možnost monitorování v cloudu, poskytují viditelnost více cloudových prostředí, umožňují dynamické zjišťování a integrují rozhraní API. (Yuchao Zhang, 2020)

IoT:

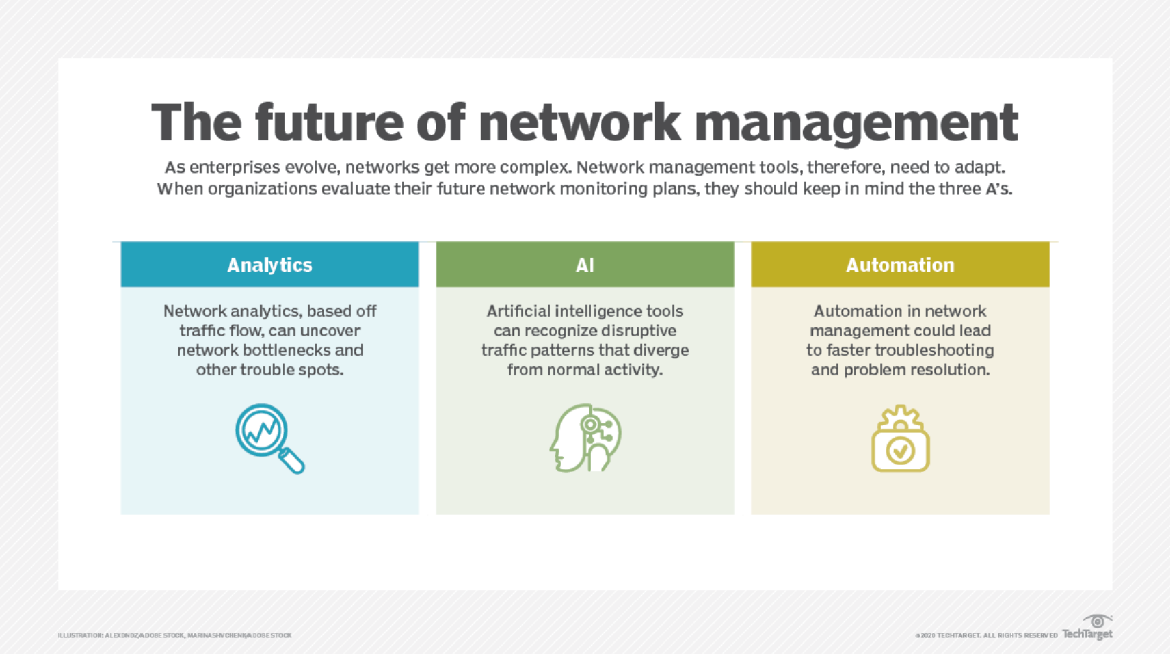
Internet věcí (IoT) zásadně proměnil monitorovací prostředí tím, že umožnil připojení drobných senzorických a komunikačních zařízení k internetu. Tato IoT zařízení, propojená s běžnými objekty každodenního života, otevírají dveře k vzdálenému monitorování a řízení. Jsou schopna v reálném čase sbírat data z rozličných zdrojů, včetně senzorů, a přenášet je do monitorovacích systémů pro další analýzu a rozhodování. Tím vznikají nové výzvy pro sledování sítí, jako jsou nárůst složitosti, rozmanitosti zařízení, zabezpečení dat a řešení latence. (Israr Ullah, 2019)

SDN:

Software Defined Networking (SDN) poskytuje vyšší úroveň programovatelnosti a flexibilitu sítě díky oddělení řídicího a datového rovna. To umožňuje centralizovanou správu a automatizaci síťových zdrojů, což zvyšuje efektivitu monitorování sítě a řešení vzniklých problémů. (De, 2023)

DEM:

Experience Management (DEM) zahrnuje systematické monitorování a analýzu uživatelských zkušeností při interakci s digitálními službami nebo aplikacemi. Tím poskytuje přehled o výkonu sítě z perspektivy uživatele a pomáhá organizacím stanovit priority a řešit problémy, které mohou mít přímý dopad na spokojenost uživatelů. (Cisco, 2023)



Obrázek 10 - Budoucnost správy sítě, zdroj: (DeCarlo, 2020)

4 Vlastní práce

V této fázi práce vyplývající z analýzy teoretických základů, bude primárním úkolem selektovat optimální monitorovací systém pro síťovou infrastrukturu společnosti Aerosol-Service a.s. Po provedeném výběru bude provedena jeho implementace a konfigurace.

4.1 Výběr vhodného monitorovacího softwaru pro Aerosol-Service a.s.

4.1.1 Představení zkoumané společnosti

Společnost Aerosol-Service a.s. je předním výrobcem a dodavatelem polyuretanových pěn, stavební chemie a technických aerosolů na českém i zahraničním trhu. Firma byla založena v roce 2001 a má sídlo v Pleteném Újezdu v okrese Kladno.

Firma disponuje moderním výrobním závodem s kapacitou 40 milionů kusů ročně, kde využívá nejnovější technologie a zařízení. Firma zaměstnává přes 100 kvalifikovaných pracovníků, kteří se starají o vývoj, výrobu, kontrolu, distribuci a servis produktů. Firma nabízí široký sortiment produktů, které jsou určeny pro různé aplikace v stavebnictví, průmyslu, domácnosti, zahradě, autoprůmyslu a dalších oblastech.

Areál firmy se skládá z několika budov, které jsou rozděleny podle jednotlivých oddělení. V každé budově se nachází několik přípojných bodů, které připojují jednotlivé počítače, tiskárny, skenery, kamerové systémy, čtečky čárových kódů, PLC (programovatelné logické automaty) a další zařízení.

V tabulce níže je popsána struktura a rozložení jednotlivých budov v areálu společnosti, včetně informací o jejich využití a počtu desktopových zařízení v každé z nich.

Budova	Počet zařízení	Popis
Budova A	8	V této budově se nachází ředitelství, účetnictví, marketing, recepce. Zde se také nachází serverovna.
Budova B	12	V této budově se nachází obchodní oddělení.
Budova C	3	V této budově se nachází výroba tmelů, přípravna pěn a archiv
Budova D	1	V této budově se nachází dílna a jídelna
Budova F	1	V této budově se nachází kompletace obalů a výroba.
Budova H	17	V této budově se nachází skladové pozice. Zde se nachází hlavní serverovna.
Budova I	1	V této budově se nachází sklad kapalin
Budova J	4	V této budově se nachází skladové pozice.
Budova K	1	V této budově se nachází skladové pozice a výroba.

Budova L	0	V této budově se nachází skladová hala. Zde je umístěna serverovna.
Budova V	3	V této budově se nachází zázemí techniků.
Budova W	16	V této budově se nachází vývojová laboratoř.

Tabulka 5 - Areál společnosti, zdroj: (Autor)

V rámci korporátní sítě společnosti Aerosol-Service a.s. je integrováno celkem 67 počítačů, které slouží k administrativním pracím a dalším operacím. V každém oddělení je k dispozici samostatná tiskárna, což zahrnuje celkem 22 zařízení v provozu. Pro pokrytí celé sítě se využívá 28 wifi access pointů Ubiquiti UniFi UAP. Wi-fi síť je spravována Unifi Controllerem, který řídí jednotlivé access pointy a segmentuje wi-fi síť na veřejnou a privátní, přičemž uživatelé ve veřejné síti nemají přístup k vnitřní infrastruktuře společnosti Aerosol-Service a.s. Aktuálně však Unifi Controller nesprávně odděluje veřejnou síť od privátní. Počítače s přístupem do vnitřní sítě společnosti skrze wi-fi jsou chráněny doménovou kontrolou, kde bez správného jména a hesla uživatele není přístup na datová řídící zařízení.

V rámci infrastruktury jsou nasazeny servery, které podporují klíčové systémy, zahrnující informačního systému Qi, účetního systému Duel, řízení projektů Redmine, znalostní databáze Dokuwiki, docházkového systému PowerKey, nástroje pro management chemických látek Casec, doménového systému a sdíleného firemního úložiště. Virtualizace softwarového vybavení probíhá pomocí technologie VMWare. Pro přenos a správu dat jsou využívány jak managovatelné, tak nemanagovatelné switche, včetně dvou centrálních routerů. Přístup k firemním zdrojům je realizován prostřednictvím lokální sítě, kterou spravují systémoví administrátoři.

Areál firmy je rozdělen do dvou samostatně řízených síťových struktur, které lze propojit v případě výpadku jedné z nich. V každé budově se nachází jedno, nebo několik přípojných míst, kde jsou umístěny switche pro každý síťový okruh zvlášť. V jednotlivých kancelářích jsou instalovány dodatečné switche pro připojení menších periférií, jako jsou tiskárny a další zařízení.

Jeden ze síťových okruhů slouží pro technickou podporu a interní systémy, zatímco druhý je využíván pro technická zařízení pro správu a kamerový dohled a docházkový systém. Tato struktura umožňuje efektivní správu a redundanci v případě výpadku jedné, či druhé sítě.

4.1.2 Topologie sítě

V infrastruktuře společnosti Aerosol-Service a.s. je implementováno páteřní propojení switchů, kde se využívá šest centrálně propojených páteřních switchů. Tyto switche jsou navzájem propojeny optickým vláknem a nacházejí se v budovách označených písmeny A, B, K, L, W a H. Celkový design propojení je realizován kombinací liniového uspořádání s topologií hvězdy. Tato konfigurace umožňuje efektivní distribuci síťového provozu a zajišťuje robustní propojení mezi jednotlivými budovami v rámci korporátní sítě.

4.1.3 Segmentace sítě

V implementaci síťové segmentace ve společnosti Aerosol-Service a.s. se využívá specifikace na bázi lokálních IP rozsahů s rozsahem mezi 10.1.4. a 10.1.7. Tento přístup zahrnuje použití podsítí s maskou 255.255.252.0, což umožňuje efektivní rozdělení síťového prostoru do diskrétních segmentů. Každý segment v rámci tohoto rozsahu má svou unikátní identifikaci a zároveň umožňuje izolaci a správu dat na úrovni podsítí.

4.1.4 Informace o serverech

V rámci vnitřní sítě jsou připojeny servery s různými účely a specifikacemi. Tyto servery plní specifické role v infrastruktuře společnosti a mají jasně stanovené parametry v souladu s jejich úkoly.

- Dell T140, hostující systém pro účetnictví, systém chemických látek, interní systém výroby – dvě virtualizované instance
- Dell T20, hostující informační systém APP, informační systém SQL – dvě virtualizované instance.
- HP ML30, hostující řízení projektů a znalostní databázi – dvě virtualizované instance
- Dell T20, hostující SMTP – jedna virtualizovaná instance
- HP ML30, hostující Windows Domain Server – nevirtualizovaná instance
- Dell T30, hostující docházkový systém – nevirtualizovaná instance

4.1.5 Aktuální stav monitorování sítě

V současné době společnost Aerosol-Service a.s. nevyužívá žádný specializovaný software či platformu pro monitorování vytížení a celkové sledování své síťové infrastruktury. Implementace síťového monitoringu se stane klíčovou iniciativou v rámci korporátní infrastruktury společnosti, představující zásadní komponentu jejího integrovaného informačního systému. S ohledem na exponenciální nárůst datového toku a rozsah připojených koncových bodů se společnost rozhodla zavést sofistikované monitorovací mechanismy s cílem efektivní správy a optimalizace svého síťového prostředí.

Hlavním úkolem síťového monitoringu je zajistit, aby celková síťová infrastruktura byla nejen dostupná a spolehlivá, ale také bezpečná, výkonná a efektivní. Tato iniciativa bude umožňovat komplexní sledování a řízení propojení mezi jednotlivými odděleními, procesy, zařízeními a klienty společnosti Aerosol-Service a.s., s důrazem na optimalizaci a zajištění maximálního výkonu. Implementace monitoringu vytížení a sledování síťových aktivit bude klíčovým krokem směrem k efektivnímu řízení a bezpečnosti sítě a zároveň posílení konkurenceschopnosti společnosti na trhu.

4.1.6 Analýza požadavků společnosti na monitorovací software

Analýza požadavků společnosti Aerosol-Service a.s. na monitorovací software je klíčovým krokem při výběru vhodného systému pro sledování a správu jejich sítě. Několik klíčových aspektů bylo identifikováno tak, aby bylo možné adekvátně vyhovět potřebám společnosti.

- Je žádoucí, aby systém byl schopen efektivně přizpůsobovat se a podporovat rozmanité typy zařízení, jako jsou servery, pracovní stanice, směrovače a přepínače.
- Poskytování vysoké úrovně bezpečnosti, včetně šifrování dat, pokročilých možností autentizace a ochrany před neoprávněným přístupem.
- Systém by měl poskytovat možnost automatické detekce a upozornění na výpadky a měl by být schopen rychle reagovat na kritické události.
- Podpora specifických protokolů, rozšiřitelnost a uživatelskou přívětivost. Specifické protokoly jsou SNMP, DNS, HTTP / HTTPS, SSH, ICMP, SYSLOG
- Sledování využití šířky pásma pro identifikaci případných úzkých hrdel v síti, především tedy páteřních switchů.

- Systém by měl být schopen zpracovávat a analyzovat data v reálném čase, aby umožnil rychlou reakci na události v síti.
- Monitorování a řízení připojených zařízení s důrazem na identifikaci nových připojení a správu přístupových práv.

Specifické potřeby firmy v oblasti monitorování sítě

Firma vykazuje konkrétní potřeby v oblasti monitorování sítě, přičemž klíčovým cílem je detailně rozkrýt zátěž na jednotlivých switchích a provést reorganizaci sítě s důrazem na zvýšení celkové datové propustnosti. Tato specifická požadavky zahrnují:

- **Detailní analýza vytížení jednotlivých switchů:**

Systém monitorování by měl poskytovat hloubkovou analýzu vytížení jednotlivých switchů. Identifikace přetížených bodů umožní efektivní plánování a distribuci zátěže pro optimalizaci výkonu.

- **Reorganizace sítě pro větší datovou propustnost:**

Získané informace z monitorování by měly být využity k přeorganizaci sítě tak, aby byla dosažena větší datová propustnost. To může zahrnovat přesun zařízení na méně zatížené segmenty nebo optimalizaci konkrétních přenosových cest.

4.1.7 Porovnání dostupných monitorovacích nástrojů s ohledem na funkce a náklady

V následující tabulce jsou uvedeny a srovnány systémy určené k monitorování firemních sítí. Tyto produkty byly pečlivě vybrány na základě detailní analýzy softwarů diskutovaných v teoretické části, a následně byly doplněny o software, který doporučil manažer technického oddělení ve společnosti Aerosol-Service a.s. Tabulka poskytuje podrobný přehled a srovnání požadavků podniku na monitorovací systémy.

Název softwaru	Škálovatelnost	Bezpečnost	Detekce a upozornění	Podpora protokolů	Sledování šířky pásma	Zpracování dat v reálném čase	Správa zařízení
PRTG Network Monitor	Ano	Ano	Ano	Ano	Ano	Ano	Ano
Obkio	Ano	Ano	Ano	Ano	Ano	Ano	Ne
ManageEngine OpManager	Ano	Ano	Ano	Ano	Ano	Ano	Ano
Auvik	Ano	Ano	Ano	Ano	Ano	Ano	Ano
Wireshark	Ne	Ne	Ne	Ano	Ano	Ano	Ne

NetWorx	Ne	Ne	Ne	Ne	Ano	Ano	Ne
SoftPerfect Network Scanner	Ne	Ne	Ne	Ano	Ne	Ne	Ano
SolarWinds	Ano	Ano	Ano	Ano	Ano	Ano	Ano
Nagios	Ano	Ano	Ano	Ano	Ano	Ano	Ano
Zabbix	Ano	Ano	Ano	Ano	Ano	Ano	Ano
Cacti	Ano	Ne	Ano	Ano	Ano	Ne	Ne

Tabulka 6 - Komparace monitorovacích softwarů, zdroj: (Vlastni zpracování dle informaci na webových stránkách jednotlivých poskytovatelů)

Legenda k uvedeným sloupcům:

- **Škálovatelnost**: Schopnost softwaru růst a přizpůsobovat se zvýšenému počtu uživatelů, nebo zařízení v síti.
- **Bezpečnost:** Míra, do jaké software chrání síť a data před neautorizovaným přístupem a útoky.
- **Detekce a upozornění:** Schopnost softwaru identifikovat a upozornit na problémy v síti, jako jsou výpadky, přetížení nebo bezpečnostní incidenty.
- **Podpora protokolů**: Podpora všech uvedených protokolů včetně SNMP, DNS, HTTP / HTTPS, SSH, ICMP, SYSLOG
- **Sledování šířky pásma**: Schopnost softwaru sledovat a analyzovat využití šířky pásma v síti.
- **Zpracování dat v reálném čase**: Schopnost softwaru shromažďovat, analyzovat a prezentovat data v reálném čase.
- **Správa zařízení**: Schopnost softwaru sledovat a spravovat jednotlivá zařízení v síti, jako jsou servery, switche, routery a další.

V tabulce níže je provedeno porovnání cenové hladiny za jednotlivá řešení, která by měla pokrýt sledování 103 zařízení, konkrétně 67 stanic, 6 switchů, 2 routerů a 28 Access-pointů. Pro získání přehledu o nákladech jsou uvedeny jak měsíční, tak roční náklady.

Rozpis na měsíční a roční náklady:

Měsíční náklady:

Uvedené náklady jsou odvozeny z cenového rozpisu poskytovatelů, které jsou rozděleny na měsíční částky, vycházející z jejich ročních sazeb za služby.

Roční náklady:

Ceny jsou odvozeny ze sazeb jednotlivých poskytovatelů za jejich služby, které zahrnují licenci na používání po dobu jednoho roku.

Tato data jsou klíčová pro plánování rozpočtu a zajištění dlouhodobé udržitelnosti investice do monitorovacích řešení. Přesné vypočítání měsíčních a ročních nákladů je důležité pro správné finanční plánování a rozhodování při výběru vhodného softwaru pro sledování a správu sítě.

Název softwaru	Cena (za měsíc)	Cena (za rok)
PRTG Network Monitor	$137.41	$1649
Obkio	$2050	$24600
ManageEngine OpManager	$149.58	$1795
Auvik	$150	$1800
SolarWinds: network performance monitor	$237,08	$2845
Nagios	$207.91	$2495
Zabbix	Zdarma	Zdarma
Wireshark	Zdarma	Zdarma
NetWorx	$500	$6000
SoftPerfect Network Scanner	Zdarma	Zdarma
Cacti	Zdarma	Zdarma

Tabulka 7 - Cenová komparace monitorovacích softwarů, zdroj: (Vlastni zpracování dle informaci na webových stránkách jednotlivých poskytovatelů)

Po analýze kontingenční tabulky je patrné, že několik softwarových nástrojů odpovídá všem stanoveným požadavkům. Tyto programy disponují rozsáhlými funkcionalitami a schopnostmi. Další postup práce bude zaměřen na tyto konkrétní nástroje, které jsou uvedeny níže:

Placené varianty:

- PRTG Network Monitor
- ManageEngine OpManager
- Auvik

- SolarWinds: network performance monitor

Open-Source varianty:

- Nagios
- Zabbix

4.1.8 Výběr optimálního monitorovacího softwaru na základě kritérií a potřeb společnosti.

V rámci procesu výběru adekvátního řešení bylo uskutečněno osobní představení jednotlivých monitorovacích programů přítomným zaměstnancům společnosti.

PRTG Network Monitor

je komplexní řešení pro monitorování sítě, které podporuje různé typy zařízení a protokolů. Nabízí automatickou detekci sítě, upozornění na výpadky, šifrování dat, monitorování šířky pásma, analýzu dat v reálném čase a uživatelsky přívětivé rozhraní. Je vhodný pro malé a střední podniky. Má bezplatnou verzi pro až 100 senzorů a placené plány od 1 649 EUR ročně za 500 senzorů.

ManageEngine OpManager

je robustní řešení pro monitorování sítě, které podporuje různé typy zařízení a protokolů. Nabízí automatickou detekci sítě, upozornění na výpadky, šifrování dat, monitorování šířky pásma, analýzu dat v reálném čase a uživatelsky přívětivé rozhraní. Je vhodný pro střední a velké podniky, ale může být složitý pro malé podniky. Má bezplatnou verzi pro až 10 zařízení a placené plány od 245 EUR ročně za 25 zařízení.

Auvik

je cloudová služba pro monitorování sítě, která se zaměřuje na správu a optimalizaci infrastruktury. Umožňuje monitorovat různé typy zařízení a protokolů, včetně směrovačů a přepínačů. Poskytuje automatickou detekci sítě, upozornění na výpadky, šifrování dat, monitorování šířky pásma, analýzu dat v reálném čase a uživatelsky přívětivé rozhraní. Je vhodný pro střední a velké podniky, ale může být drahý pro malé podniky. Má bezplatnou zkušební verzi a placené plány od 150 EUR měsíčně za 50 zařízení.

SolarWinds Network Performance Monitor

je komplexní řešení pro monitorování výkonu sítě, které podporuje různé typy zařízení a protokolů. Nabízí automatickou detekci sítě, upozornění na výpadky, šifrování dat, monitorování šířky pásma, analýzu dat v reálném čase a uživatelsky přívětivé rozhraní.

Je vhodný pro střední a velké podniky, ale může být nákladný pro malé podniky. Má bezplatnou zkušební verzi a placené plány od 2 845 EUR ročně za licenci.

Nagios

je open-source software pro monitorování sítě, který podporuje různé typy zařízení a protokolů. Nabízí automatickou detekci sítě, upozornění na výpadky, šifrování dat, monitorování šířky pásma, analýzu dat v reálném čase a uživatelsky přívětivé rozhraní. Je vhodný pro střední a velké podniky, ale může být náročný na konfiguraci a správu. Má bezplatnou verzi pro neomezený počet zařízení a placené plány od 2 495 EUR ročně za 100 zařízení.

Zabbix

je open-source software pro monitorování sítě, který podporuje různé typy zařízení a protokolů. Nabízí automatickou detekci sítě, upozornění na výpadky, šifrování dat, monitorování šířky pásma, analýzu dat v reálném čase a uživatelsky přívětivé rozhraní. Je vhodný pro střední a velké podniky, ale může být složitý na instalaci a integraci. Má bezplatnou verzi pro neomezený počet zařízení.

Finální výběr:

Do finálního výběru se dostaly pouze placené verze programů, a to PRTG Network monitor a ManageEngine OpManager, kde rozhodovaly následující faktory:

Cena:

PRTG Network Monitor je licencován podle počtu senzorů, které měří různé aspekty sítě a zařízení, zatímco ManageEngine OpManager je licencován podle počtu zařízení, které monitoruje. Pro podnik, kde je 67 desktopových stanic, 6 switchů, dva centrální routery a 28 AP od unifi, by bylo zapotřebí asi 500 senzorů pro PRTG Network Monitor a 103 zařízení pro ManageEngine OpManager. Podle jejich oficiálních ceníků by to znamenalo, že PRTG Network Monitor by nás stál 1 649 EUR ročně, zatímco ManageEngine OpManager by nás stál 1795 EUR ročně. PRTG Network Monitor by byl levnější.

Instalace a konfigurace:

PRTG Network Monitor je on-premise řešení, které běží na Windows platformě, zatímco ManageEngine OpManager nabízí jak on-premise, tak cloud-hosted verze, které běží na Windows nebo Linuxu. PRTG Network Monitor používá bezagentový přístup k monitorování, což znamená, že není třeba instalovat žádný software na monitorovaných zařízeních, zatímco ManageEngine OpManager vyžaduje instalaci agentů na některých

zařízeních. V tomto srovnání by bylo použití PRTG Network Monitoru jednodušší a efektivnější.

Funkce a rozšiřitelnost:

Obě aplikace nabízejí širokou škálu funkcí, jako jsou upozornění, přehledné panely, monitorování virtualizace, podpora různých protokolů a technologií a další. Nicméně, PRTG Network Monitor má některé výhody, jako je podpora monitorování cloudu, jako jsou služby Amazon Web Services (AWS) a Microsoft Azure, možnost vytvářet vlastní senzory pomocí skriptů, nebo aplikací třetích stran, podrobné zprávy o výkonu sítě a zařízení, které lze exportovat do různých formátů, integrace se službami třetích stran, jako jsou Slack, PagerDuty, Zapier a další, a podpora 10 jazyků, včetně češtiny.

Závěrečné stanovisko:

V rámci výběrového řízení rozhodl CIO firmy pro variantu PRTG Network Monitor, která splňovala veškeré stanovené podmínky uvedené v kapitole analýzy požadavků společnosti.

4.1.9 Příprava serveru

Pro výběr fyzického serveru bylo nutné zvážit hardwarové požadavky, které jsou specifikované na webových stránkách výrobce. Ty se odvíjí od počtu senzorů, které budou sledovány v rámci jednotlivých sledovaných zařízení. Pro účely implementace postačila první kategorie, ovšem při výběru byl brán zřetel na možnost budoucího růstu a potřebu server upgradovat.

Sensors per PRTG Core server	Cpu cores	Ram	Disk space	Concurrently active administrator sessions
Up to 500	4	4 GB	100 GB	<30
Up to 1 000	6	6 GB	500 GB	<30
Up to 2 500	8	8 GB	750 GB	<60
Up to 5 000	8	12 GB	1 000 GB	<60
Up to 10 000	10-12	16 GB	1 500 GB	<80

Tabulka 8 - Systémové požadavky, zdroj (Paessler, 2023)

Na základě uvedených technických specifikací byl vybrán věžový server od společnosti HPE, konkrétně model ProLiant ML30 Gen10. Tento server již byl nasazen v korporátním prostředí, kde běžel s virtualizovanou instancí na platformě Esxi verze 6.7. Co se týče hardwarového vybavení, server disponuje následujícími komponenty:

- procesor typu Intel(R) Xeon(R) E-2124 s frekvencí 3,30 GHz,
- operační paměť o kapacitě 32 GB,
- diskové řešení 2TB SSD v konfiguraci RAID 1 s dalšími 2TB SSD.

PRTG Network monitor lze instalovat dle parametrů na stránkách výrobce na operační systémy od společnosti Microsoft, konkrétněji:

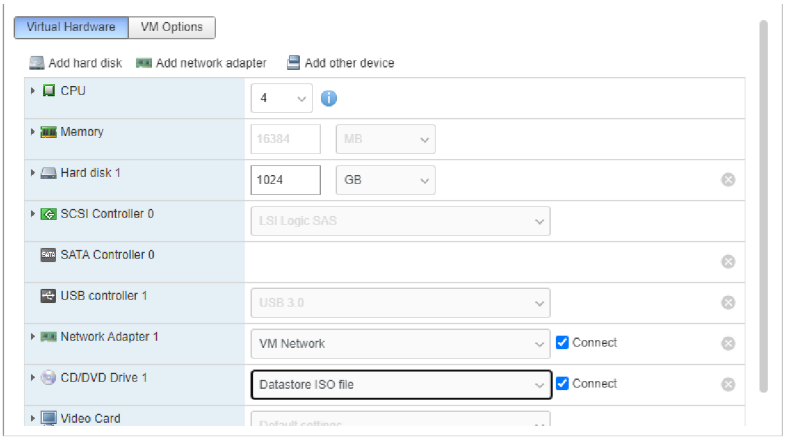
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows 10 a 11.

Na server byla v prostředí ESXI přidána další instance, která běží v prostředí Windows 10, zkrácený proces instalace virtuálního stroje je popsán níže.

Při instalaci nového virtuálního stroje ve VMWare byl spuštěn proces vytvoření nové virtuální instance. Na počátku této konfigurace bylo prezentováno několik možností, z nichž byla vybrána varianta vytvoření nového virtuálního stroje.

Následovalo určení názvu virtuální instance a výběr operačního systému. Specificky bylo rozhodnuto pro rodinu operačních systémů Microsoft s verzí Microsoft Windows 10 ve 64bitové podobě.

Následně byla provedena konfigurace různých parametrů, jako jsou počet procesorů, operační paměť, umístění na disku a instalační zdroj. Pro virtuální instanci bylo alokováno 16 GB operační paměti a plná kapacita procesoru. V oblasti operační paměti bylo rovněž aktivně využito možnosti dynamické alokace dalších prostředků v případě, že by byl detekován nedostatek zdrojů.



Obrázek 11 - Konfigurace stroje, zdroj: (Autor)

Po úspěšném provedení všech kroků této posloupnosti byla vytvořena nová virtuální instance, na které bylo nutné provést čistou instalaci operačního systému Windows 10. Tato instalace zahrnuje inicializaci a konfiguraci operačního systému od začátku, zajišťující tak optimální funkčnost vytvořené instance.

4.2 Implementace monitorovacího softwaru

Na připravenou instanci s čistou instalací operačního systému Windows proběhla instalace .NET frameworku 4.8. V následující podkapitole bude popsán proces implementace a konfigurace.

4.2.1 Postup instalace zvoleného monitorovacího softwaru do infrastruktury sítě Aerosol-Service a.s

PRTG Network Monitor byl implementován pomocí instalačního souboru ve formátu .exe, který je definován jako jediný oficiálně podporovaný a doporučený distribuční mechanismus. Proces instalace je navržen tak, aby byl uživatelsky přívětivý a srozumitelný.

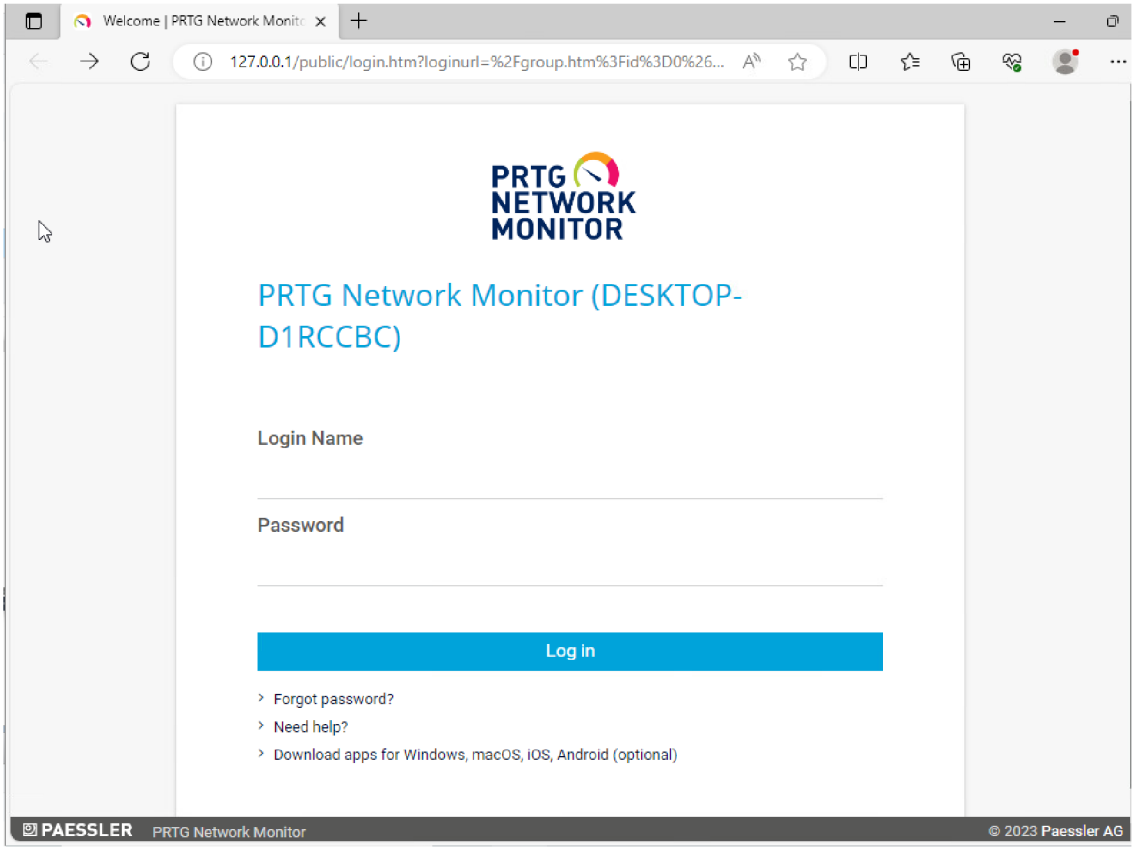
Během počáteční fáze instalace je uživateli nabídnuta možnost volby preferovaného jazyka, který bude následně implementován v celém instalačním procesu a v uživatelském rozhraní softwaru.

V následujícím kroku instalace je prezentována možnost volby mezi dvěma různými variantami instalátoru. Tato volitelnost umožňuje specifikaci preferovaného způsobu instalace a přizpůsobení procesu instalace individuálním požadavkům uživatele. A to možnost expresní a vlastní instalace.

V kontextu nasazení byla zvolena "Vlastní" konfigurace instalace, která nabízí větší flexibilitu a možnost přizpůsobení konkrétním potřebám, například zvolení cesty instalace a ukládání dat a zapnutí automatické detekci zařízení v síti.

Úspěšný proces instalace si lze ověřit, pokud instalátor po dokončení instalace uživatele přesměruje na webové rozhraní monitoringu, které se nachází na adrese http://ip_serveru:80.

V prvotním nastavení je využíván protokol http, kdy je nezbytné po přihlášení přepnout na využívání šifrované komunikace https, čímž se změní i adresa webového rozhraní na https://ip_serveru/443.

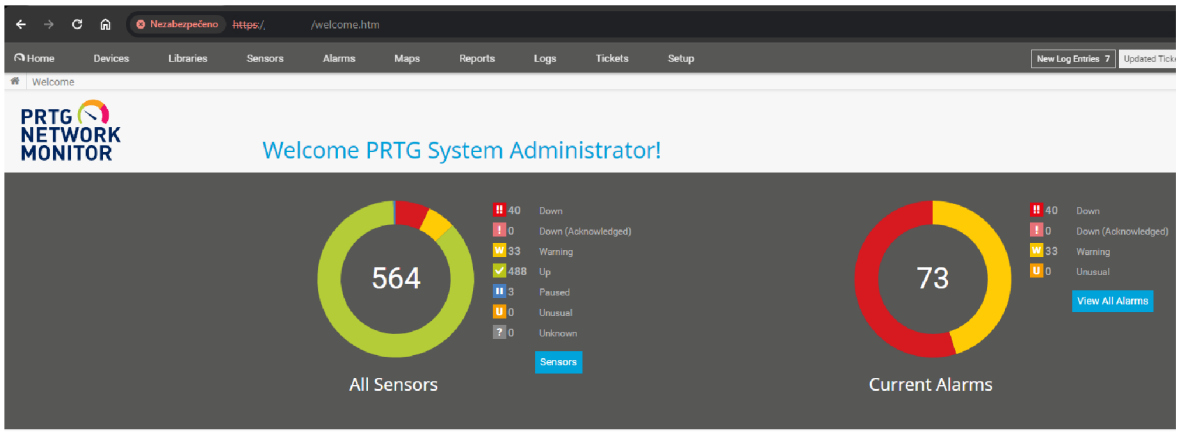


Obrázek 12 - Webové rozhraní, zdroj: (Autor)

Po úspěšném ověření uživatelských přihlašovacích údajů se uživateli zobrazí hlavní řídicí panel aplikace PRTG. Tento panel poskytuje ucelený přehled o aktuálním stavu monitorování. V jeho středu je umístěna informace o celkovém počtu aktivních senzorů, což je klíčový ukazatel pro sledování dostupnosti a výkonu sledovaných prvků v infrastruktuře.

Kromě toho je v hlavním panelu také zobrazen seznam chyb a varování, které slouží jako upozornění na potenciální problémy nebo anomálie v monitorovaném prostředí.

V horní části řídicího panelu je umístěna navigační lišta, která obsahuje odkazy na různé sekce a funkce, které PRTG nabízí. Tato struktura usnadňuje uživatelům navigaci a rychlý přístup k specifickým informacím, konfiguraci senzorů, alarmům, historii dat a dalším klíčovým funkcím aplikace.



Obrázek 13 - Úvodní stránka PRTG, zdroj: (Autor)

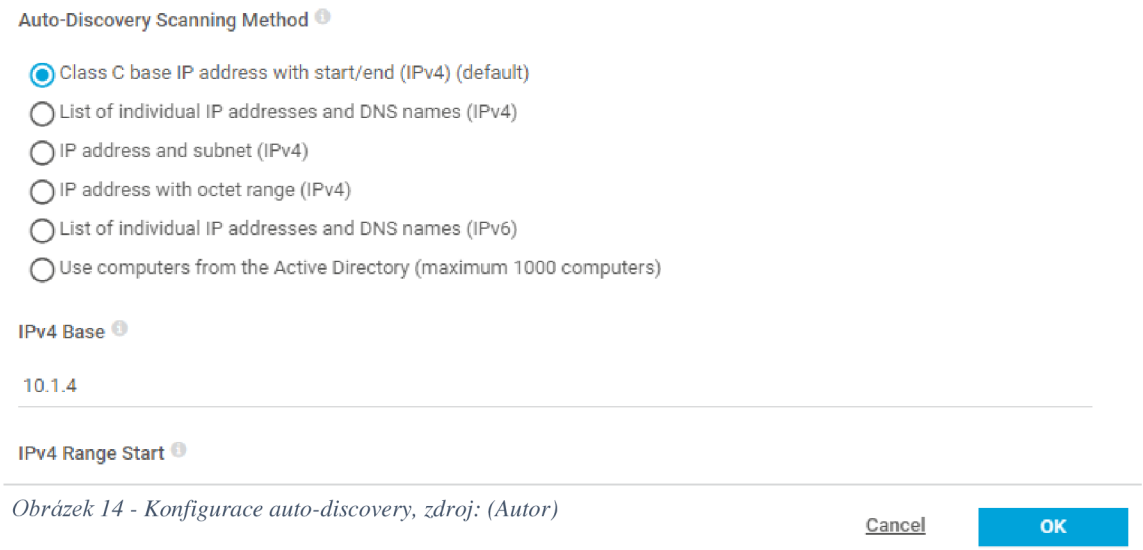
4.2.2 Konfigurace monitorování

Základní konfigurace probíhá po inicializaci správcovského účtu, kdy dochází k přesnému nastavení nového přihlašovacího hesla a doplnění nadřazeného názvu sítě. Tato konfigurace slouží jako výchozí bod, ze kterého jsou následně přidávána individuální zařízení a skupiny do spravované sítě. Taktéž zahrnuje záznam přihlašovacích údajů pro operační systémy, jako jsou Windows a Linux, a také specifické informace pro SNMP, databázová a virtuální zařízení.

Pro sledování zařízení v síti je nutné aktivovat SNMP protokol na těchto zařízeních. Tento postup zahrnuje přihlášení do konkrétního prvku pomocí jeho IP adresy a následná aktivace a konfigurace.

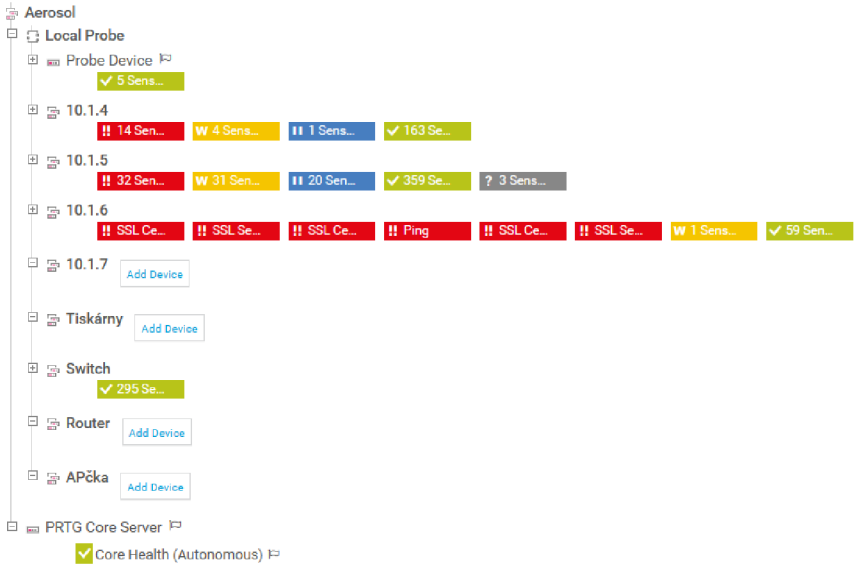
Další kroky zahrnují identifikaci zařízení v jednotlivých rozsazích. Platforma PRTG poskytuje dvě metody přidání nových prvků: ruční přidání a automatické skeny. Automatické skeny disponují rozšířenými funkcemi a periodicitou. V záložce „Devices“ se v pravé části obrazovky nachází modré okno s bílým znakem plusu, které po rozkliknutí nabízí několik možností, jako je přidání vzdálené sondy, vytvoření skupiny bez funkce skenování, vytvoření skupiny s funkcí skenování, přidání samostatného zařízení a přidání senzoru.

Pro potřeby implementace byly vytvořeny skupiny s funkcí skenování v rozsahu IP adres od 10.1.4 do 10.1.7, přičemž byla nastavena funkce „Auto-Discovery“ na týdenní bázi. Auto-Discovery poskytuje šest možností vyhledávání v síti, jak je znázorněno na příslušném obrázku.



Obrázek 14 - Konfigurace auto-discovery, zdroj: (Autor)

V každé skupině byla zvolena první varianta, kde po specifikování počátku a konce IP adresy v rámci stejné třídy dochází k provádění skenování aktivních zařízení. Mimo tyto rozsahové skupiny byly vytvořeny další skupiny, jako jsou „Tiskárny“, „Switch“, „Router“ a „Apčka“, do nichž byla systematicky začleněna nalezená zařízení odpovídající jejich názvům. Finální hierarchii lze vizualizovat na příslušném obrázku níže.



Obrázek 15 - Finální hierarchie, zdroj: (Autor)

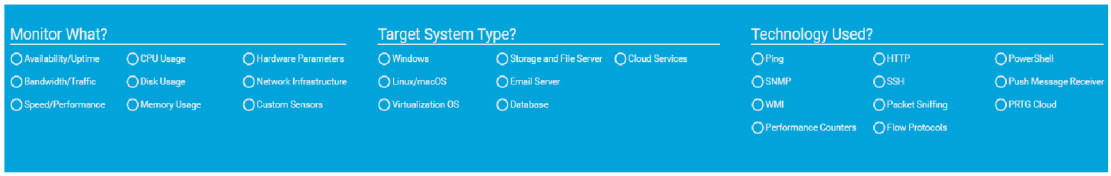
Po úspěšném vytvoření skupin byla provedena kompletní identifikace všech dostupných zařízení a jejich systematické seskupení podle předem stanovených parametrů.

Software následně automaticky přiřadil odpovídající senzory, které byly relevantní pro sledování uživatelem.

4.2.3 Nastavení triggerů a senzorů

V některých případech byly zjištěny nadbytečné senzory u některých prvků, což mohlo zbytečně omezené licenční limity. Z tohoto důvodu byla provedena individuální úprava konfigurace v souladu s firemní politikou s cílem optimalizovat využití licencí a zamezit neefektivnímu využívání senzorů.

Přidání nového senzoru je možné prostřednictvím interakce se sledovaným zařízením, a to v sekci „Overview“. Po rozkliknutí tohoto segmentu má uživatel možnost vybrat „Add Sensor“, kde se mu nabídne rozsáhlý výběr potenciálních metrik pro sledování. V horní části obrazovky následně software žádá uživatele o konkrétní informace, které umožňují systematické ohraničení a zúžení výběru vhodných senzorů. Tímto postupem se dosahuje rychlejšího a efektivnějšího nastavení senzorů, jak ukazuje přiložený obrázek níže.



Obrázek 16 - Nastavení senzoru, zdroj: (Autor)

PRTG Network Monitor umožňuje konfiguraci pěti typů trigger oznámení, a to konkrétně:

1. Trigger stavu
2. Trigger rychlosti
3. Trigger velikosti
4. Threshold trigger
5. Trigger změny

Pro každý typ triggeru oznámení jsou k dispozici rozmanité možnosti nastavení. U triggeru pro sledování rychlosti je například možné specifikovat následující parametry:

- **Zvolení prahové rychlosti:** Uživatel má možnost definovat specifickou rychlost, při které dojde k vyvolání triggeru.

- **Časový rámec:** Umožňuje stanovit časové období, v němž má trigger sledovat rychlost.
- **Volitelné opakování:** Možnost nastavit opakování triggeru v případě, že specifikovaná rychlost přetrvává po delší dobu.
- **Akce při dosažení prahu:** Uživatel může definovat konkrétní akce, které mají být vykonány, když je dosaženo stanovené rychlostní hranice.

Tímto způsobem poskytuje PRTG Network Monitor uživatelům flexibilitu a detailní kontrolu nad konfigurací trigger oznámení, což výrazně přispívá k efektivnímu monitorování sítě.

Obrázek 17 - Speed trigger, zdroj: (Autor)

V souladu s prvotním zadáním a specifikacemi od firmy Aerosol-Service a.s. byla dočasně konfigurována upozornění pro všechny aktivní síťové prvky, konkrétně pro všechny switche, routery a přístupové body.

4.2.4 Nastavení upozornění

V rámci monitorovacího systému hraje klíčovou roli mechanismus upozornění, neboť tato upozornění slouží k informování správce a dalších relevantních osob o nežádoucích událostech v sledované infrastruktuře. Každé upozornění je propojeno s nastavením triggerů, kde uživatel definuje specifika, jakým způsobem má být upozornění odesláno, zda má být spuštěn skript nebo jakékoliv další úpravy v konfiguraci sledovaného zařízení. Standardním postupem výchozí konfigurace PRTG je odesílání upozornění prostřednictvím e-mailu.

4.2.5 Mapa topologie sítě

Síťová mapa reprezentuje strukturu uzlů v síti, která odpovídá reálné síti a obsahuje identickou sadu prvků. Existují dva typy síťových map – veřejné a soukromé. V rámci aktuální implementace byla vytvořena veřejná mapa.

Pro manipulaci s grafickým zobrazením topologie sítě slouží záložka „Maps“. Je důležité, aby po vytvoření mapy byly síťové prvky umístěny správně. Podle konkrétního nastavení mohou detaily mapy proměnlivě zahrnovat uzly podnikové sítě, podsítě nebo

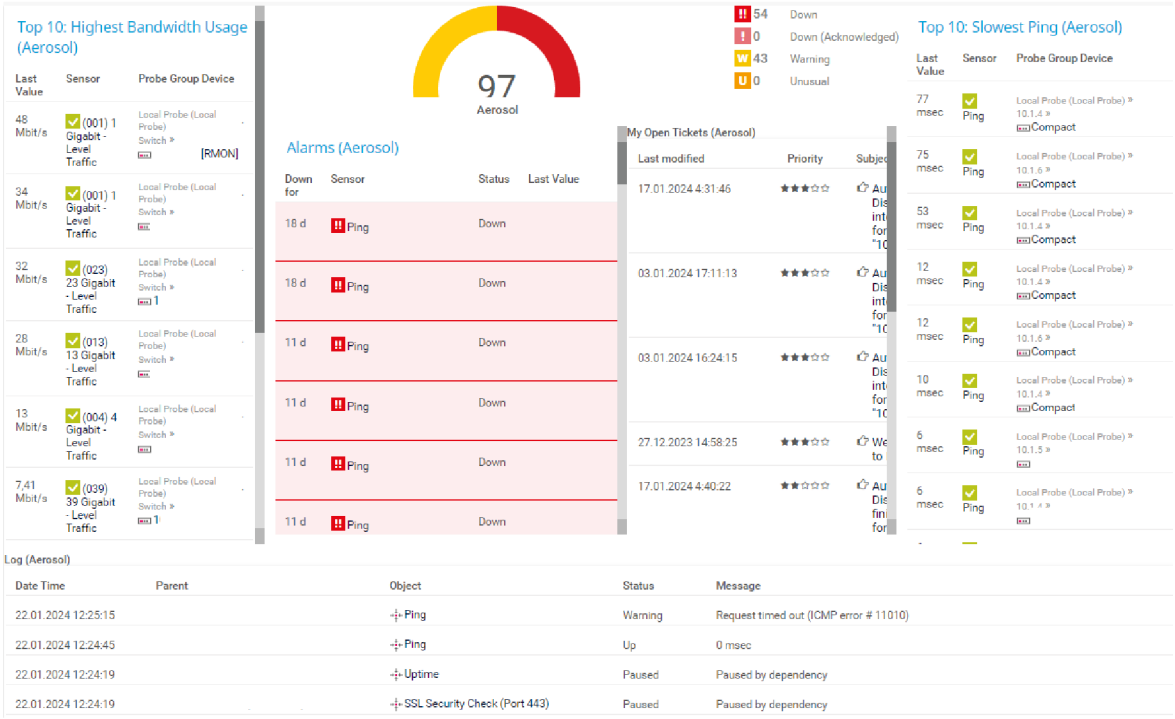
uživatelské počítače. V současném scénáři je mapa konfigurována tak, aby zobrazovala hlavní uzly podnikové sítě, pro které bylo monitorování specificky nakonfigurováno.

Vzhledem k nemožnosti deaktivace IP adres jednotlivých síťových prvků v grafickém zobrazení a s ohledem na nezbytnost uchování citlivých informací o těchto IP adresách ve firmě Aerosol-Service a.s., není v rámci této práce možné prezentovat úplnou topologii sítě.

4.2.6 Řídící panel

V rámci PRTG není pouze dostupná síťová topologie, ale také možnost vytvoření přehledového panelu, který poskytuje dynamický a personalizovatelný přehled v reálném čase. Byl vytvořen specifický panel obsahující klíčové informace, jako jsou zařízení s největším datovým tokem, záznamy logů, seznam aktuálních alarmů a zařízení s nejdelším pingem. Tato konfigurovatelná a živá nástěnka umožňuje uživatelům rychlý a efektivní přístup ke klíčovým informacím o sledované síťové infrastruktuře.

Uživatel má možnost vytvářet libovolný počet těchto přehledových panelů a jeden z nich může nastavit jako výchozí při přihlášení do monitorovacího systému.



Obrázek 18 - Dashboard, zdroj: (Autor)

4.2.7 Reportovací panel

Reporty v PRTG Network Monitor zobrazují výsledky sledování na základě dat ze senzorů, která byla shromážděna během určitého časového období. Jednou z klíčových vlastností reportovacího panelu v PRTG je jeho plná přizpůsobitelnost. Uživatelé mohou využívat širokou škálu předdefinovaných reportů, které pokrývají různé aspekty monitorování, jako jsou výkazy dostupnosti, výkonu a stavu senzorů.

Automatizace je další významnou charakteristikou reportovacího panelu. Možnost plánovat automatické generování reportů umožňuje pravidelný přehled bez potřeby manuální intervence. Exportní možnosti do formátů jako PDF, HTML a CSV usnadňují sdílení a archivaci informací.

Historie reportů, kterou reportovací panel uchovává, umožňuje uživatelům sledovat změny a vývoj sledovaných parametrů v čase. Tato funkce má klíčový význam pro analýzu dlouhodobých trendů a identifikaci potenciálních problémů.

Pro potřeby organizace zatím nebyly vytvářeny nové reportovací sestavy, protože stávající nabídka je pro dané potřeby více než dostačující. Nicméně, v budoucnu je plánováno větší zaměření na tuto sekci a případné rozšíření jejího použití.

Top 100 Most/Least Used Bandwidth Sensors (01.01.2024 0:00:00 - 31.01.2024 0:00:00 24 / 7)

Highest Averages (5 Minute Interval)

	Sensor	Average	Minimum	Maximum
1.	(041) 41 Gigabit - Level Traffic	40 Mbit/s	0,05 Mbit/s	1 000 Mbit/s
2.	(025) 25 Gigabit - Level Traffic	39 Mbit/s	0,06 Mbit/s	998 Mbit/s
3.	(001) 1 Gigabit - Level Traffic	38 Mbit/s	18 Mbit/s	120 Mbit/s
4.	(001) 1 Gigabit - Level Traffic	30 Mbit/s	8,94 Mbit/s	383 Mbit/s
5.	(023) 23 Gigabit - Level Traffic	30 Mbit/s	9,42 Mbit/s	382 Mbit/s
6.	(013) 13 Gigabit - Level Traffic	26 Mbit/s	0,91 Mbit/s	49 Mbit/s
7.	(039) 39 Gigabit - Level Traffic	7,19 Mbit/s	0,07 Mbit/s	66 Mbit/s
8.	(009) 9 Gigabit - Level Traffic	4,11 Mbit/s	0,07 Mbit/s	63 Mbit/s
9.	(015) 15 Gigabit - Level Traffic	3,17 Mbit/s	0,18 Mbit/s	272 Mbit/s
10.	(021) 21 Gigabit - Level Traffic	3,17 Mbit/s	0,18 Mbit/s	266 Mbit/s

Obrázek 19 - Report, zdroj: (Autor)

4.3 Zhodnocení účinnosti monitorování sítě v praxi

V závěrečné fázi diplomové práce proběhlo kritické hodnocení účinnosti implementace monitorování sítě v reálném podnikovém prostředí. Po důkladném zkoumání teoretických základů a konkrétní aplikaci monitorovacího softwaru byl kladen důraz na to, jak se tyto teoretické koncepty projevily v každodenní praxi a s jakými měřitelnými výsledky.

4.3.1 Sběr dat a informací o provozu sítě před a po implementaci monitorovacího softwaru

Popis vstupního stavu:

Identifikace klíčových metrik před implementací monitorovacího softwaru představovala výzvu v důsledku chybějícího systematického přístupu k monitorování síťových parametrů. Organizace se spoléhala na intuitivní a ad-hoc metody pro identifikaci metrik, které by měly být sledovány. Scházela jim struktura a jasně definovaný rámec pro určení, které klíčové metriky by měly být monitorovány a sledovány pro efektivní správu a optimalizaci síťové infrastruktury.

Celkově lze konstatovat, že před implementací monitorovacího softwaru byla identifikace klíčových metrik spíše neformální a intuitivní. Před tím, než byl monitorovací software nasazen, charakterizovala síť organizace stav nedostatečného sběru dat a nulové úrovně monitoringu. Sledování klíčových síťových metrik bylo neexistující, což vedlo k několika závažným problémům.

V této fázi byl výskyt výpadků a podobných poruch řešen reaktivně na základě spontánních oznámení koncových uživatelů, což vedlo k opožděným intervencím a neschopnosti rychle a efektivně řešit potenciální problémy. Absence celkového přehledu o toku dat v síti a stavu přetížení jednotlivých síťových uzlů dále komplikovala situaci.

Uživatelé se potýkali s řadou specifických problémů, včetně stížností na zpomalený provoz firemního disku a dlouhotrvající načítání dat v rámci interních informačních systémů a dalších firemních aplikací. Nedostatek transparentnosti a přehledu o síťovém provozu znesnadňoval odhalování a odstraňování kořenových příčin těchto problémů.

Sběr dat probíhal neorganizovaně a spíše reaktivně, což mělo za následek neschopnost poskytnout aktuální a relevantní informace o stavu sítě. Identifikace klíčových

metrik byla prováděna intuitivně a bez systematické analýzy, což znamenalo, že chyběly stanovené normy pro sledování klíčových aspektů síťového provozu.

V případě výpadku celé sítě neexistovala možnost rychlé analýzy, což mělo za následek obtížnou identifikaci příčiny a konkrétního místa poruchy. Tato situace představovala značný zásah do spolehlivosti a dostupnosti firemní infrastruktury, což mělo negativní dopad na celkovou produktivitu a efektivitu podnikových operací.

Stav po implementaci:

Po implementaci monitorovacího softwaru PRTG Network Monitor došlo k výraznému zlepšení správy a monitorování síťových metrik v organizaci. Nový nástroj poskytl strukturovaný přístup k sledování klíčových síťových parametrů, což vedlo k efektivnější správě infrastruktury a nastavení limitů a upozornění na případné anomálie nebo nadměrné zatížení, což umožňuje předcházet potenciálním problémům a optimalizovat výkon sítě.

Implementace PRTG Network Monitor umožnila centralizovaný sběr dat a monitorování síťového provozu. Organizace nyní disponuje přehledem o toku dat v síti, aktuálním stavu přetížení jednotlivých uzlů a identifikací případných výpadků. Tato nová transparentnost výrazně usnadnila řízení síťových operací a umožnila rychlejší reakci na výzvy prostředí.

4.3.2 Analyzování získaných dat a hodnocení účinnosti monitorovacího softwaru

Srovnání před a po

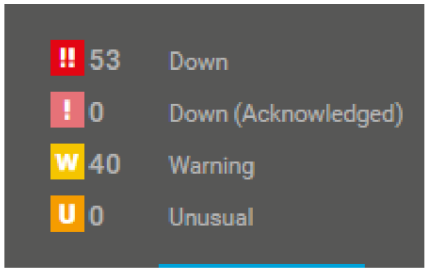
V předešlé podkapitole bylo konstatováno, že v původním stavu nedocházelo k monitorování stavu sítě ze strany IT oddělení. Po úspěšné implementaci PRTG Network Monitor došlo k identifikaci nových klíčových metrik, mezi něž patří sledování využití šířky pásma, latence a dostupnosti. Monitorovací systém poskytl důležitý nástroj pro analýzu provozu sítě a detekci případných anomálií. Výstupy monitorovacího systému odhalily celkem 53 závažných problémů a 40 varování, tyto anomálie se dále štěpí dle dopadu na výkon sledovaného zařízení, některá nemají velkou prioritu, jiná zase svou závažností ohrožují provoz zařízení, či firemní sítě.

Po korekci a optimalizaci nastavení softwaru se počet problémů snížil na 30. Těmito problémy byly především chybějící SSL certifikáty v tiskárnách a závažnější problémy spojené s nedostupností virtuálních instancí. Dále bylo odhaleno, že jeden ze switchů byl

přetížen, což vedlo ke snížení kvality uživatelského prostředí. Tato identifikace měla klíčový význam při odhalení příčiny zhoršeného chování informačního systému u uživatelů v budově A.

Získané informace z monitorování nyní slouží jako základ pro proaktivní a systematické řízení síťových operací ve firmě Aerosol-Service a.s.. Reportovací nástroj integrovaný v PRTG slouží jako podnět k pravidelným schůzkám IT oddělení, během kterých jsou plánovány a provedeny úpravy infrastruktury podle aktuálních potřeb a zjištěných nedostatků.

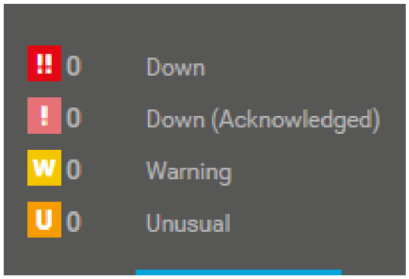
V rámci celkového rozvoje síťové infrastruktury došlo k výměně neřízených („hloupých“) switchů za takové s možností managementu, čímž se i navýšil počet celkových switchů ze 7 zařízení na celkový počet 12 zařízení. Kromě toho se implementovalo vytváření VLAN pro zlepšení toku sítě, což povede k efektivnější správě datového toku a celkové optimalizaci síťového prostředí v Aerosol-Service a.s.



Obrázek 20 - Anomálie před, zdroj:(Autor)

Lze konstatovat, že implementace přinesla pozoruhodné výsledky a výrazně přispěla k vylepšení síťového provozu ve firmě Aerosol-Service a.s. Zejména efektivitu identifikace problémů, která byla jedním z klíčových cílů nasazení tohoto monitorovacího řešení.

Monitorovací software prokázal svou schopnost systematicky sledovat klíčové metriky, což umožnilo identifikaci potenciálních problémových oblastí. Tato dynamická identifikace problémů představuje významný krok vpřed oproti předchozímu stavu, kde nebylo systematické sledování síťových parametrů.



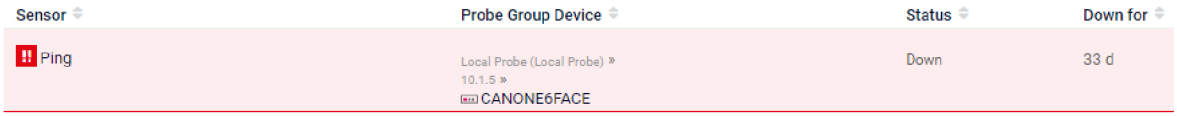
Obrázek 21 - Anomálie po, zdroj: (Autor)

Exemplární příklady výstupů:

V PRTG Network Monitoru existuje několik různých typů alarmů, které upozorňují na problémy ve sledované síti. Tyto výstupy jsou rozděleny do kategorií podle důležitosti. Například můžeme mít výstup označený jako "Down", což znamená, že zařízení nebo služba je nedostupná. Další kategorií je "Warning", která naznačuje, že něco není úplně v pořádku a mohlo by to vyžadovat pozornost. Existují také kategorie "Down acknowledged", která označuje problémy, které již byly identifikovány a uznány a "Unusual", což jsou situace, které jsou neobvyklé a mohou vyžadovat další zkoumání.

Každá kategorie má svou prioritu, která se odvíjí od toho, jak závažným způsobem daný problém ovlivňuje provoz sítě.

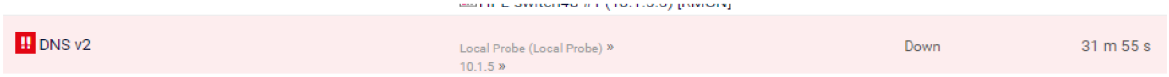
Jako ilustrativní příklad alarmu může posloužit varovná zpráva signalizující nedostupnost určitého zařízení v síti, které není dostupné z hlediska síťové sondy nacházející se v místní síti.



Obrázek 22 - Alarm error ping, zdroj: (Autor)

Další ilustrativní chybou může být 'DNS Domain name not found', která se vyskytuje v okamžicích, kdy zařízení nespatřuje požadované doménové jméno v rámci systému Domain Name System (DNS). Tento druh problému se obvykle objevuje, když požadované doménové jméno není správně nakonfigurováno či není dostupné v DNS databázi.

V důsledku této chyby může uživatel narazit na potíže s připojením k určitému serveru či webové stránce, neboť DNS selhává v překladu doménového jména na odpovídající IP adresu



Obrázek 23 - Alarm error dns, zdroj: (Autor)

Mezi další typy alaramů, které může PRTG Network Monitor detekovat, je neobvyklé chování, například nárůst nebo pokles toku dat na konkrétním switchi v síti. Takové změny mohou naznačovat možné problémy s výkonem switchu nebo neplánovanou aktivitu na této konkrétní síťové části.

Obrázek 24 - Alarm unusual traffic, zdroj: (Autor)

4.3.3 Diskuse o přínosech a případných vylepšeních v praxi.

I přes výrazné zlepšení by mělo být zváženo několik možných vylepšení pro další optimalizaci síťové infrastruktury.

Rozšíření monitoringu: Zvážit rozšíření monitoringu na další klíčové metriky nebo oblasti sítě, které mohou ovlivnit celkový výkon a bezpečnost. To může zahrnovat sledování dalších zařízení, aplikací nebo služeb.

Automatizace reakcí: Implementovat automatizované reakce na identifikované problémy, což umožní rychlejší a efektivnější řešení potenciálních hrozeb a výpadků.

Školení personálu: Poskytnout další školení zaměstnancům odpovědným za monitorovací systém, aby byli schopni plně využít jeho funkcionalitu a efektivně reagovat na identifikované problémy.

Pravidelné aktualizace a optimalizace: Udržovat monitorovací systém aktuální a provádět pravidelné aktualizace a optimalizace nastavení softwaru v souladu s měnícími se potřebami organizace.

Rozšíření infrastruktury: V případě potřeby zvážit další rozšíření infrastruktury, například vylepšení síťových zařízení nebo kapacity, aby byla zajištěna optimální výkonnost.

Implementace IDS/IPS systému: S ohledem na dosažené zlepšení je vhodné zvážit další posílení bezpečnosti síťové infrastruktury. Integrování Intrusion Detection System (IDS) a Intrusion Prevention System (IPS) přináší možnost identifikace potenciálních hrozeb a aktivního omezení rizikového provozu. Tato bezpečnostní vrstva by mohla efektivně doplňovat existující monitorovací opatření, zajišťující tak komplexní ochranu proti bezpečnostním rizikům a podporující rychlé reakce na identifikované problémy.

Závěrem lze konstatovat, že implementace monitorovacího softwaru přinesla mnoho významných výhod, ale stále existuje prostor pro další zdokonalení a růst v oblasti správy sítě ve firmě Aerosol-Service a.s.

5 Závěr

Hlavním cílem diplomové práce bylo vybrat a implementovat monitorovací software do sítě společnosti Aerosol-Service a.s. na základě teoretických poznatků a potřeb organizace. Tato práce nejen poskytuje podrobný přehled o současných trendech a technologiích v oblasti síťového monitorování, ale také konkrétní aplikaci těchto poznatků v reálném podnikovém prostředí.

V průběhu teoretické části práce byly zkoumány klíčové aspekty síťového monitorování, včetně jeho významu, metodiky a nástrojů. Důraz byl kladen na pochopení specifických potřeb společnosti Aerosol-Service a.s. a identifikaci klíčových metrik pro monitorování síťové infrastruktury. Tato analýza vedla k výběru vhodného monitorovacího softwaru, který byl následně úspěšně implementován do stávající infrastruktury.

V praxi bylo demonstrováno výrazné zlepšení ve správě sítě. Před implementací monitorovacího softwaru docházelo k neorganizovanému sběru dat a nedostatečnému sledování klíčových metrik. To mělo za následek reaktivní řešení problémů a neschopnost efektivně reagovat na výzvy síťového provozu. Po implementaci PRTG Network Monitor se situace výrazně zlepšila. Nový nástroj poskytl strukturovaný přístup k monitorování, transparentnost síťového provozu a rychlou identifikaci potenciálních problémů.

Sběr dat před a po implementaci monitorovacího softwaru ukázal značné snížení počtu anomálií a výrazné zvýšení přehledu o síťovém provozu. Díky dynamické identifikaci problémů může organizace systematicky reagovat na aktuální potřeby a optimalizovat síťové operace. Analyzované údaje také slouží jako základ pro pravidelná školení a plánování úprav infrastruktury.

V diskuzi o přínosech a případných vylepšeních v praxi bylo identifikováno několik oblastí pro další optimalizaci. Vzhledem k dosaženým výsledkům je vhodné zvážit rozšíření monitoringu, automatizaci reakcí na problémy a pravidelné aktualizace monitorovacího systému. Navíc by implementace IDS/IPS systému mohla posílit bezpečnost sítě.

Celkově lze konstatovat, že diplomová práce úspěšně přispěla k efektivnějšímu a bezpečnějšímu provozu sítě ve společnosti Aerosol-Service a.s. Implementovaný monitorovací software se stal klíčovým nástrojem pro správu a optimalizaci síťové infrastruktury. Dosažené výsledky nabízejí nejen aktuální přehled o stavu sítě, ale také strategický základ pro budoucí rozvoj a zdokonalení síťových operací v organizaci.

Dále je důležité poznamenat, že výsledky této práce nejsou omezeny pouze na prostředí společnosti Aerosol-Service a.s., ale lze je zobecnit pro nasazení v jiných systémech. Metodologie vybraná pro analýzu a implementaci monitorovacího softwaru poskytuje univerzální přístup, který může být aplikován i v jiných firemních prostředích s podobnými potřebami. Tím se otevírají možnosti využití této práce jako inspirace pro řešení podobných problémů v širším kontextu firemního síťového managementu.

6 Seznam použitých zdrojů

A10. 2023. The OSI Network Model and Types of Load Balancers. *A10.* [Online] 2023. https://www.a10networks.com/glossary/osi-network-model-and-types-of-load-balancers/.
Accyotta. 2023. PRTG Network Monitor. *Accyotta.* [Online] 2023. https://www.accyotta.com/paessler/prtg.
Acharya, Durga Prasad. 2023. ManageEngine OpManager Makes Monitoring Simple and Effective. *GeekFlare.* [Online] 2023. https://geekflare.com/manageengine-opmanager-review/.
Anderson, Paul. 2018. ManageEngine OpManager Review. *Network Admin Tools.* [Online] 2018. https://www.netadmintools.com/network-monitoring-software/opmanager-manageengine/.
Andrew Tanenbaum, David Wetherall. 2010. *Computer Networks.* London : Pearson, 2010. 978-0132126953.
Aquasec. 2023. What is a Containerized Architecture? *Aquasec.* [Online] 2023. https://www.aquasec.com/cloud-native-academy/container-security/containerized-architecture/.
Aston, Ben. 2023. 10 Best User Behavior Analytics Tools in 2023. *The Product Manager.* [Online] 6. Srpen 2023. https://theproductmanager.com/tools/best-user-behavior-analytics-tools/.
Bäckström, Tom. 2018. *Speech Coding: with Code-Excited Linear Prediction.* Berlin : Springer, 2018. 978-3319843445.
Benoît Claise, Joe Clarke, Jan Lindblad. 2019. *Network Programmability with YANG: The Structure of Network Automation with YANG, NETCONF, RESTCONF, and gNMI.* Massachusetts : Addison-Wesley Professional, 2019. 978-0135180396.
Bhardwaj, Rashmi. 2023. What is PRTG Network Monitor? *Network Interview.* [Online] 2023. https://networkinterview.com/what-is-prtg-network-monitor/.
Bhargava, Ayushi. 2022. What is Behavior Monitoring in Cybersecurity? *TutorialsPoint.* [Online] 16. Srpen 2022. https://www.tutorialspoint.com/what-is-behavior-monitoring-in-cybersecurity.
Burke, J. 2003. *Network Management: Concepts And Practice, A Hands-On Approach.* London : Pearson, 2003. 978-0130329509.
Burke, John. 2022. Throughput. *TechTarget.* [Online] 20. Listopad 2022. https://www.techtarget.com/searchnetworking/definition/throughput.
Cacti. 2023. About Cacti. *Cacti.* [Online] 2023. http://cacti.net/.
Cisco. 2023. What Is Cloud Monitoring? *Cisco.* [Online] 2023. https://www.cisco.com/c/en/us/solutions/cloud/what-is-cloud-monitoring.html.
—. 2023. What is Digital Experience Monitoring? *AppDynamics.* [Online] 2023. https://www.appdynamics.com/topics/what-is-digital-experience-monitoring.
Clinton, David. 2018 . *Linux in Action.* Alberta : Manning, 2018 . 978-1617294938.
CloudFlare. 2023. What is data privacy? *CloudFlare.* [Online] 2023. https://www.cloudflare.com/learning/privacy/what-is-data-privacy/.
Cloudian. 2023. What is Data Protection and Privacy? *Cloudian.* [Online] 2023. https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/.
Comer, Douglas E. 2014. *Computer Networks and Internets.* London : Pearson, 2014. 978-0133587937.

COOPER, STEPHEN. 2023. SolarWinds Network Performance Monitor (NPM) Review. *CompariTech.* [Online] 19. Srpen 2023. https://www.comparitech.com/net-admin/solarwinds-network-performance-monitor-review/.
De, Abhishek. 2023. Software defined Networking(SDN). *GeeksforGeeks.* [Online] 2023. https://www.geeksforgeeks.org/software-defined-networking/.
DeCarlo, Amy Larsen. 2020. AI, analytics, automation fuel the future of network management. *TechTarget.* [Online] 20. Březen 2020. https://www.techtarget.com/searchnetworking/feature/AI-analytics-automation-fuel-the-future-of-network-management.
DigitalOcean. 2023. What is cloud monitoring? Best practices for your startup's cloud monitoring strategy. *DigitalOcean.* [Online] 2023. https://www.digitalocean.com/resources/article/cloud-monitoring.
FirstLight. 2023. SolarWinds Network Performance Monitor (NPM). *FirstLight Shop.* [Online] 2023. https://shop.firstlight.net/product/solarwinds-network-performance-monitor-npm/.
Froehlich, Andrew. 2021. 4 categories of network monitoring. *TechTarget.* [Online] 1. Říjen 2021. https://www.techtarget.com/searchnetworking/tip/4-categories-of-network-monitoring.
—. 2023. streaming network telemetry. *TechTarget.* [Online] 15. Leden 2023. https://www.techtarget.com/searchnetworking/definition/streaming-network-telemetry.
GeeksforGeeks. 2023. Basics of Computer Networking. *GeeksForGeeks.* [Online] 17. Květen 2023. https://www.geeksforgeeks.org/basics-computer-networking/.
GetApp. 2023. ManageEngine Endpoint Central MSP. *GetApp.* [Online] 2023. https://www.getapp.ae/software/2063688/manageengine-desktop-central-msp.
Gillis, Alexander S. 2023. Nagios. *TechTarget.* [Online] Červenec. 15 2023. https://www.techtarget.com/searchitoperations/definition/Nagios.
—. 2023. TechTarget. *IT monitoring.* [Online] 1. Duben 2023. https://www.techtarget.com/searchitoperations/definition/IT-monitoring.
Griffin, Janis. 2021. How to Monitor Logs Guide With Recommended Automated Tools. *LogicalRead.* [Online] 7. Červenec 2021. https://logicalread.com/log-monitoring-tools/.
Grimmick, Robert. 2023. Network Flow Monitoring Explained: NetFlow vs sFlow vs IPFIX. *Varonis.* [Online] 23. Červen 2023. https://www.varonis.com/blog/flow-monitoring.
Hein, Daniel. 2019. 5 Network Monitoring Techniques Your Enterprise Needs to Use. *Solutions Review.* [Online] 26. Březen 2019. https://solutionsreview.com/network-monitoring/5-network-monitoring-techniques-your-enterprise-needs-to-use/.
—. 2019. 6 Essential Security Features for Network Monitoring Solutions. *Solutions Review.* [Online] 17. Prosinec 2019. https://solutionsreview.com/network-monitoring/6-essential-security-features-for-network-monitoring-solutions/.
Huy Nguyen, Tam V. Nguyen, Dong II Kim, Choi Deokjai. 2008. Network traffic anomalies detection and identification with flow monitoring. *ResearchGate.* [Online] Červen 2008. https://www.researchgate.net/publication/4340083_Network_traffic_anomalies_detection_and_identification_with_flow_monitoring.
Charbonneau, Pierre-Luc. 2023. Top 7 Reasons Why You Should Monitor Network Performance. *Obkio Blog.* [Online] 21. Duben 2023. https://obkio.com/blog/top-7-reasons-why-you-should-monitor-network-performance/.

Chris Sanders, Jason Smith. 2013. *Applied Network Security Monitoring: Collection, Detection, and Analysis.* Oxford : Syngress, 2013. 978-0124172081.
IBM. 2023. TCP/IP protocols. *IBM.* [Online] 24. Březen 2023. https://www.ibm.com/docs/en/aix/7.2?topic=protocol-tcpip-protocols.
—. 2023. What is network monitoring? *IBM.* [Online] 2023. https://www.ibm.com/topics/network-monitoring.
Imperva. 2023. OSI Model. *Imperva.* [Online] 2023. https://www.imperva.com/learn/application-security/osi-model/.
Israr Ullah, Shakeel Ahmad, DoHyeun Kim, Faisal Mehmood. 2019. Cloud Based IoT Network Virtualization for Supporting Dynamic Connectivity among Connected Devices. *MDPI.* [Online] 2019. https://www.mdpi.com/2079-9292/8/7/742.
John Arundel, Justin Domingus. 2019. *Cloud Native DevOps with Kubernetes: Building, Deploying, and Scaling Modern Applications in the Cloud.* California : O'Reilly Media, 2019. 978-1492040767.
Julian, Mike. 2017. *Practical Monitoring: Effective Strategies for the Real World.* California : O'Reilly Media, 2017. 978-1491957356.
Kinzie, Kody. 2022. How to Use Wireshark: Comprehensive Tutorial + Tips. *Varonis.* [Online] 19. Srpen 2022. https://www.varonis.com/blog/how-to-use-wireshark.
Klosowski, Thorin. 2021. The State of Consumer Data Privacy Laws in the US (And Why It Matters). *The New York Times.* [Online] 6. Září 2021. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.
KnowledgeNile. 2023. Active vs. Passive Network Monitoring: Difference Explained. *KnowledgeNile.* [Online] 14. Červenec 2023. https://www.knowledgenile.com/blogs/active-vs-passive-network-monitoring.
Kozierok, Charles M. 2005. *The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference.* San Francisco : No Starch Press, 2005. 978-1593270476.
KUMAR, RAJESH. 2022. What is Zabbix and How it works? An Overview and Its Use Cases. *DevOpsSchool.* [Online] 24. Březen 2022. https://www.devopsschool.com/blog/what-is-zabbix-and-how-it-works-an-overview-and-its-use-cases/.
Lamberti, Alyssa. 2023. Network Speed vs. Bandwidth vs. Throughput: Understanding Network Performance Metrics. *Obkio.* [Online] 9. Březen 2023. https://obkio.com/blog/network-speed-bandwidth-throughput/.
Lanesskog, Jorgen. 2019. *Ping: Basic IP Network Troubleshooting.* Bergen : Independently published, 2019. 978-1520610542.
Larry L. Peterson, Bruce S. Davie. 2011. *Computer Networks: A Systems Approach.* Cambridge : Morgan Kaufmann, 2011. 978-0123850591.
Ligus, Slawek. 2012. *Effective Monitoring and Alerting: For Web Operations.* California : O'Reilly, 2012. 978-1449333524.
Lin, Pohan. 2023. A Beginner's Guide To Anomaly Detection and its Role in the Network. *PingPlotter.* [Online] 2023. https://www.pingplotter.com/wisdom/article/anomaly-detection-role-in-networks/.
LiveAction. 2023. Flow Monitoring. *LiveAction.* [Online] 20. Duben 2023. https://www.liveaction.com/glossary/flow-monitoring/.
Lord, Nate. 2023. What is User Activity Monitoring? How It Works, Benefits, Best Practices, and More. *Fortra.* [Online] 6. Květen 2023. https://www.digitalguardian.com/blog/what-user-activity-monitoring-how-it-works-benefits-best-practices-and-more.

Loshin, Peter. 2022. user behavior analytics (UBA). *TechTarget.* [Online] 1. Červenec 2022. https://www.techtarget.com/searchsecurity/definition/user-behavior-analytics-UBA.
Lucas, Michael W. 2015. *Networking for System Administrators.* Michigan : Tilted Windmill Press, 2015. 978-1642350333.
Lulka, Jess. 203. What Is Container Monitoring? *TheNewStack.* [Online] 5. Duben 203. https://thenewstack.io/what-is-container-monitoring/.
ManageEngine Blog. 2021. Network monitoring tools: The good, the bad, and the ugly. *ManageEngine Blog.* [Online] 13. Listopad 2021. https://blogs.manageengine.com/corporate/general/2021/10/13/network-monitoring-tools-the-good-the-bad-and-the-ugly.html.
ManageEngine. 2023. Comprehensive Network Monitoring Solution for IT Managers and Network Administrators. *ManageEngine.* [Online] 2023. https://manageengine.optrics.com/opmanager.html.
—. 2023. Network Monitoring. *ManageEngine OpManager.* [Online] 2023. https://www.manageengine.com/network-monitoring/.
ManageEngine OpManager. 2023. Editions and Pricing. *ManageEngine OpManager.* [Online] 10. Říjen 2023. https://www.manageengine.com/network-monitoring/opmanager-editions.html?btmMenu.
—. 2023. ManageEngine OpManager - Network Monitoring Software. *ManageEngine OpManager.* [Online] 2023. https://www.manageengine.com/network-monitoring/help/.
ManageEngine. 2023. Top 5 network management trends in 2023. *ManageEngine Blog.* [Online] 11. Srpen 2023. https://blogs.manageengine.com/corporate/general/2023/08/11/top-5-network-management-trends-in-2023.html.
—. 2023. What is SNMP? *ManageEngine.* [Online] 14. Duben 2023. https://www.manageengine.com/network-monitoring/what-is-snmp.html.
MarketsandMarkets. 2022. Network Management Systems market. *MarketsandMarkets.* [Online] 2022. https://www.marketsandmarkets.com/Market-Reports/network-management-market-1041.html.
MCS. 2023. 5 Reasons Organizations of any size need Network Monitoring. *ThinkMCS.* [Online] 2023. https://thinkmcs.com/5-reasons-network-monitoring/.
Mohanakrishnan, Ramya. 2023. What Is a Computer Network? Definition, Objectives, Components, Types, and Best Practices. *SpiceWorks.* [Online] 17. Květen 2023. https://www.spiceworks.com/tech/networking/articles/what-is-a-computer-network/.
NetApp. 2023. What is cloud monitoring? *NetApp.* [Online] 2023. https://www.netapp.com/cloud-services/what-is-cloud-monitoring/.
Nicola Da Dalt, Ali Sheikholeslami. 2018. *Understanding Jitter and Phase Noise: A Circuits and Systems Perspective.* Cambridge : Cambridge University Press, 2018. 978-1107188570.
Paessler AG. 2022. White Paper: Security. *Paessler The Monitoring Experts.* [Online] 2022. https://www.paessler.com/learn/whitepapers/security.
Paessler. 2023. PRTG Manual: System Requirements. *Paessler.* [Online] 2023. https://www.paessler.com/manuals/prtg/system_requirements.
—. 2023. PRTG Network monitor. *Paessler.* [Online] 2023. https://www.paessler.com/prtg/prtg-network-monitor.
Posey, Brien. 2021. Comparing data protection vs. data security vs. data privacy. *TechTarget.* [Online] 2. Únor 2021.

https://www.techtarget.com/searchdatabackup/tip/Comparing-data-protection-vs-data-security-vs-data-privacy.
Red Sift. 2022. Active vs. Passive Monitoring: what's the difference & why it matters. *Red Sift Blog.* [Online] 7. Srpen 2022. https://blog.redsift.com/brand-protection/active-vs-passive-monitoring-whats-the-difference-why-it-matters/.
Renata Teixeira, Sue B. Moon, Steve Uhlig. 2009. *Passive and Active Network Measurement.* New York City : Springer, 2009. 978-3642009761.
Sanders, Chris. 2011. *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems.* California : No Starch Press, 2011. 978-1593272661.
Scott, Russell. 2019. *Networking for Beginners.* Meridian : Nezávislé publikováno, 2019. 978-1704314105.
Security Scorecard. 2021. How to Identify and Prepare for Network Security Threats and Vulnerabilities. *Security Scorecard.* [Online] 26. Květen 2021. https://securityscorecard.com/blog/identify-network-security-threats-and-vulnerabilities/.
Sidheeq, Saifudheen. 2023. What is SNMP and how it works? *Get Labs Done.* [Online] 2023. https://getlabsdone.com/what-is-snmp-and-how-it-works/.
Snyk. 2023. The Importance of Container Monitoring. *Snyk.* [Online] 2023. https://snyk.io/learn/container-security/container-monitoring/.
SolarWinds. 2023. Flexible Licensing Options. *SolarWinds.* [Online] 2023. https://www.solarwinds.com/licensing-options.
—. 2023. Hybrid cloud monitoring. *SolarWinds.* [Online] 2023. https://www.solarwinds.com/server-application-monitor/use-cases/hybrid-cloud-monitor.
—. 2023. Network Monitoring Tool. *SolarWinds.* [Online] 25. Září 2023. https://www.solarwinds.com/network-performance-monitor/use-cases/network-monitoring-tool.
—. 2023. NPM licensing model. *SolarWinds documentation.* [Online] 2023. https://documentation.solarwinds.com/en/success_center/npm/content/npm_licensing_model.htm.
—. 2023. Response Time Monitor. *SolarWinds.* [Online] 24. Červen 2023. https://www.solarwinds.com/engineers-toolset/use-cases/response-time-monitor.
Solarwinds. 2022. What is Packet Capture (PCAP)? *Solarwinds.* [Online] 15. Leden 2022. https://www.solarwinds.com/resources/it-glossary/pcap.
Stephen F. Bush, Amit B. Kulkarni. 2013. *Active Networks and Active Network Management: A Proactive Management Framework.* New York City : Springer, 2013. 978-1475774849.
Subramanian, Mani. 2012. *Network Management: Principles and Practice.* New Jersey : Prentice Hall, 2012. 978-8131734049.
The Progress team. 2020. Active Vs. Passive Monitoring: Which is Best for Your Network? *WhatsUpGold.* [Online] 12. Březen 2020. https://www.whatsupgold.com/blog/active-vs.-passive-monitoring-which-is-best-for-your-network.
TRIPATHY, SUSNIGDHA. 2023. What Is Network Monitoring? Definition, Benefits, and Types. *Enterprise Networking Planet.* [Online] 24. Červenec 2023. https://www.enterprisenetworkingplanet.com/management/network-monitoring/.
TutorialsPoint. 2023. Nagios - overview. *TutorialsPoint.* [Online] 2023. https://www.tutorialspoint.com/nagios/nagios_overview.htm.
Verizon. 2023. Bandwidth. *Verizon.* [Online] 21. Únor 2023. https://www.verizon.com/articles/internet-essentials/bandwidth-definition/.

VMWare. 2023. What is Cloud Infrastructure? *VMWare.* [Online] 2023. https://www.vmware.com/topics/glossary/content/cloud-infrastructure.html.
Williams, Frank. 2018. Virtualization of Your Network: five most serious challenges. *IIoT World.* [Online] 8. Únor 2018. https://iiot-world.com/industrial-iot/connected-industry/virtualization-of-your-network-five-most-serious-challenges/.
Wilson, Ed. 2000. *Network Monitoring and Analysis: A Protocol Approach to Troubleshooting.* místo neznámé : Prentice Hall, 2000. 978-0130264954.
Wilson, Marc. 2023. Network Throughput – What is It, How To Measure & Optimize! *PCWDLD.* [Online] 29. Srpen 2023. https://www.pcwdld.com/network-throughput/.
WireShark. 2023. Chapter 1. Introduction. *WireShark.* [Online] 2023. https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html.
Yasar, Kinza. 2023. network protocol. *TechTarget.* [Online] Březen 2023. https://www.techtarget.com/searchnetworking/definition/protocol.
Yuchao Zhang, Ke Xu. 2020. *Network Management in Cloud and Edge Computing.* London : Springer Nature, 2020. 978-9811501388.
Yulei Wu, Jingguo Ge, Tong Li. 2022. *AI and Machine Learning for Network and Security Management.* New Jersey : Wiley-IEEE Press, 2022. 978-1119835875.
Zabbix. 2023. Overview of Zabbix. *Zabbix.* [Online] 2023. https://www.zabbix.com/documentation/1.8/en/manual/about/overview_of_zabbix.
Zeoss. 2011. Network Management and the Impact from Virtualization. *Zenoss.* [Online] 4. Květen 2011. https://www.zenoss.com/blog/network-management-and-the-impact-from-virtualization.

7 Seznam obrázků, tabulek, grafů a zkratek

7.1 Seznam obrázků

Obrázek 1 - TCP/IP a OSI modely, zdroj: (A10, 2023) 18
Obrázek 2 - Aktivní vs Pasivní monitoring, zdroj: (KnowledgeNile, 2023) 21
Obrázek 3 - SNMP, zdroj: (Sidheeq, 2023) 23
Obrázek 4 - SolarWinds GUI, zdroj: (SolarWinds, 2023) 25
Obrázek 5 - PRTG Network monitor GUI, zdroj: (Paessler, 2023) 27
Obrázek 6 - ManageEngine GUI, zdroj: (GetApp, 2023) 29
Obrázek 7 - SNMP vs Telemetry, zdroj: (Froehlich, 2023) 33
Obrázek 8 - Propustnost vs Šířka pásma, zdroj: (Burke, 2022) 37
Obrázek 9 - Předpokládaná hodnota trhu s monitoringem, zdroj: (MarketsandMarkets, 2022) 44
Obrázek 10 - Budoucnost správy sítě, zdroj: (DeCarlo, 2020) 46
Obrázek 11 - Konfigurace stroje, zdroj: (Autor) 57
Obrázek 12 - Webové rozhraní, zdroj: (Autor) 59
Obrázek 13 - Úvodní stránka PRTG, zdroj: (Autor) 60
Obrázek 14 - Konfigurace auto-discovery, zdroj: (Autor) 61
Obrázek 15 - Finální hierarchie, zdroj: (Autor) 61
Obrázek 16 - Nastavení senzoru, zdroj: (Autor) 62
Obrázek 17 - Speed trigger, zdroj: (Autor) 63
Obrázek 18 - Dashboard, zdroj: (Autor) 64
Obrázek 19 - Report, zdroj: (Autor) 65
Obrázek 20 - Anomálie před, zdroj:(Autor) 68
Obrázek 21 - Anomálie po, zdroj: (Autor) 68
Obrázek 22 - Alarm error ping, zdroj: (Autor) 69
Obrázek 23 - Alarm error dns, zdroj: (Autor) 69
Obrázek 24 - Alarm unusual traffic, zdroj: (Autor) 70

7.2 Seznam tabulek

Tabulka 1 - Ceník SolarWinds, zdroj: (FirstLight, 2023) 26
Tabulka 2 - Ceník PRTG, zdroj: (Paessler, 2023) 27
Tabulka 3 - Ceník ManageEngine, zdroj: (ManageEngine OpManager, 2023) 29
Tabulka 4 - Nástroje pro monitorování sítě, zdroj: (ManageEngine Blog, 2021) 31
Tabulka 5 - Areál společnosti, zdroj: (Autor) 48
Tabulka 6 - Komparace monitorovacích softwarů, zdroj: (Vlastni zpracování dle informaci na webových stránkách jednotlivých poskytovatelů) 52
Tabulka 7 - Cenová komparace monitorovacích softwarů, zdroj: (Vlastni zpracování dle informaci na webových stránkách jednotlivých poskytovatelů) 53
Tabulka 8 - Systémové požadavky, zdroj (Paessler, 2023) 56