Ekonomická fakulta
Faculty of Economics
Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Jihočeská univerzita v Českých Budějovicích
Fakulta ekonomická
Katedra aplikované matematiky a informatiky

Bakalářská práce

Implementace dohledového systému do firemní počítačové sítě

Vypracoval: Panuška Václav
Vedoucí práce: Ing. Hanzal Petr Ph.D.

České Budějovice 2020

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
Ekonomická fakulta
Akademický rok: **2017/2018**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Václav PANUŠKA**
Osobní číslo:	**E16523**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Ekonomická informatika**
Název tématu:	**Implementace dohledového systému do firemní počítačové sítě**
Zadávající katedra:	**Katedra aplikované matematiky a informatiky**

Zásady pro vypracování:

Cílem bakalářské práce je navrhnout a popsat implementaci zvoleného dohledového systému do firemní počítačové sítě. Součástí práce bude popsání monitorovacích systémů, jejich rozdělení a způsob monitorování konkrétních služeb a komponent počítačové sítě.

Metodický postup:

1. Studium odborné literatury.
2. Obecný popis dohledového systému.
3. Teoretický popis konkrétních dostupných systémů.
4. Popis implementace zvoleného řešení.
5. Vypracování doporučení a závěrů.

Rozsah grafických prací: **dle potřeby**

Rozsah pracovní zprávy: **40 - 50 stran**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

1. **Badger, M. (2008).** *Zenoss Core Network and System Monitoring.* **Birmingham, US: Packt Publishing Limited.**
2. **Bouška, P. (2009).** *Začínáme s monitoringem sítě.* **http://www.samuraj-cz.com. [Online]. [Citace: 5. únor 2012.] http://www.samuraj-cz.com/clanek/zaciname-s-monitoringem-site/.**
3. **Kurose, J. F., & Ross, K. W. (2014).** *Počítačové sítě.* **Brno: Computer Press.**
4. **MonitorTools.com. Network Monitor Software and Windows Development Tools. Network Monitor Software and Windows Development Tools. [Online] 2012. http://www.monitortools.com/.**
5. **Wolfgang, B. (2008).** *Nagios: System and Network Monitoring.* **Daly City, California: No Starch Press.**

Vedoucí bakalářské práce: **Ing. Petr Hanzal, Ph.D.**
Katedra aplikované matematiky a informatiky

Datum zadání bakalářské práce: **19. ledna 2018**

Termín odevzdání bakalářské práce: **12. dubna 2019**

doc. Ing. Ladislav Rolínek, Ph.D.
děkan

JIHOČESKÁ UNIVERZITA
V ČESKÝCH BUDĚJOVICÍCH
EKONOMICKÁ FAKULTA
Studentská 13 (2e)
370 05 České Budějovice

L.S.

doc. RNDr. Jana Klicnarová, Ph.D.
vedoucí katedry

V Českých Budějovicích dne 29. března 2018

Prohlašuji, že svou bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to - v úpravě vzniklé vypuštěním vyznačených částí archivovaných Ekonomickou fakultou - elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. v platném znění zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

…… …….....

Datum Panuška Václav

Poděkování

Velice rád bych poděkoval Ing. Petrovi Hanzalovi Ph.D. za vedení mé bakalářské práce a jeho cenné rády a připomínky, které mě vždy navedly správným směrem. Velice si vážím jeho přístupu a ochoty mi vždy pomoci a věnovat svůj čas ať už prostřednictvím osobních a telefonických konzultací tak prostřednictvím mailových zpráv. Dále bych rád poděkoval společnosti ČD-Telematika a.s. za možnost uskutečnit praktickou část v jejich síti a možnost řízení celé implementace. Především bych chtěl poděkovat panu Ing. Zdeňkovi Slámovi, Ing. Janovi Mračkovi a Ing. Janovi Guzejovi za cenné rady a pomoc při implementaci a rozhodování o navrhovaném řešení. Závěrem bych rád poděkoval celé své rodině, přítelkyni a přátelům za psychickou podporu a neustálé pohánění vpřed. Všem moc děkuji!

Obsah

1 Úvod

Hlavním tématem následujících stran bude dohledový systém v počítačové síti. Nicméně na úvod je třeba věnovat pár slov oblasti, ve které je možno se s pojmem počítačová síť setkat. Základním předmětem je zde počítač. Současné počítače se od svých předchůdců v mnoha ohledech liší, a to nejen z hlediska funkcí, ale také rozměry. První počítače, které svou velikostí obsáhly i celou místnost, byly vynalezeny před mnoha lety a dokázaly provádět jen některé jednoduché matematické výpočty. V současné době v jakékoliv společnosti nebo domácnosti nalezneme alespoň nějaké informační zařízení, může se jednat například o počítače, skenery, servery, mobilní telefony atd. Ke konektivitě mezi zařízeními se využívá počítačová síť, jejíž pomocí dochází k přenosu dat mezi jednotlivými zařízeními.

S rostoucí popularitou informačních zařízení roste důležitost počítačových sítí a také jejich využitelnost, a to jak v pracovní sféře, tak i ve všedním životě. To má za následek neustálé zvyšování výpočetní síly, sdílení zdrojů a komunikaci mezi uživateli. Svět výpočetní techniky však není nahodilý, ale vyžaduje dohled v osobě správce sítě, který musí mít počítačovou síť pod kontrolou. V každé počítačové síti mohou nastat problémy a tyto problémy se musí dostat ke správcům sítě, kteří je musí aktivně řešit a odstraňovat. Potřeba monitoringu a správy sítě vzniká přímo úměrně při růstu počítačové sítě. V průběhu let zlepšování technologií se počítačové sítě změnily z propojení pár počítačů na připojení několika milionů zařízení v mnoha sítích. Tuto síť nazýváme internet. Je zřejmé, že takto rozmanitá síť vyžaduje bohatou správu.

Termín monitoring počítačové sítě je spojen se sledováním a kontrolou připojení zařízení v síti a jeho následnou kontrolu a detekci nesprávného fungování nebo škodlivé činnosti v síti. V menších sítích určených pro domácnosti nemusí být monitoring tak nezbytný, ale pro velké organizace by měl být prioritou. Jestliže nebudou mít velké organizace spolehlivý monitorovací nástroj, tak mohou ztratit velké množství dat včetně citlivých informací nutných pro zachování zdravého chodu společnosti, což s sebou může přinést finanční ztráty, případně to může znamenat i bankrot firmy. Může se jednat například o banky, letecké společnosti, knihovny a mnoho dalších organizací. Ty v případě problému ve své síti nemohou poskytovat slíbené služby či mohou ohrozit soukromí svých klientů, případně i svou existenci. Každá organizace si z tohoto důvodu musí udržovat svoji síť v dobrém stavu tak, aby mohla poskytovat kvalitní služby, které svým zákazníkům zaručila.

V dřívější době se pro řešení problémů využívaly systémy, které byly provozovány jako sběr logů velkého množství informací ze zařízení v síti. Tyto informace byly ručně zpracovávány správci sítě, ale navzdory znalostem bylo pro správce obtížné takové množství dat správně vyhodnotit. To je zejména případ, kdy se zařízení stala více inteligentními a více efektivními.

Pro tyto účely je žádoucí poskytnout automatizovaný systém pro monitoring sítě, který bude schopný převést znalosti správce do tohoto systému a včas detekovat problémy v síti a upozornit pracovníky na tento problém dříve, než se stane kritickým. Existuje velké množství aplikací, které jsou určeny pro monitoring sítí. Obecně lze aplikace rozlišovat na open source aplikace, které jsou volně dostupné, a na aplikace placené.

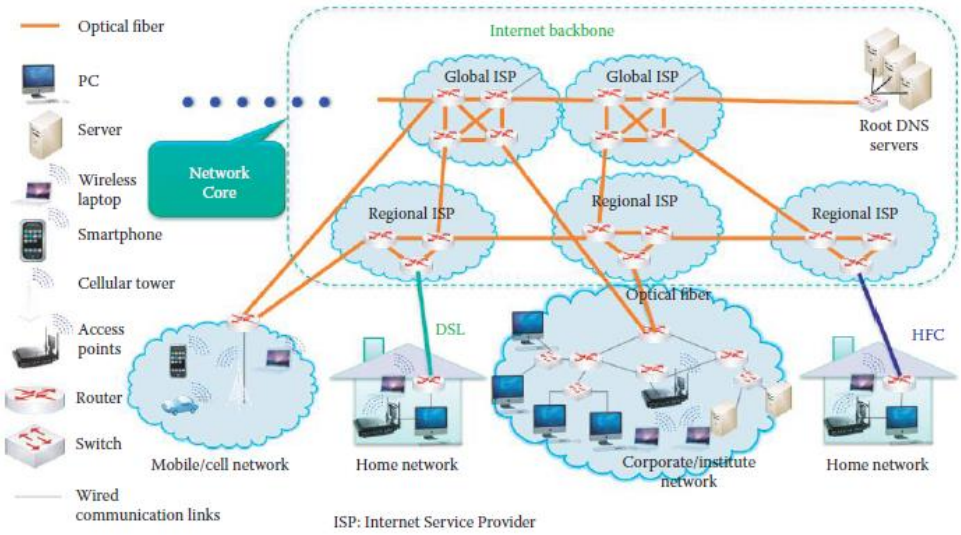
Cílem této bakalářské práce je ukázat, jak lze problémy související s počítačovou sítí monitorovat a řešit pomocí open source monitorovací aplikace. Konkrétně s použitím aplikace Centreon, která je postavena nad jádrem aplikace Nagios. Aplikace Centreon slouží pro sledování dostupných zařízení, dostupnosti služeb a dalších prahových hodnot zařízení v síti a je využívána k detekci problému v síti a upozornění na vzniklé problémy pomocí různých notifikací.

2 Počítačové sítě

Počítačovou síť lze popsat jako propojení dvou a více počítačů nebo jiných síťových zařízení, která spolu mohou komunikovat a vyměňovat si informace pomocí takové sítě. Komunikace mezi jednotlivými uzly probíhá dle předem určených pravidel. Většina počítačových sítí je propojena do globální sítě Internet, která ke své komunikaci používat sadu protokol TCP/IP. (Počítačová síť, 2019)

Na obrázku 1 je znázorněn globální pohled na počítačovou síť zapojenou do internetu. Internetová síť má hierarchickou strukturu a obrázek znázorňuje postup od jednoho počátečního uzlu, kterým může být například počítač nebo mobilní telefon, k regionálnímu poskytovateli internetových služeb (ISP) po globálního poskytovatel internetových služeb (ISP) až k cílovému zařízení. Na obrázku je vyznačena cesta odeslání zprávy z jednoho koncového uzlu na jiný koncový uzel. Způsob komunikace mezi sítěmi může být pomocí kabelu nebo bezdrátového spojení. Kabelové připojení je na obrázku realizováno pomocí digitální linky (DSL), hybridního opticko-koaxiálního kabelu (HFC), optického kabelu a pomocí bezdrátového spojení. Páteřní síť (Internet Backbone) je složena z globálních poskytovatelů internetových služeb (ISP) a z několika regionálních poskytovatelů internetových služeb (ISP), kteří jsou vzájemně propojeni, aby mohlo docházet k výměně dat mezi odesílatelem a příjemcem. Cesta mezi odesílatelem a příjemcem většinou obsahuje několik switchů a routerů a tato zařízení směřují tok informací mezi jednotlivými sítěmi. (Wu, 2013)

Obrázek 1: Počítačová síť



(Wu, 2013)

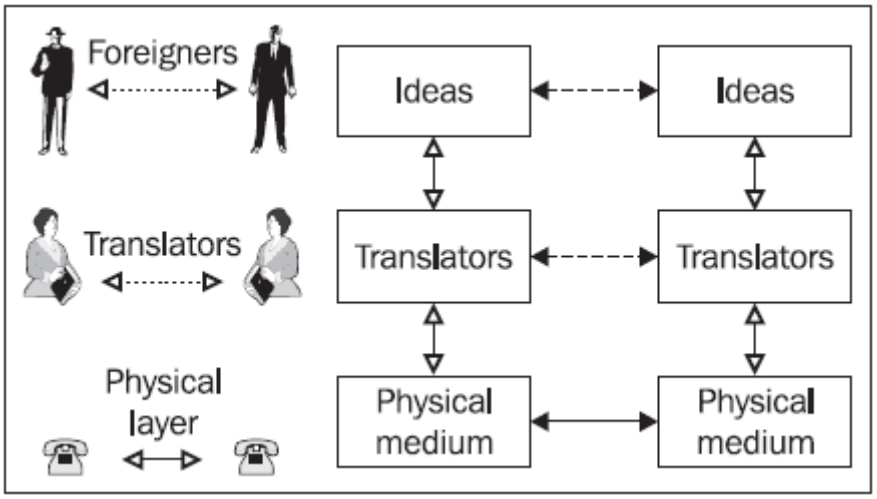
Internet je v dnešní době využíván k propojení miliard zařízení po celém světě a tato zařízení mohou prostřednictvím internetu provozovat široké spektrum aplikací. V každém okamžiku je počítačovými sítěmi přeposíláno ohromné množství dat. Zařízení, kterými jsou například servery, počítače a mobilní telefony, jsou mezi sebou propojena prostřednictvím spojů a informace procházejí skrz routery, switche a přístupové body (AP). Pro komunikaci může být využita kabelová nebo bezdrátová cesta. Jednotlivé komunikační linky jsou definovány přenosovou rychlostí a šířkou pásma. Routery jsou v síti využívány k oddělení jednotlivých sítí a mohou připojovat lokální sítě k dalším sítím. Takovou činnost router provádí pomocí směrovacích tabulek a následně předává informace na cestě od zdroje k cíli. Na obrázku 1 si můžeme všimnout, že páteřní síť tvoří skupina směrovačů a DNS (Domain Name System) server, které jsou propojeny optickými vlákny. DNS servery v sobě obsahují názvy zařízení v síti. Zařízení, která leží mimo páteřní síť, jsou nazývána přístupovými body, jak je znázorněno v obrázku 1. (Wu, 2013)

Internet sdružuje různé sítě v jednu rozsáhlou síť, dá se tedy říci, že internet je síť propojených sítí. Hierarchická struktura internetu je z pohledu shora dolů složena z páteřní sítě, která spojuje globální poskytovatele internetových služeb (ISP) s regionálními poskytovateli internetových služeb (ISP). Tito regionální poskytovatelé internetových služeb slouží k připojení lokálních sítí LAN (Local Area Network), ve kterých jsou připojeni hostitelé, kteří využívají například webové stránky (HTTP) nebo mail. (Wu, 2013)

3 Síťové protokoly

S počítačovými sítěmi jsou spjaty síťové protokoly. V obecném slova smyslu, pokud mluvíme o protokolu, mluvíme o souboru pravidel, která se týkají chování a lidé je dodržují. Jako příklad protokolu lze uvést situaci z lidského života. Když se dva známí lidé potkají, pozdraví se a zeptají se, jak se ten druhý má; jde se o rozšířený způsob chování, kterým mohou lidé začít komunikovat, jedná se o protokol. Stejně jako u lidí i v počítačových sítích dochází ke spojení mezi počítači a komunikaci pomocí předem definovaného protokolu. Protokol obsahuje jednotlivé vrstvy. Pokud znovu použijeme příklad z běžného života, může se jednat o situaci, kdy si dva ředitelé v různých zemích na světě vyměňují e-mail. První z ředitelů zprávu vymyslí a předá ji své sekretářce, která zprávu přeloží do příjemcova jazyka a odesílá ji e-mailem druhé sekretářce, která zprávu předá druhému řediteli. V tomto příkladu jsou použity 3 vrstvy pro komunikaci: první vrstva ředitelů, kteří vymyslí text zprávy, druhá vrstva sekretářek, které zprávu přeloží a třetí vrstva fyzická, která slouží pro přenos dat. Celý tento příklad je vyobrazen na obrázku 2. (Leiden & Wilensky, 2009)

Obrázek 2: příklad vrstev u protokolu

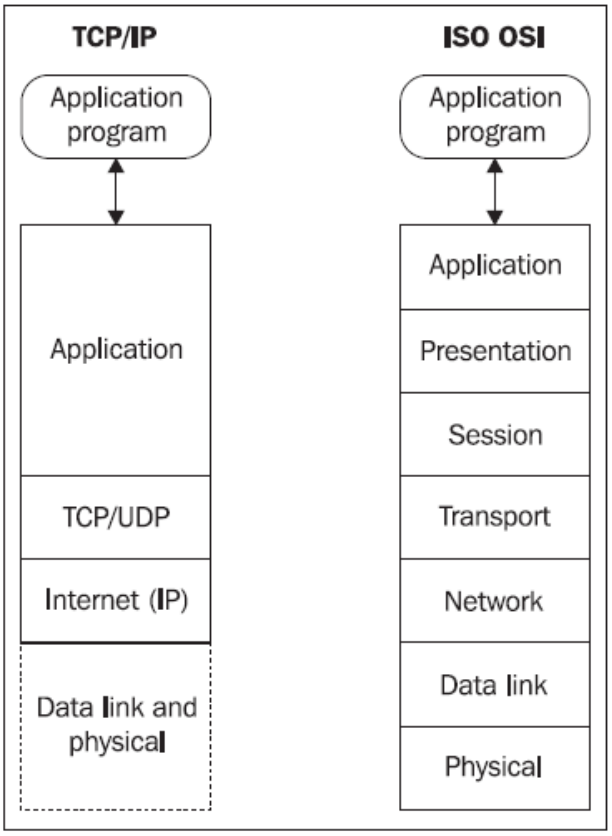


(Kabelová & Dostálek, 2006)

V příkladu jsme použili 3 vrstvy, v počítačových sítích se používá více vrstev. Počet vrstev závisí na tom, jaký systém síťových protokolů je použit. Systém síťových protokolů bývá také označován jako síťový model. Nejčastěji se setkáme s protokolem, který je využíván pro internet a označuje se jako rodina protokolů TCP/IP. Lze se také často setkat se síťový model ISO/OSI, který je standardizován organizací OSI. (Kabelová & Dostálek, 2006)

Rodina protokolů TCP/IP používá čtyři vrstvy, zatímco model ISO/OSI požívá vrstev sedm, jak je znázorněno na obrázku 3 níže. Systémy TCP/IP a ISO/OSI se od sebe navzájem liší, ačkoliv jsou si velice podobné na síťové a transportní vrstvě. (Kabelová & Dostálek, 2006)

Obrázek 3: porovnání síťového modelu TCP/IP a ISO/OSI



(Kabelová & Dostálek, 2006)

4 Dohledový systém

Dohledový systém je aplikační nástroj, který slouží pro monitoring a diagnostiku sítě v pravidelných časových intervalech. Hodnoty měření následně zaznamenává a uchovává pro další použití při analýze síťových problémů. Dohledové systémy umožňují správcům kontrolu sítě v reálném čase nebo pomáhají při zpětném dohledávání stavu sítě v určitém okamžiku. Často jsou tyto systémy vytvářeny jako komplexní nástroj pro centrální správu a monitoring sítě, který v síti zaznamenává informace o jejich jednotlivých parametrech. Je možné měřit například výkon sítě a identifikovat problémy a výkonnostní anomálie před tím, než bude ovlivněna funkčnost u koncových zákazníků. Je možné sledovat různé metriky na koncových stanicích, aktivních prvcích sítě nebo na serverech a to například dostupnost pomocí ICMP (Internet Control Message Protocol) protokolu, vytíženost operační paměti, obsazenost disků, teplotu, stav a případné alarmy na záložních bateriích, stav jednotlivých služeb a aplikací nebo dostupnost webových aplikací. Rozmanitost monitoringu je velice široká a lze sledovat prakticky všechno, na co je administrátor schopný napsat kontrolní skript. (Bouška, 2009)

Systémy uchovávají nasbíraná data a následně je prezentují do reportů událostí nebo v grafické podobě do grafů a statistických reportů. V případě, že nastane kritická chyba, kterou monitoring zachytí, je možné nastavit různá upozornění. Nástroje umožňují zvuková upozornění přímo v dohledovém nástroji, odeslání SMS, emailu nebo upozornění na pager a mnoho dalších upozornění. Pokročilejší monitorovací nástroje podporují i reakci na vzniklý problém v podobě automatického nebo poloautomatického zásahu, kdy je například spuštěn skript opravy chyby, restartována služba na vzdáleném zařízení, případně restartováno celé zařízení. Tato skutečnost je následně zadokumentována a správci jsou upozorněni na tuto skutečnost. Pomocí těchto upozornění a včasné informovanosti správce systémů dochází ke snížení času potřebnému k odhalení problému a snížení nedostupnosti zařízení v síti. (Pleskot, 2012)

Pravděpodobně nejdůležitější metrikou monitoringu je síťová konektivita, která je ve většině případů monitorována na každém prvku v síti. Síťová konektivita mezi jednotlivými prvky v síti má nejvyšší prioritu, jelikož zaručuje komunikaci mezi koncovými zařízeními. Nejčastěji je konektivita zjišťována pomocí ICMP protokolu, který dokáže zjistit i případné zpoždění na lince, které lze použít k vyhodnocení výkonnosti síťové cesty. Dalším velice důležitým parametrem monitoringu je sledování míry zahození paketů na rozhraních routerů, které je měřeno pomocí SNMP (Simple Network

Management Protocol). Sledování míry zahození paketů je velice důležité pro poskytovatele internetových služeb, kteří se snaží co nejvíce snižovat míru zahozených paketů. Velmi často je převážně na aktivních prvcích v síti, ale také na serverech měřena vytíženost jednotlivých portů. Měření probíhá pomocí SNMP a dává správcům sítě informaci o aktuálním vytížení jednotlivých linek. (Hu, 2006)

Monitorovací funkce jsou v dnešních sítích velice zásadní, protože jejich účinnost určuje kvalitu služeb, která bude poskytnuta zákazníkům. Hlavním cílem nasazení dohledového systému do sítě je zvýšit spolehlivost sítě a jednotlivých zařízení v síti, a to primárně klíčových prvků v síti, jako jsou servery, páteřní linky a páteřní aktivní prvky a dále snížení reakčních časů správců sítě a snížení doby nedostupnosti zařízení pomocí včasného varování. (Hu, 2006) (Pleskot, 2012)

5 Způsoby monitorování

Z pohledu monitoringu lze rozlišit několik způsobů, jakými je možné zařízení v síti monitorovat. Výběr vhodného způsobu závisí na tom, jaké metriky jsou na daném zařízení kritické a jaké jsou možnosti zařízení. Každé zařízení na síti podporuje alespoň základní monitoring dostupnosti, pokud však chceme monitoring rozšířit o pokročilý monitoring a vyčítat data například z logů nebo získávat stavové informace o jednotlivých službách nebo komponentách, je potřeba zvolit monitoring založený na agentovi nebo SNMP. Zařízení však musí daný typ monitoringu podporovat a umět stavové informace prezentovat jedním ze způsobů. (Ligus, 2013) (Julian, 2018)

5.1 Agent

Monitoring pomocí agenta vyžaduje instalaci aplikace na straně zařízení, a proto je nezbytné, aby daný agent podporoval operační systém zařízení a byl pro dané zařízení kompatibilní. Instalace agenta na zařízení má svá pozitiva i negativa.

Mezi největší pozitiva patří možnost vytvářet podrobnější a přesnější monitoring. Jelikož nejsme závislí na tom, zda dané zařízení podporuje prezentaci stavových informací například pomocí SNMP, veškeré informace je možné získat přímo pomocí skriptů spouštěných na zařízení. Skripty si správce může sám naprogramovat, ale pro nejznámější a nejpopulárnější druhy monitoringu je možné skripty dohledat na internetu. Agenti se hojně využívají na serverech Windows pro vyčítání logů, provádění testů stavových informací pomocí powershellu apod. (Papež, 2014)

Oproti tomu najdeme i negativa, mezi která můžeme zařadit nutnost instalovat na server agenta. S tím je spojené nebezpečí softwaru třetích stran, ve kterých může být ukryt nebezpečný kód, případně může být kód agenta špatně zabezpečený a server se stane snadno napadnutelným. Dalším negativem může být spouštění skriptů přímo na serveru, je tedy nutná alespoň základní znalost skriptovacího jazyka, jelikož dochází ke spuštění skriptu třetích stran a po spuštění skriptu může dojít na našem serveru ke změnám, které jsme nepředpokládali. (Papež, 2014)

5.1.1 NSClient++

NSClient je jedním z nejznámějších agentů pro monitorovací systémy, jeho cílem je být jednoduchý a zároveň výkonný a flexibilní. Původně byl postaven pro monitorovací systém Nagios, ale v agentovi není nic specifického pro tento systém a může být použit i pro jiné dohledové systémy. Agent je instalován na monitorovaných serverech a

eliminuje veškeré potřeby, které jsou spojeny s používáním monitoringu bez agenta, jelikož umožňuje spouštět skripty přímo lokálně na serveru. Jedná se o open source agenta, jehož cílem je být otevřený pro podporu většiny protokolů pro integraci do různých dohledových systémů. Agent je schopný monitorovat jak Windows servery, tak Linux servery. (NSClient++, 2008)

Pro monitoring lze využít vestavěných kontrol, které jsou připraveny pro základní monitoring systémových metrik. Největší síla NSClienta je však ve spouštění externích skriptů, které je možné psát v jakémkoliv oblíbeném programovacím jazyce, které jsou spouštěny NSClientem na serveru a výsledky jednotlivých testů jsou předávány zpět do dohledového nástroje, který je prezentuje správcům. (NSClient++, 2008)

Kromě základních metrik, které dokážeme monitorovat i pomocí SNMP, jako vytížení CPU, operační paměti, linek, obsazenost disků a podobně, je možné pomocí NSClienta monitorovat další rozšířené metriky, které protokol SNMP nedokáže. Mezi pokročilé metriky lze zařadit například kontrolu Event logu ve Windows a v případě nalezení hlášky ve stavu warning nebo error upozornit správce v dohledovém systému. Dalšími pokročilými kontrolami je například kontrola aktualizací na serveru, stavu naplánovaných úloh, zálohování serveru a mnoha dalších metrik, na které jsme schopni si napsat skript. (NSClient++, 2008)

5.2 Bez agenta

Pro monitoring bez agenta je využíváno základních protokolů k ověření funkčnosti služeb a stavu jednotlivých metrik. Využívány jsou například protokoly HTTP (Hypertext Transfer Protocol), SNMP, FTP (File Transfer Protocol) a podobně. Není potřeba na zařízení instalovat žádný software třetích stran, ale jen povolení portů a případně konfiguraci SNMP. Monitoring následně probíhá zasláním požadavku na server, který vrátí stavovou hodnotu. Například u webového serveru a použití protokolu HTTP, pokud je vrácen kód 200, můžeme předpokládat, že je vše v pořádku a webový server odpovídá správně. Podobně fungují i ostatní protokoly. Nejvyužívanějším protokolem pro monitoring bez agenta je SNMP, pomocí kterého je možné ze zařízení získat velké množství informací. U monitoringu bez agenta určitě nalezneme pozitiva i negativa. (Papež, 2014)

Zásadním pozitivem je fakt, že není na zařízení potřeba instalovat žádný software, tudíž nedochází k bezpečnostním rizikům a ani skripty nejsou spouštěny na monitoro-

vaném zařízení, ale jsou spouštěny přímo na dohledovém nástroji. Dalším pozitivem je rychlost vrácených požadavků, které jsou podstatně rychlejší než pomocí agenta, kdy dohledový nástroj musí nejprve navazovat spojení s agentem a až poté provádět požadavek.

Mezi negativa je důležité zařadit, že zařízení musí umět jednotlivé stavy prezentovat pomocí protokolů. Pokud se jedná o standartní služby, jako je HTTP, FTP, SSH (Secure Shell) a další, tak není problém s podporou a prezentací jednotlivých stavů. Problém nastává u monitoringu pokročilejších metrik, které musí být od výrobce implementovány do SNMP stromu MIB (Management Information Base), z kterého je možné následně data čerpat. Většina výrobců s tímto počítá a data jsou pomocí SNMP prezentována, následně je potřeba buď na internetu stáhnout skript pro monitoring jednotlivých stavů, nebo vytvořit vlastní skript.

5.2.1 Ping

Základní metrikou pro každé zařízení by mělo být ověření dostupnosti hosta v TCP/IP síti. Ověření dostupnosti hosta funguje na principu zasílání ICMP zpráv. Dohledový nástroj využije skript a zašle echo-request na IP adresu nebo DNS (Domain Name System) záznam zařízení a čeká na echo-replay, skript dále měří dobu mezi odesláním požadavku a přijetím odpovědi, která je měřena v milisekundách a nazývá se zpoždění. V případě, že paket s odpovědí nedorazí, předpokládáme ztrátu paketu a tudíž nedostupnost zařízení. V dohledovém nástroji následně zařízení přejde do kritického stavu a upozorní správce. (Pleskot, 2012)

5.2.2 SNMP

SNMP (Simple Network Management Protocol) je založeno na sadě několika jednoduchých operací, které správcům zařízení umožňují správu zařízení s podporou SNMP. Pomocí SNMP je možné na jednotlivých prvcích například vypnout rozhraní na routeru, kontrolovat stav CPU na switchi nebo měřit rychlost ethernetového rozhraní. Je možné také sledovat různé prahové hodnoty na zařízeních a v případě překročení takové hodnoty odeslat upozornění. Příkladem může být upozornění na příliš vysokou teplotu zařízení. (Mauro & Schmidt, 2005)

V dnešní době je možné SNMP používat na většině zařízení, která jsou zapojena do sítě. Může se jednat o Windows nebo Unix systémy, switche, routery, převodníky, modemy, tiskárny, UPS (Uninterruptible Power Supply) a řadu dalších. Monitoring po-

mocí SNMP však není spjat jen s monitoringem fyzických zařízení, ale je možné monitorovat i na úrovni softwaru. Příkladem takového monitoringu je kontrola, zda jsou spuštěny jednotlivé služby a procesy, funkčnost webových stránek nebo databáze a mnoho dalších metrik. (Mauro & Schmidt, 2005)

Každý protokol prochází vývojem a jinak tomu není ani u protokolu SNMP. Díky tomu je protokol SNMP rozdělen do různých verzí, které se označují SNMPv1, SNMPv2 a SNMPv3. Posloupnost verzí je založena na vývoji konstrukce a funkcí protokolu. SNMPv1 byla založena na lehké konstrukci a ukázala se jako dobrá volba pro správu malých sítí. Hlavním důvodem vyvinutí druhé generace standardu SNMP bylo překonání nedostatků první generace. Druhá verze byla v podstatě první verze rozšířená o funkce založené na ISO/OSI a TCP/IP. Druhá generace přinesla lepší robustnost a správu, jelikož nabízí podrobnější kontrolu chyb a komunikace. Do druhé verze byla implementována funkce getbulk namísto funkcí get a getnext, která umožňuje jednou žádostí dostat odpověď pro celou tabulku stromu MIB. U verze 3 bylo hlavním přínosem zabezpečení, jelikož v první a druhé verzi je heslo zasíláno jen v podobě textu, u verze 3 se již používá jméno a heslo. (Mauro & Schmidt, 2005)

K popisu toho, jak protokol SNMP funguje, je potřeba rozlišit, že se skládá z manažera, agenta a sady objektů známé jako MIB. SNMP obvykle používá UDP (User Datagram Protocol) port 161 pro komunikaci s agentem a port 162 pro předávání informací od agenta k manažerovi. Manažer sbírá data z agenta pomocí SNMP dotazů na jednotlivé MIB objekty. Existují dva typy komunikace. První je, že manažer odešle žádost agentovi, může se jednat o žádosti pro získání informací get, v tomto případě chce manažer získat data z agenta. Pokud je nutné informace modifikovat, je odeslána žádost set. V druhém typu komunikace chce agent upozornit manažera na problém, v takovém případě agent odesílá SNMP trap. Pomocí SNMP je možné sbírat velké množství dat z jednotlivých zařízení a ta následně zapisovat do reportů nebo zobrazovat v grafech, jako například vytížení síťového portu, upozornění na prahové stavy nebo nedostupnost nějaké služby. (Mauro & Schmidt, 2005)

5.2.2.1 SNMP Management Information Base (MIB)

SNMP používá OID (Object Identifier) k identifikaci datových objektů, na které následně odkazuje. Každé OID vždy definuje jedinečný objekt pro určitého SNMP agenta. OID jsou uspořádána do hierarchického tvaru podobně jako domény na internetu. (Kocjan, 2008)

Identifikátor se skládá ze série čísel oddělených tečkami, každé číslo představuje jednu část stromu, která se může nadále větvit. Příkladem může být například OID .1.3.6.1.2.1.1.5.0, které prezentuje název zařízení. Protože by bylo velice složité zapamatovat si jednotlivá OID, existuje standard pro popis a pojmenování, standard se nazývá MIB. MIB definuje parametry, kterými jsou pojmenování hodnoty, typ hodnoty. Definice MIB se zapisují jako textové soubory a můžou popisovat malé či velké MIB stromy. (Kocjan, 2008)

Jedním z nejdůležitějších OID je .1.3.6.1.2.1, které je používáno všemi zařízeními k oznámení základních informací o zařízení, jedná se o kořenovou část pro většinu standardních objektů. Tato část je povinná pro všechna zařízení, která podporují SNMP a musí poskytovat alespoň základní informace v tomto podstromu. Nalezneme zde například kontaktní informace, umístění, název, verzi systému, typ zařízení. (Kocjan, 2008)

Pomocí SNMP lze získat informace různého druhu. Informace jsou seskupeny do různých kategorií a tyto kategorie mají pak vytvořené alias názvy. Mezi nejdůležitější části stromu MIB patří informace pro síťové připojení, které jsou označeny alias názvy IF-MIB, IP-MIB, IPv6-MIB, RFC1213-MIB, IP-FORWARD-MIB, TCP-MIB a UDP-MIB, dále SNMPv2-MIB a HOST-RESOURCES-MIB. Ty popisují systémové informace a aktuální hodnoty systému, je možno zde najít informaci o úložišti, procesorech, aplikacích, hardwaru apod. (Kocjan, 2008)

6 Analýza požadavků pro výběr dohledového systému

Analýza požadavků je jedním z nejdůležitějších kroků při výběru správného dohledového nástroje. Při analýze je důležité zohlednit velikost monitorované sítě, počet monitorovaných hostů a nejdůležitějším kritériem je počet monitorovaných metrik. Prostor pro práci jsem dostal ve firmě ČD - Telematika a.s., kde pracuji. Firma se zabývá správou sítě pro drážní sektor, tudíž se jedná o druhou největší síť v České republice. Pod dohledový nástroj je potřeba zahrnout přibližně 11 tisíc zařízení a 23 tisíc metrik, které jsou aktuálně monitorovány systémem Nagios. Je potřeba počítat s rozšiřováním sítě a počtem hostů.

6.1 Sledovaná zařízení

Rozmanitost sledovaných zařízení je ve velké síti obrovská. Je potřeba sledovat servery, modemy, převodníky, switche, routery a mnoho dalších zařízení. Mezi nejdůležitější zařízení patří servery, páteřní routery a switche. Na serverech je nutné monitorovat hardware, virtualizační platformu a samotný operační systém, ve všech případech se bude jednat o monitoring vytíženosti zdrojů a monitoring základních služeb, jak na úrovni stavu služby, tak na aplikační úrovni. Virtualizační platforma je sjednocena na VMware a jako operační systémy jsou použity Windows a Linux. Síťové prvky budou ve většině případů hlídány na dostupnost a vytížení jednotlivých páteřních linek. Síťová infrastruktura je postavena nad technologií Cisco. Pro servery Windows by mělo být využito monitoringu pomocí agenta a u Linuxových serverů pomocí protokolu SNMP.

6.2 Finanční požadavky

Aktuálně firma používá zastaralou verzi open source řešení Nagios a i nadále je požadavkem nový dohledový nástroj provozovat na open source řešení bez nákladů na komerční řešení monitoringu. Firma je schopna investovat do vybraného řešení maximálně 700 tisíc korun na nákup serverové části a zálohovacího řešení.

6.3 Aplikační požadavky

Dohledový nástroj musí podporovat grafické rozhraní skrz webové stránky a možnost administrace jednotlivých hostů a metrik prostřednictví webového rozhraní s podporou notifikací prostřednictví e-mailu a telefonu. Systém by měl být založen na jádru Nagios z důvodu aktuálního napojení na ostatní systémy. Dalším požadavkem je prezentace jednotlivých metrik do grafů a udržování historie událostí po dobu jednoho roku. Nutností je také napojení na Active Directory a importování uživatelů do systému.

7 Výběr monitorovacího nástroje

Oddělení architektury do výběru zařadilo tři dohledové systémy založené na jádru Nagios. Jedná se o samotný Nagios, dále dohledové nástroje Centreon a Icinga. Do porovnání byl zařazen i systém Zabbix, který je velice rozšířeným dohledovým nástrojem, ale není založen na jádru Nagios, tudíž nesplňuje jedno z kritérií pro výběr. Ostatní systémy splňují podmínky, které byly vytvořené analýzou požadavků.

7.1 Nagios

Nagios je jedním z nejpoužívanějších monitorovacích nástrojů, je vyvíjen jako open source řešení. Jeho počátky sahají až do roku 1996, kdy byl představen pod názvem NetSaint. Ke konečnému přejmenování na Nagios došlo až v roce 2002. Nagios je aplikace běžící na Linuxu s možností administrace prostřednictvím webového rozhraní nebo konzole. (Kocjan, 2008)

Nástroj umožňuje monitoring síťových služeb, jako jsou SSH, HTTP, SNMP, FTP a mnoho dalších. Dále je pomocí nástroje možné monitorovat využití zdrojů na monitorovaném zařízení. Systém Nagios podporuje monitoring Windows, Linux, Cisco a další operační systémy, které podporují SNMP nebo monitoring pomocí agenta. Monitorované objekty jsou v Nagiosu rozděleny do dvou kategorií: na hosty a services. Hosty jsou myšlena fyzická zařízení, jedná se tedy o servery, routery, tiskárny, switche, modemy a další, které je možné monitorovat prostřednictvím sítě TCP/IP. Pod services je možné zařadit jednotlivé funkce hostů, pro příklad je možné uvést dostupnost HTTP na webovém serveru nebo dostupnost služby syslogd na serveru pro sběr syslog zpráv. Jednotlivé services jsou definovány pro každé zařízení a následně jsou pravidelně monitorovány v nastaveném intervalu. (Yusuff, 2012)

Samotný monitoring probíhá pomocí pluginů, které je možné vytvářet v různých programovacích jazycích. Nejpoužívanějším programovacím jazykem pro pluginy je Perl, ale je možné vytvořit plugin v jazyce Shell, C++, Python a tak dále. V případě problému je Nagios schopný odesílat různá upozornění, která je možné nastavit buď na jednotlivá zařízení, nebo monitorované metriky. Notifikace mohou být odeslány různými způsoby, jako je email, telefon nebo pager. (Yusuff, 2012)

7.2 Centreon

Vznik monitorovacího nástroje Centreon se datuje do roku 2003, kdy vznikl jako open source řešení pod názvem Oreon, následně byl nástroj v roce 2005 převzat fran-

couzskou firmou Merethis a přejmenován na Centreon. Monitorovací systém Centreon vychází z jádra Nagios, tudíž veškeré funkcionality fungují na podobném principu. Dlouho dobu byl Centreon používán jen jako webová nadstavba nad systémem Nagios. K rozdělení došlo až v roce 2011, kdy vzniklo vlastní jádro systému Centreon. Od roku 2011 bylo možné při instalaci vybírat, zda zákazník zvolí jádro Nagiosu a nebo Centreonu. V aktuálních verzích již tato možnost není a využívá se jen jádro Centreonu. Základní verze monitorovacího nástroje Centreon je zdarma a je dostačující k monitoringu rozsáhlé sítě. Zpoplatněné jsou rozšířené balíčky, které přidávají do Centreonu funkcionality jako monitoring business aktivit, připravené šablony pro monitoring různých platforem nebo autodiscovery nástroj. V roce 2015 se firma Merethis přejmenovala na Centreon. (Centreon)

Jádro Centroenu je rozděleno na Centreon Engine a Centreon Broker. Centreon Engine vykonává samotný monitoring nad jednotlivými zařízeními a Centreon Broker se stará o přijímání dat z Centreon Engine a ukládání nasbíraných dat do databáze. Monitorovací systém Centreon má velice propracované webového rozhraní, které nabízí stavové informace k jednotlivým zařízením zařazeným v nástroji, ale také globální pohled na počet zařízení v jednotlivých stavech. (Centreon)

Data, která jsou ukládána do databáze, mohou být dále využívána k analýze jednotlivých zařízení prostřednictvím event logu a grafů. V event logu můžeme najít historii změn stavů na jednotlivých zařízeních za určité období, v grafech lze zobrazit vývoj jednotlivých metrik jako například využití diskové kapacity, vytíženost linky nebo vytížení CPU. Pomocí webového rozhraní je velice jednoduché přidávání a odebírání zařízení a metrik a jejich následné upravování, je také možné vytvoření šablon. Z nich je pak jednoduché vytvořit nový monitoring jen vytvořením zařízení a přiřazením šablony. Metriky jsou aplikovány automaticky pomocí předdefinované šablony. (Centreon)

Jako u monitorovacího systému Nagios je možné vytvářet pro Centreon pluginy a jejich pomocí jsou následně monitorovány jednotlivé metriky. Pluginy jsou nejčastěji vytvářeny v programovacím jazyku Perl, ale je možné použít skripty a pluginy v jazyce Shell, C++, Python a podobné. (Centreon)

Součástí monitorovacího nástroje Centreon je také reportovací systém, který v případě problému dokáže informovat správce, a ti pak mohou daný problém vyřešit. Centreon podporuje upozornění prostřednictvím emailu, SMS zprávy, zprávy na pager

nebo odesláním informace do jiného systému. Upozornění je možné nastavit nad jednotlivými zařízeními, ale i nad jednotlivými metrikami. (Centreon)

7.3 Icinga

Icinga je poměrně mladý monitorovací nástroj, který vznikl v roce 2009 po vnitřních neshodách v týmu Nagios. Hlavní důvodem neshod byla neochota nasazovat nové vlastnosti, které by systém vylepšily. Z toho důvodu vznikl monitorovací systém Icinga založený na jádru systému Nagios. Monitorovací systém Icinga je open source aplikace, kterou je možné získat zdarma. Jelikož Icinga přímo vychází z Nagiosu, přebírá všechny jeho vlastnosti a mechanizmy pro vytváření monitoringu. Icingu je možné využít jak pro malé firemní sítě, tak pro rozsáhlé sítě se stovkami zařízení. (Icinga)

Stejně jako Nagios a Centreon podporuje Icinga vytváření vlastních pluginů v různých programovacích jazycích a těmito pluginy lze prakticky kontrolovat jakoukoliv hodnotu, kterou je možné ze zařízení vyčíst. Mezi nejpoužívanější programovací jazyky se znovu řadí Perl. (Icinga)

Reportovací systém je založený na stejném principu jako u Nagiosu a Centreunu, tudíž je možné zasílat informace o změnách stavu prostřednictvím emailu, sms zpráv, pageru i jinak. (Icinga)

7.4 Zabbix

První zmínky o monitorovacím systému Zabbix sahají až do roku 1998, kdy byl zahájen vývoj systému jako interní projekt pro banku. První verze, která byla uvolněna pod open source licencí, byla vydána v roce 2001, ale první stabilní verze byla uvedena až v roce 2004. Systém Zabbix nevychází z jádra Nagiosu a tudíž používá vlastní mechanizmy k provádění monitoringu. (Zabbix)

Zabbix podporuje velké množství databází včetně komerčních řešení pro ukládání dat. Podporuje databáze MySQL, PostreSQL, Oracle, IBM DB2 a další. Architektura Zabbix serveru je rozdělena na Zabbix server a Zabbix agent. Zabbix server je centrálním prvkem, na kterém je spuštěno webové rozhrání a jsou zde uloženy všechny konfigurace. Na Zabbix serveru se nachází také databáze, do které jsou ukládána data monitoringu, která jsou sbírána ze Zabbix agentů. Zabbix agenti slouží k aktivnímu monitoringu a sběru stavu z jednotlivých zařízení v síti. Agenti svá data následně odesílají na Zabbix server, kde jsou data zpracována a uložena do databáze. (Zabbix)

Zabbix má v sobě integrovány různé šablony pro sledování jednotlivých druhů zařízení. Šablony jsou psány v programovacím jazyce XML a na internetu je možné stáhnout různé šablony pro sledování různých zařízení, jako jsou aktivní prvky sítě, webové stránky, servery, operační systému, hardwarové platformy a mnoho dalších. (Zabbix)

Webové rozhraní systému Zabbix nabízí velmi rozsáhlé využití, od konfigurace celého systému až ke sledování jednotlivých stavů a vytváření analytických podkladů. Pomocí webového rozhraní je možné do systému přidat jednotlivá zařízení a přiřadit k němu jednotlivé šablony. K analýze monitorovaných dat slouží grafy a event logy, ve kterých jsou data přehledně prezentována. Za zmínku také stojí přehledný úvodní dashboard, ve kterém jsou zobrazeny stavové informace a přehledy o celém systému Zabbix. (Zabbix)

Zabbix podporuje různé nastavení upozornění. Je možné definovat různé způsoby upozornění na problémy, mezi nejčastější patří odeslání upozornění pomocí e-mailu nebo sms zprávy. (Zabbix)

7.5 Vyhodnocení požadavků a výběr nástroje

Pro vyhodnocení požadavků a výběr dohledového nástroje byla zvolena metoda vícekriteriálního rozhodování. Úkol této metody bude posoudit vybrané dohledové systémy z hlediska splnění jednotlivých hodnotících kritérií a zvolit dohledový systém, který bude celkově nejvýhodnější.

Budeme postupovat označením jednotlivých systémů, každý systém je v tabulce reprezentován písmenem: Nagios – N, Centreon – C, Icinga – I, Zabbix – Z. Dále byly zvoleny kritéria pro jejich hodnocení, které jsou označené K1 až K13:

- K1: Monitoring rozsáhlé sítě (přibližně 23 tisíc metrik)
- K2: Podrobný monitoring serverů, routerů, switchů
- K3: Open source řešení
- K4: Přehledné grafické rozhraní skrz web
- K5: Jednoduchá administrace systému skrz webové rozhraní
- K6: Notifikace pomocí emailu a mobilu
- K7: Systém založený na jádru Nagios
- K8: Prezentace metrik do přehledných grafů
- K9: Historie událostí po dobu 1 roku
- K10: Možnost napojení na Active Directory
- K11: Podpora SNMP a SNMP trapů
- K12: Podpora NSClienta++
- K13: Dřívější zkušenosti ve firmě

Po určení jednotlivých kritérií byly určeny váhy kritérií, které vyjadřují jejich odlišnou důležitost. Pro váhy byla zvolena stupnice 0 až 9, kdy 0 odpovídá kritériu s nejmenším významem a 9 s nejvyšším významem.

Pro výběr dohledového systému byla sestavena hodnotitelská komise, která byla složena ze dvou členů oddělení architektury, dvou členů oddělení provozu informačních systémů a jedním specialistou dohledových nástrojů, kterého ve firmě zastupuji já.

V tabulce číslo 1 jsou zobrazeny váhy, které byly jednotlivým kritériím přiřazeny. Nejvyšší váha byla udělena kritériu open source, které je z pohledu firmy nejdůležitějším kritériem pro výběr produktu. Ohodnocení jednotlivých dohledových nástrojů probíhalo formou porady celé hodnotitelské komise. Pro kritéria u kterých se určuje,

zda daný produkt kritérium splnil či nesplnil byla učena poloviční hodnota 5 ze stupnice 0 až 9 pro splnil a hodnota 0 pro nesplnil.

Tabulka 1: Hodnocení dohledových systémů

Kritérium hodnocení	Váhy kritérií	Ohodnocení dohledových systémů			
		N	C	I	Z
K1	8	5	5	5	5
K2	6	6	7	5	7
K3	9	5	5	5	5
K4	7	3	8	6	7
K5	6	4	7	7	9
K6	4	5	5	5	5
K7	8	5	5	5	0
K8	5	2	8	6	7
K9	4	5	5	5	5
K10	3	5	5	5	5
K11	7	5	5	5	5
K12	7	5	5	5	0
K13	6	5	9	0	0

Vlastní zdroj

Jak můžeme vidět v tabulce číslo 1, každému systému bylo přiřazeno ohodnocení jednotlivých kritérií. Pro dokončení hodnocení je nutné ohodnocení systému vynásobit váhou kritéria. Celkové hodnocení systémů je možné vidět v tabulce číslo 2.

Tabulka 2: Celkové hodnocení dohledových systémů

Kritérium hodnocení	Váhy kritérií	Ohodnocení dohledových systémů			
		N	C	I	Z
K1	8	40	40	40	40
K2	6	36	42	30	42
K3	9	45	45	45	45
K4	7	21	56	42	49
K5	6	24	42	42	54
K6	4	20	20	20	20
K7	8	40	40	40	0
K8	5	25	40	30	35
K9	4	20	20	20	20
K10	3	15	15	15	15
K11	7	35	35	35	35
K12	7	35	35	35	0
K13	6	30	54	0	0
Celkové hodnocení		**386**	**484**	**394**	**355**

Vlastní zdroj

V tabulce číslo 2 je v posledním řádku zobrazeno celkové hodnocení vybraných systémů. Nejlépe dopadl systém Centreon, který kandidáta na druhém místě překonal o 90 bodů. Na úplném konci skončil systém Zabbix, která ztratil velký počet bodů na nezkušenosti ve firmě a také skutečnosti, že systém nevychází z jádra Nagiosu. Na základě předložených informací k jednotlivým monitorovacím systémům se hodnotitelská komise rozhodla zvolit řešení Centreon.

8 Implementace monitorovacího systému Centreon

Základní popis monitorovacího systému Centreon je uveden v kapitole Výběr monitorovacího nástroje. V této kapitolu je Centreon popsán detailněji a jsou vysvětleny základní funkcionality a možnosti monitorovacího systému Centreon.

Centreon je open source aplikace určená pro monitoring počítačových sítí. Monitorovací systém Centreon je vyvíjen stejnojmennou společností Centreon, která sídlí v Paříži.

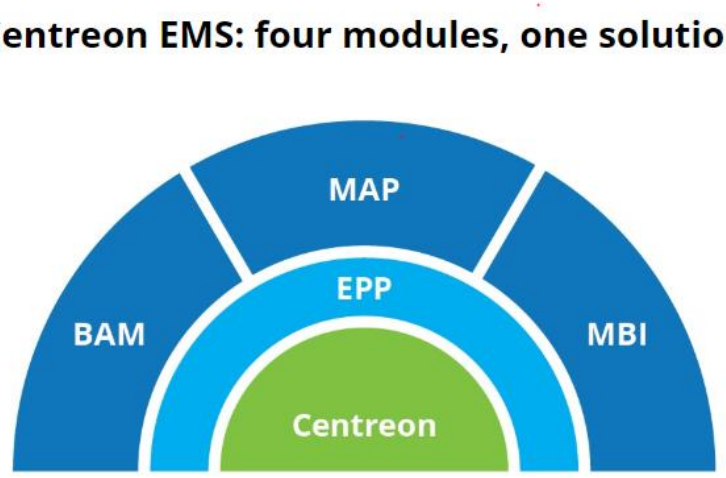
Aplikace Centreon je připravena pro snadnou instalaci a nabízí několik rozšíření, která je možné do systému doinstalovat. Systém Centreon disponuje všemi potřebnými komponentami, které jsou potřebné pro monitoring jakéhokoliv informačního systému. Monitorovací nástroj obsahuje například komponenty a funkce, kterými jsou:

- jádro programu pro sběr monitorovacích dat
- kompletní knihovnu pluginů pro monitoring infrastruktury, aplikací, ale i síťových prvků
- víceuživatelské a přehledné uživatelské rozhraní pomocí webu
- pokročilá správa uživatelů pomocí přístupových listů (ACL)
- kompletní správa alarmů a vytváření upozornění na alarmy
- přizpůsobitelné panely ve webovém rozhraní
- reporty dostupnosti jednotlivých služeb

8.1 Komponenty monitorovacího systému Centreon

Základní aplikace, která je zdarma, může být rozšířena o různé komponenty, které podléhají licenční politice společnosti a jsou zpoplatněny měsíční platbou. Celkově se systémem Centreon, zahrnující veškeré komponenty, nazývá Centreon EMS. EMS pochází z anglického spojení Enterprise Monitoring Solution, které ve volném překladu znamená řešení pro monitoring na podnikové úrovni. Obrázek 4 zobrazuje rozdělení Centreonu EMS na jednotlivé komponenty, celkově se jedná o pět komponent, ze kterých se Centreon skládá.

Obrázek 4: Komponenty monitorovacího systému Centreon



(Centreon)

8.1.1 Komponenta Centreon

Základní komponentou je samotný Centreon, pod kterým se skrývá samotná aplikace sloužící pro monitoring. Jako jediná z komponent je komponenta Centreon zdarma a je možné pomocí této jediné komponenty monitorovat celou infrastrukturu podnikové sítě, následné komponenty jsou již jen doplňující a slouží buď k jednoduššímu ovládání a zařazování nových zařízení, nebo k monitoringu podnikových procesů.

Komponentu Centreon je možné zdarma získat z oficiálních stránek Centreonu na adrese https://download.centreon.com/. Instalační soubor je možné stáhnout ve formátu ISO, OVA nebo OVF, existuje také možnost přímé instalace z příkazové řádky Linuxového systému přímo z RPM balíčku. Společnost Centreon doporučuje instalaci provádět pomocí ISO souboru nebo pomocí RPM balíčku.

Součástí komponenty Centreon je i webové rozhraní bohaté na funkcionality, které je uživatelsky velice přívětivé. Dříve bylo webové rozraní jedinou komponentou společnosti Centreon, webové rozhraní bylo využíváno nad jádrem Nagiosu a sloužilo k administraci a sledování stavů v monitoringu. Nyní je webové rozhraní postaveno nad bohatou monitorovací platformou společnosti Centreon, která se skládá z komponent Centreon Engine, Centreon Broker a Centreon Web.

Ostatní komponenty je možné do systému Centreon doinstalovat prostřednictvím webového rozhraní nainstalované komponenty Centreon. Komponenty je nutné mít zakoupené prostřednictvím svého účtu u společnosti Centreon a prostřednictvím svého webového rozhraní se přihlásit k účtu. Veškeré komponenty jsou následně zpřístupněny.

V našem řešení je použita jen komponenta Centreon, která je dostupná pod open source licencí, ostatní komponenty jsou jen představeny pro znázornění, jaké možnosti monitorovací systém Centreon nabízí.

8.1.2 Komponenta EPP

První rozšiřující komponentou Centreonu je komponenta EPP, její název je odvozen z anglického pojmenování Enterprise Plugin Pack, který ve volném překladu znamená balík pluginů pro podnikové prostředí.

Komponenta EPP je balíček předpřipravených šablon pro většinu známých technologií. Jedná se o předpřipravené šablony pro monitoring hardwaru, databází, cloudu, aplikací, operačních systémů a mnoho dalších balíčků. Seznam veškerých dostupných balíčků pro monitoring je možné zobrazit pod následujícím odkazem https://www.centreon.com/en/plugins-pack-list/. Na obrázku 5 můžeme vidět vyjmenované jednotlivé technologie, které jsou v EPP zahrnuty.

Obrázek 5: Technologie komponenty EPP

(Centreon)

Balíček šablon je skvělým pomocníkem pro uživatele, kteří se nechtějí zdržovat psaním vlastních monitorovacích skriptů a vytvářením vlastních šablon pro jednotlivé technologie. Šablony od společnosti Centreon jsou určeny k implementaci ihned po instalaci komponenty.

Komponenta je zpoplatněna měsíční sazbou, Centreon nabízí zdarma jen 6 balíčků, které si uživatel může nainstalovat a vyzkoušet. Zdarma dostává uživatel přístup k balíčkům pro monitoring serverů Centreon, operačního systému Linux a Windows,

databází MySQL a MariaDB, základní balíček Cisco, standartních tiskáren a standartních UPS.

8.1.3 Komponenta BAM

Druhou rozšiřující komponentou je komponenta BAM, název je odvozen od anglického sousloví Business Activity Monitoring, který ve volném překladu znamená monitoring obchodních aktivit.

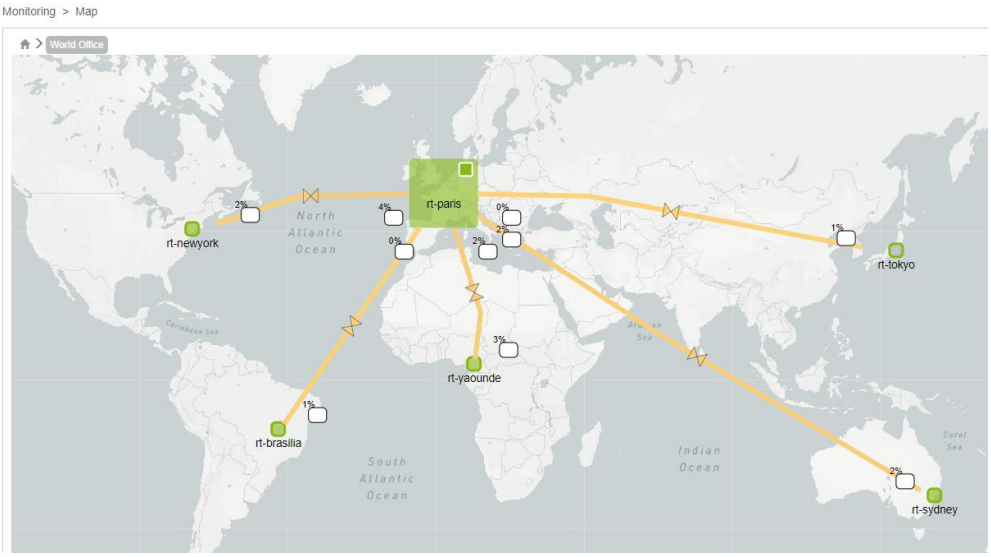
Komponenta zaměřená na ITIL má za úkol sladit poskytování IT služeb s obchodními potřebami. Komponenta na základě postupů ITIL měří provozní vitalitu IT v reálném čase na základě dat z monitoringu, aby ukázala zásadní korelace s výkonem služby. Pomocí komponenty jsou snadno spravované IT operace a jsou stanoveny priority poskytovaných IT služeb. Hlavním úkolem komponenty je zobrazit vazby mezi aplikacemi a kritickými IT zařízeními.

8.1.4 Komponenta MAP

Třetí komponentou je komponenta MAP, název je odvozen od anglického Data Mapping And Visualization, což ve volném překladu znamená mapování a vizualizace dat.

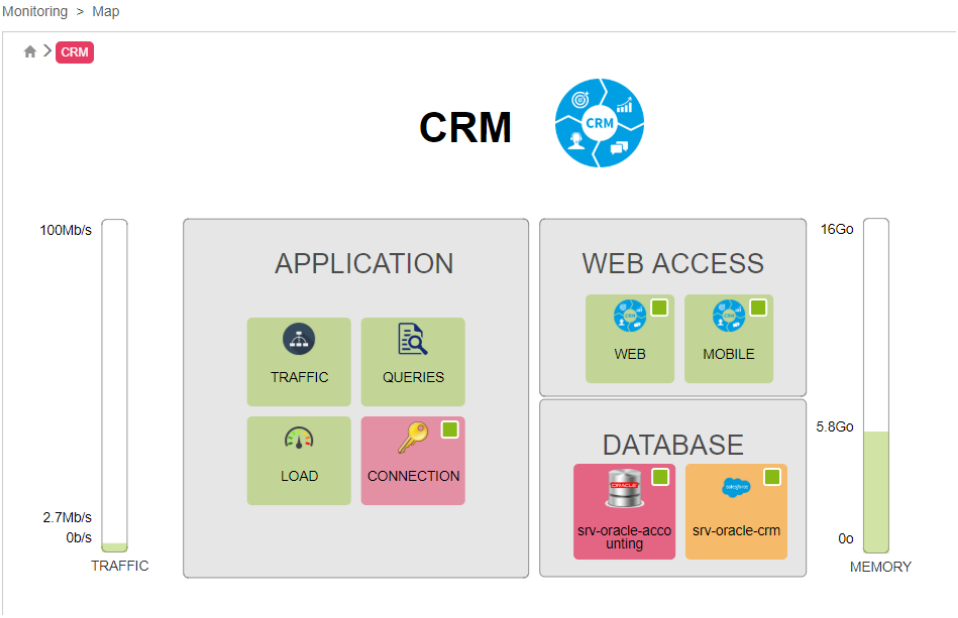
Komponenta slouží k zobrazení jednotlivých zařízení a jejich stavu v mapě. Centreon MAP je bohatý nástroj pro mapování a vizualizaci dat, který může být vyžadován od správců a vývojářů. Data jsou mapována pomocí grafického informačního systému GIS. Na obrázku 6 lze vidět, jakým způsobem jsou data v mapě zobrazena. Vidíme zde jednotlivé kanceláře napříč celým světem a také vazby mezi jednotlivými kancelářemi i aktuální vytíženost linek. Obrázek 7 zobrazuje také mapu vytvořenou pomocí komponenty MAP, ale tentokrát se zaměřením na jednu část podnikového systému, a to konkrétně CRM.

Obrázek 6: Komponenta MAP



(Centreon)

Obrázek 7: Komponenta MAP



(Centreon)

8.1.5 Komponenta MBI

Čtvrtou komponentou je komponenta MBI, název je odvozen od anglického Monitoring Business Intelligence, který ve volném překladu znamená monitoring podnikové inteligence.

Komponenta slouží k transformaci naměřených dat a metrik do reportů, které mohou být užitečné při rozhodování. Jedná se o jednoduchý reportovací modul, který usnadňuje práci při vyhodnocování operací a výkonosti IT. V komponentě je předdefi-

nováno více než 30 šablon pro vytváření reportů. Mezi předdefinované reporty patří například dostupnost zařízení, obsazenost kapacit a výkonu, vytížení portů, spotřeba energie a mnoho dalších. Reporty je možné zasílat prostřednictvím mailu v různých formátech, ale je možné reporty ukládat i na vyhrazené úložiště.

8.2 Architektura systému Centreon

Centreon umožňuje několik variant, kterými lze systém implementovat. Je možné zvolit jednoduchou architekturu, ve které jeden server obsluhuje veškerou činnost monitoringu, včetně dotazování na jednotlivá zařízení v síti až ke složitým architekturám, kde je použito více serverů. Základní rozdělení serverů je na centrální servery a poller servery.

Centrální server je plnohodnotný server, který obsahuje databázi, kam jsou ukládána data, Centreon Engine a Centreon Broker. Jak již bylo řečeno v kapitole Výběr monitorovacího nástroje, Centreon Engine provádí samotný monitoring nad zařízeními a následně je odesílá do Centreon Broker, který je přijímá a ukládá do databáze. Centrální server je sám schopný monitorovat zařízení pomocí pluginů. Součástí centrálního serveru je také Centreon web, pomocí kterého je možné provádět konfiguraci a výčet stavových informací.

Oproti tomu poller server je jednoduchý server obsahující jen Centreon Engine, který provádí samotný monitoring pomocí pluginů. Ty jsou na poller serverech také implementovány a následně nasbíraná data odesílá do centrálního serveru.

V této kapitole budou stručně představeny jednotlivé architektury systému Centreon, které je možné implementovat.

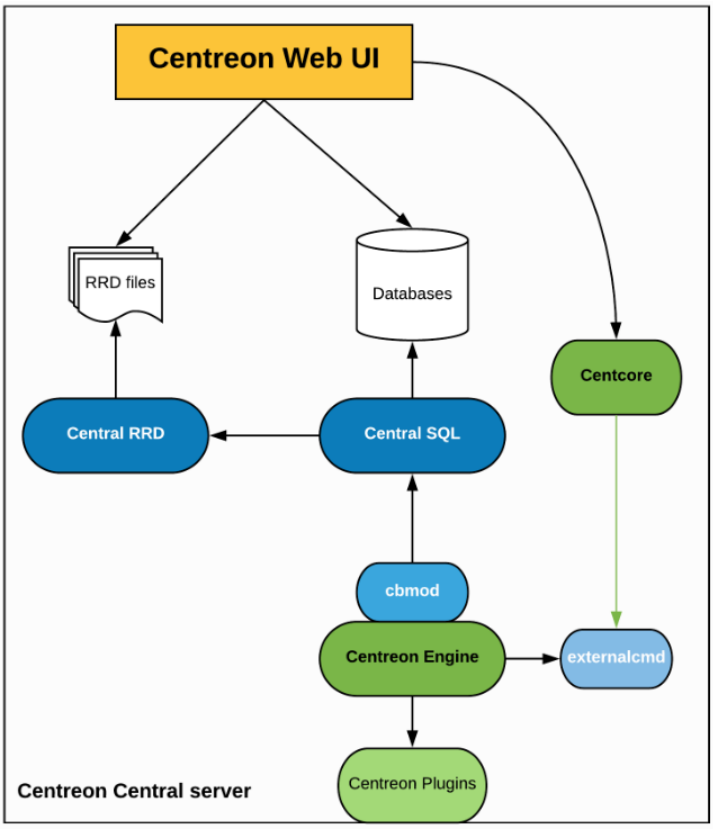
8.2.1 Základní architektura

Základní architektura obsahuje jen jeden centrální server, který se stará jak o samotný monitoring prostřednictvím Centreon Engine, tak o ukládání do databáze prostřednictvím Centreon Brokeru. Samozřejmostí je také webové rozhraní, kde je možná konfigurace a sledování monitoringu.

Jedná se o nejjednodušší způsob instalace. Pomocí této architektury není zajištěna žádná redundance dat a pokud server selže, nemáme žádná data z monitoringu pro případnou analýzu problémů.

Na obrázku 8 je zobrazena základní architektura. Můžeme vidět jednotlivé komponenty, které jsou na serveru spuštěny. Základem je Centreon Web UI, jedná se o webové rozhraní, které čerpá data z databáze a nástroje RRD. RRD slouží pro vykreslování grafů nad jednotlivými metrikami. Dále na obrázku nalezneme Centreon Engine, který provádí samotný monitoring prostřednictvím pluginů.

Obrázek 8: základní architektura



(Centreon)

8.2.2 Distribuovaná architektura

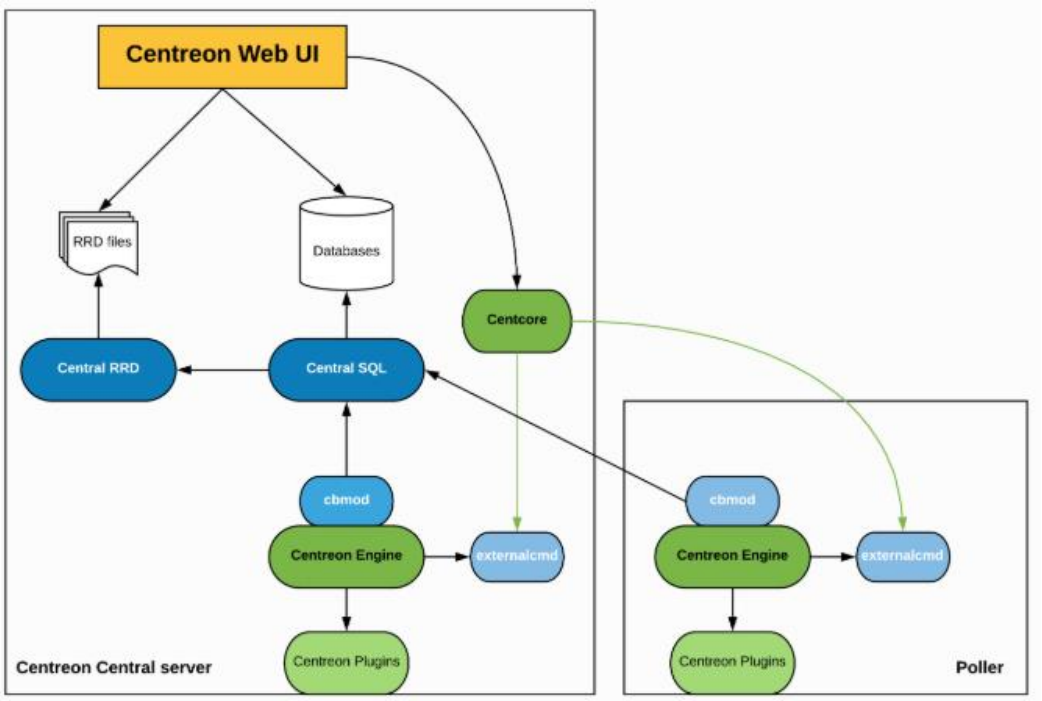
Další architekturou je distribuovaná architektura, která již využívá rozdělení serverů na minimálně jeden centrální server a jeden poller server.

Centrální server se neodlišuje od základní architektury, obsahuje Centreon Web UI, databázi, Centreon Engine a Centreon Broker. Pomocí centrálního serveru je možné provádět monitoring, ale k tomu účelu jsou spíše využívány jen poller servery.

Poller server v sobě obsahuje jen Centreon Engine, který se stará o samotný monitoring, a Centreon Broker, který zajišťuje odeslání dat do Centrálního serveru.

Architektura se používá v rozsáhlejších sítích, kdy je potřeba zátěž monitoringu rozdělit na více poller serverů. Jednotlivým poller serverům je možné přiřadit libovolný počet zařízení, která budou prostřednictvím pollera monitorována. Dále je tato architektura využívána pro monitoring DMZ, jelikož je snazší a bezpečnější umístit do oddělené sítě jeden poller server, který bude danou lokalitu monitorovat a následně odesílat data do centrálního serveru. Schéma architektury je zobrazeno na obrázku 9.

Obrázek 9: Distribuovaná architektura

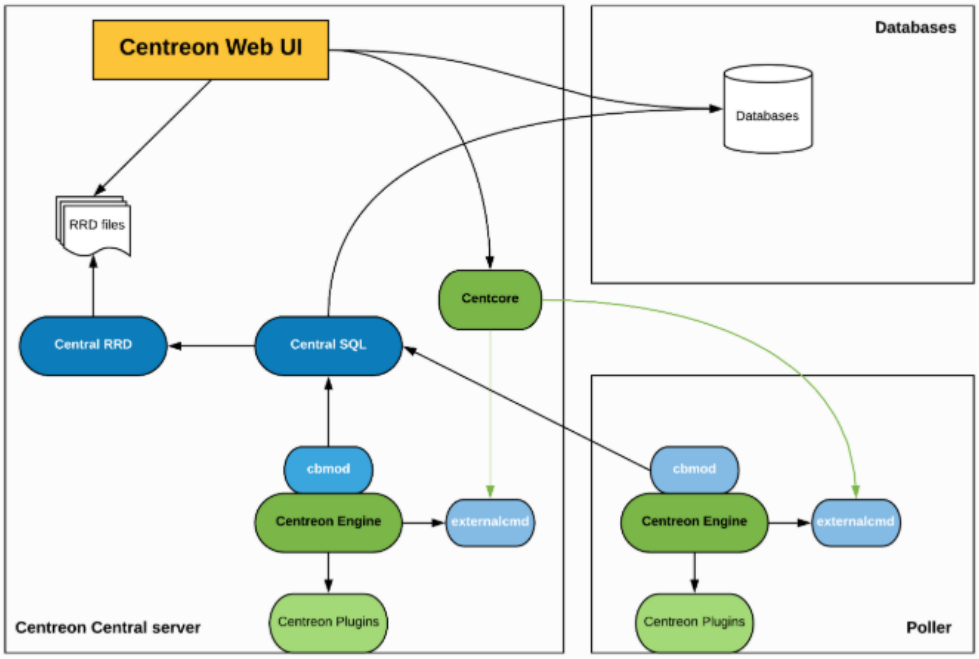


(Centreon)

8.2.3 Distribuovaná architektura se vzdálenou databází

Architektura je totožná s předchozí distribuovanou architekturou, jediným rozdílem je vzdálená databáze, která běží na vlastním serveru. Rozdělení je zobrazeno na schématu této architektury na obrázku 10. Architektura má stejné výhody jako předchozí architektura, dále se přidává výhoda oddělené databáze, která je v případě pádu centrálního serveru stále k dispozici a je možné využívat data z databáze, případně napojit na nový centrální server.

Obrázek 10: Distribuovaná architektura se vzdálenou databází



(Centreon)

8.2.4 Distribuovaná architektura s podporou převzetí služeb při selhání

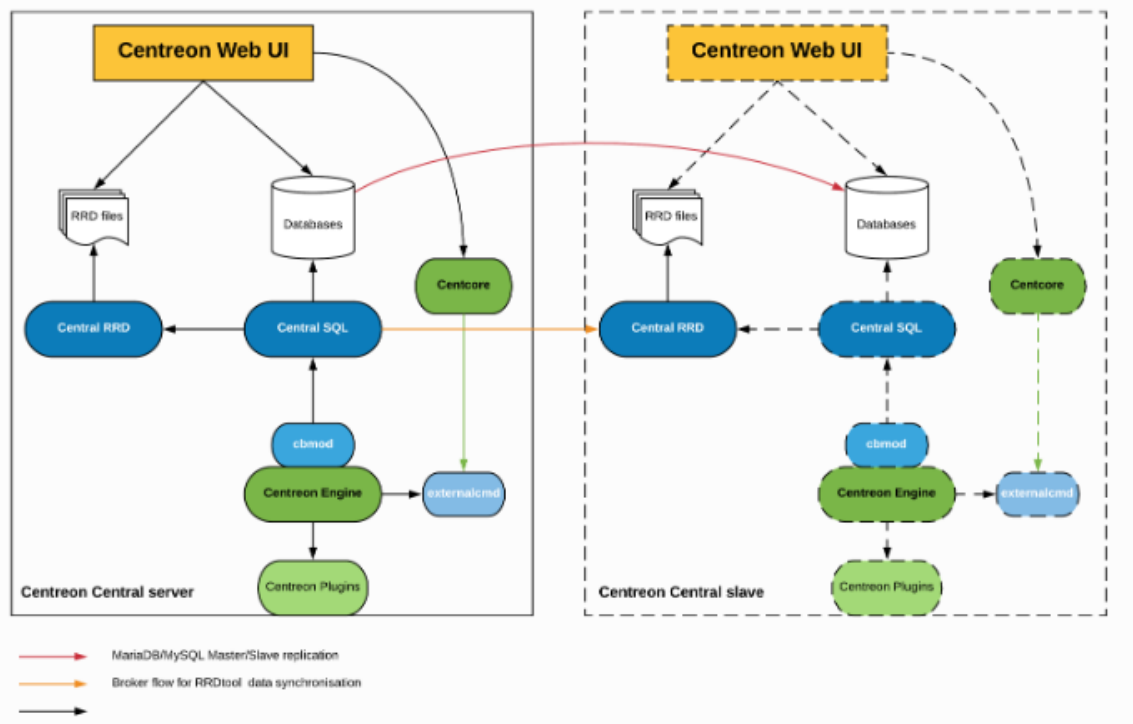
Tato architektura přebírá všechny vlastnosti ze základní distribuované architektury. Přidán je jen další centrální server, dva centrální servery jsou následně rozděleny do rolí master a slave. Toto rozdělení slouží k převzetí služeb monitoringu v případě pádu centrálního serveru. Oba servery jsou v aktivním stavu, první server ve stavu master provádí veškerou činnost spojenou s monitoringem a následně data předává do druhého serveru, označovaného slave. Architektura je zobrazena na obrázku 11.

Hlavní výhodou této architektury je možnost převzetí služeb monitoringu slave server v případě pádu master serveru. Slave server plně nahradí master server a je možné pokračovat v zobrazování dat prostřednictvím webového rozhraní na slave serveru, dokud není master server zprovozněn.

Slave server je používán v běžném režimu, ale není na něm aktivně spuštěn Centreon Engine, tato komponenta je na serveru spuštěna až v případě pádu master serveru. Data do databáze jsou replikována z master serveru pomocí MySQL replikace dat. RRD soubory, které slouží k zobrazení grafů, jsou do systémů přenášeny pomocí Centreon Brokeru. V případě pádu je na slave serveru spuštěn webový server, služba CentCore, Centreon Engine, Centreon Broker SQL. Převzetí služeb a správa komponent jsou nej-

častěji realizovány pomocí linuxového nástroje Corosync/Pacemaker, ale je možno využít jakýkoliv nástroj, který takovou funkcionalitu umožňuje. Centreon nemá sám implementovaný nástroj.

Obrázek 11: Distribuovaná architektura s podporou převzetí služeb při selhání



(Centreon)

8.2.5 Výběr architektury pro implementaci

Pro implementaci v rámci práce byla vybrána základní distribuovaná architektura s jedním centrálním serverem a minimálně jedním poller serverem.

Základní architektura byla zamítnuta, jelikož se jedná o nedostatečné řešení v rámci rozsáhlé počítačové sítě. Dále byla z výběru odebrána distribuovaná architektura se vzdálenou databází, jelikož jedním z aplikačních požadavků je běh databáze na centrálním serveru. Do závěrečného rozhodování se tedy dostala distribuovaná architektura a distribuovaná architektura s podporou převzetí služeb při selhání. Pro konečné rozhodnutí bylo vytvořeno testovací prostředí, ve kterém bylo zjištěno, že aplikace Centreon je spolehlivá aplikace a její rozdělení na dva centrální servery není nutné. Při replikaci velkých objemů dat, které se na takto velké síti dají očekávat, dochází při použití architektury master a slave server ke značnému zatížení serveru a přínos této architektury je spíše negativní. Proto bylo rozhodnuto při implementaci zvolit základní dis-

tribuovanou architekturu a v případě pádu obnovení centrálního serveru ze záloh, které budou pravidelně prováděny.

8.3 Instalační požadavky sytému Centreon

Požadavky na instalaci systému Centreon vychází z tabulky číslo 3, která je převzata z oficiální dokumentace k systému Centreon. V tabulce jsou v prvních dvou sloupcích reprezentována rozmezí metrik a zařízení, která budou monitorovacím nástrojem Centreon monitorována a ve třetím sloupci jsou k dispozici minimální požadavky na počet centrálních a poller serverů. V posledních dvou sloupcích jsou definovány systémové prostředky na centrální servery a poller server. Jsou zde vyjádřeny požadavky na počet virtuálních CPU a velikost paměti RAM.

Tabulka 3: Systémové požadavky na instalaci

Počet monitorovaných metrik	Počet monitorovaných zařízení	Počet poller serverů	Požadavky na Centrální server	Požadavky na Poller server
< 500	50	1 central	1 vCPU / 1 GB	
500 – 2000	50 – 200	1 central	2 vCPU / 2 GB	
2000 - 7000	200 - 700	1 central + 1 poller	4 vCPU / 4 GB	1 vCPU / 4 GB
7000 - 14000	700 - 1400	1 central + 1 poller	4 vCPU / 8 GB	2 vCPU / 4 GB
14000 - 21000	1400 - 2100	1 central + 2 pollers	4 vCPU / 8 GB	2 vCPU / 4 GB
21000 - 28000	2100 - 2800	1 central + 3 pollers	4 vCPU / 8 GB	2 vCPU / 4 GB
...	...	...	...	...

(Centreon)

Dalším oficiálním požadavkem Centreonu je, aby každý poller server monitoroval maximálně sedm tisíc metrik a jeho virtuální CPU mělo frekvenci kolem 3 GHz. Základní požadavky v tabulce jsou jen orientační, záleží na složitosti jednotlivých měření, podle kterých je případně nutné systémové prostředky upravit.

Z kapitoly Analýza požadavků je zřejmé, že aktuální počet metrik je přibližně kolem 23 tisíc metrik a 12 tisíc zařízení. Je nutné do budoucna počítat s rozšiřováním sítě a síťových zařízení. Navrhované řešení se hodí svými parametry do šestého řádku a bude potřeba počítat minimálně s jedním centrálním serverem a třemi poller servery. Centrální server bude disponovat alespoň čtyřmi virtuálními CPU a pamětí RAM o velikosti 8 GB, poller servery minimálně dvěma virtuálními CPU a RAM pamětí o velikosti 4 GB.

Dále je nutná definice diskové kapacity jednotlivých serverů. Disková kapacita na centrálním serveru se odvíjí od počtu monitorovaných metrik, protože jsou na server ukládána data monitoringu, poller servery mají danou jednotnou velikost, jelikož nedochází k ukládání dat. Disková kapacita na centrálním serveru je dále ovlivněna také frekvencí provádění jednotlivých metrik a časovým obdobím, po které se budou data uchovávat. V tabulce číslo 4 jsou definované doporučené dynamické diskové kapacity pro databázi a aplikaci Centreon podle počtu monitorovaných metrik. Běžně Centreon počítá s frekvencí monitoringu jednotlivých metrik každých pět minut a uchováváním dat po dobu půl roku.

Tabulka 4: Dynamické požadavky na diskovou kapacitu pro centrální server

Počet monitorovaných metrik	/var/lib/mysql (v GB)	/var/lib/centreon (v GB)
500	10	02.5
2000	42	10
10 000	93	27
20 000	186	54
50 000	465	135
100 000	930	270
...	...	...

(Centreon)

Tabulka číslo 5 zobrazuje doporučené statické diskové kapacity pro systém na centrálním serveru. Na rozmyšlení pro uživatele je hodnota pro zálohování, jelikož systém Centreon disponuje funkcí, ve které je možné definovat pravidelné zálohy.

Tabulka 5: Statické požadavky na diskovou kapacitu pro centrální server

Souborový systém	Velikost
Swap	1 až 1.5 násobek celkové RAM
/	alespoň 20 GB
/var/log	alespoň 10 GB
/var/lib/centreon	definováno v předchozí tabulce
/var/lib/centreon-broker	alespoň 5 GB
/var/cache/centreon/backup	alespoň 10 GB (záleží na počtu uchovávaných záloh)

(Centreon)

Tabulka číslo 6 definuje doporučené kapacity pro poller servery. Hodnoty se prakticky neliší od požadavků na centrální server, rozdíl je jen ve velikosti pro zálohování, které si uživatel určuje sám podle počtu záloh.

Tabulka 6: Statické požadavky na diskovou kapacitu pro poller server

Souborový systém	Velikost
Swap	1 až 1.5 násobek celkové RAM
/	alespoň20 GB
/var/log	alespoň10 GB
/var/lib/centreon-broker	alespoň 5 GB
/var/cache/centreon/backup	alespoň 5 GB (záleží na počtu uchovávaných záloh)

(Centreon)

Dle oficiálních požadavků si každý uživatel systému Centreon může dopočítat, kolik přibližně bude potřebovat diskové kapacity a systémových zdrojů. Pro přesnější výpočty slouží tabulka od společnosti Centreon, do které je možné zadat všechny parametry, definice zdrojů se pak přehledně zobrazí v tabulce. Ta zobrazuje i doporučený počet poller serverů. Tabulku je možné stáhnout pod následujícím odkazem https://documentation.centreon.com/docs/centreon/en/latest/_downloads/Centreon_platform_sizing.xlsx.

Navržené řešení, pokud budeme počítat s rezervou, by spadalo přibližně do 30 až 40 tisíc metrik. Pro centrální server je nutné alokovat alespoň 550 GB diskové kapacity a pro každý poller server alespoň 50 GB diskové kapacity.

8.3.1 Definice instalačních požadavků pro implementaci

Dle předložených definic instalačních požadavků se společnost rozhodla rozdělit monitorovací servery na tři fyzické servery. Servery budou rozděleny do dvou lokalit, v první lokalitě budou umístěny dva a v druhé lokalitě jeden fyzický server.

Architektura systému byla zvolena základní distribuovaná, tudíž budeme mít jeden centrální server a dle požadavků minimálně čtyři poller servery. Centrální server bude umístěn v první lokalitě na jednom fyzickém serveru, poller servery budou umístěny v první a druhé lokalitě také samostatně na fyzických serverech. Celkem bylo rozhodnuto, že bude zprovozněno osm poller serverů, čtyři poller servery v první lokalitě a čtyři poller servery v druhé lokalitě. Naddimenzování je z důvodu redundance a v případě pádu jedné lokality existuje možnost migrování veškerých metrik do druhé lokality.

V první lokalitě poběží na jednom fyzickém serveru centrální server, který bude mít minimální zdroje 35 CPU, 50 GB RAM a 2,5 TB diskové kapacity. Další dva servery určené pro poller servery budou mít minimální zdroje 30 CPU, 32 GB RAM a 650

GB diskové kapacity. Požadavky na servery byly naddimenzovány, aby bylo do budoucna možné navyšovat zdroje a případně rozšiřovat monitoring o nové komponenty, případně pro vytvoření testovacích prostředí a při instalaci podpůrných systémů.

8.4 Životní cyklus systému Centreon

Společnost Centreon se rozhodla od roku 2018 vydávat pravidelně ve stejných intervalech nové verze monitorovacího systému Centreon. Toto rozhodnutí vede k možnosti plánovat si dopředu aktualizaci systémů a dává uživatelům záruku jeho neustálého vývoje.

8.4.1 Formát verzí

Verze monitorovacího systému jsou odvozeny od data, kdy byla daná verze vydána. Například verze 19.10 byla vydána v říjnu roku 2019, všechny moduly a komponenty používají stejné označení verzí. Centreon podle plánu každý rok vydává dvě hlavní verze, první v dubnu a druhou v říjnu. Mezi těmito verzemi zpřístupňuje aktualizace a opravy chyb.

8.4.2 Výběr verze pro implementaci

Pro implementaci byla zvolena nejnovější verze monitorovacího systému Centreon 19.10 a instalace prostřednictvím ISO souboru.

8.5 Nákup serverů pro dohledový nástroj

V kapitole Analýza požadavků byly definovány finanční požadavky na nákup nových serverů a zálohovacího řešení. Pro nákup nových serverů bylo vyčleněno 700 tisíc korun. V kapitole Definice instalačních požadavků pro implementaci byly definovány zdroje pro jednotlivé servery. Požadavky na jednotlivé fyzické servery, které byly odeslány dodavatelům, jsou následující:

- 1x server pro centrální server
    - 35 CPU
    - Operační paměť RAM 50 GB
    - Disková kapacita 2,5 TB
- 2x server pro poller servery
    - 30 CPU
    - Operační paměť RAM 32 GB
    - Disková kapacita 650 GB

- 2x zálohovací server
    - Disková kapacita 32 TB

Firma se rozhodla oslovit společnosti Dell, Huatech, C-Systém, HP, aby dodaly nabídky na servery pro monitoring a společnost Kobe, která výhradně dodává zálohovací značky firmy Synology. Do výběrového řízení byly zařazeny všechny nabídky od vybraných společností.

Finanční oddělení ve spolupráci s oddělením Provozu informačních systémů rozhodlo o nákupu fyzických serverů pro monitoring od společnosti C-Systém, která dodala nabídku se servery Lenovo. Zálohovací servery byly poptávány jen u jedné společnosti Kobe, která nabídla zálohovací řešení Synology.

Společnost C-Systém dodala servery v následující specifikaci:

- 1x server pro centrální server ThinkSystem SR570
    - 2x Intel Xeon Gold 18 C = 36 CPU
    - 4x ThinkSystem 16GB DDR4 = operační paměť RAM 64 GB
    - 4x ThinkSystem 2.5" 5210 1.92TB SSD = disková kapacita 7,68 TB
- 2x server pro poller servery ThinkSystem SR570
    - Intel Xeon Silver 16 C = 32 CPU
    - 2x ThinkSystem 16GB DDR4 = operační paměť RAM 32 GB
    - 2x ThinkSystem 2.5" Intel S4510 960GB SSD = disková kapacita 1,92 TB

Společnost Kobe dodala zálohovací řešení v následující specifikaci:

- 2x zálohovací server Synology RS819
    - 4x Seagate Enterprise NAS HDD 8TB = 32 TB

Celková hodnota investice se vyšplhala na částku 672 tisíc korun. Servery pro centrální a poller servery celkově stály 556 tisíc korun a zálohovací řešení 116 tisíc korun. Nákupem byl splněn finanční limit 700 tisíc korun, který byl definován v analýze požadavků.

8.6 Instalace monitorovacího systému Centreon

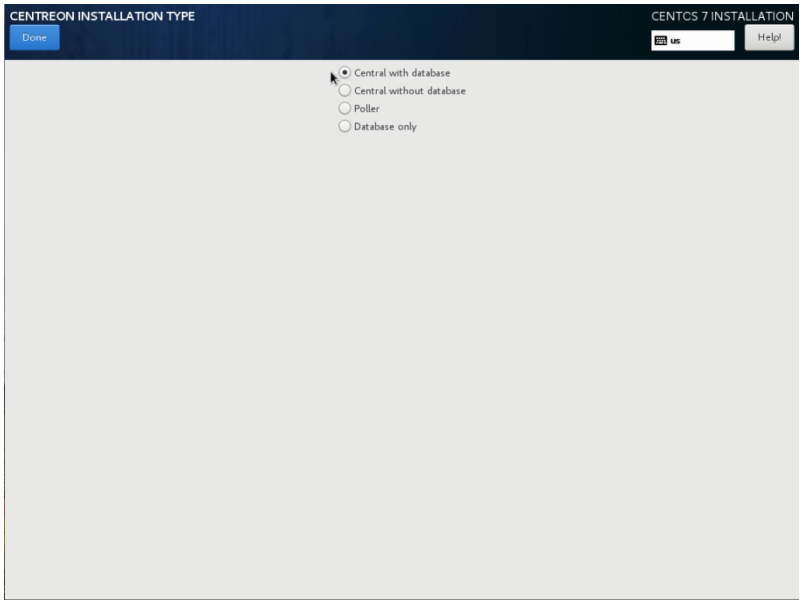
8.6.1 Instalace operačního systému

Pro instalaci byl zvolen postup pomocí ISO souboru, což patří k nejjednodušším způsobům instalace, protože je celá instalace od společnosti Centreon, zároveň je tento druh instalace doporučován společností Centreon předpřipravena.

ISO soubor je možné stáhnout z oficiálních stránek Centreonu, v našem případě verze 19.10, která běží nad systémem CentOS 7. Pro instalaci jednotlivých virtuálních serverů byla na fyzické servery nainstalována virtualizační platforma VMware. Po spuštění instalace se dostáváme do klasického průvodce, který je totožný s instalací operačního systému CentOS.

Po zvolení instalace operačního systému CentOS 7 je uživatel vyzván k výběru jazyka, který bude zvolen pro operační systém. Instalace je totožná s instalací operačního systému CentOS 7, jediným rozdílem je možnost zvolit druh Centreon serveru, zda se bude jednat o centrální server, poller server, centrální server bez databáze, nebo server jen s databází. Volba druhu Centreon serveru je zobrazena v následujícím obrázku 12.

Obrázek 12: Volba druhu Centreon serveru

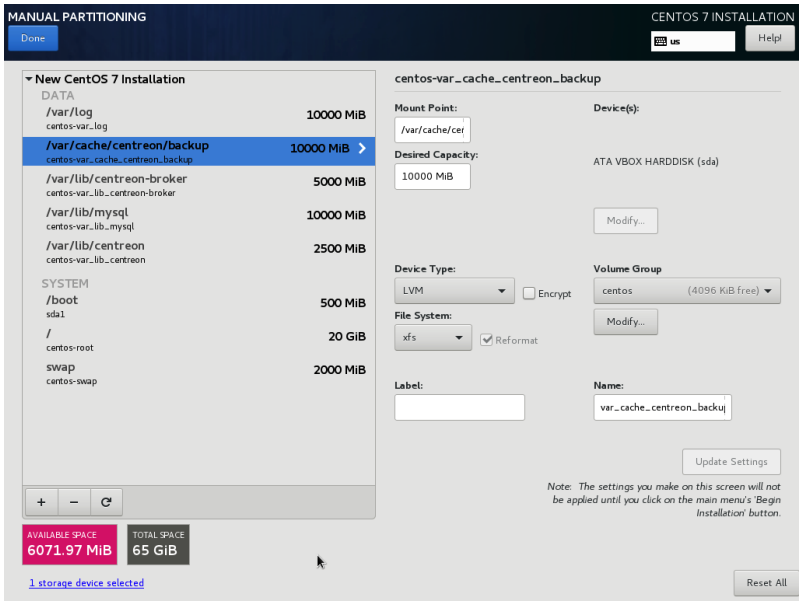


(Centreon)

Po volbě druhu Centreon serveru je doporučeno rozdělit diskovou kapacitu Centreonu na jednotlivé oddíly. Centreon doporučuje rozdělit diskovou kapacitu dle poža-

davků v tabulkách s diskovou kapacitou, tabulky jsou vloženy v kapitole Instalační požadavky sytému Centreon, v obrázku 13 můžeme vidět ukázkové rozdělení.

Obrázek 13: Rozdělení diskové kapacity na jednotlivé oddíly



(Centreon)

Po vytvoření jednotlivých diskových oddílů je důležité nastavit datum a čas. Nejprve je nutné vybrat časovou zónu, v našem případě Europe/Prague, a je možné zadat čas ručně, ale spíše je doporučováno připojit server na některý časový server ve firmě nebo na internetu. Je možné vložit i více časových serverů.

Dalším důležitým krokem v instalaci je konfigurace síťového rozhraní. Je nutné síťové rozhraní povolit a přiřadit k síťovému rozhraní IP adresu, v nastavení síťového rozhraní je dobré také nastavit název serveru, který se vkládá do políčka hostname.

Po nastavení těchto základních kroků je možné spustit samotnou instalaci serveru, po spuštění instalace je ještě uživatel požádán o zadání hesla pro uživatele root, tedy super uživatele v systému linux s administrátorským oprávněním. Po dokončení instalace je nutné provést restart serveru a instalační proces je dokončen. Po restartování serveru je nainstalován systém CeonOS 7 s monitorovacím systémem Centreon.

Po dokončení instalace operačního systému je možné se na server připojit pomocí protokolu SSH a provést doporučený update celého systému. Systém linux je možné updatovat pomocí příkazu *yum update*, po dokončení veškerých aktualizací je nezbytné systém restartovat.

V rámci této práce byl jeden server nainstalován jako centrální server a osm serverů jako poller servery podle zde popsaného postupu. Po dokončení aktualizace a restartovaní všech serverů je možné pokročit k dalšímu kroku implementace.

8.6.2 Dokončení instalace systému Centreon

Po instalaci operačního systému je nutné přistoupit k dokončení instalace prostřednictvím webového prostředí. Prvotním krokem je zjištění IP adresy centrálního serveru. Adresu lze převzít z instalačního procesu, nebo je možné ji zjistit například pomocí příkazu *ip addr*, který se zadá na SSH konzoli centrálního serveru.

Adresa centrálního serveru se použije pro připojení do webového rozhraní serveru pomocí webového prohlížeče, adresa se zadá ve tvaru http://[IP_adresa_centrálního_serveru]/centreon. Po zadání adresy do prohlížeče se zobrazí webový průvodce, který slouží pro dokončení instalace systému Centreon. Stejný průvodce je zobrazen i v případě aktualizace systému Centreon po vydání nové verze. První obrazovka v průvodci je spíše informativní a sděluje uživateli, že průvodce pomůže s konfigurací databáze a monitorovacího systému, další informací je, že konfigurace bude trvat přibližně deset minut.

Po kliknutí na tlačítko další průvodce přejde na druhou obrazovku, na které jsou zkontrolovány moduly, které jsou nutné pro systém Centreon. Veškeré moduly by měly být nainstalovány, jelikož byla použita instalace pomocí oficiálního ISO souboru společnosti Centreon. V případě, že je instalace prováděna pomocí RPM balíčků, může kontrola skončit nezdarem a je nutné doinstalovat požadované moduly. Kontrolované moduly jsou zobrazeny na obrázku 14.

Obrázek 14: Průvodce konfigurací - kontrola modulů

(Vlastní zdroj)

Na dalších dvou obrazovkách vidíme umístění jednotlivých souborů v systému, je možné uvedené cesty změnit, ale změny je nutno si pamatovat a případně soubory hledat v novém umístění.

Dalším krokem je nastavení administrátorského přístupu do systému Centreon. Je nutné vyplnit heslo pro přístup do systému, uživatelské jméno, příjmení a email administrátorského účtu.

Po vytvoření prvního administrátorského účtu je nutné nastavit databázové parametry. Defaultně jsou hodnoty předvyplněné a je nezbytné doplnit heslo pro přístup do databáze. V tomto kroku je také možné upravit jména databází, případně upravit jméno uživatele. Jedním volitelným parametrem je adresa databáze, která je ve většině instalací na localhostu, jen v případě volby architektury se vzdálenou databází je nutné tento parametr vyplnit. Druhým volitelným parametrem je heslo pro root účet, který může zůstat defaultně prázdný.

Dokončením konfigurace databáze a kliknutím na tlačítko další je spuštěna konfigurace nad databází, průběh celé konfigurace je zobrazen na další obrazovce, kde je v případě chyby zobrazena chyba a konfigurace není dokončena.

Konfigurace databáze je posledním konfiguračním krokem v průvodci, další krok je již volitelný a je na uživateli, jaké rozšíření do Centreonu přidá. V poslední obrazovce průvodce je možnost do systému Centreon doinstalovat jednotlivá rozšíření v podobě modulů a widgetů. Běžně jsou do systému Centreon nainstalovány všechny dostupné moduly a widgety. Uživatel ale může zvolit jen některé z uvedených modulů a widgetů.

Standardně jsou do systému nainstalovány tři moduly. První je licenční modul, který složí pro instalaci dalších komponent, viz kapitola Komponenty monitorovacího systému Centreon. Pomocí tohoto modulu je možné přihlásit se do svého účtu u společnosti Centreon a využít své předplacené komponenty. Dalším nainstalovaným modulem je komponenta Plugin Packs Manager, která slouží k instalaci šablon pro monitoring. Komponenta je zpoplatněna, ale je možné využít pěti šablon, které jsou zdarma, proto je dobré instalaci toho modulu ponechat a šablony využít. Posledním modulem je modul Auto Discovery, který spolupracuje s komponentou Plugin Packs Manager a slouží k automatické detekci možných metrik na jednotlivých zařízeních. Celý modul je dostup-

ný jen v případě zakoupení komponenty Plugin Pack Manager, pokud tedy uživatel neuvažuje o nákupu této komponenty, není tento modul nutný.

Dalším rozšířením systému Centreon jsou widgety, které jsou všechny zdarma a slouží k vytváření přehledných pohledů pro uživatele. Příkladem může být vytvoření widgetu Service Monitoring, který primárně zobrazuje veškeré metriky, které jsou v systému vloženy, widget ale umožňuje filtr například jen na metriky v kritickém stavu nebo jen metriky určité skupiny. Widgety usnadňují práci správcům a mohou sloužit k včasnému odhalení problému, je proto dobré widgety do systému nainstalovat a aktivně využívat.

Po instalaci rozšíření přechází instalační průvodce do poslední obrazovky, kde je zobrazeno poděkování společnosti Centreon za využívání produktu a výběr, zda chceme odesílat analytická data společnosti Centreon.

Po dokončení instalace je možné se do systému Centreon přihlásit pomocí administrátorského účtu, který byl nakonfigurován v průvodci instalace, a začít monitorovat svoji infrastrukturu. Přihlašovací okno je zobrazeno na obrázku 15.

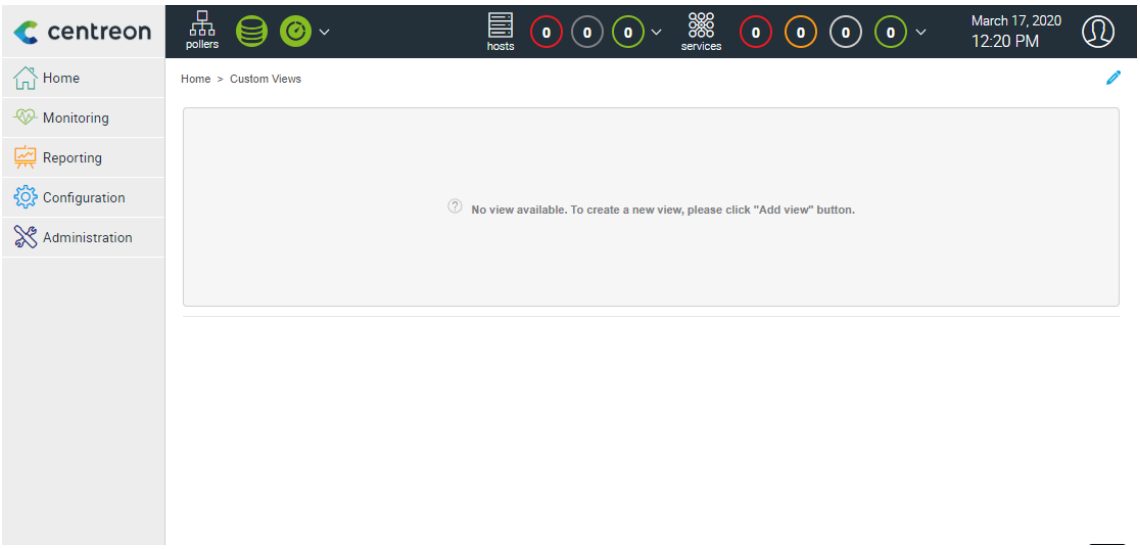
Obrázek 15: Přihlašovací okno do systému Centreon

(Vlastní zdroj)

8.7 Základní popis webového rozhraní Centreon

Po přihlášení do systému Centreon se zobrazí úvodní stránka Home, tuto stránku lze vidět na obrázku 16. Webové rozhraní je rozděleno do několika sekcí, hlavní menu je v levé části stránky a je možno zde najít pět sekcí Home, Monitoring, Reporting, Configuration, Administration, které obsahují další pod menu. V horní části webového rozhraní lze vidět vlevo stav poller serverů a vpravo počet zařízení a metrik v jednotlivých stavech. V této kapitole budou popsány jednotlivé sekce a možnosti, které sekce nabízí.

Obrázek 16: Webové rozhraní Centreon



(Vlastní zdroj)

8.7.1 Sekce Home

Celá sekce Home slouží k vytváření vlastních pohledů s widgety, které si uživatel může definovat podle svých potřeb. Uživatel může vytvořit několik pohledů s různými widgety. Většina uživatelů Centreonu má tuto stránku nastavenou jako defaultní stránku po přihlášení do systému Centreon a díky definovaným pohledům může ihned vidět například všechna zařízení ve stavu Critical a řešit problémy.

Sekce Home slouží spíše k usnadnění práce správců a k zobrazení důležitých informací. Centreon nabízí velké množství widgetů a je možné filtrovat zařízení podle jednotlivých stavů, vytvořených skupin zařízení, vytíženosti zdrojů apod. Nabízené jsou také widgety pro zobrazení stavu Centreon serveru a poller serverů nebo zobrazení grafů jednotlivých metrik.

8.7.2 Sekce Monitoring

Další sekcí je Monitoring, slouží k zobrazení stavových informací zařízení, která jsou v systému monitorována.

V podmenu Status Details lze nalézt aktuální stavy zařízení a jejich metrik, je zde možné filtrovat podle nejrůznějších parametrů, také je zde možnost zobrazit informace ohledně zařízení a metrik. V části Performances je možné zobrazit grafy nad metrikami, které podporují vykreslovaní grafů. V posledním podmenu Event logs je možno nad jednotlivými zařízeními nebo metrikami zobrazit historii změn stavů podle zadaného časového rozmezí.

8.7.3 Sekce Reporting

Sekce Reporting slouží k jednoduchému reportingu dat nad zařízeními. Je zde možné zadat časové rozmezí a vybrat zařízení, která mají být do reportu zařazena, následně jsou zobrazena statistická data nad jednotlivými zařízeními, například jak dlouho bylo zařízení nebo metrika v kritickém stavu.

8.7.4 Sekce Configuration

Tato sekce patří k nejdůležitějším, v ní jsou nastavovány veškeré parametry, které se týkají monitorovaných zařízení a jejich metrik, uživatelů, upozornění a mnoha dalšího. Je zde možnost přidat zařízení do monitoringu a následně jim přiřadit metriky, které je nutné na zařízeních monitorovat. Vkládají se zde také zařazení do skupin hostů a metrik, podle kterých je možné následně v monitoringu filtrovat nebo reportovat. Uživatelé si mohou v této sekci nastavit i upozornění na změny stavů prostřednictvím různých kanálů, jako je email, SMS zpráva nebo zpráva na pager. Sekce dále slouží k přidávání uživatelů do systému a samozřejmostí je možnost napojení na Active Directory a možnost se do systému hlásit pomocí doménového účtu v konkrétní společnosti. Velmi důležitá je také konfigurace poller serverů, u kterých je možné v této sekci zobrazit stav napojení na centrální server a přidat nové poller servery. Dále jsou v této sekci konfigurovány například SNMP trapy, šablony pluginů od společnosti Centreon, ale i uživateli vytvořené šablony nebo příkazy pro monitoring metrik.

8.7.5 Sekce Administration

Poslední sekcí je sekce Administration, sloužící k administraci systému Centreon. Jsou zde především konfigurace systémových proměnných. V sekci lze nalézt také konfiguraci přístupových pravidel pro uživatele, podle kterých je možné vytvořit nad skupinami uživatelů omezení v přístupu do jednotlivých sekcí. Lze také omezit přístup na jaké skupiny zařízení uživatelé v systému uvidí.

8.8 Napojení poller serverů na centrální server

Posledním krokem implementace dohledového nástroje Centreon je napojení poller serverů, které provádí předdefinovaná měření, na centrální server, který data ukládá do databáze a prezentuje uživatelům.

Napojení poller serverů na centrální server probíhá prostřednictvím webového rozhraní v sekci Configuration, kde se nachází pod menu Pollers. Přidání poller serveru není těžké, pro přidání je v horní části připraveno tlačítko „Add server with wizard“,

které po kliknutí otevře průvodce a jeho pomocí se poller server do systému přidá. Po otevření průvodce jsou zadány základní parametry, jako jsou název poller serveru, IP adresa poller serveru a adresa centrálního serveru, kam se budou data odesílat. Po vyplnění údajů se poller server přidá do seznamu. Poller server v tuto chvíli však není aktivní, pro aktivaci je nutné ještě provést načtení konfigurace a odeslání na poller server, tato akce se provádí druhým tlačítkem „Export configuration“. Po exportování konfigurace a pokud bylo naše nastavení správné, se u poller serveru změní stav na running a od tohoto okamžiku je možné pomocí nově přidaného poller serveru monitorovat zařízení a jejich metriky.

V rámci této práce bylo implementováno do společnosti celkem osm poller serverů, které lze vidět v obrázku 17.

Obrázek 17: Poller servery

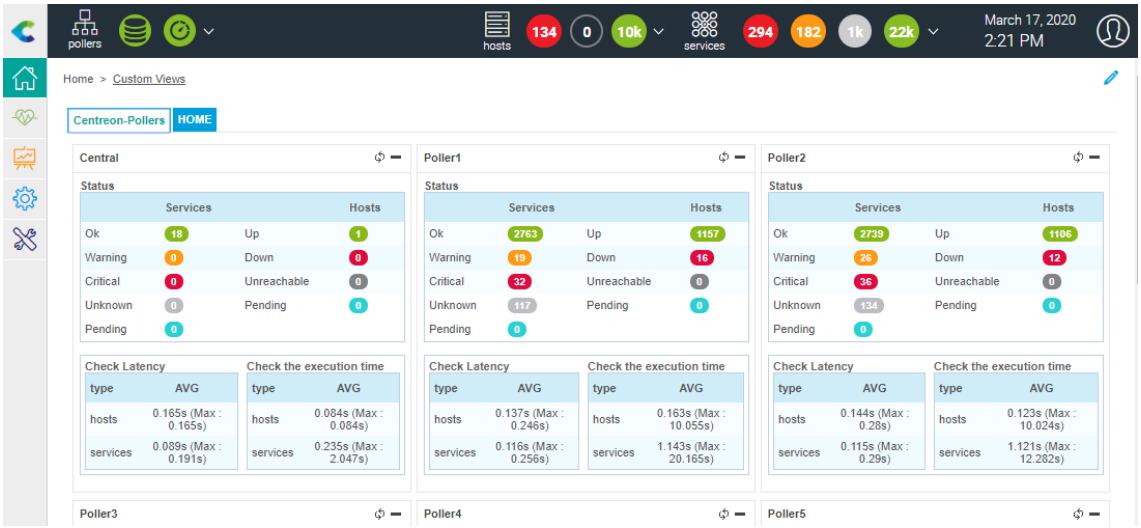
(Vlastní zdroj)

8.9 Migrace zařízení a metrik ze systému Nagios

Do systému bylo také nutné importovat veškerá měření, která byla prováděna monitorovacím systémem Nagios. Migrace ze systému Nagios je poměrně jednoduchá, protože pro exportování dat ze systému Nagios byl vytvořen skript, který je dostupný na platformě Git Hub. Skript musí být nainstalován na Nagios server a pomocí jednoduchého příkazu je spuštěn export veškerých zařízení a metrik ze systému Centreon do textového souboru. Tento textový soubor je následně přenesen na Centreon server, kde je integrována open source komponenta Centreon CLAPI, jejíž pomocí jsou data z textového souboru do systému naimportována.

Veškerá zařízení a metriky se podařilo bez problému přesunout na monitorovací systém Centreon. Na obrázku 18 v horní části je zobrazen stavový řádek, ve kterém můžeme vidět počty zařízení v jednotlivých stavech. Z dat na obrázku je patrné, že celkově bylo importováno přes deset tisíc zařízení a přes dvacet tři tisíc metrik.

Obrázek 18: Migrace zařízení a metrik ze systému Nagios



9 Ekonomické zhodnocení

V této kapitole bude ekonomicky zhodnocena implementace dohledového nástroje Centreon do podnikové sítě. Ekonomické zhodnocení implementace je provedeno pro monitorovací nástroj Centreon, který byl vybrán jako nejvhodnější kandidát.

9.1 Náklady

Finanční náklady, které je nutné vynaložit na implementaci, je možné rozdělit do několika částí.

První částí jsou náklady na hardwarovou část řešení. Celkové náklady na zakoupení nového hardwarového řešení se vyšplhaly na částku 672 tisíc korun, kdy do ceny byly zahrnuty tři servery určené pro instalaci dohledového systému a dva servery pro zálohování.

Druhou částí nákladů jsou náklady na software. Náklady na software byly nulové, jelikož bylo použito open source řešení Centreon, které je distribuováno pod licenci GNU GPL, tedy je možné ho použít pro jakýkoliv účel.

Další částí, kterou je nutné zařadit mezi náklady, jsou náklady na lidskou práci. Pro lidskou práci je většinou používána jednotka manday a jeden manday odpovídá osmi pracovním hodinám. Společně s určením jednotky je potřeba si určit hodinovou mzdu zaměstnance, který bude implementaci systému provádět. Hodinová mzda specialisty v naší společnosti se pohybuje kolem 300 korun za jednu hodinu, tudíž bude počítáno s tímto číslem ve vyjádření nákladů. Celkové montáž hardwaru do dvou lokalit trvala 2 mandays a implementace dohledové systému včetně migrace monitorovaných zařízení a metrik zabrala 5 mandays. Celkově se tedy náklady na lidskou práci vyšplhaly na 7 mandays, kdy po vynásobení hodinovou sazbou dostáváme náklady v hodnotě 16 800 korun.

Do nákladů je také důležité promítnout náklady na následný provoz systému a serverů. Ze zkušeností v naší společnosti jsou náklady na provoz jednoho hardware odhadnuty na 2 hodiny měsíčně na jeden server. V rámci této práce jsou náklady na tři servery pro monitoring a dva servery pro zálohování 10 hodin měsíčně. Náklady na provoz systémů a serverů jsou stanoveny na 3 000 korun měsíčně.

Do nákladů na implementaci dohledové systému je také nutné započítat jednorázové náklady na vytvoření testovacího prostředí a výběr monitorovacího nástroje. Tato

část testování a výběru monitorovacího zařízení zabrala celkově 8 mandays, vynásobením hodinovou sazbou se jedná o celkovou částku 19 200 korun.

Tabulka 7: Náklady na implementaci a provoz dohledového systému

Produkt	Množství	Cena	Poznámka
Nákup hardware	1	672 000 Kč	Cena za nákup tří serverů pro monitoring a dvou serverů pro zálohování
Software	1	0 Kč	Použito open source řešení pod licencí GNU GPL
Montáž hardware	2 mandays	4 800 Kč	Montáž hardware do dvou lokalit
Implementace software	5 mandays	12 000 Kč	Implementace dohledové systému Centreon
Provoz	10 hodin/měs.	3 000 Kč	Provoz pěti kusů hardware
Testování a výběr software	8 mandays	19 200 Kč	Testování a výběr dohledového nástroje

(Vlastní zdroj)

V tabulce číslo 7 jsou přehledně vyčísleny náklady na implementaci dohledové systému do podnikové sítě. Při nasazení dohledové systému se počítá s pětiletou dobou provozu na zakoupeném hardwaru. Celkové náklady se při sečtení a vynásobení sazby provozu na pět let vyšplhají na 888 tisíc korun.

9.2 Reálný přínos

Při prvním pohledu na celkové náklady se může zdát částka velmi vysoká, ale díky kvalitnímu dohledovému systému je možno ušetřit statisíce díky včasné reakci na problémy v síti. Hlavním nebezpečím v případě, kdy by nebyl implementován kvalitní dohledový systém v podnikové síti, jsou sankce od zákazníků za nedodržení smlouvy o poskytovaných službách. Může se tak stát v případě, že přestane fungovat například server, na kterém má zákazník zaplacené služby, a společnost by si toho nevšimla včas, v tomto případě jsou stanovené velké penále za nedodržení služby zákazníkovi.

Díky dohledovému systému je správce včas informován o problémech v síti a může je řešit prakticky ihned po detekování v dohledovém systému. Díky řadě upozornění může být správce informován prostřednictvím emailu, SMS zprávy nebo například pageru během několika sekund a problémem se zabývat.

Na závěr je nutné si uvědomit, že náklady na implementaci dohledového nástroje jsou minimální v porovnání s možnými sankcemi od zákazníků. Díky dohledovému systému také správce získává přehled o výpadcích s jejich historií a časovými údaji, které může využít při následné analýze a vylepšení podnikové sítě.

10 Závěr

Bakalářská práce se zabývá implementací dohledové nástroje do podnikové sítě. Cílem práce bylo ukázat, jak je možné monitoring rozsáhlé sítě řešit pomocí open source aplikace.

Teoretická část práce seznamuje čtenáře s počítačovými sítěmi, základy síťových protokolů a dohledovými nástroji. Největší část teoretické části se zabývá popisem dohledových nástrojů a k čemu nástroje slouží. Společně s popisem dohledových nástrojů jsou také popsány způsoby, jakými lze monitoring provádět.

Praktická část práce začíná výběrem čtyř nástrojů, které byly popsány a otestovány a prostřednictvím hodnotící komice ohodnoceny. V případě této práce, bylo pomocí metody vícekriteriálního rozhodování, rozhodnuto o implementaci nástroje Centreon, který se stal nejvhodnějším kandidátem. V práci je detailně popsán dohledový systém Centreon a jeho implementace do podnikové sítě včetně migrace předchozího monitoringu zařízení a metrik ze systému Nagios.

Na konci práce bylo vytvořeno ekonomické zhodnocení, které poukazuje na náklady spojené s implementací systému. Jelikož bylo zvoleno open source řešení, náklady jsou spojené jen s implementačními pracemi, nákupem nového hardwaru a provozními náklady, nejsou zde žádné náklady na licence dohledové sytému.

Nasazení systému splnilo veškerá očekávání firmy ČD – Telematika a.s., která chtěla modernizovat svůj zastaralý dohledový systém Nagios. Dohledový systém Centreon se stal plnohodnotnou náhradou systému Nagios a přinesl mnoho nových funkcionalit. Aktivně systém slouží pro několik oddělení ve firmě. Nejvíce využíván je systém na dohledovém pracovišti, kde jsou data využívána k řešení poruch na síti. Dohledové pracoviště sleduje systém Centreon nepřetržitě 24 hodin denně a veškeré události ihned přebírají a řeší prostřednictvím vzdálených zásahů nebo vysláním techniků. Dalším oddělením, které hojně systém využívá je oddělení správy datových sítí, které využívá především data z aktivních prvků. Prostřednictvím systému Centreon mohou například sledovat zatížení jednotlivých portů na routeru nebo switchi. V neposlední řadě využívá systém také oddělení provozu IT, které sleduje především metriky spojené se servery, jako jsou dostupnost portů, stav procesu nebo aplikace a především překračování mezních hodnot například u disků, paměti nebo CPU.

I. Summary and keywords

This bachelor thesis describes the design and implementation of a monitoring tool into corporate networks. Monitoring tools play an important role for administrator who use them to identify network problems. Using monitoring tools, we collect individual statuses of the metrics we have predefined, such as device availability, interface traffic, disk usage, etc. This information is then used by the administrator for a timely response to problems in the computer network.

The theoretical part describes computer networks and protocols that use by monitoring tools most often. The next section describes the Centreon open source solution, which is implemented as a monitoring tool within a corporate network and describes the possibilities and functions of the Centreon monitoring tool. The practical part of the thesis includes implementation of the Centreon monitoring tool into a corporate network.

Key words: monitoring, computer network, monitoring systems, Centreon, open-source, SNMP

II. Bibliografie

Bouška, P. (21. 9 2009). *Zařízení v síti pod kontrolou*. Získáno 27. 02 2020, z samuraj-cz: https://www.samuraj-cz.com/clanek/zarizeni-v-siti-pod-kontrolou/

Centreon. (nedatováno). Získáno 4. 2 2020, z Centreon: https://www.centreon.com/

Hu, N. (2006). Network Monitoring and Diagnosis Based on Available Bandwidth Measurement. Pittsburgh: Carnegie Mellon University, Computer Science Department.

Icinga. (nedatováno). Získáno 5. 2 2020, z Icinga: https://icinga.com/

Julian, M. (2018). *Practical monitoring.* Beijing: O'Reilly.

Kabelová, A., & Dostálek, L. (2006). *Understanding TCP.* Birmingham: Packt Publishing.

Kocjan, W. (2008). *Learning Nagios 3.0.* Birmingham: Packt Publ.

Leiden, C. H., & Wilensky, M. (2009). *Tcp/ip for dummies(r), 6th edition.* Indianapolis, IN: Wiley Pub., Inc.

Ligus, S. (2013). *Effective Monitoring and Alerting.* Farnham: O'Reilly.

Mauro, D. R., & Schmidt, K. J. (2005). *Essential SNMP.* Sebastopol, CA: O'Reilly.

NSClient++. (2008). Získáno 10. 11 2019, z https://nsclient.org/

Papež, T. (2014). Monitoring počítačové sítě. Brno: Mendelova univerzita v Brně, Provozně ekonomická fakulta.

Pleskot, V. (2012). *Dohledové systémy pro počítačové sítě.* Pardubice: Univerzita Pardubice, Fakulta elektrotechniky a informatiky.

Počítačová síť. (8. 10 2019). Načteno z Wikipedia: https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5

Wu, C.-H. (2013). *Introduction to computer networks and cybersecurity.* Boca Raton: CRC Press/Taylor & Francis Group.

Yusuff, A. A. (2012). *NETWORK MONITORING: Using Nagios as an Example Tool.* Kokkola: CENTRAL OSTROBOTHNIA UNIVERSITY OF APPLIED SCIENCES.

Zabbix. (nedatováno). Získáno 6. 2 2020, z Zabbix: https://www.zabbix.com/

III. Seznam obrázků a tabulek