Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Monitoring sítě

Zdeněk Jirásek

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Zdeněk Jirásek

Informatika

Název práce

Monitoring sítě

Název anglicky

Network monitoring

Cíle práce

Cílem práce je zavedení a nastavení monitorovacího softwaru Centreon pro zdravotnické zařízení Synlab czech, s.r.o..
Dílčím cílem práce je zpracovat téma monitoringu sítě ve formě literární rešerše. Důrazem bude kladen na rozbor způsobů monitorování síťových prvků a síťového provozu. Objasněna bude také důležitost těchto systémů ve firemním prostředí.

Metodika

Ke zpracování teoretické části práce budou využity české i cizojazyčné zdroje, které budou uceleny do formy přehledné literární rešerše. Praktická část práce bude probíhat v IT oddělení firmy synlab czech, s.r.o.. Pro zavedení a nastavení softwaru bude využito řešení s volně dostupným zdrojovým kódem pro monitorování IT od pařížské softwarové společnosti Centreon. Tento open source software bude následně nakonfigurován pro specifické potřeby synlab czech, s.r.o. pomocí protokolu Simple Network Management (SNMP), postup bude v práci popsán konkrétně v jednotlivých krocích.

Doporučený rozsah práce

35-45s.

Klíčová slova

monitoring, software, server, počítačová síť, konfigurace, síťová infrastruktura, síťové zařízení, síťový provoz

---

Doporučené zdroje informací

KRETCHMAR, J M. – DOSTÁLEK, L Administrace a diagnostika sítí: pomocí OpenSource utilit a nástrojů. Brno: Computer Press, 2004. ISBN 80-251-0345-5.

KUROSE, J F. – ROSS, K W. *Počítačové sítě.* Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

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

MAURO, D. – SCHMIDT, K. Essential SNMP, Second Edition. Beijing: O'Reilly Media, 2005. ISBN 05-960-0840-6.

VELTE, T J. – VELTE, A T. – KRÁSENSKÝ, D. *Síťové technologie Cisco : velký průvodce.* Brno: Computer Press, 2003. ISBN 80-7226-857-0.

Předběžný termín obhajoby

2021/22 LS – PEF

Vedoucí práce

Ing. Martin Havránek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 10. 8. 2021

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 5. 10. 2021

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 23. 10. 2021

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Monitoring sítě" jsem vypracoval(a) samostatně pod vedením vedoucího bakalářské 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 bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne _____

Poděkování

Rád bych touto cestou poděkoval svému vedoucímu doktorovi Martinu Havránkovi za vstřícnost, trpělivost, a hlavně dobrou náladu při konzultacích. Velké díky také patří mé sestře Markétě, která mě ve vzdělávání podporovala, a to vždy, v dobrých i špatných chvílích.

Monitoring sítě

Abstrakt

Ve své bakalářské práci se věnuji problematice monitorování počítačové sítě. Cílem práce je implementace monitorovacího softwaru Centreon, včetně konfigurace, dle specifických potřeb podniku. Dílčím cílem je zpracování literární rešerše na téma monitoring sítě. Ke splnění těchto cílů budou využity české i cizojazyčné zdroje. Teoretická část podrobně popisuje náležitosti monitoringu jako počítačovou síť, způsoby monitorování síťových zařízení a provozu, protokol SNMP a vybrané monitorovací řešení. V praktické části, která probíhá na IT oddělení podniku, je provedena analýza síťové infrastruktury a následně, u jednotlivých zařízení v síti (např. u různých typů serverů), je zhodnocena důležitost a potřeba pro monitorování. Při porovnání zadání pro monitorování s funkcemi vybraných monitorovacích systémů z teoretické části vyšlo najevo, že požadavky by mohl splňovat téměř každý z nich. Výsledná instalace a následná konfigurace monitorovacího systému Centreon proběhla bez větších komplikací a současně překvapila svou intuitivností.

Klíčová slova: monitoring, software, server, počítačová síť, konfigurace, síťová infrastruktura, síťové zařízení, síťový provoz

Network monitoring

Abstract

In my bachelor's thesis I am dealing with the problem of computer network monitoring.

The objective of the thesis is the implementation of Centreon monitoring software, including configuration, according to the specific needs of the company. A sub-objective is the development of a literature review on network monitoring. Czech and foreign language sources will be used to meet these objectives. The theoretical part describes in detail the essentials of monitoring such as computer network, methods of monitoring network devices and traffic, SNMP protocol and selected monitoring solutions. In the practical part, which takes place in the IT department of the company, an analysis of the network infrastructure is performed and then the importance and need for monitoring is evaluated for individual devices in the network (e.g., different types of servers). In comparison of the company's monitoring requirements with functions of the selected monitoring systems from the theoretical part, it becomes clear, that almost every monitoring system described below would meet the requirements of the company. The installation and subsequent configuration of the Centreon monitoring system was without severe complication. Beside this Centreon surprised with intuitive user-friendly installation as well.

Keywords: monitoring, software, server, computer network, configuration, network infrastructure, networking hardware, network traffic

Obsah

1 Úvod

V dnešní době jsou počítačové sítě používány v téměř každém podniku nehledě na jeho velikost. Všechna zařízení připojená do těchto podnikových sítí plní svůj specifický účel.

Koncová zařízení, jako počítače či notebooky, využívají zaměstnanci k výkonu své práce. Přičemž prvky síťové infrastruktury, jako switche, routery či firewally, zprostředkovávají komunikaci mezi zařízeními v síti, a to jak v rámci podniku, tak i s okolním světem pomocí internetu.

Dále se v podnicích používají servery, jejichž cílem je nabízet služby ostatním zařízením v síti. Těchto služeb je mnoho a jsou různorodé. Od databázového serveru, který může obsahovat citlivé informace, až po e-mailový, pomocí kterého zaměstnanci komunikují.

V určitém okamžiku mohou některé z těchto zařízení přestat fungovat. Selhání výše jmenovaných zařízení může narušit činnost podniku a tím zapříčinit peněžní ztrátu. Z tohoto důvodu jsou používány monitorovací systémy, které mají za cíl těmto výpadkům zabránit nebo na ně alespoň včas upozornit tak, aby jej stihli IT administrátoři co nejdříve opravit a tím minimalizovat dopad na podnik.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je zavedení a nastavení monitorovacího softwaru Centreon pro zdravotnické zařízení synlab czech, s.r.o. Dílčím cílem práce je zpracovat téma monitoringu sítě ve formě literární rešerše. Důrazem bude kladen na rozbor způsobů monitorování síťových prvků a síťového provozu. Objasněna bude také důležitost těchto systémů ve firemním prostředí.

2.2 Metodika

Ke zpracování teoretické části práce budou využity české i cizojazyčné zdroje, které budou uceleny do formy přehledné literární rešerše. Praktická část práce bude probíhat v IT oddělení firmy synlab czech, s.r.o. Pro zavedení a nastavení softwaru bude využito řešení s volně dostupným zdrojovým kódem pro monitorování IT od pařížské softwarové společnosti Centreon. Tento open source software bude následně nakonfigurován pro specifické potřeby synlab czech, s.r.o. pomocí protokolu Simple Network Management (SNMP), postup bude v práci popsán konkrétně v jednotlivých krocích.

3 Teoretická východiska

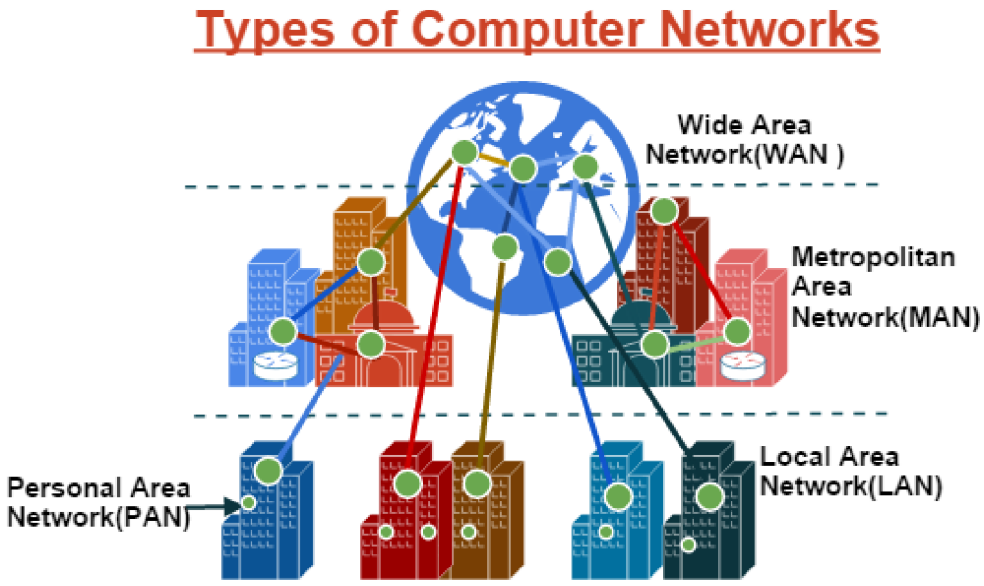
3.1 Počítačová síť

Počítačová síť je skupina navzájem propojených zařízení, která jsou schopna spolu vzájemně komunikovat. Zařízení jsou propojena sítí komunikačních linek a paketových přepínačů. Komunikační linky se skládají z rozličných typů fyzických médií, včetně koaxiálního kabelu, měděných vodičů, optických vláken a rádiového spektra. Různé linky jsou schopny přenášet data různou rychlostí. Velikost a důležitost počítačových sítí se může značně lišit. Od malých sítích v domácnostech až po masivní sítě velkých organizací, které mohou přijít o velké sumy peněž s každou minutou, co jsou jejich sítě nedostupné či nefunkční. Nejznámější a největší počítačová síť je internet. Internet propojuje sítě po celém světě. (1)

3.1.1 Typy sítí

Počítačové sítě se rozdělují podle geografického území, které pokrývají (viz. Obrázek č. 1). Mezi nejzákladnější typy počítačových sítí se řadí:

- PAN (Personal Area Network) – Malá síť, dosahující několik metrů. Patří do ní komunikační zařízení (drátové i bezdrátové) v rámci pracovního prostoru jednotlivce, proto si nese označení osobní síť. Např. bezdrátová myš, tablet atd.
- LAN (Local Area Network) – Počítačová sít, která propojuje malý počet zařízení v blízké geografické oblastí. Např. patro, domácnost.
- MAN (Metropolitan area Network) – Komunikační infrastruktura, která byla vybudována ve velkých městech a jejich okolí.
- WAN (Wide Area Network) – Síť, která propojuje dvě nebo více místních sítí na velkou geografickou vzdálenost. Rozprostírá se na velkém geografickém území, jako je stát, provincie nebo země. (2)



Obrázek č. 1: Typy počítačových sítí (2)

3.1.2 Zařízení v síti

Koncová zařízení v počítačových sítích jsou označovány jako hostitelé (aj. hosts). V dřívějších dobách se jednalo hlavně o PC desktopy a Linuxové pracovní stanice. Postupem času se začalo připojovat do sítě více zařízení např. televizory, herní konzole, termostaty, domácí bezpečností systémy, domácí spotřebiče, hodinky, brýle, automobily. Koncová zařízení můžeme dále rozdělit na klienty a servery. Server poskytuje službu či funkci, kterou klienti využívají. Například webový server poskytuje webovou stránku, pro kterou klient zasílá požadavek. Klient následně může komunikovat přímo s koncovými uživateli.

Většina sítí propojuje koncová zařízení pomocí switchů a routerů. Switche přesměrovávají komunikaci mezi logicky sousedícími zařízeními, zatímco routery poskytují funkci směrování, které zajišťuje strukturu sítě a umožňuje komunikaci mezi podsítěmi. (1)

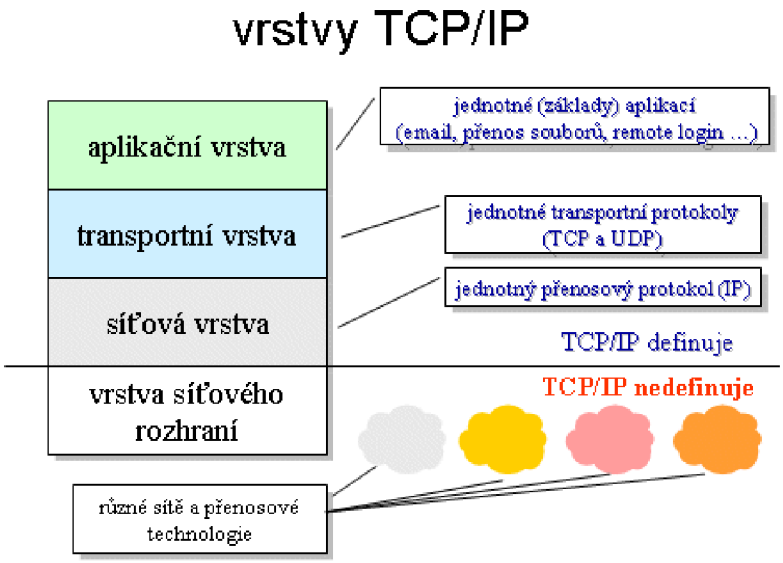
3.1.3 Principy komunikace v síti

Na počátku lidstva bylo třeba nalézt společný nástroj, kterému budou všichni lidé rozumět. Tímto nástrojem se stal jazyk. V případě počítačových síti je tímto nástrojem protokol. Protokol definuje formát a pořadí zpráv vyměňovaných mezi dvěma nebo více komunikujícími subjekty, stejně tak i akce prováděné při přenosu, přijetí zprávy nebo jiné události. Koncové zařízení, které chce zaslat data, je nejprve rozdělí na menší části a ke každé přidá hlavičku. Hlavička obsahuje informace jako je identifikace odesílatele a

příjemce, používaný protokol atd. Výsledný balíček informace nazýváme paket. Po doručení všech paketů, na které jsou data rozdělena, si je adresované zařízení opět složí do původního stavu, ve kterém byly odeslány. (1)

3.2 TCP/IP

TCP/IP je sada protokolů, která je standardně využívána k propojení hostitelů, sítí a internetu. Název sady pochází ze dvou nejdůležitějších protokolů: Transmission Control Protocol (TCP) a Internet Protocol (IP). Návrháři sítí organizují protokoly – a síťový hardware a zařízení, který tyto protokoly implementuje – do vrstev. Rozdělení komunikačního softwaru do vrstev umožnuje lepší dělbu práce, snadnou implementaci a testování kódu. Jednotlivé vrstvy komunikují s vrstvami nad a pod nimi. Vrstva poskytuje službu pro vrstvu, která je nad ní, a využívá služeb poskytovaných vrstvou pod ní (viz. Obrázek č. 2). (1)



Obrázek č. 2: Vrstvy TCP/IP (3)

3.2.1 Aplikační vrstva (Application Layer)

V této abstraktní vrstvě se nachází sítové programy v rámci TCP/IP. Aplikační vrstva zajišťuje přenos a srozumitelnost zpráv. Protokoly aplikační vrstvy využívá více koncových zařízení, které si pomocí programů v této vrstvě navzájem vyměňují informace. Paket v aplikační vrstvě nazýváme zpráva. Komunikační rozhraní mezi aplikační a transportní vrstvou je určeno číslem portu a soketu. Příklady známých protokolů aplikační vrstvy:

- HTTP (Hypertext Transfer Protocol) – Navržen pro komunikaci mezi webovými prohlížeči a webovými servery. Jeho hlavní funkce je přenos hypertextových dokumentů, jako je HTML, XML apod.

- HTTPS (Hypertext Transfer Protocol Secure) – Jedná se o zabezpečenou variantu protokolu HTTP. Komunikace mezi prohlížečem a webovým server je zašifrována pomocí kryptografického protokolu TLS (Transport Layer Security), či jeho předchůdcem SSL (Secure Sockets Layer).
- Telnet – Vzdálené obousměrné terminálové připojení. Používá se např. ke vzdálenému nastavování síťových prvků – switchů, routerů, firewallů apod.
- SSH (Secure Shell) – Stejně jako Telnet umožnuje vzdálené obousměrné terminálové připojení, s rozdílem použití zabezpečené šifrované relace. Z tohoto důvodu je v dnešní době preferován nad Telnetem.
- SMTP (Simple Mail Transfer Protocol) – Odesílání internetové pošty mezi hostiteli.
- SNMP (Simple Network Management Protocol) – shromažďuje a organizuje data spravovaných zařízení v sítích IP. Používá se především k monitorování a správě sítě. Protokol bude více rozebrán v samostatné kapitole.
- FTP (File Transfer Protocol) – Přenos souborů z jednoho hostitele na druhého.
- DNS (Domain Name System) – Překládá číselné IP adresy zařízení na snadně lidsky zapamatovatelná textová doménová jména.
- DHCP (Dynamic Host Configuration Protocol) – Dynamické přiřazování IP adres k libovolnému zařízení nebo uzlu v síti.
- NTP (Network Time Protocol) – Synchronizuje čas v zařízeních v síti. (1, 3)

3.2.2 Transportní vrstva (Transport Layer)

Transportní vrstva přenáší komunikaci aplikační vrstvy mezi zařízeními. Podporuje více aplikací současně. Paket v transportní vrstvě nazýváme segment. K účelu přenosu segmentů jsou používány dva transportní protokoly:

- TCP – Nejvíce používaný transportní protokol, poskytuje spojovanou (potvrzovanou) službu připojení, garantuje spolehlivost, řídí tok dat vyrovnáním rychlosti odesílatele a příjemce, omezuje rychlost přenosu v případě přetížení sítě.
- UDP – Nevyžaduje navázání spojení a nezaručuje spolehlivost přenosu, oproti TCP nabízí vyšší rychlost spojení, ale horší stabilitu, která může vést ke ztrátě dat. (3)

3.2.3 Síťová vrstva (Network Layer)

Síťová vrstva se stará o přesun informací od hostitele k hostiteli. Paket v síťové vrstvě nazýváme datagram. Tato vrstva je zodpovědná za oddělení vyšších vrstev od fyzické vrstvy síťového rozhraní, která je pod ní. Transportní vrstva (TCP nebo UDP) odesílajícího hostitele

nejprve předá segment a cílovou adresu síťové vrstvě a poté za pomocí IP protokolu odešle segment transportní vrstvě adresovaného hostitele. Síťová vrstva používá následující protokoly:

- IP (Internet Protocol) – Poskytuje adresovací a směrovací funkci s jediným cílem co nejrychlejšího doručení datagramů po síti ke svému adresátovi. Z tohoto důvodu se jedná o nespojovací protokol, který neposkytuje spolehlivost, řízení toků a nabízí pouze částečnou detekci chyb. Tyto funkce musí být zajištěny ve vyšších vrstvách. V dnešní době je nejčastěji používána verze IPv4. Z důvodu postupného docházení IP adres ve verzi IPv4 byl vyvinut nástupce IPv6, který kapacitu adres rozšiřuje.
- ICMP (Internet Control Message Protokol) – Poskytuje možnost odesílání řídících a chybových zpráv. Stejně jako IP protokol je nespolehlivý a nespojovaný. Pomocí tohoto protokolu lze zjišťovat propustnost a dostupnost sítě/síťových prvků – např. příkaz ping. ICMP protokol hlásí: zahozené pakety (informace přicházejí příliš rychle na to, aby mohly být zpracovány), selhání spojení (nelze se spojit s cílovým hostitelem), přesměrování (odesílající hostitel musí použít jiný router).
- ARP (Address Resolution Protokol) – Přiřazuje k proměnlivým logickým IP adresám jejich permanentní fyzické MAC adresy zařízení a tím pomáhá protokolu IP při směrování ke správnému hostiteli.
- RARP (Reverse Address Resolution Protocol) – Stejná funkčnost jako ARP, ale opačně (získávání IP adresy z MAC adresy). (1, 3)

3.2.4 Vrstva síťového rozhraní (Network Interface Layer)

Vrstva síťové rozhraní zajišťuje fyzický přenos informací mezi dvěma propojenými zařízeními tak, že formátuje IP datagramy síťové vrstvy do paketů, kterým můžou síťové technologie rozumět a přenášet je. Základní jednotkou informace v této vrstvě je rámec. Jak jsou zařízení propojena závisí na použité přenosové technologii (rozhraní, typu fyzického média) a síťového hardwaru hostitelů (síťová karta). TCP/IP podporuje tyto síťové rozhraní:

- Ethernet,
- IEEE 802.3,
- Token-ring,
- SLIP (Serial Line Internet Protocol),
- Loopback,
- FDDI,

- Serial Optical,
- Dvoubodový spoj (Point-to-Point Protocol),
- VIP (virtual IP adress).

Rozhraní Ethernet, IEEE 802.3 se používají v LAN sítích. Rozhraní SLIP v připojení pomocí sériového kabelu. Loopback se používá, když hostitel komunikuje sám se sebou (např. při vytváření lokálního webového serveru). Dvoubodový spoj se využívá pro připojení k počítači či síti prostřednictvím modemu. Rozhraní VIP se neváže s konkrétním síťovým adaptérem, protože na jednom zařízení lze nastavit více instancí virtuálního IP rozhraní. Příchozí pakety směrované na virtuální IP adresu jsou doručeny síťovým adaptérem, který nabízí nejlepší cestu. (3)

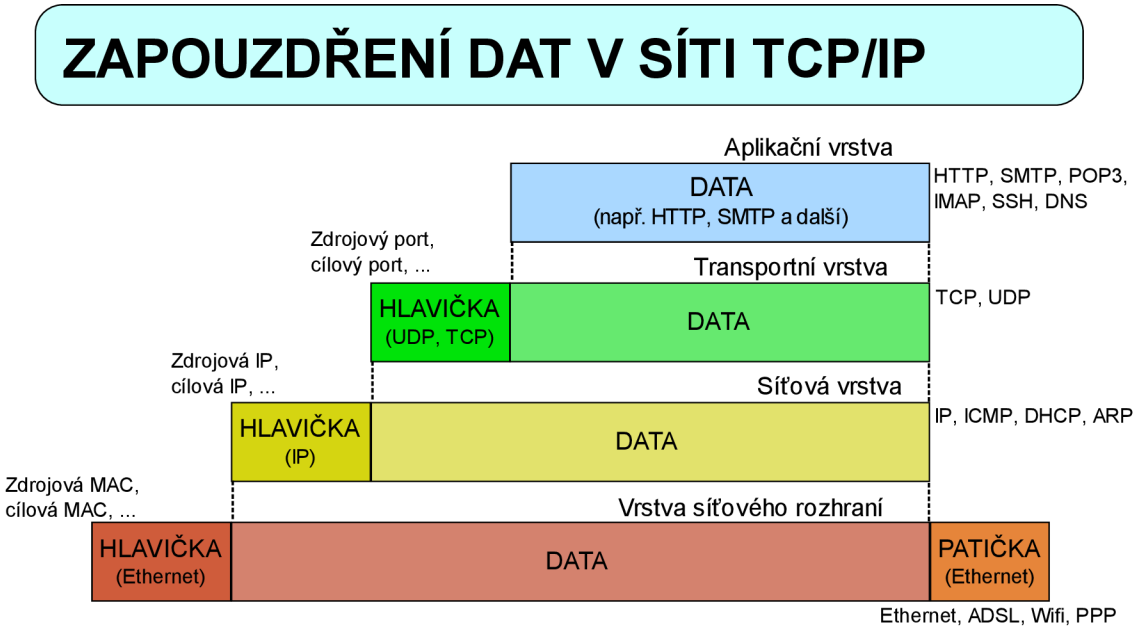
Přenosová média:

- Elektrické vodiče (obvykle měděné),
    - Koaxiální kabel,
    - Kroucená dvojlinka.
- Optická vlákna.
- Vzduch (bezdrátový přenos).

Nicméně, TCP/IP model tyto přenosové technologie nedefinuje, protože je navržen tak, aby byl hardwarově nezávislý. To znamená, že v této vrstvě může být implementována jakákoli přenosová technologie. Nejpoužívanější technologií je Ethernet. Z tohoto důvodu se tato vrstva někdy označuje jako vrstva ethernetová. (3)

3.2.5 Zapouzdření

TCP/IP je rozdělen na vrstvy, ve kterém každá vrstva vykonává určitý úkol. Odeslaná data se vrstvami přesouvají odshora dolů. Každá vrstva přidá k datům hlavičku, která obsahuje řídící informace potřebné k úspěšnému doručení dat. Balíček dat vyšší vrstvy obsahující hlavičku a data se pak stává daty, která jsou zaslána do nižší vrstvy a znovu zapouzdřena s hlavičkou nižší vrstvy (viz. Obrázek č. 4). Balíček dat obsahující záhlaví a data nazýváme protokolová datová jednotka (PDU). Koncové zařízení, které data přijímá, provádí obrácený postup (rozbalování) od nejnižší vrstvy nahoru. (1)



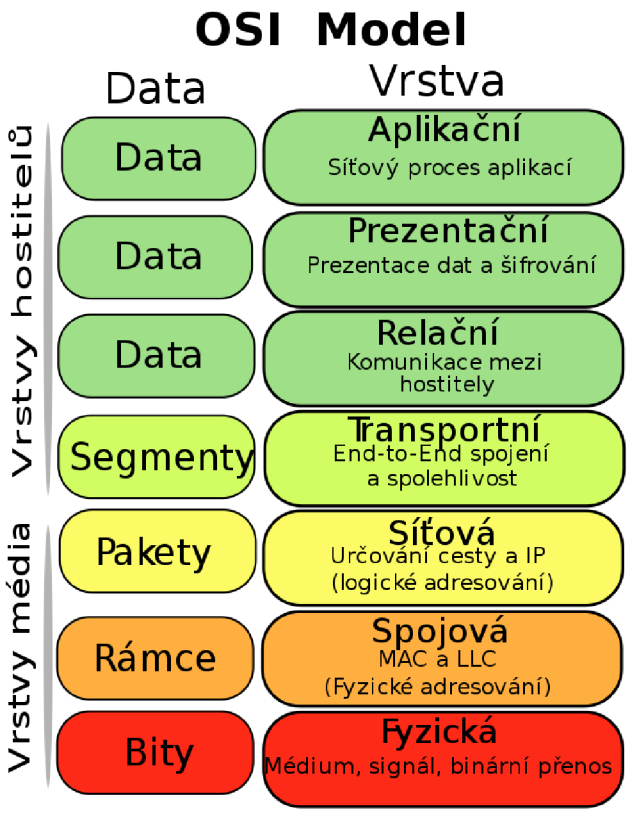
Obrázek č. 3: Zapouzdření dat v síti TCP/IP (4)

3.3 Model OSI

Tento model byl vyvinut koncem sedmdesátých let Mezinárodní organizací pro normalizaci (ISO) v době, kdy byly internetové protokoly sady TCP/IP i mnoho jiných sad protokolů teprve v ranném stádiu vývoje. Model OSI je dalším modelem, pomocí kterého mohou být přenášeny data po síti i internetu. Největší rozdíl v porovnání s TCP/IP modelem je, že má 7 vrstev místo 5 – OSI přidává 2 nové vrstvy. Vrstvy OSI modelu jsou:

- Aplikační,
- Prezentační,
- Relační,
- Transportní,
- Síťová,
- Linková,
- Fyzická.

Prezentační vrstva dodává a formátuje vyměňovaná data. Tento úkol vykonává pomocí komprese a šifrování dat. Také se stará o popis dat a tím usnadňuje práci aplikační vrstvě, která se nemusí starat o formát (může se lišit mezi zařízeními), ve kterém jsou data ukládána. Relační vrstva vytváří, ukončuje, synchronizuje a obnovuje relační spojení, ve kterém řídí výměnu dat. Spojení linkové a fyzické vrstvy je identické s vrstvou síťového rozhraní u TCP/IP. (1)



Obrázek č. 4: OSI Model (5)

3.4 Monitoring

Monitoring sítě se zabývá používáním softwarových a hardwarových systémů k neustálému sledování stavu zařízení v síti. Monitorování pomáhá síťovým a systémovým administrátorům identifikovat případné problémy předtím, než by mohly ovlivnit provoz podniku. Ať se jedná o menší podnik s 50 prvky či velkou organizaci s 1000 prvky, nepřetržitý monitoring pomáhá rozvoji a údržbě výkonnosti sítě s co nejmenšími výpadky. V podnicích se běžně používají aplikace, které jsou instalovány na serverech v lokální síti daného podniku či v datovém centru. Služby těchto serverů jsou používány hostiteli (zaměstnanci) v rámci podnikové sítě. Servery poskytují další nástroje pro správu sítě a jejich uživatelů např. DNS, Active Directory, DHCP atd. Přítomnost podnikových aplikací na serverech si vyžaduje jejich konstantní monitorování. K tomu, abychom mohli efektivně monitorovat síť, je potřeba disponovat:

- Daty a informacemi ze síťových zařízení. Například: dostupnost, vytížení zdrojů.
- Aplikací nebo monitorovacím systémem, který je schopný shromažďovat, zpracovávat a prezentovat data v uživatelsky přívětivém formátu. Tento software by měl také být

schopný upozorňovat administrátory na hrozící problémy v případě překročení mezních hodnot.

- Protokolem či metodou pomocí které budeme transportovat informace mezi sledovaným zařízením a monitorovacím softwarem. (6)

3.4.1 Základní způsoby

Základní monitorování můžeme provádět pomocí příkazové řádky bez pomoci speciálního softwaru. Monitorovací softwary mohou tyto příkazy používat v rámci svých funkcí, ale jsou schované za grafickým rozhraním. Příkazy, které můžeme využít k monitorování sítě:

- PING – Příkaz umožnuje testovat dosažitelnost a odezvu zařízení v síti.
- TRACERT – Sleduje trasu paketů po cestě ke svému adresátovi. Zobrazuje odezvu a informaci o každém uzlu, přes kterou pakety projdou.
- IPCONFIG – Zobrazí síťové adaptéry a jejich nastavení.
- NETSTAT – Zobrazuje aktivní TCP připojení a porty, které má otevřené. Také je schopen zobrazit statistiky Ethernetu, IP směrovací tabulku, IPv4 a IPv6 statistiky.

3.4.2 Disky

Organizace ukládají data, která mohou obsahovat důvěrné osobní údaje, na diskové pole. Problémy s těmito disky mohou vážně ovlivnit provoz organizace. Monitorování disků je možné těmto problémům předcházet. A to pomocí upozornění v případě dovršení kritických hodnot. Na discích monitorujeme:

- Čtení/sek – Kolik čtecích operací se provádí za sekundu.
- Zápis/sek – Kolik zápisových operací se provádí za sekundu.
- Délka fronty – Počet čekajících požadavků na operace zápisu a čtení.
- Doba zaneprázdnění – Procento času, ve kterém je disk zaneprázdněn vykonáváním čtení a zápisu. (6)

3.4.3 Aktivní síťové prvky

Aktivní síťové prvky, zejména switche, routery a firewally, plní funkce jako směrování, připojení, chránění sítě či filtraci toků dat. Tento hardware pomáhá udržovat celou IT infrastrukturu. Selhání tohoto hardwaru může vést k výpadku celé sítě. U síťových prvků monitorujeme:

- Dostupnost.

- Využití – Konstantní stoprocentní využití může vést k selhání některých funkcí zařízení.
- Teplota – Vysoká teplota ovlivňuje výkon zařízení. V extrémních případech může vést k úplnému poškození.
- Propustnost dat.
- Rychlost ventilátoru – Sledováním otáček ventilátoru víme, že ventilátor funguje a plní funkci chlazení, kterým vyrovnává teplotu zařízení.
- Stav napájecího zdroje – Výkyv v napájení může vést k poruše zařízení. (6)

3.4.4 Servery a jejich služby

Servery jsou navrženy k tomu, aby nabízely určité služby. Například: mailový server ukládá a zasílá internetovou poštu mezi svými klienty. Print server připojuje tiskárny k počítačům a spravuje tiskové úlohy. Aplikační server hostuje software a jeho data. Hlavním aspektem serverů je, že služby a data svým klientům nabízí vzdáleně pomocí sítě, čímž není funkčnost služby vázána na klientovo zařízení. Obzvlášť ve firemním prostředí je důležité, aby tyto servery a jejich služby udržovali síťoví administrátoři v nepřetržitém běhu. Na serverech monitorujeme:

- Dostupnost.
- Doba provozu (uptime) – Doba, co server běží bez restartu nebo vypnutí.
- Využití procesoru.
- Teplota.
- Propustnost dat.
- Volné místo RAM, Disků.
- Běžící služby a výkon, který využívají – Na serveru může běžet služba, která není potřebná a zbytečně využívá výpočetní prostředky či služba s podvodnými úmysly (v případě kyberútoku). Také může služba využívat neadekvátní množství výkonu např. z důvodu zaseknutí, chyby. (7)

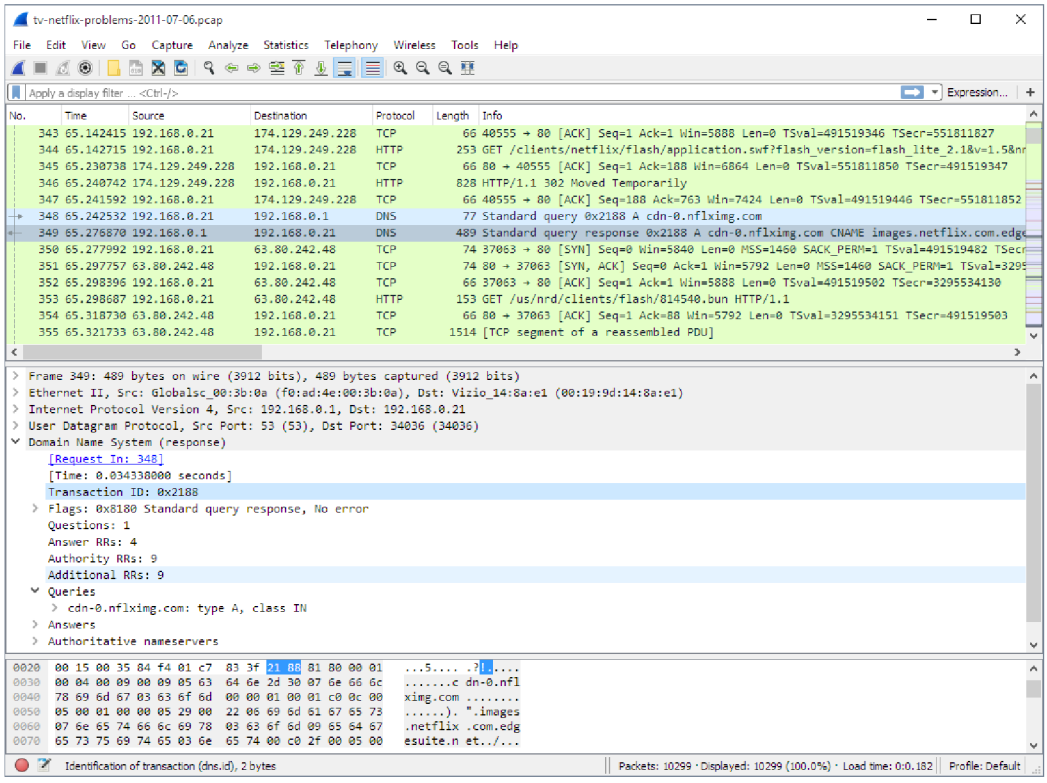
3.4.5 Síťový provoz

Monitorování síťového provozu sleduje objem a vlastnosti stahovaných a nahrávaných dat, které se pohybují po lokální síti. Stav síťového provozu ovlivňuje kvalitu síťového připojení, protože velký provoz může způsobit pomalejší přenos dat po síti. Díky analyzování síťového provozu identifikujeme slabá místa (aj. bottleneck) či problémy se šířkou pásma, které mohou

být způsobeny vysokým počtem uživatelů. Bezpečnost sítě je také zlepšena, jelikož neobvykle velký síťový provoz může značit možný kyberútok. (6)

3.4.6 Wireshark

Wireshark je grafická aplikace, která se používá pro analýzu paketů. Jedná se o tzv. packet sniffer. Aplikace nejprve naslouchá v reálném čase síťovému připojení v zařízení, ve kterém je spuštěna. Poté zachytí celý proud provozu a graficky ho interpretuje. Zachycené pakety je poté možné prohlížet a filtrovat podle specifických potřeb uživatele. Hlavní využití tohoto programu spočívá v diagnostice a řešení problému se sítěmi. (8)



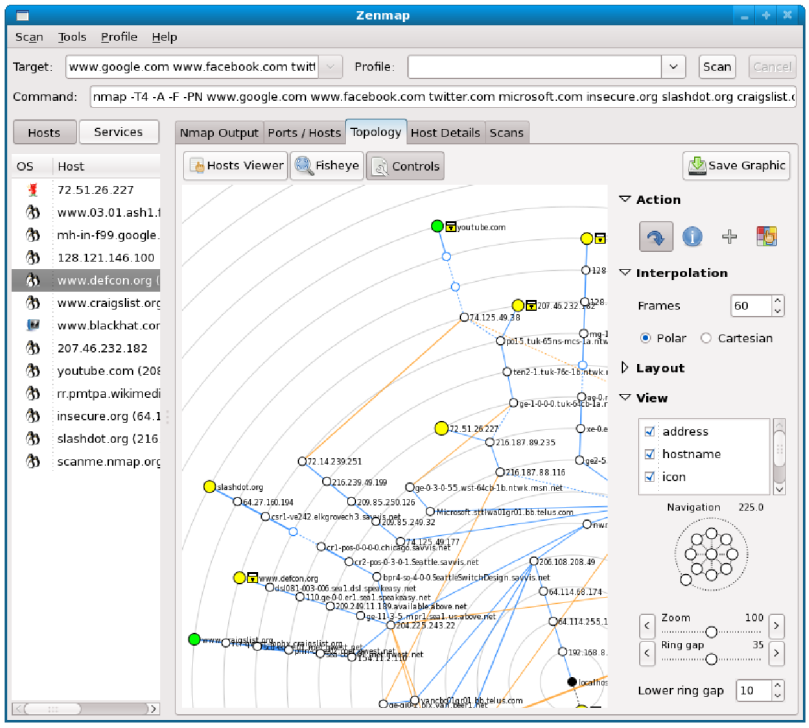
Obrázek č. 5: Wireshark (9)

3.4.7 Nmap

Nmap je síťový skener s otevřeným zdrojovým kódem vyvinutý Gordonem Lyonem. Byl navržen tak, aby byl schopný analyzovat rozsáhlé sítě i jednotlivé zařízení. Disponuje mnoha funkcemi např. rozpoznaní otevřených portů, zařízení připojené k síti a zranitelnosti sítí. Z tohoto důvodu je využíván správci sítě k mapování a bezpečnostním auditům. (10)

3.4.7.1 Zenmap

Jedná se o oficiální grafickou nadstavbu příkazového programu Nmap. Zenmap byl vytvořen za účelem usnadnit práci začátečníkům a zároveň poskytovat pokročilé funkce zkušenějším uživatelům. Kvůli usnadnění práce program umožnuje uložení skenování do jednotlivých profilů, které je možné poté opětovně spouštět. Výsledky analýzy lze ukládat a zobrazovat později. Program také umožnuje výsledky skenování vzájemně porovnávat a zobrazit, jak se od sebe liší. (11)



Obrázek č. 6: Zenmap (11)

3.4.8 PuTTY

PuTTY je aplikace s otevřeným zdrojovým kódem, která byla vyvinuta Simonem Tathamem. Jedná se o emulátor terminálu. Tato aplikace pracuje se síťovými protokoly jako SSH, Telnet a Rlogin. Zmíněné protokoly jsou používány ke vzdálené relaci po síti. V praxi se tento program využívá ke vzdálené správě a konfiguraci síťových prvků a serverů. (12)

3.5 SNMP

SNMP je zkratka pro Simple Network Monitoring Protocol. SNMP je nejrozšířenějším síťovým protokolem pro správu a monitorování zařízení připojených v síti. Princip jeho fungování je založen na modelu manažer/agent pomocí formátu požadavek/odpověď. Tento protokol je zabudovaný v téměř každém zařízení, jako jsou routery, switche, servery, firewally, přístupové body. SNMP je obvykle zaváděn pomocí UDP. To znamená, že na rozdíl od TCP nefunguje při přenosu spolehlivé doručování informací. UDP odesílá datagramy příjemci bez ohledu na to, zda jsou přijímány či nikoliv. SNMP používá UDP port 161 pro komunikaci mezi manažery a agenty (tzv. polling) a UDP port 162 pro zasílání zpráv o výskytu událostí (trapy). (14, 15)

3.5.1 Verze

- SNMPv1 – Původní verze protokolu, která byla uvedena v roce 1988 skupinou výzkumných pracovníků na univerzitě Carnegieho-Mellonových. V roce 1990 byla schválena IAB (Internet Architecture Board) jako internetový standard. Konfigurace je snadná, protože probíhá ve formě prostého textu. Ačkoliv svůj cíl jakožto otevřený standardní protokol splňuje, v mnoha klíčových oblastech má své nedostatky, například podpora pouze 32-bitových čítačů či nízká úroveň zabezpečení.
- SNMPv2c – Navržen v roce 1993. Přidává novou metodu Inform, která umožňuje potvrzení o přijetí zprávy a odpověď na ni. Další výhodou je vylepšená metoda SET a lepší zpracovávání chyb.
- SNMPv3 – Jedná se o nejnovější verzi protokolu vydanou v roce 1998. Rozdíl oproti předchozím verzím je převážně ve zvýšení úrovně zabezpečení. Dále přidává tzv. „EngineID“ identifikátor, který slouží k jednoznačné identifikaci entit. Jeho architektura nabízí nový USM (User-based Security Model) pro zabezpečení zpráv a VACM (View-based Access Control Model) pro řízení přístupů. Tyto bezpečnostní modely mají především 2 podoby:
    - Ověřování – Zajišťuje, aby byly zprávy čteny pouze zamýšleným příjemcem. Ke každé zprávě je přidělen speciální klíč, který se odvíjí od Engine ID entity. Speciální klíč je poté sdílen s příjemcem, který ho použije pro obdržení zprávy.
    - Šifrování – SNMP zprávy jsou šifrovány, aby nemohly být čteny neoprávněnými uživateli. Tato funkce je obzvlášť užitečná v případech, kdy je komunikace SNMP vedena přes internet. (14, 16)

3.5.2 Komponenty

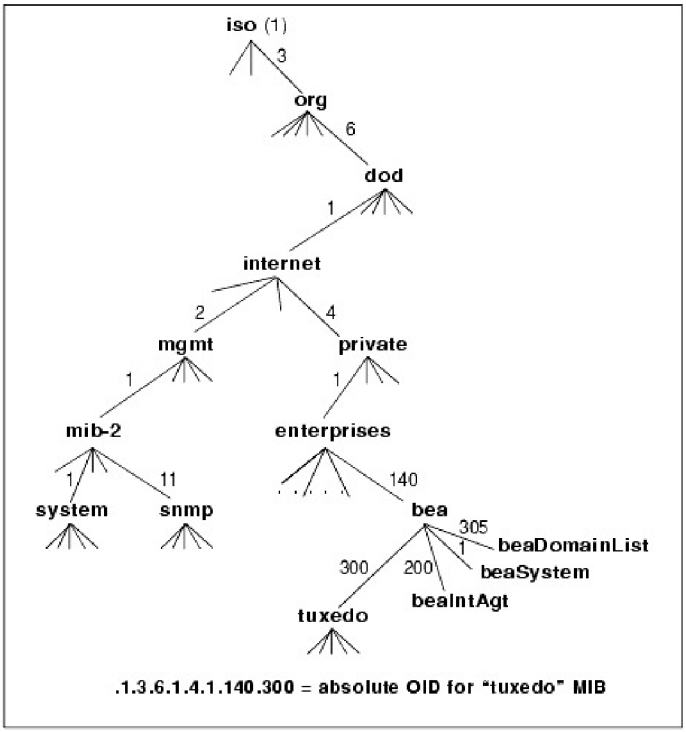
3.5.3 MIB

Management information base (MIB) je datová struktura, která specifikuje formát výměny informací v SNMP architektuře. MIB určuje, jaké informace lze z SNMP monitorovaných zařízení získat, a co na nich lze změnit a nakonfigurovat. Velké množství MIB je definováno normalizačními orgány, například Internet Engineering Task Force (IETF) nebo International Organization for Standardization (ISO). MIB také definují výrobci IT zařízení, jako je Cisco, a dodavatelé softwaru, jako jsou Microsoft a Oracle. Spravované objekty, které se nachází v MIB se rozlišují pomocí identifikátorů objektů. MIB organizuje OID hierarchicky, tak aby je bylo možné reprezentovat stromovou strukturou. Tato datová struktura je ukládána jako textový soubor s příponou mib. (15, 17)

3.5.4 Identifikátory objektů

OID (Object Identifier) jednoznačně identifikuje spravované objekty pomocí posloupnosti celých čísel oddělených tečkami. Jsou dva typy spravovaných objektů:

- Skalární – Objekty, které mají pouze jedinou instanci.
- Tabulkové – Objekty, které mají více souvisejících instancí.



Obrázek č. 7: Hierarchie a formát identifikátorů objektů SNMP MIB (17)

3.5.5 Manažer

Manažer SNMP je centrální systém, který je zodpovědný za komunikaci se zařízeními s agenty SNMP. Manažer se těchto agentů dotazuje, získává odpovědi, vyvolané události a nastavuje v nich proměnné. Získaná data jsou ukládána do MIB jako sdílená databáze mezi agentem a manažerem. Tato data manažer shromažďuje z důvodu správy poruch, řízení výkonu a plánování kapacity. Aktivně vyžaduje, aby monitorovaná zařízení odesílala SNMP aktualizace v pravidelných intervalech. Bývá také označován jako NMS (Network Management station) či SNMP server. (15)

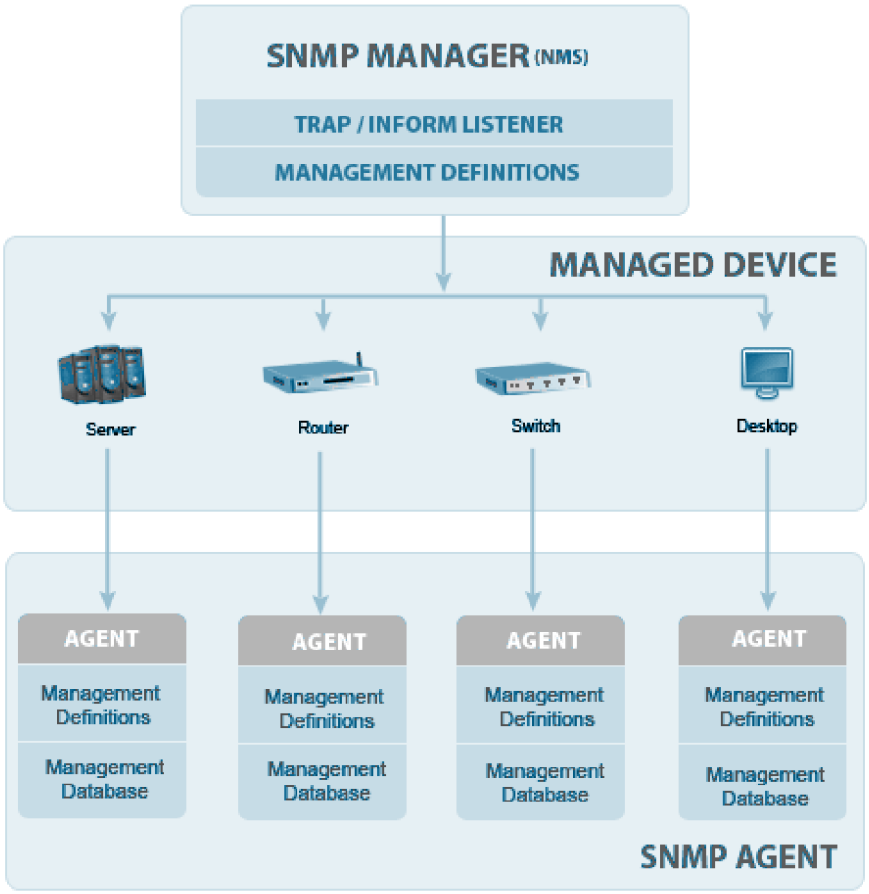
3.5.6 Agent

Agent SNMP je software, který je konstantně spuštěn na SNMP monitorovaném zařízení či službě. Tento software shromažďuje, ukládá a přenáší data o zařízení, na kterém běží. Na základě požadavků od SNMP manažera vykonává i různé další akce. (15)

3.5.7 Metody

SNMP disponuje metodami (příkazy), pomocí kterých mezi sebou prvky systému komunikují. Mezí základní funkce patří příkazy pro čtení a zápis, např. resetování hesla či změna konfiguračního nastavení. SNMP podporuje následující metody:

- GET – Účelem tohoto příkazu je získání jedné či více hodnot uložených v proměnných ze spravovaného zařízení.
- GET NEXT – Podobná operace jako GET s rozdílem, že GET NEXT získává hodnotu dalšího objektového identifikátoru v MIB hierarchii.
- GET BULK – Požadavek, který je využíván k získání velkých tabulek dat pomocí řetězení několika metod GET NEXT.
- SET – Metoda, kterou používá manažer k modifikování nebo přiřazení hodnoty či příkazu spravovaného zařízení.
- TRAP – Mechanismus přerušení. Jedná se o signál, který zasílá agent manažerovi v případě výskytu určité události. Například při dovršení kritických hodnot apod.
- Response – Příkaz, který používá agent k zasílání odpovědí manažerovi.
- Inform – Potvrzuje obdržení zprávy. V případě neobdržení je zasílán znovu. (15)



Obrázek č. 8: Komunikační diagram SNMP (18)

3.6 Monitorovací řešení

Trh se softwarem pro monitorování sítě je velice rozsáhlý. V dnešní době firmy sahají po komplexních řešeních, která dokážou vykonávat všechny potřebné funkce pod jednou střechou. Mezi funkce, které jsou v monitorovacích systémech vyhledávány, patří:

- Automatické zjišťování zařízení v síti,
- Mapovač topologie sítě,
- Aktivní sledování běžících zařízení pomocí SNMP,
- Schopnost analyzovat výkon sítě v průběhu času,
- Grafická interpretace shromažďovaných dat pomocí tabulek a grafů,
- Upozorňovací systém pomocí e-mailu či SMS.

Tyto monitorovací systémy se dále dělí na:

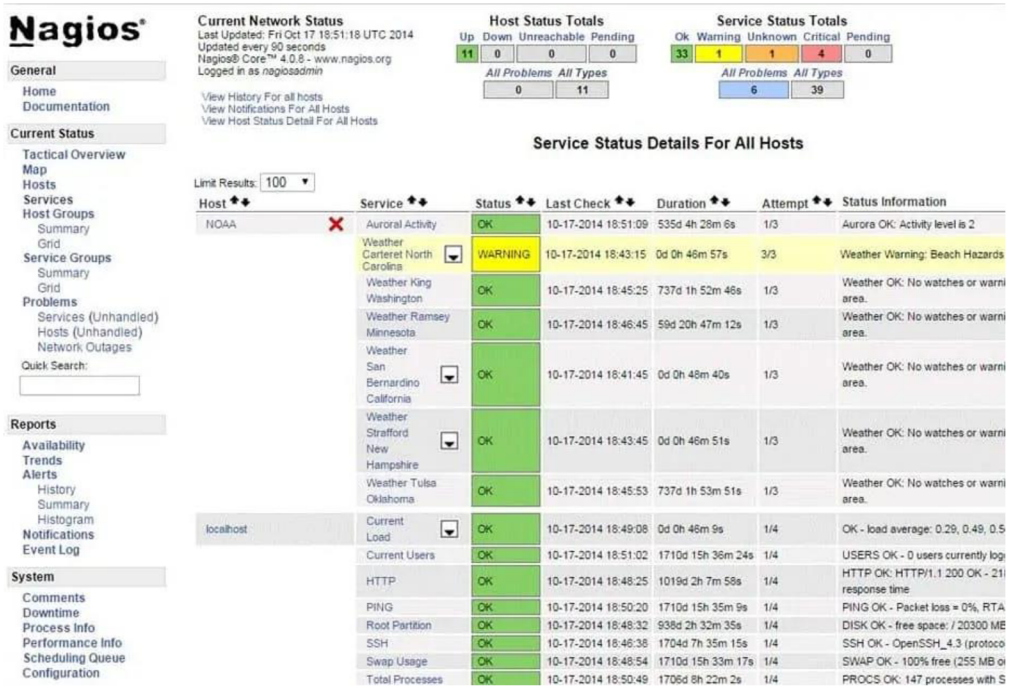
- Open source – Software disponuje otevřeným zdrojovým kódem, který je volně dostupný všem. Většina takových systému je zdarma. Nicméně i open source software může být zpoplatněn.
- Proprietární – Software, kde autor specifikuje možnosti jeho používání – typicky pomocí licence (EULA). Jeho zdrojový kód je uzavřený (aj. closed source). Obvykle je takový software zpoplatněn.

Vzhledem k tomu, že open source monitorovací systémy nemusí být nutně zdarma a proprietární nutně zpoplatněny, jsou následující rozebírané monitorovací řešení děleny podle toho, zda jsou zpoplatněny či nikoliv. (19)

3.6.1 Bezplatné

3.6.1.1 Nagios Core

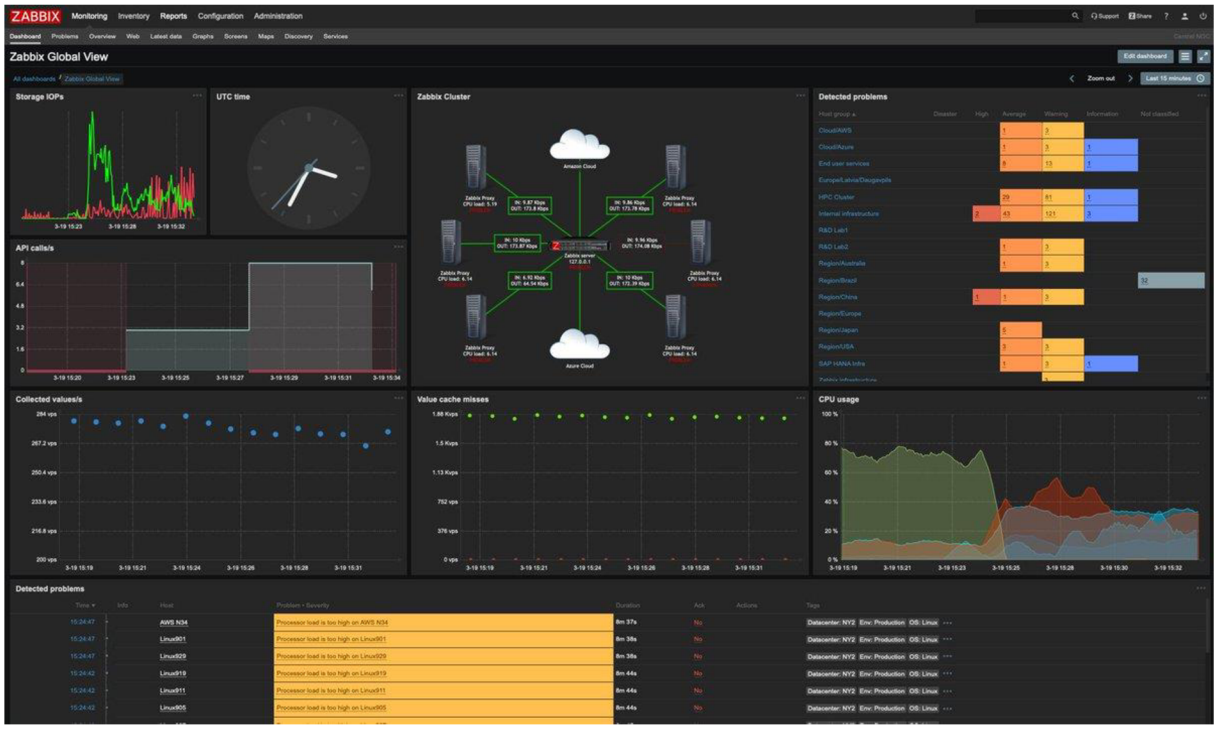
Nagios Core, dříve pouze Nagios, je světově známý monitorovací software s otevřeným zdrojovým kódem. Toto monitorovací řešení nabízí základní funkce jako plánovač a zpracovatel událostí. Dále nabízí správce upozornění pro sledované prvky. Vzhledem k tomu, že se jedná o software s otevřeným zdrojovým kódem, existuje mnoho doplňků, díky kterým lze systém přizpůsobit konkrétním potřebám. Pomocí doplňků lze přidat například push oznámení či grafické znázornění dat. (20)



Obrázek č. 9: Nagios (20)

3.6.1.2 Zabbix

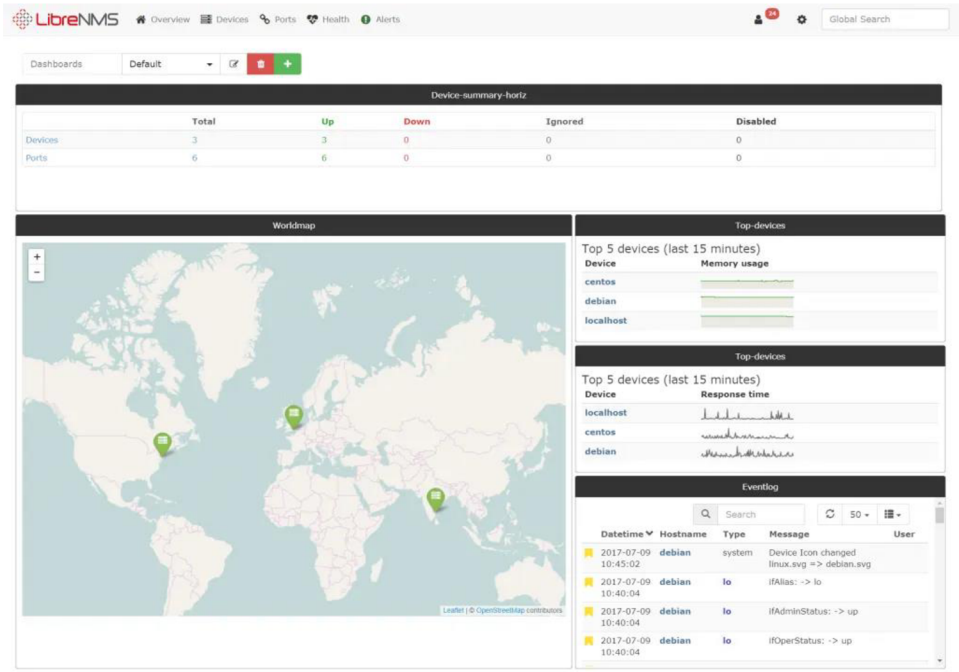
Monitorovací systém Zabbix byl navržen pro firmy podnikové třídy. Jakožto monitorovací software s otevřeným zdrojovým kódem dokáže monitorovat výkon a dostupnost serverů či síťových zařízení. Také je schopný monitorovat webové aplikace a databáze. Zabbix používají tisíce společností po celém světě např. DELL, Orange. (21)



Obrázek č. 10: Zabbix (22)

3.6.1.3 LibreNMS

LibreNMS je monitorovací systém založený na PHP/MySQL. Podporuje širokou škálu síťového hardwaru a operačních systémů jako Cisco, Linux, FreeBSD. Nabízí řadu funkcí, například automatické zjišťování a přizpůsobitelné upozorňování. LibreNMS umožnuje plný přístup k API pro správu, tvorbu grafů. Tento monitorovací systém disponuje i mobilní aplikací pro iPhone a Android. (23)

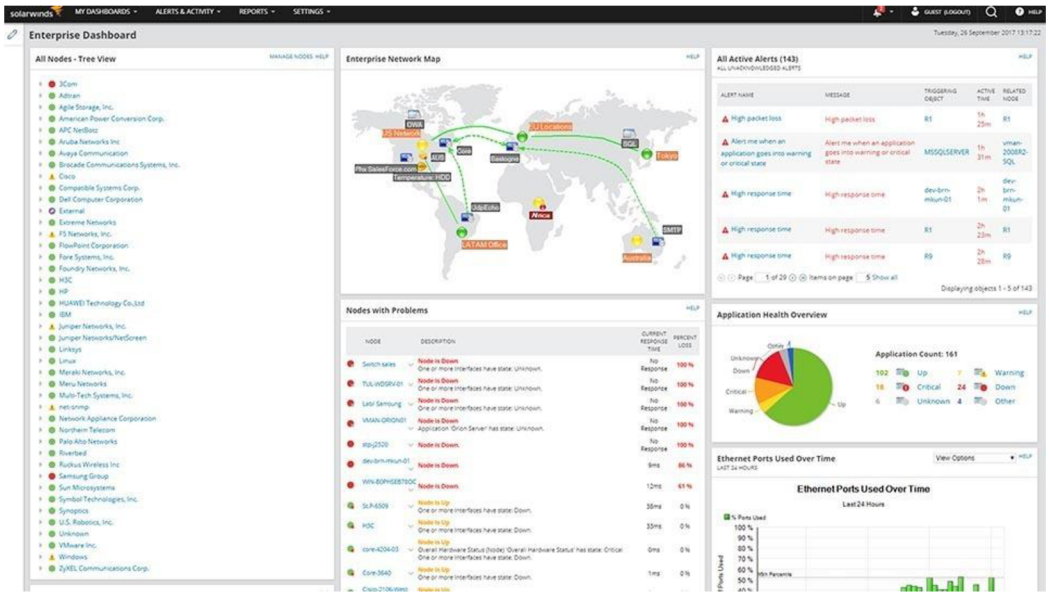


Obrázek č. 11: LibreNMS (24)

3.6.2 Komerční

3.6.2.1 SolarWinds Network Performance Monitor

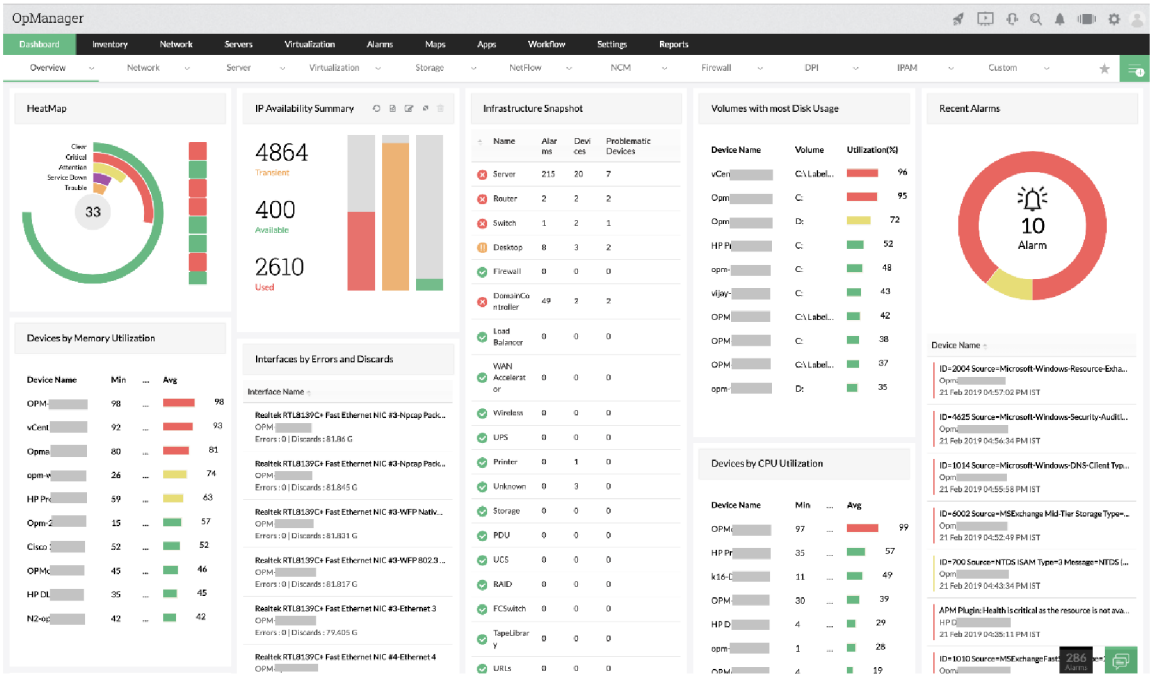
SolarWinds Network Performance Monitor je komplexní nástroj pro monitorování výkonu sítě, který sleduje zařízení pomocí SNMP. Tento nástroj zvládá i analýzu síťového provozu. Nabízí funkci automatické zjišťování, která v reálném čase vytváří inventář majetku a topologii sítě. Stejně jako většina monitorovacích systému disponuje funkcionalitou výstrah a hlášení. Jako jedno z mála monitorovacích řešení beží na Windows serverech. (19)



Obrázek č. 12: SolarWinds (25)

3.6.2.2 ManageEngine OpManager

Kromě monitorovacího systému je ManageEngine OpManager softwarem pro správu infrastruktury a výkonu aplikací (s doplňkem APM). ManageEngine OpManager dokáže spravovat síť, servery, konfiguraci sítě, poruchy a výkon. Zvládá i analýzu síťového provozu a je dodáván s před konfigurovanými šablonami síťových zařízení, které obsahují předdefinované parametry monitorování a intervaly konkrétních typů zařízení. (19)



Obrázek č. 13: OpManager (26)

3.6.2.3 PRTG Network Monitor

PRTG Network Monitor využívá k monitorování sítě technologie SNMP, WMI, REST API atd. Zařízení, systémy, provoz a aplikace v síti zobrazuje v hierarchickém zobrazení. PRTG disponuje snadným uživatelským rozhraním. Také umožňuje skenovat síťové segmenty dle definovaného rozsahu IP adres. (19)

Obrázek č. 14: PRTG (27)

4 Vlastní práce

Na základě získaných poznatků z teoretické části jsem se zaměřil na implementaci a konfiguraci zvoleného monitorovacího systému pro síťovou infrastrukturu podniku synlab czech, s. r. o. V této společnosti jsem druhým rokem zaměstnán na IT oddělení s pozicí specialisty pro podporu infrastruktury a díky tomu jsem měl dost času se s tamní IT infrastrukturou dobře seznámit. Získané zkušenosti ve firmě mi umožnily získat v rámci řešení této práce plný přístup k síťové infrastruktuře.

4.1 Vybraný podnik

Podnik synlab czech s. r. o. je od svého založení v roce 1993 členem německé skupiny SYNLAB Group. Skupina SYNLAB Group se nachází ve více než 36 zemích světa a má přes 20 tisíc zaměstnanců. Oblastí podnikání firmy je poskytování zdravotních služeb a laboratorní vyšetření. Synlab v česku zaměstnává přibližně tisíc zaměstnanců a má přes 60 odběrových pracovišť a 11 laboratoří. (28)

4.2 Analýza síťové infrastruktury

Před samotným výběrem a následnou implementací monitorovacího systému je nejprve zapotřebí kompletně zmapovat síť a zařízení v ní připojené. U jednotlivých typů zařízení je také nutné zvážit jejich důležitost a na základě toho určit, zda by měly být monitorovány. Vzhledem k rozsáhlosti sítě není efektivní monitorovat každé zařízení.

4.2.1 IP rozsahy

Fyzické lokality (pobočky) jsou virtuálně rozděleny pomocí jednotlivých podsítí. Tyto podsítě zvyšují efektivitu datových proudů a udržují přehlednost. Celkově tyto rozsahy umožnují až 256 lokalit, do kterých lze zapojit až 254 různých hostitelů. V současné době je pro lokality využíváno 105 podsítí (včetně virtuálních LAN) s více než 2000 hostiteli.

	Třída	maska	CIDR	rozsah
Lokality	C	255.255.255.0	/24	192.168.0.x - 192.168.256.x
Hostitelé (v lokalitách)		255.255.0.0	/16	192.168.x.0 - 192.168.x.254

Tabulka č. 1: IP Rozsahy (zdroj: autor)

Pro hostitele v lokalitách jsou dále vyhrazeny stanovené rozsahy, což napomáhá správě, dokumentaci a orientaci v síťové infrastruktuře jednotlivých lokalit. Tento rozsah je dělen podle velikosti pobočky:

- Velká lokalita (100 a více stanic)
    - Servery, úložiště –192.168.x.1-50.
    - Stanice – 192.168.x.51-199.
    - Tiskárny, kamery, wifi – 192.168.x.200-240.
    - Externí zařízení, jiné (teploměry, čidla apod.) – 192.168.x.241-250.
    - Síťové prvky – 192.168.x.251-253.
    - Brána – 192.168.x.254.
- Malá lokalita (do 100 stanic)
    - Servery, úložiště – 192.168.x.1-50.
    - Stanice – 192.168.x.51-150.
    - Portboxy, analyzátory – 192.168.x.151-170.
    - Kamery, wifi – 192.168.x.171-199.
    - Tiskárny – 192.168.x.200-240.
    - Externí zařízení, jiné (teploměry, čidla apod.) – 192.168.x.241-250.
    - Síťové prvky – 192.168.x.251-253.
    - Brána – 192.168.x.254.

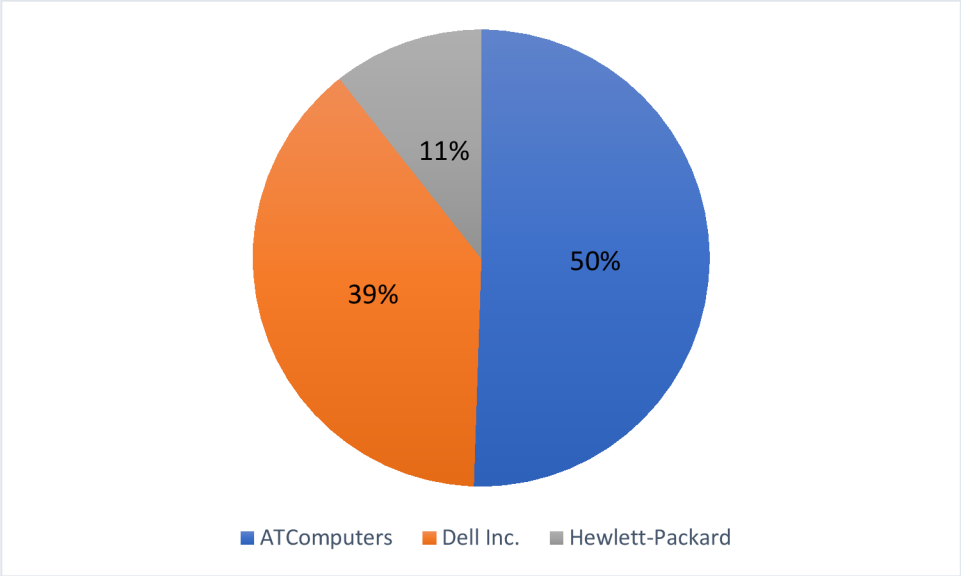
4.2.2 VLAN

Větší pobočky rozdělují podsítě pomocí tzv. VLAN neboli virtuálních lokálních sítí. VLAN logicky rozdělují síť bez ohledu na jejich fyzické uspořádání. Hlavním důvodem pro používání virtuálních lokálních sítí je zvýšení zabezpečení dat a řízení síťového provozu. Zvýšení zabezpečení spočívá v oddělení komunikace mezi zařízeními, která se nachází ve stejné fyzické síti.

4.2.3 Zařízení

K síťové infrastruktuře podniku je připojena široká škála různých zařízení:

- Stanice – desktopy a notebooky, které jsou používány uživateli (zaměstnanci). Hlavním výrobcem tohoto hardwaru ve firmě synlab czech, s. r. o. je Dell Inc., avšak ve firmě se kromě toho také používají sestavené desktopy od minulého dodavatele AT Computers a.s. a notebooky od Hewlett-Packard. V síti se nachází zhruba 600 stanic.



Graf č. 1: Stanice v síti (zdroj: autor)

- Tiskárny – pro menší pracoviště se používají tiskárny výrobců HP, Oki či Brother. Na velkých pobočkách jsou na chodbách také velké multifunkční tiskárny Konica Minolta. Specialitou v této firmě jsou štítkové tiskárny Zebra, pomocí kterých se označují zkumavky se vzorky.
- Síťové prvky
    - Switche – díky spolupráci s mateřskou pobočkou v Německu se nedávno veškeré switche v infrastruktuře měnily na model od společnosti Cisco, konkrétně řada Catalyst 9200. Kvůli zvýšení počtů portů bez přidělávání práce s konfigurací jsou tyto switche na velkých pobočkách zapojeny v jednom celku – tzv. stack.

Obrázek č. 15: switch Cisco Catalyst 9200 (29)

- Firewally – podobně jako switche byly všechny v rámci modernizace vyměněny na Fortinet FortiGate 60F.

Obrázek č. 16: firewall Fortinet FortiGate 60F (30)

- Přístupové body – všechny větší lokality mají oddělené bezdrátové sítě pro zaměstnance a hosty. Šíření těchto Wi-Fi sítí zajišťují přístupové body od výrobců Ubiquiti a Cisco.
- VoIP – interní hlasová komunikace pro zaměstnance prostřednictvím sítě. Tato komunikace je standardně oddělena od všech ostatních pomocí virtuální LAN. Ve firmě jsou používány IP telefony od společnosti Cisco.

- Analyzátory – zařízení v laboratořích, která jsou určeny k analýze krve a dalších typů vzorků v rámci nabízených vyšetření. Tyto analyzátory jsou prostřednictvím sítě a tzv. portboxů napojeny na laboratorní informační systém. Výrobci používaných analyzátorů v podniku jsou různorodí - např. Abbott, Bio-Rad a podobní. Veškerá komunikace těchto zařízení je oddělena od interní sítě pomocí separátní virtuální sítě.

Obrázek č. 17: analyzátor Abbott ARCHITECT c4000 (31)

- Portbox – jedná se o konvertor komunikačního rozhraní RS-232 (sériový port) na standardní Ethernet. Většina analyzátoru nedisponuje ethernetovým portem, a proto se používá tento konvertor prostřednictvím kterého se připojují do lokální sítě. Konfigurace tohoto zařízení probíhá pomocí vzdáleného terminálového připojení (SSH, Telnet) či webového rozhraní.
- Servery – v sítí se jich nachází přibližně 80 a každý plní svůj specifický účel. Velká část serverů využívá virtualizační technologii Hyper-V k rozdělení jednotlivých fyzických serverů na více virtuálních. Až na pár výjimek servery používají operační systém Windows Server.
    - OpenLims – Laboratorní informační systém běžící na aplikačním serveru. V tomto systému jsou evidovány pacienti a výsledky jejich vyšetření. Dále také řídí tisk štítků na zkumavky.
    - Selma – Aplikační server systému evidence laboratorního materiálu. Realizuje logistický pohyb lékařských požadavků a výsledků. Tento systém úzce komunikuje s laboratorním systémem OpenLims.
    - Řadič domény – Obsahuje databázi uživatelů, práv a ověřuje autentizační požadavky (Active Directory). Dále automaticky přiděluje novým hostitelům IP adresy (DHCP). IP adresám hostitelů jsou určovány názvy (DNS). Také interně řídí aktualizace operačního systému Windows pomocí služby WSUS.
    - Navision – Databázový server, na kterém je evidováno plánování podnikových zdrojů firmy.
    - Elisa – Docházkový systém.
    - Printserver – Řízení úloh tisků z tiskáren. Hlavní využití je u tzv. výsledkových tiskáren, které každý den tisknou tisíce papírových výsledků vyšetření z laboratorního systému OpenLims.
    - Sharepoint – Interní webový portál pro zaměstnance.

4.2.4 MPLS

V síti je zavedeno multiprotokolové přepojování podle návěstí. Zprostředkovatel tohoto přepojování v podniku je telekomunikační společnost Vodafone. Tato MPLS umožňuje vysokorychlostní propojení vzdálených poboček a datacenter, aplikačních serverů.

4.3 Zhodnocení monitorování

U jednotlivých zařízení v síti bude určena jejich důležitost ve firmě dle bodového hodnocení 1 – nejnižší až 5 – nejvyšší. Dále bude slovně zhodnocena jejich potřeba pro monitorování.

Název zařízení	Důležitost	Zhodnocení
Stanice	NA (záleží na pracovní pozici vlastníka)	Jednotlivé stanice není potřeba monitorovat. V případě problémů se zařízením nás upozorní zaměstnanec, který ho využívá.
Tiskárny	4 (velké tiskárny)	Monitorování menších tiskáren je zbytečné. Nicméně funkčnost velkých multifunkčních tiskáren, které jsou používány pro tisk výsledků je stěžejní a tím pádem by měly být monitorovány, a to jak dostupností, tak i počtem zbývajícího toneru.
Switche	5	Výpadek switche znamená odpojení veškerých zařízení v pobočce od interní i internetové sítě. Z tohoto důvodu je monitorování velice důležité.
Firewally	5	Firewall brání síť před možnými kyberútoky. Dále blokuje nežádoucí webové stránky. Monitorování těchto zařízení je nezbytné
Přístupové body	3	Na některých pobočkách je bezdrátové připojení preferovaným způsobem připojení k síti. Monitorování je vhodné.
Analyzátory	4	Správný chod analyzátorů zajištuje firmě příjem, výpadek může znamenat velké ztráty. Nicméně monitorování těchto zařízení již zajištují obsluhující pracovníci.
Portbox	4,5	Funkčnost analyzátorů závisí na portboxech, které je připojují k sítí. Monitorování dostupnosti je nutnost.
Server – OpenLims	4,5	Monitorování laboratorního informačního systému je prioritou.
Server – Selma	4	Bez funkčního aplikačního serveru Selma nemůžou odběrová pracoviště evidovat vyšetření – monitorování je nezbytností.
Server – Řadič domény	5	Řadič domény udržuje v síťové infrastruktuře systém – monitoring je nutný
Server – Navision	4	Funkčnost databázového serveru pro účetnictví a evidenci majetku je stěžejní. Monitorování je nezbytné
Server – Elisa	2	Monitoring je vhodný, ale dá se bez něj obejít. Nefunkčnost tohoto docházkového systému mohou nahlásit zaměstnanci.
Server – Printserver	4,5	Printserver řídí tiskové úlohy zaměstnanců a výsledků. Monitorování je potřebné.
Server – SharePoint	2	Zaměstnanecký portál používá téměř každý pracovník. Monitorování je vhodné.

Tabulka č. 2: Zhodnocení monitorování (zdroj: autor)

4.4 Zadání pro monitorovací systém

Potřebu pro monitorování sítě jsem podrobně probral se svým vedoucím. Společnost v minulosti již používala dva bezplatné monitorovací systémy:

- Zabbix – Vyhovoval díky své všestrannosti a možnosti konfigurace do nejmenších detailů. Nicméně důvodem, proč přestal být používán, bylo nedodělané a neintuitivní uživatelské rozhraní.
- LibreNMS – Byl nainstalován s cílem řešit problémy, které nastaly s předchozím monitorovacím systémem Zabbix. Tento cíl splnil, ačkoliv i tento systém měl své nedostatky. Jako třeba dlouhá prodleva zasílání upozornění či nepřehlednost grafů.

Na základě získaných poznatků ze zkušeností s předchozími monitorovacími systémy a konzultací s mým vedoucím bylo sestaveno následující zadání potřebných funkcí:

- Nepřetržité získávání dat o monitorovaných zařízeních pomocí protokolu SNMP.
- Přehledné grafické zobrazení získaných dat v grafech.
- Intuitivní uživatelské rozhraní.
- Uživatelský systém, který lze propojit s účty v Active Directory použitím LDAP serveru.
- Upozorňovací systém v případě kritických událostí prostřednictvím SMS či e-mailu.
- Konfigurační šablony, a to hlavně pro používané switche Cisco a firewally Fortinet.

4.5 Porovnání monitorovacích systémů dle zadání

V následující tabulce jsou porovnány monitorovací systémy z teoretické části vůči zadání.

	SNMP monitoring	Grafické zobrazení v grafech	Uživatelské rozhraní	LDAP propojení	Upozorňovací systém	Konfigurační šablony
Nagios Core	✓	✗	✓ (zastaralé)	✓	✓	✗
Zabbix	✓	✓	✓ (neintuitivní)	✓	✓	✓
LibreNMS	✓	✓ (nepřehledné)	✓	✓	✓ (prodlevy)	✓
SolarWinds	✓	✓	✓	✓	✓	✓
ManageEngine OpManager	✓	✓	✓	✓	✓	✓
PRTG Network Monitor	✓	✓	✓	✓	✓	✓

Tabulka č. 3: Porovnání monitorovacích řešení dle zadání (zdroj: autor)

Z tabulky vyplívá, že až na zastaralý Nagios, splňuje požadavky pro síťový monitoring podniku téměř každý monitorovací systém v porovnání.

4.6 Centreon

Výběrové řízení v podniku shledalo Centreon jako nejlepší monitorovací systém splňující stanovené zadání. Tento monitorovací systém byl vydaný v roce 2008 stejnojmennou společností. Centreon disponuje kompletním otevřeným kódem a je do 100 připojených zařízení zdarma. Jeho otevřený kód je založen na zdrojovém kódu Nagiosu. Funkce Centreonu lze dále rozšířit pomocí zpoplatněných či bezplatných doplňků. (32)

Obrázek č. 18: Centreon (33)

4.7 Architektury

Monitorovací systém Centreon lze implementovat několika způsoby a každý má svůj specifický případ užití. Jednotlivé komponenty systému lze instalovat na separátní fyzické servery např. kvůli rozložení zátěže, či zvýšení zabezpečení. Stavebními kameny těchto architektur jsou následující komponenty:

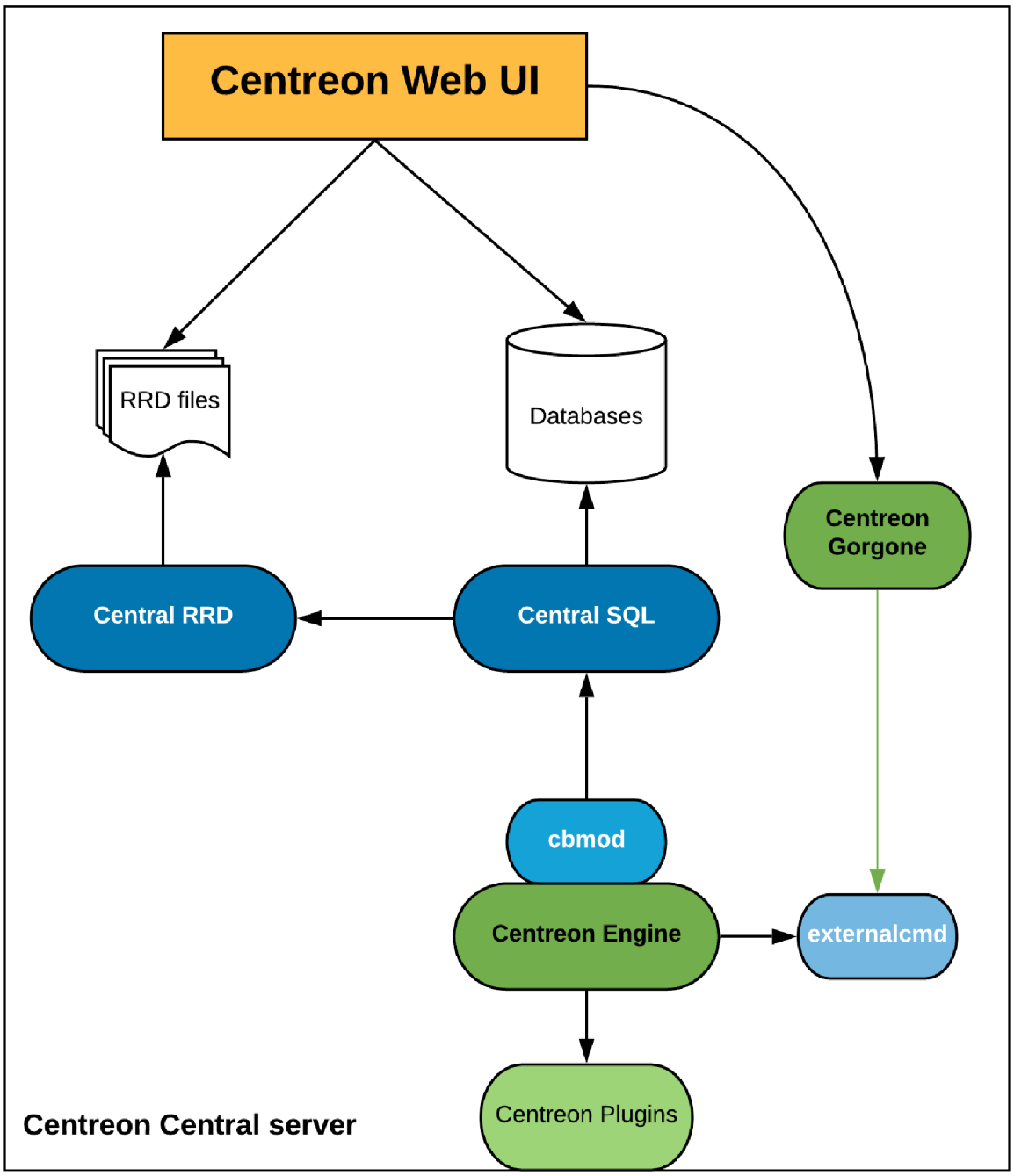
- Webový server Apache – Slouží k zobrazení grafického rozhraní prostřednictvím protokolu HTTP/S
- MariaDB – Databázový server, který je určen k ukládání konfigurací a získaných dat o monitorování a výkonu

- Monitorovací engine – Shromažďuje data o monitorovaných zařízeních. Tato data poté zasílá SQL Broker komponentě pomocí modulu cbmod.
- Broker – Vysílač monitorovacích událostí. Jakožto komunikační páteř celého systému je většina událostí v rámci Centreonu zpracována jedním nebo více jeho moduly. Následující seznam popisuje ty nejběžnější z nich:
    - SQL – Ukládání monitorovacích událostí v reálném čase do databáze typu SQL.
    - storage – Analýza a ukládání dat o výkonu do SQL databáze.
    - RRD – Generování a ukládání grafů ze získaných monitorovacích dat o výkonech ve formátu souboru RRD.
    - BAM – Výpočet stavu a dostupnosti obchodní činnosti.
    - Graphite – Zapisování monitorovacích dat o výkonu do nástroje pro generování grafů.
    - InfluxDB – Zapisování monitorovacích dat o výkonu do databáze typu InfluxDB.
- Gorgone – lehký, distribuovaný a modulární zpracovatel úloh, který pracuje jako tzv. deamon neboli program běžící na pozadí. Poskytuje sadu úloh, jako třeba:
    - Spouštění příkazů.
    - Odesílání souborů/složek.
    - Plánování úloh podobné unixovému cronu.
    - Odesílání nebo spouštění úloh prostřednictvím SSH. (35)

4.7.1 Jednoduchá architektura

V této architektuře jsou všechny komponenty monitorovacího systému na stejném fyzickém serveru. Entity v jednoduché architektuře jsou:

- Webové rozhraní Centreon,
- Databáze (MariaDB + RRD),
- Monitorovací engine,
- Broker. (35)



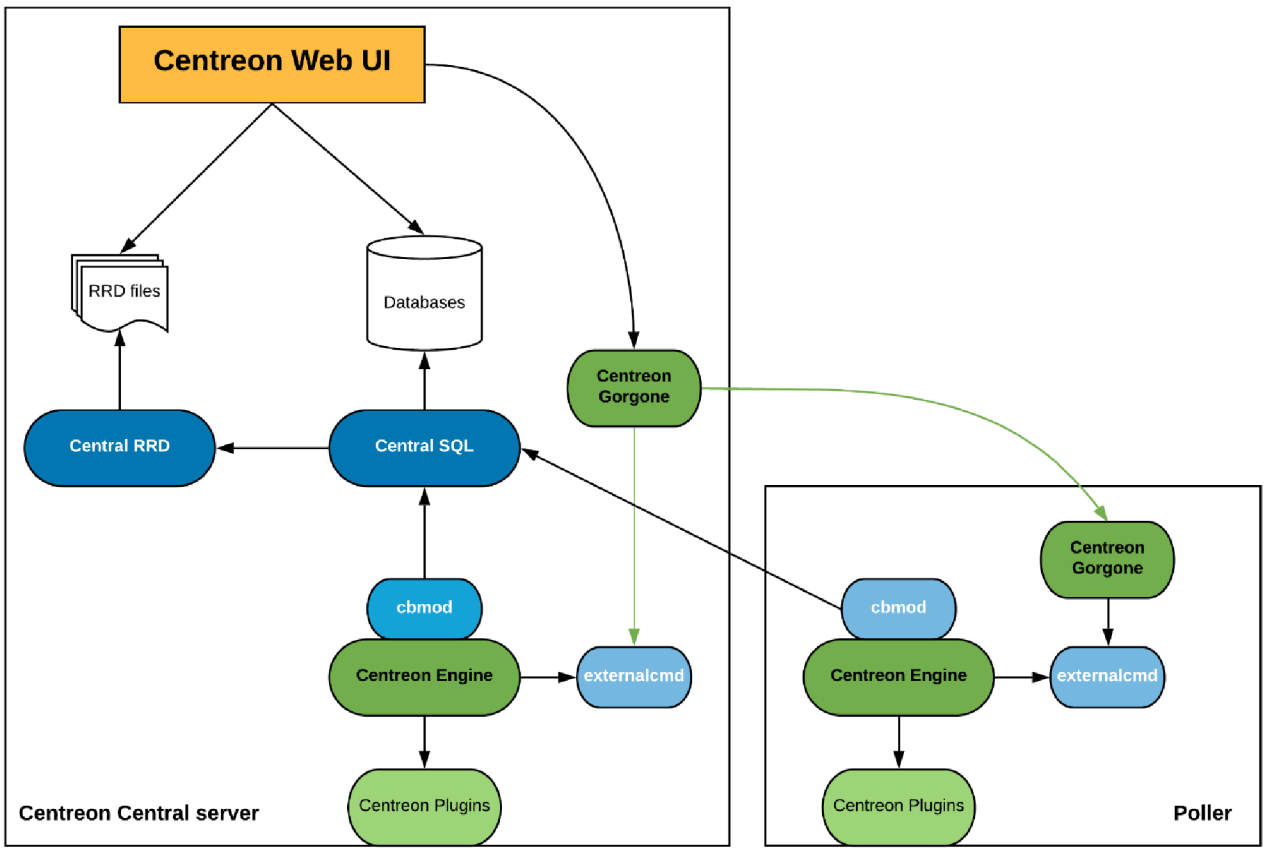
Obrázek č. 19: Diagram jednoduché architektury (35)

4.7.2 Distribuovaná architektura

Distribuovaná architektura rozděluje monitorovací systém na dva typy entit:

- Centrální monitorovací server, který je určen k zobrazování informací.
- Jeden či více vzdálených serverů, které sbírají data o monitorovaných zařízeních neboli v anglickém jazyce tzv. poller.

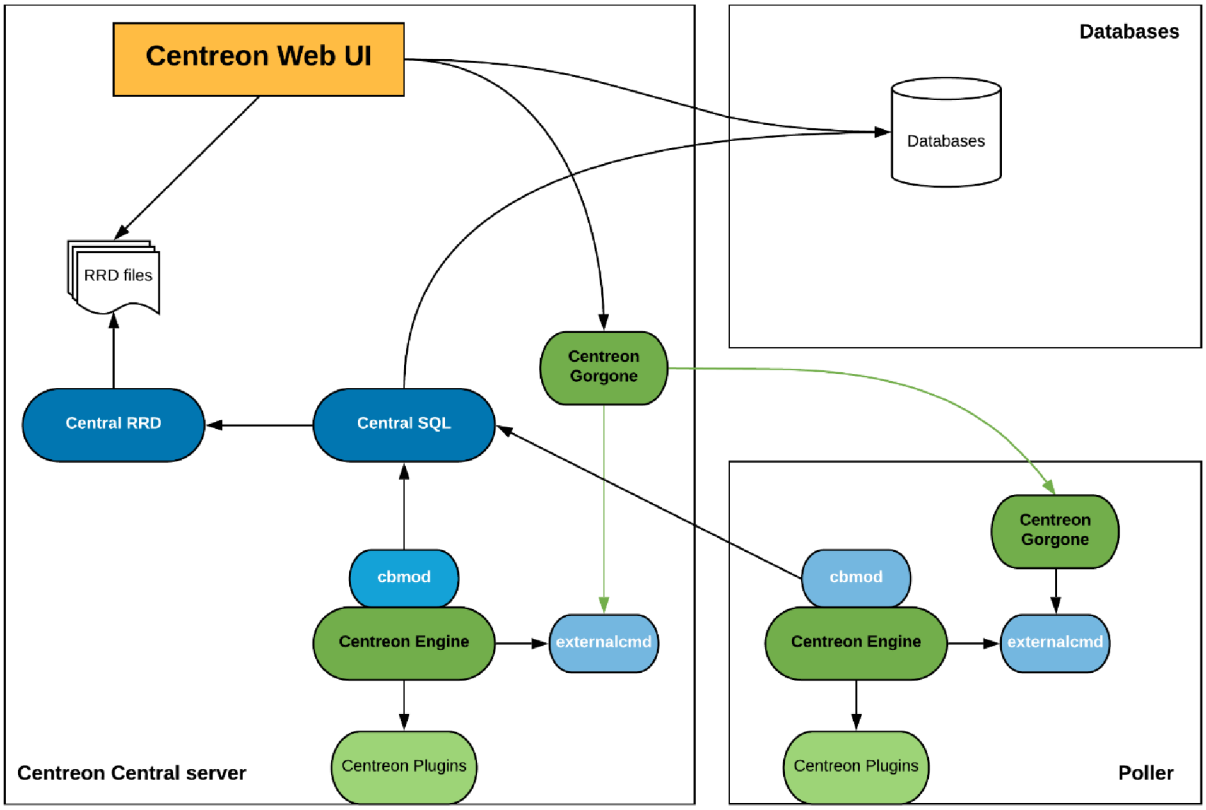
Výhoda této architektury spočívá v možnosti vyrovnání zátěže mezi více vzdáleně umístěnými servery pro sběr dat. Další výhodou je izolace síťových proudů. Pokud je potřeba monitorovat síť, která byla oddělena od těch ostatních z důvodu bezpečnosti je lepší praktikou umístit server pro sběr dat přímo do oddělené sítě. (35)



Obrázek č. 20: Diagram distribuované architektury (35)

4.7.3 Vzdálený DBMS

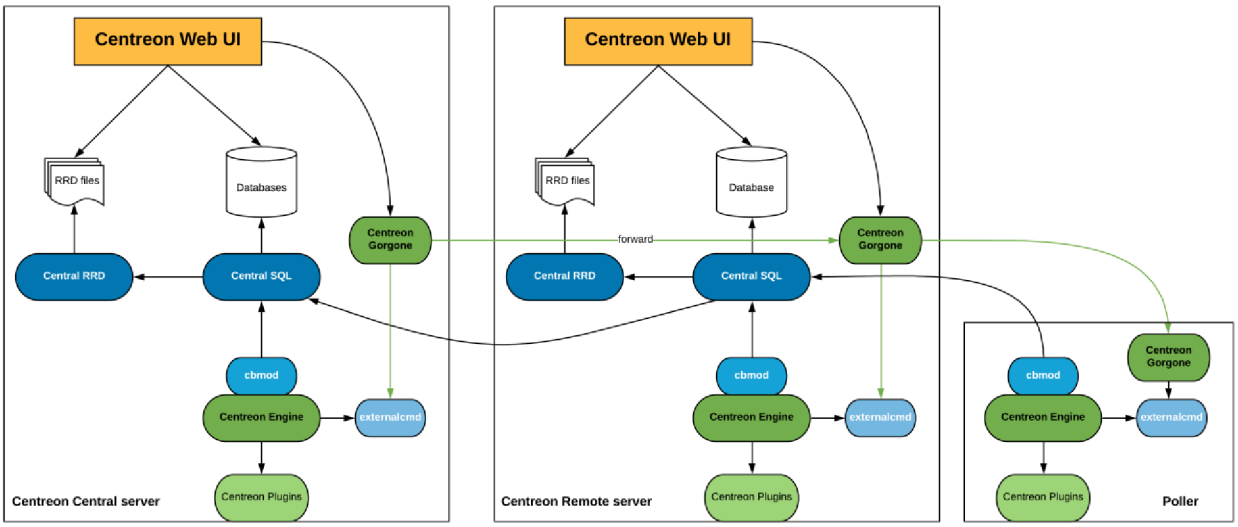
Tato architektura vychází z distribuované – disponuje odděleným centrálním serverem a jedním či více servery pro sběr dat. Z důvodu zvýšení zabezpečení je oddělený i databázový server na kterém jsou ukládány konfigurační parametry a data o monitorování, výkonu. (35)



Obrázek č. 21: Diagram architektury se vzdáleným DBMS (35)

4.7.4 Vzdálený server

Jedná se o další architekturu, která vychází z distribuované. Tato architektura obsahuje kromě centrálního a sběrového serveru i další vzdálené servery Centreon, které disponují stejnými komponenty jako centrální server. To znamená, že jednotlivé vzdálené servery pracují pouze s podmnožinou získaných dat z jejich pollerů a mají své vlastní webové rozhraní. Přičemž centrální server má přístup k datům všech vzdálených serverů. Tato architektura může být užitečná v rozsáhlých sítích (např. typu WAN). (35)



Obrázek č. 22: Diagram architektury se vzdáleným serverem (35)

4.7.5 Datové toky

K implementaci jedné z těchto architektur monitorovacího systému do síťové infrastruktury je zapotřebí znát následující tabulku datových toků:

Od	Do	Protokol	Port	Význam
Centrální server/Poller	NTP server	NTP	UDP 123	Synchronizace času
Centrální server/Poller	DNS server	DNS	UDP 53	Překlad doménových jmen
Centrální server/Poller	SMTP server	SMTP	TCP 25	E-mailové notifikace
Centrální server	LDAP(s) server	LDAP(s)	TCP 389 (636)	Propojení a následná autentifikace účtů k přístupu do webového rozhraní
Centrální server	DBMS server	MySQL	TCP 3306	Přístup k databázím Centreonu
Centrální server	HTTP Proxy	HTTP(s)	TCP 80, 8080 (443)	Připojení k webové proxy
Centrální server/Poller	Úložiště	HTTP (FTP)	TCP 80 (FTP 20)	Úložiště systémových a aplikačních balíčků

Tabulka č. 4: Datové toky (35)

Monitorovací systém Centreon dále používá tyto datové toky pro účely samotného monitorování:

Od	Do	Protokol	Port	Význam
Centrální server	Poller	ZMQ	TCP 5556	Export konfigurace Centreonu
Centrální server	Poller	SSH (legacy)	TCP 22	Export konfigurace Centreonu
Centrální server	Vzdálený server	HTTP(S)	TCP 80 (443)	Export konfigurace vzdáleného serveru
Poller	Centrální server	BBDO	TCP 5669	Přenos získaných dat
Poller	Síťové vybavení, servery atd.	SNMP	UDP 161	Monitorování
Síťové vybavení	Poller	Trap SNMP	UDP 162	Monitorování
Poller	Servery	NRPE	TCP 5666	Monitorování
Poller	Servery	NSClient++	TCP 12489	Monitorování
Vzdálený server	Centrální server	HTTP(S)	TCP 80 (443)	Aktivace funkce vzdáleného serveru

Tabulka č. 5: Datové toky určené k monitorování (35)

4.8 Zvolená architektura

Jako způsob zapojení monitorovacího systému Centreon byla zvolena jednoduchá architektura. Důvodem bylo převážně usnadnění dohledu nad správným chodem jednotlivých komponentů v systému. Dále se je pravděpodobné, že síťová infrastruktura firmy není tak rozsáhlá, aby výhody ostatních architektur byly aplikovatelné, konkrétně:

- Vyrovnání zátěže – s rostoucím počtem zařízení je možné v budoucnu dodatečně přidat k centrálnímu serveru další poller.
- Vzdálený server – další webové rozhraní a rozdělovaní monitorovaných dat do dalších podmnožin, stejně jako s pollery lze vzdálený server dodatečně přidat

Na druhou stranu, výhody ostatních architektur z pohledu zabezpečení:

- Oddělení databázového serveru
- Izolace datových toků umístěním pollerů do fyzicky či virtuálně separátních sítí.

Jsou žádoucí, nicméně k základnímu zprovoznění nepotřebné. Díky modulárnosti systému lze architekturu v případě potřeby překonfigurovat.

4.9 Server

Při výběru fyzického serveru, na kterém bude monitorovací systém konstantně spuštěn, bylo nutné zvážit hardwarové nároky – ty se odvíjejí od počtu sledovaných zařízení, služeb:

Počet služeb	Přibližný počet sledovaných zařízení	Počet pollerů	Centrální server	Poller
< 500	50	1 centrální	1 vCPU / 1 GB	-
500 - 2000	50 - 200	1 centrální	2 vCPU / 2 GB	-
2000 - 7000	200 - 700	1 centrální + 1 poller	4 vCPU / 4 GB	1 vCPU / 4 GB
7000 - 14000	700 - 1400	1 centrální + 1 poller	4 vCPU / 8 GB	2 vCPU / 4 GB
14000 - 21000	1400 - 2100	1 centrální + 2 pollery	4 vCPU / 8 GB	2 vCPU / 4 GB
21000 - 28000	2100 - 2800	1 centrální + 3 pollery	4 vCPU / 8 GB	2 vCPU / 4 GB

Tabulka č. 6: Hardwarové nároky (36)

Poller je schopný monitorovat zhruba 7000 aktivních služeb. Frekvence virtuálních procesorů musí být kolem 3 GHz. Počet potřebných virtuálních procesorů je závislý na složitosti kontrol.

Nárok na velikost úložiště pro ukládání získaných dat o monitorování závisí na několika kritériích:

- Počet kontrol
- Frekvence kontrol
- Doba uchování získaných dat

Následující tabulka odhaduje potřebnou velikost úložiště, pokud systém získává data každých 5 minut, uchovává je 6 měsíců a každý graf má 2 křivky. (36)

Počet služeb	Velikost databáze (v GB)	Velikost Centreonu (v GB)
500	10	2,5
2000	42	10
10 000	93	27
20 000	186	54
50 000	465	135
100 000	930	270

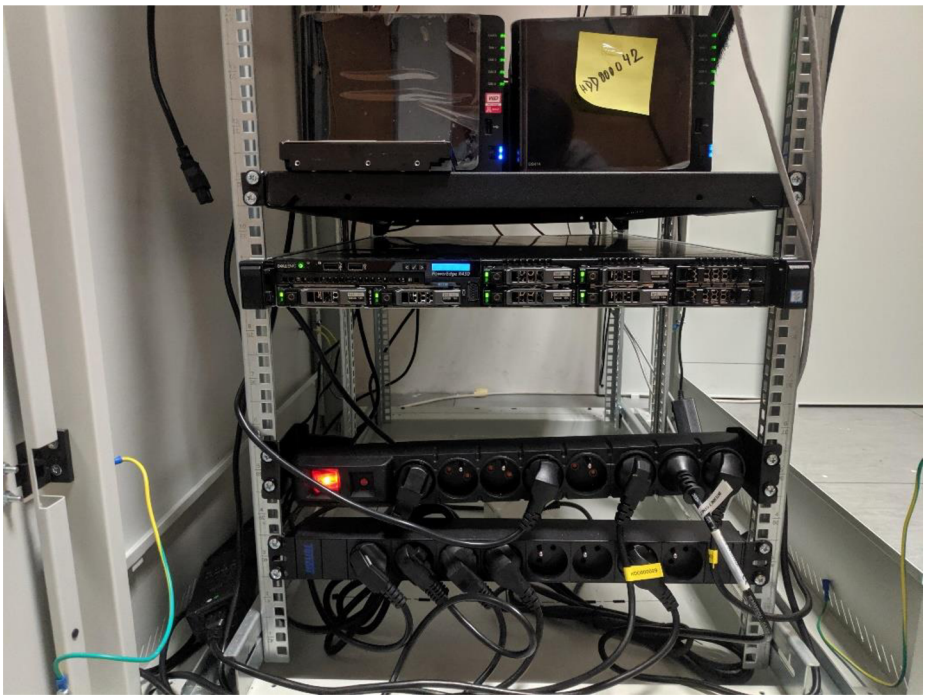
Tabulka č. 7: Odhad velikostních nároků (36)

Na základě hardwarových požadavků byl zvolen rackový server od dodavatele našeho hardwaru Dell. Jedná se o Dell PowerEdge R430 s následujícím hardwarem:

- Intel Xeon E5-2600 v4 CPU
- 64 GB DDR4 RAM
- 6x SAS 600 GB

Na první pohled se může zdát, že použitý hardware je více než dostatečný pro monitorovací systém Centreon. Nicméně, je důležité podotknout, že daný server bude využívat virtualizační technologii HyperV, což znamená, že na něm bude běžet více virtuálních serverů najednou a monitorovací systém Centreon bude jedním z nich. Na fyzický server je tedy kromě monitorovacího systému v plánu instalovat software pro správu adres IPplan, kontrolér pro přístupové body UniFI či SMTP relay pro O365.

Fyzický server byl namontován do racku v serverovně na centrále společnosti. Toto umístění je výhodné, protože na centrále se nachází také hlavní IT oddělení. V případě závady systému, u které by byla nutnost fyzického zákroku, nebude problém povolat kolegy. Server bylo dále třeba zapojit do napájení, a to jak do elektrické sítě, tak i do záložního zdroje UPS v případě výpadku elektrické energie. Následujícím krokem bylo zapojení serveru do portu na switchy a nastavit ho jako tzv. trunk, aby měl přístup do všech virtuálních LAN, a tak měl přístup ke všem zařízením, které je potřeba monitorovat. Po zapojení byl na server nainstalován operační systém Windows Server 2016 Datacenter.



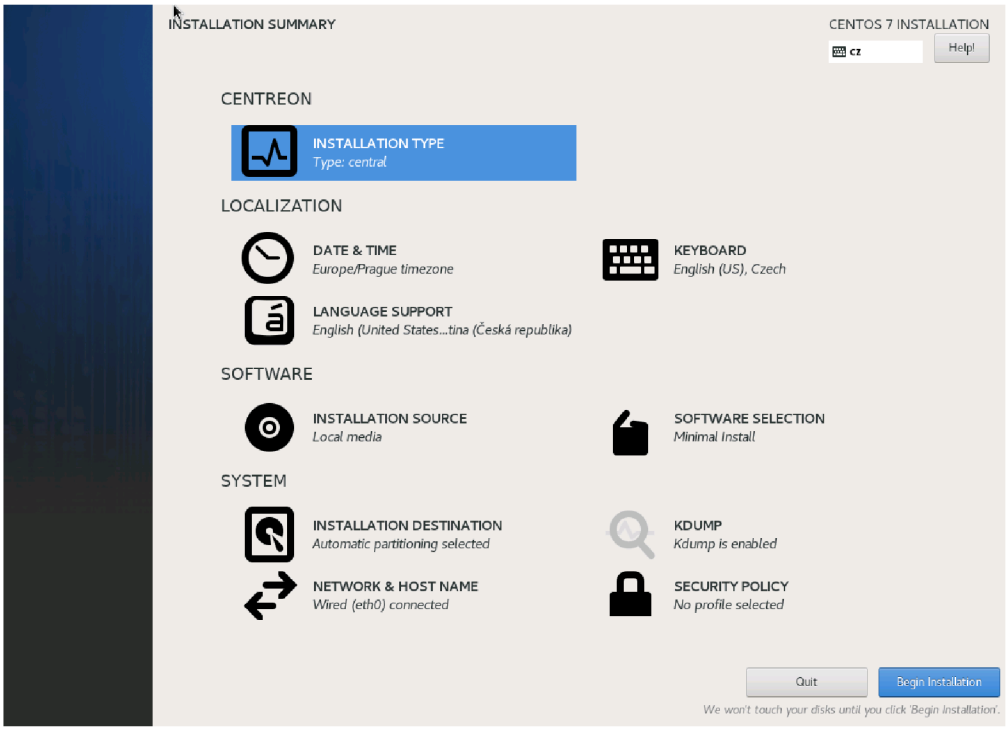
Obrázek č. 23: Server (zdroj: autor)

4.10 Instalace

Před zahájením instalace bylo potřeba ve správci technologie Hyper-V na serveru vytvořit nový virtuální stroj. Tomuto stroji bylo dle hardwarových požadavků z minulé kapitoly přiděleno 2 GB RAM a 2 virtuální procesory. Centreon lze instalovat na 64bitové GNU/Linux operační systémy. Nicméně oficiální podporu a repozitáře s instalačními balíčky nabízí pouze pro Linuxové distribuce CentOS 7 a Redhat/OracleLinux 7/8. U všech ostatních linuxových distribucí, které jsou podporovány pouze komunitou, je jedinou možností instalace sestavení jednotlivých balíčků monitorovacího systému ze zdrojového kódu. Nutno podotknout, že moduly zpoplatněných verzí Centreonu na těchto nepodporovaných distribucí nefungují. Dále Centreon nabízí tyto způsoby instalace:

- Instalační ISO CentOS 7 s již obsaženým Centreonem
- Virtuální stroje ve formátu OVA s předinstalovaným Centreonem pro virtualizační prostředí VMware a Oracle VirtualBox (36)

Monitorovací systém Centreon, konkrétně verze 21.10, byl instalován pomocí instalačního ISO obrazu, protože se jedná o způsob doporučovaný samotnými autory. Zvolený instalační proces mě překvapil svým přívětivým grafickým rozhraním. Kromě nastavení základních parametrů jako jazyk, rozložení klávesnice atd., jsem nastavil typ instalace dle zvolené architektury – centrální (s databází) a hostitelský název dle jmenné konvence – MET-SRV-MON. MET – lokalita, SRV – server, MON – monitoring.



Obrázek č. 24: Shrnutí instalace (zdroj: autor)

Důležité je během probíhající instalace změnit heslo pro root uživatele. Tento uživatel má plný přístup do celého operačního systému, proto je podstatné mu nastavit silné heslo.

Po restartu a přihlášení root uživatele je vhodné aktualizovat systém na nejnovější verzi (případně přijmout všechny GPG klíče) a restartovat:

```
$ yum update
......
$ reboot
```

Obrázek č. 25: Update systému (zdroj: autor)

Dalším krokem je povolení automatického spouštění služeb, tak aby se monitorovací systém spouštěl i po restartu serveru:

```
$ systemctl enable php-fpm httpd24-httpd mariadb centreon cbd centengine gorgoned snmptrapd centreontrapd snmpd
```

Obrázek č. 26: Automatické spouštění služeb (zdroj: autor)

Následně se musí nastavit MySQL databáze pomocí následující příkazu:

```
$ mysql_secure_installation
```

Obrázek č. 27: Nastavení MySQL (zdroj: autor)

Na všechny otázky kromě „Disallow root login remotely?“ se odpoví ano. Je velice důležité nastavit bezpečné heslo pro databázového root uživatele.

K úplnému dokončení instalace už zbývá pouze nastavení, které se nachází ve webovém rozhraní. URL webové rozhraní je: http://[ip_adresa_serveru]/centreon. Webové rozhraní nejprve zkontroluje dostupnost všech potřebných modulů. Poté přichází definování umístění složek pro engine a broker komponenty – je doporučeno neměnit výchozí nastavení. Na další obrazovce se provede nastavení účtu správce. Dále je na řadě nastavení databáze – použije se heslo, které se definovalo v příkazovém řádku. Po vybrání a nainstalování modulů a widgetů je instalace kompletně dokončena.

4.11 Konfigurace

Před zahájením konfigurace zařízení se nejprve musí inicializovat proces monitorování. V nabídce konfigurace ve webovém rozhraní se vyberou pollery, dále se zaklikne centrální poller a klikne se na tlačítko „Export configuration“. V nadcházející nabídce musí být zakliknuta možnost „Move Export Files“, poté se stiskne tlačítko „Export“. Posledním krokem je spuštění/restartování jednotlivých služeb monitorovacího systému z příkazové řádky:

```
$ systemctl restart cbd centengine
```

Obrázek č. 28: Restart sběrných procesů (zdroj: autor)

```
$ systemctl restart gorgoned
```

Obrázek č. 29: Restart zpracovatele úloh (zdroj: autor)

```
$ systemctl start snmptrapd centreontrapd
```

Obrázek č. 30: Start pasivních monitorovacích služeb (zdroj: autor)

Přidávání monitorovaných zařízení je jednoduché, a to díky instalaci pluginů, které obsahují konfigurační šablony pro téměř každé zařízení. Pro instalaci pluginů je vyžadován „Base Pack“ plugin.

4.11.1 Aktivace SNMP

Na zařízeních, které chceme monitorovat, musí být povolen protokol a spuštěna služba SNMP. Kvůli bezpečnosti je vhodné SNMP povolit pouze pro IP adresu monitorovacího serveru. Dále musí být nastaven tzv. SNMP community string, který je určen k ověření oprávněného přístupu k datům o zařízení. Postup nastavení se odvíjí od typu zařízení:

- Windows – V programu „Služby“.
- Linux – V konfiguračním souboru: /etc/snmp/snmpd.conf.
- Switch/Firewall – Konfigurace v terminálovém připojení například příkaz snmp-server u switchů Cisco.
- Tiskárny – Ve webovém rozhraní.

4.11.2 Přidání zařízení

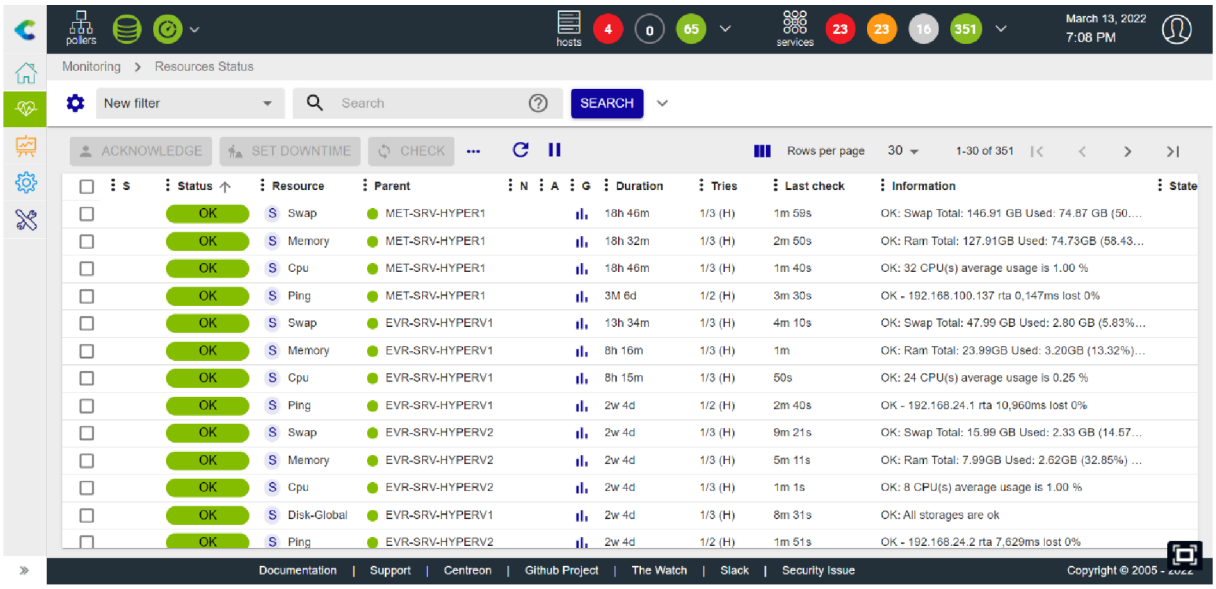
Po povolení a spuštění služby SNMP je potřeba nainstalovat plugin pro dané zařízení. Například:

- Windows SNMP
- Linux SNMP
- Cisco Standard
- Fortinet Fortigate
- Printer Standard

Plugin přidá šablonu nastavení zařízení se sledovanými parametry a jejich kritické hodnoty. Poté je potřeba přidat samotné zařízení v Configuration > Hosts a vyplnit údaje o zařízení, jako:

- Jméno a popis
- IP adresa
- Verze a community string SNMP zařízení
- Šablona

Po vyplnění údajů a uložení se po pár minutách objeví první výsledky monitorování:



S	Status	Resource	Parent	N	A	G	Duration	Tries	Last check	Information	State
	OK	Swap	MET-SRV-HYPER1				18h 46m	1/3 (H)	1m 59s	OK: Swap Total: 146.91 GB Used: 74.87 GB (50....	
	OK	Memory	MET-SRV-HYPER1				18h 32m	1/3 (H)	2m 50s	OK: Ram Total: 127.91GB Used: 74.73GB (58.43...	
	OK	Cpu	MET-SRV-HYPER1				18h 46m	1/3 (H)	1m 40s	OK: 32 CPU(s) average usage is 1.00 %	
	OK	Ping	MET-SRV-HYPER1				3M 6d	1/2 (H)	3m 30s	OK - 192.168.100.137 rta 0,147ms lost 0%	
	OK	Swap	EVR-SRV-HYPERV1				13h 34m	1/3 (H)	4m 10s	OK: Swap Total: 47.99 GB Used: 2.80 GB (5.83%...	
	OK	Memory	EVR-SRV-HYPERV1				8h 16m	1/3 (H)	1m	OK: Ram Total: 23.99GB Used: 3.20GB (13.32%)...	
	OK	Cpu	EVR-SRV-HYPERV1				8h 15m	1/3 (H)	50s	OK: 24 CPU(s) average usage is 0.25 %	
	OK	Ping	EVR-SRV-HYPERV1				2w 4d	1/2 (H)	2m 40s	OK - 192.168.24.1 rta 10,960ms lost 0%	
	OK	Swap	EVR-SRV-HYPERV2				2w 4d	1/3 (H)	9m 21s	OK: Swap Total: 15.99 GB Used: 2.33 GB (14.57...	
	OK	Memory	EVR-SRV-HYPERV2				2w 4d	1/3 (H)	5m 11s	OK: Ram Total: 7.99GB Used: 2.62GB (32.85%) ...	
	OK	Cpu	EVR-SRV-HYPERV2				2w 4d	1/3 (H)	1m 1s	OK: 8 CPU(s) average usage is 1.00 %	
	OK	Disk-Global	EVR-SRV-HYPERV1				2w 4d	1/3 (H)	8m 31s	OK: All storages are ok	
	OK	Ping	EVR-SRV-HYPERV2				2w 4d	1/2 (H)	1m 51s	OK - 192.168.24.2 rta 7,629ms lost 0%	

Obrázek č. 31: Výsledky monitorování (zdroj: autor)

4.11.3 LDAP

Nastavení LDAP serveru se nachází v Administration > Parameters > LDAP. Centreon neumožňuje automatický import všech uživatelů, nicméně vytvoření uživatele v systému provede po prvním přihlášení LDAP účtu do webového rozhraní. Do nastavení bylo potřeba

zadat IP adresu LDAP serverů a vytvořit speciálního uživatele pro čtení uživatelských účtů, které se nachází v doméně.

4.11.4 E-mailové notifikace

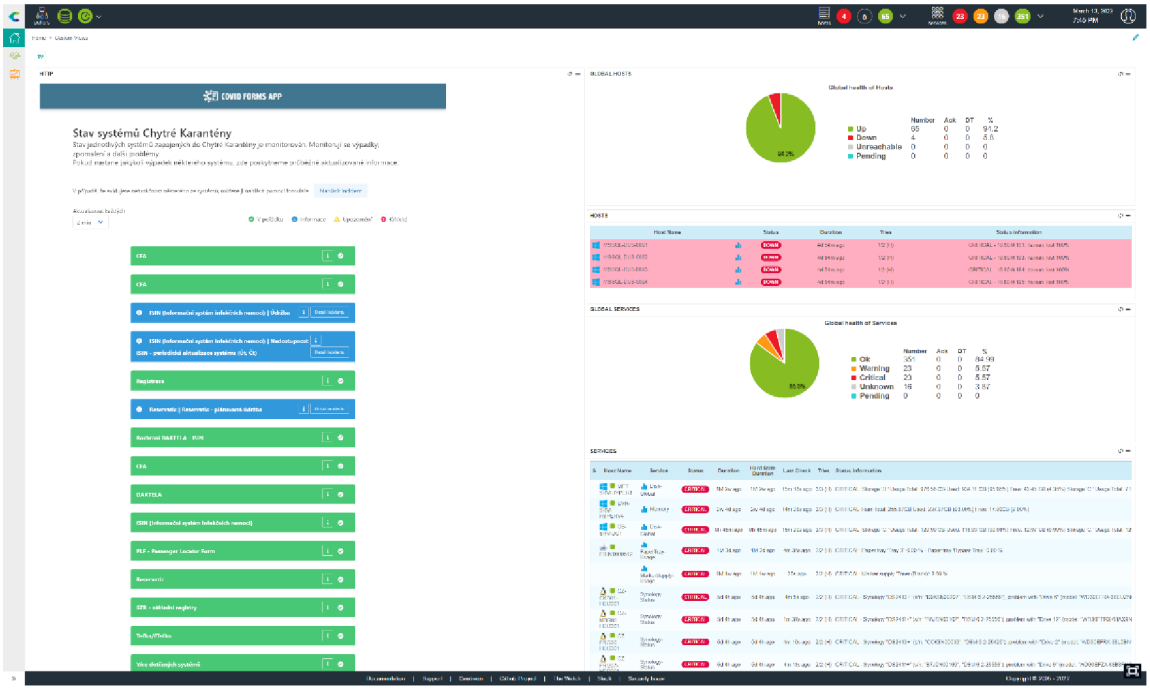
Notifikace se odesílají prostřednictvím SMTP relay serveru. Konkrétně se jedná o metodu host-notify-by-email. Pro zasílání jednotlivých notifikací byl použit následující příkaz:

```
$ /usr/bin/printf "%b" "***** centreon Notification
*****\n\nType:$NOTIFICATIONTYPE$\nHost: $HOSTNAME$\nState: $HOSTSTATE$\nAddress:
$HOSTADDRESS$\nInfo: $HOSTOUTPUT$\nDate/Time: $DATE$" | sendemail -f
monitoring.cz@synlab.com -t $CONTACTEMAIL$ -s 192.168.100.199 -u "Host $HOSTSTATE$
alert for $HOSTNAME$!"
```

4.11.5 Monitorovací panel

Monitorovací panel, také označován v aj. jako dashboard, je vizuální znázornění stavu monitorovaných zařízení, parametrů – v Centreonu označován jako „Custom View“. Pro účely konstantního monitorování tohoto panelu přítomnými kolegy byla zakoupena 4K televize, která byla následně nainstalována na IT oddělení. Monitorovací panel se upravuje přidáváním tzv. widgetů. Widgety lze dále nastavit podle specifických potřeb. Do monitorovacího panelu byly přidány tyto widgety:

- HTTP Loader – Obsah webové stránky. Jedná se o stránku zobrazující stav systémů chytré karantény, důležité pro aplikační tým.
- Global Health – Výsečový graf ukazující status zařízení a jejich parametrů.
- Host/Service Monitoring – Seznam ukazující status zařízení či jejich parametrů.



Obrázek č. 32: Monitorovací panel (zdroj: autor)

5 Závěr

Ačkoliv monitorovací systém Centreon vychází ze zdrojového kódu jednoho z nejstarších monitorovacích systémů zvaný Nagios, nebylo nic, co by tomu tak nasvědčovalo. Bylo zřejmé, že vývojáři Centreonu vynaložili značné úsilí, aby zdrojový kód modifikovali tak, aby splňoval aktuální požadavky společností na trhu. Instalace probíhala bez problémů a překvapila svou intuitivností a uživatelskou přívětivostí. Přitom samotný systém je vysoce modulární a umožnuje customizaci do nejmenších detailů. Je otázkou, zda by tomu tak bylo, kdyby se vývojáři nerozhodli jít cestou otevřeného zdrojového kódu. Při samotné konfiguraci byla nápomocná podrobně popsaná oficiální dokumentace. Nutno dodat, že potřeby pro monitorování podniku splňoval téměř každý monitorovací systém z teoretické části. Na druhou stranu podnik neměl tak vysoké nároky a požadoval funkce, kterými disponuje prakticky každý monitorovací systém na trhu. Hlavním důvodem byl fakt, že mnoho funkcí, které monitorovací systémy nabízí, již zajišťoval v podniku nainstalovaný systém pro inventarizaci sítě, softwaru a hardwaru, Lansweeper. Kritickým pohledem by pravděpodobně bylo možné naplnit interní požadavky firmy synlab s.r.o. pro monitorování podniku i jinými monitorovacími systémy. Avšak systém Centreon se v rámci výběrového řízení jevil nejen jako ekonomicky přívětivý, ale také vzbuzoval příslib hladké implementace, která opravdu bez komplikací proběhla.

6 Seznam použitých zdrojů

1. KUROSE, J F. -- ROSS, K W. Počítačové sítě. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.
2. 5 Common Types of Computer Networking. [online]. [cit. 2021-10-31]. Dostupné z: https://www.brainwareuniversity.ac.in/blog/5-common-types-of-computer-networking/
3. Jiří Peterka, Báječný svět počítačových sítí, část IV. – Rodina protokolů TCP/IP. [online]. [cit. 2005-06-01]. Dostupné z: https://www.earchiv.cz/b05/b0600001.php3
4. Autor David Mudrák (mudrdmz) – Vlastní produkt, CC BY-SA 3.0. [online]. Dostupné z: https://commons.wikimedia.org/w/index.php?curid=5181616
5. By Osi-model-jb.png: Original created by JB Hewitt (Johnblade) at en.wikipedia Later version(s) were uploaded by PeterC, Brakcen, Chai at en.wikipedia.derivative work: Puchy (talk) - Osi-model-jb.png, CC BY-SA 3.0. [online]. Dostupné z: https://commons.wikimedia.org/w/index.php?curid=7624179
6. Network Monitoring: Protocols, Best Practices, and Tools. [online]. [cit. 2020-05-04]. Dostupné z: https://www.tek-tools.com/network/network-monitoring-guide-and-tools
7. The 4 types of metrics you should monitor to keep your servers under control. [online]. [cit. 2019]. Dostupné z: https://www.site24x7.com/blog/the-4-types-of-metrics-you-should-monitor-to-keep-your-servers-under-control.
8. What is Wireshark and How Is It Used? [online]. Dostupné z: https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it
9. The Main window. Wireshark User's Guide. [online]. Dostupné z: https://www.wireshark.org/docs/wsug_html_chunked/ChUseMainWindowSection.html
10. Nmap: the Network Mapper – Free Security Scanner. [online]. Dostupné z: https://nmap.org/
11. Zenmap – Official cross-platform Nmap Security Scanner GUI. [online]. Dostupné z: https://nmap.org/zenmap/
12. Putty. [online]. Dostupné z: https://www.putty.org/
13. Visual Network Topology Map? [online]. Dostupné z: https://superuser.com/questions/4682/visual-network-topology-map
14. MAURO, D. -- SCHMIDT, K. Essential SNMP, Second Edition. Beijing: O'Reilly Media, 2005. ISBN 05-960-0840-6.
15. What is Simple Network Management Protocol (SNMP)? [online]. Dostupné z: https://www.thousandeyes.com/learning/techtorials/snmp-simple-network-management-protocol
16. What is SNMPv1, SNMPv2c, and SNMPv3? [online]. Dostupné z: https://www.dpstele.com/snmp/v1-v2c-v3-difference.php
17. SNMP MIB. [online]. Dostupné z: https://docs.oracle.com/cd/E13203_01/tuxedo/tux90/snmpmref/1tmib.htm
18. A beginner's guide to SNMP. [online]. Dostupné z: http://www.snmplink.org/articles/abeginnersguide/
19. 12 Best Network Monitoring Tools & Software of 2022. [online]. Dostupné z: https://www.comparitech.com/net-admin/network-monitoring-tools/
20. Network Monitoring Tools you must know in 2021. [online]. Dostupné z: https://network-king.net/best-network-monitoring-tools/

21. Zabbix. [online]. Dostupné z: https://www.zabbix.com/
22. How to install Zabbix Server 5.0 LTS on Ubuntu 20.0 LTS. [online]. Dostupné z: https://www.valters.eu/how-to-install-zabbix-server-5-0-lts-on-ubuntu-20-0-lts/
23. LibreNMS. [online]. Dostupné z: https://www.librenms.org/
24. Install LibreNMS on CentOS 7 / Ubuntu 16.04 – A Network and Server Monitoring Tool. [online]. Dostupné z: https://www.itzgeek.com/how-tos/linux/centos-how-tos/install-librenms-on-centos-7-ubuntu-16-04-a-network-and-server-monitoring-tool.html/2
25. SolarWinds. [online]. Dostupné z: https://www.solarwinds.com/network-performance-monitor
26. ManageEngine. [online]. Dostupné z: https://www.manageengine.com/network-monitoring/
27. Paessler. [online]. Dostupné z: https://www.paessler.com/prtg
28. O nás: SYNLAB. [online]. Dostupné z: https://www.synlab.cz/human/patient/o-nas
29. Cisco Catalyst 9200 Series Switches – Cisco. [online]. Dostupné z: https://www.cisco.com/c/en/us/products/switches/catalyst-9200-series-switches/index.html
30. Fortinet FortiGate 60F | AVFirewalls.com. [online]. Dostupné z: https://www.avfirewalls.com/FortiGate-60F.asp
31. ARCHITECT c4000 Clinical Chemistry | Abbott Core Laboratory. [online]. Dostupné z: https://www.corelaboratory.abbott/int/en/offerings/brands/architect/architect-c4000
32. Centreon. [online]. Dostupné z: https://www.centreon.com/
33. Github – Centreon. [online]. Dostupné z: https://github.com/centreon/centreon
34. Centreon Documentation. [online]. Dostupné z: https://docs.centreon.com/
35. Architectures | Centreon Documentation. [online]. Dostupné z: https://docs.centreon.com/docs/installation/architectures
36. Prerequisites | Centreon Documentation. [online]. Dostupné z: https://docs.centreon.com/docs/installation/prerequisites

7 Seznam obrázků, tabulek a grafů

7.1 Seznam obrázků

7.2 Seznam tabulek

7.3 Seznam grafů