VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Absolvování individuální odborné praxe

Individual Professional Practice in the Company

2017 Michal Winter

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání bakalářské práce

Student: **Michal Winter**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2601R013 Telekomunikační technika

Téma: Absolvování individuální odborné praxe
Individual Professional Practice in the Company

Jazyk vypracování: čeština

Zásady pro vypracování:

1. Student vykoná individuální praxi ve firmě: Pramet Tools, s.r.o.
2. Struktura závěrečné zprávy:
a. Popis odborného zaměření firmy, u které student vykonal odbornou praxi a popis pracovního zařazení studenta
b. Seznam úkolů zadaných studentovi v průběhu odborné praxe s vyjádřením jejich časové náročnosti
c. Zvolený postup řešení zadaných úkolů
d. Teoretické a praktické znalosti a dovednosti získané v průběhu studia uplatněné studentem v průběhu odborné praxe
e. Znalosti či dovednosti scházející studentovi v průběhu odborné praxe
f. Dosažené výsledky v průběhu odborné praxe a její celkové zhodnocení

Seznam doporučené odborné literatury:

Podle pokynů konzultanta, který vedl odbornou praxi studenta

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Zdeňka Chmelíková, Ph.D.**

Konzultant bakalářské práce: Ing. Roman Winter

Datum zadání: 01.09.2016

Datum odevzdání: 28.04.2017

doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA * Fakulta elektrotechniky a informatiky * 1D16 * OSTRAVA *

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: *16. dubna 2017*

.....
podpis studenta

Prohlášení zástupce spolupracující právnické nebo fyzické osoby

„Souhlasím se zveřejněním této bakalářské práce dle požadavků čl. 26, odst. 9 Studijního a zkušebního řádu pro studium v bakalářských programech VŠB-TU Ostrava."

Dne: *16. dubna 2017*

.....
podpis zástupce

Rád bych poděkoval Ing. Zdeňce Chmelíkové, Ph.D. za konzultace spojené s absolvováním bakalářské praxe. Dále bych rád poděkoval společnosti Pramet Tools, s.r.o. za možnost vykonávat odbornou praxi v jejich prostorách a za poskytnutí potřebných prostředků s touto praxí spojených, oddělení informatiky za vstřícný přístup a přijetí do kolektivu. Zvláštní poděkování patří Ing. Romanu Winterovi za odbornou pomoc a konzultaci při absolvování této individuální odborné praxe.

Abstrakt

Bakalářská práce shrnuje absolvování individuální odborné praxe ve společnosti Pramet Tools, s.r.o. na oddělení informatiky na pozici síťového správce. Mým úkolem bude řešit každodenní problémy a požadavky uživatelů, řešit problémy vzniklé expanzí počítačové sítě. Jako hlavní dlouhodobý předmět práce jsem dostal výběr a následnou implementaci systému pro monitorování a hlášení chyb komplexní výpočetní a komunikační infrastruktury podniku. K hlavnímu úkolu praxe chci, díky jeho obsáhlosti, přistupovat systematicky a řešení rozdělit do několika etap: seznámení s místní síťovou infrastrukturou, průzkum dostupných monitorovacích systémů, výběr systému, implementace systému, test základní funkcionality, přidání monitorovaných zařízení, grafické zobrazení měřených veličin, měření a vyhodnocení zatížení sítě a prostředků vzniklé přidáním monitorovacího systému. Jako výsledek mé práce by měl vzniknout robustní, komplexní a centrální monitorovací systém, který bude spuštěný jako služba na serveru a který nahradí stávající separátní monitorovací aplikace. Systém bude schopný informovat administrátora o vzniklém problému.

Klíčová slova: Monitorovací systém, hlášení chyb, výpočetní a komunikační infrastruktura, počítačová síť, přepínač, směrovač, záložní zdroj, diskové pole, server

Abstract

The bachelor thesis summarizes the completion of individual professional practice in Pramet Tools, s.r.o. in the IT department as a computer network administrator. My task will be to solve everyday problems and user requirements, to solve the problems caused by the expansion of the computer network. The main long-term subject of my thesis is to select and implement the system for monitoring and reporting errors of complex computing and communication infrastructure of the company. I want to separate the main task into several stages: to discover local network infrastructure, survey available monitoring systems, system selection, system implementation, basic functionality test, addition of monitored devices, graphical representation of measured values, measurement and assessing the network load and resources generated by adding a monitoring system. As a result of my work, a robust, comprehensive and central monitoring system should be created, which will run as a service on the server and replace the existing separate monitoring applications. The system will be able to inform the administrator of a problem.

Key Words: Monitoring system, reporting errors, computing and communication infrastructure, computer network, switch, router, uninterruptible power supply, disk array, server.

Obsah

Seznam použitých zkratek a symbolů

VSS	–	Virtual Switching System
SNMP	–	Simple Network Management Protocol
PTC	–	Pramet Trainning Centrum
PHS	–	Pravoúhlá Hysterezní Smyčka
AC	–	Alternating Current
DC	–	Direct Current
PoE	–	Power over Ethernet
QoS	–	Quality of Service
SAN	–	Storage Area Network
LAN	–	Local Area Network
SSID	–	Service Set Identifier
MPLS	–	Multiprotocol Label Switching
HSRP	–	Hot Standby Routing Protocol
OS	–	Operating System
LTS	–	Long Term Support
CPU	–	Central Processing Unit
SSD	–	Solid State Disk
DHCP	–	Dynamic Host Configuration Protocol
IPMI	–	Intelligent Platform Management Interface
ICMP	–	Internet Control Message Protocol
UDP	–	User Datagram Protocol
MIB	–	Management Information Base
OID	–	Object Identifier

Seznam obrázků

Seznam tabulek

Seznam výpisů zdrojového kódu

1 Úvod

Tématem bakalářské práce je podat informaci o absolvování individuální odborné praxe ve společnosti Pramet Tools, s.r.o. na oddělení informatiky a pozici správce sítě. Řešil jsem krátkodobé, spontánní úkoly vzniklé potřebami uživatelů, ale i plánované změny v páteřní síti. Souvisle jsem vykonával dlouhodobý úkol, který spočíval ve výběru a implementaci centrálního monitorovacího systému síťové a výpočetní infrastruktury podniku.

Jako první uvedu pole působnosti samotné firmy Pramet Tools, s.r.o. a vyzdvihnu její nejdůležitější milníky v historii až po současnost. Následně popíšu mé pracovní zařazení, oddělení, na kterém jsem praxi vykonával a jeho infrastrukturu. Uvedu náplň práce zaměstnanců, kteří zde působí.

Následnou kapitolu věnuji popisu a dokumentaci síťové a výpočetní infrastruktury podniku. Uvedu zde výčet síťových a výpočetních prvků, jejich počty a umístění. Bude se především jednat o prvky páteřní sítě (přepínače, směrovače, bezdrátové přístupové body) a o výpočetní techniku (servery, tiskárny, různá dohlížecí zařízení a klíčové aplikace). Tahle kapitola úzce souvisí s tou následující, kde provedu výběr a implementaci vhodného monitorovacího systému na základě těchto poznatků a požadavků.

Tři čtvrtiny bakalářské práce budou věnovány mému dlouhodobému úkolu, a to výběru, implementaci a ladění monitorovacího systému pro síťovou a výpočetní infrastrukturu podniku. Provedu zde určité srovnání dostupných monitorovacích systémů. Kompletně popíšu proces zavádění a nastavení monitorování. Uvedu různé vrstvy monitorování. Provedu teoretický rozbor protokolu SNMP, který se z velké části používá právě k monitorování daných zařízení. Získaná data budou vhodně reprezentována v podobě grafů v závislosti na čase. Následně provedu analýzu zátěže, kterou daný monitorovací systém působí na výpočetní výkon a na síťové prostředky.

V poslední části bakalářské práce se budu věnovat možnosti rozšíření sítě o další přepíač a jeho implementaci do stávající sítě pomocí technologie EtherChannel.

2 Představení firmy a pracovního zařazení

2.1 Informace o firmě

Od roku 2014 firma Pramet Tools, s.r.o. figuruje jako člen uskupení Dormer Pramet. Tohle uskupení vzniklo spojením dvou monolitních výrobců Dormer Tools a Pramet Tools, kteří se specializují na výrobu nástrojů s vyměnitelnými břitovými destičkami ze slinutého karbidu. Společně tak mají obě značky více než sto padesáti letou historii.

Jejich komplexní sortiment nabízí celou řadu nástrojů pro všeobecné strojírenství: monolitní nástroje a nástroje s vyměnitelnými břitovými destičkami pro soustružení, frézování, vrtání a závitování.

Své služby poskytují prostřednictvím více než 30 poboček, které působí na více než sto různých trzích po celém světě. Obchodní síť zahrnuje přibližně 600 lidí. Disponují 5 specializovanými školícími centry po celém světě: Česká republika, Velká Británie, Švédsko, Rusko a USA. Důležité milníky v historii společnosti Pramet Tools, s.r.o.: [1]

- 1932 - Společnost Stelleag zahájila výrobu slinutých karbidů a nástrojů s přírodním diamantem v Šumperku.
- 1950 - Pramet navazuje na tradici výroby slinutého karbidu v Šumperku, kde zakládá svůj výrobní podnik.
- 1998 - Pramet se stává součástí skupiny Sandvik.
- 2004 - Certifikace integrovaného systému kvality 9001:2000 a životního prostředí ISO 14001:2004
- 2011 - Rekord ve výrobě destiček. Celkem vyrobeno 22,5 milionu destiček za rok.
- 2013 - Pramet propojen se společnostmi Impero a Safety.
- 2014 - Vznik uskupení Dormer Pramet

2.2 Pracovní zařazení

Mé pracovní zařazení bylo na oddělení informatiky, které se stará o veškerou výpočetní techniku, programové vybavení, programování SAP a počítačovou síť. Tohle oddělení má přímého nadřízeného, ředitele pro IT & Operations Department. Pod něj spadají tři skupiny lidí. Skupina Demand Managerů čítající 4 lidi, skupina aplikačních programátorů SAP zahrnující 7 lidí a technická skupina tvořená 5 osobami. Já jsem byl zařazen do technické skupiny. Tato technická skupina má na starost zavádění a údržbu osobních počítačů, mobilních telefonů, správu sítě, údržbu telefonní ústředny, údržbu serverů a programového vybavení počítačů. Mé zaměření bylo na již zmíněnou počítačovou síť, telefonní ústřednu a případná údržba serverů a osobních počítačů.

3 Popis síťové infrastruktury a výpočetní techniky

3.1 Struktura výpočetní techniky a sítě v podniku

Serverový výpočetní výkon je rovnoměrně rozložen do dvou serveroven, které jsou vzájemně zastupitelné a které jsou umístěny v různých lokalitách firmy kvůli možnosti vzniku požáru a podobných živelných katastrof. Existuje zde existuje 100 % redundance a možnost nedostupnosti aplikací a databáze je velmi nepravděpodobná. Serverovny budeme označovat písmeny A a B.

Dále zde nalezneme místnost s telefonní ústřednou, která se nachází částečně pod zemí. Je zde ukončení optického přívodu internetu. V posledním patře výškové budovy nalezneme rozvaděč s ukončením bezdrátového přívodu intranetu. Tyto dva přívody primárně slouží k rozdílným účelům, ale z důvodu zajištění vysoké dostupnosti jsou vzájemně zastupitelné.

Další klíčová místa počítačové sítě jsou rozvaděče rozmístěné po celém areálu firmy. Slouží k přívodu počítačové sítě ke koncovým uživatelům a výrobním strojům. Těchto míst je tu 10: metrologie, logistika, PTC, lisovací nástroje, energetika, PHS, oddělení obrábění, galerie, broušení, administrativní budova.

3.2 Výpočetní výkon

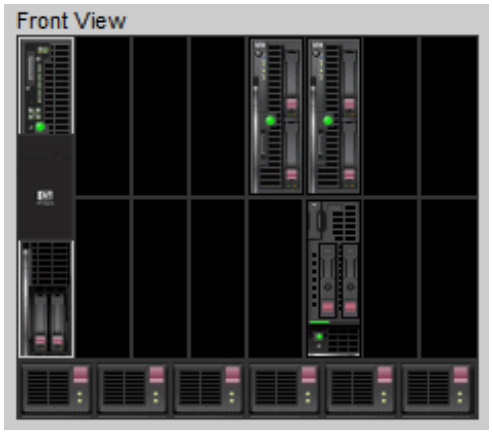
3.2.1 Blade system

Výpočetní výkon zprostředkovává HPE BladeSystem c7000 enclosure. HPE BladeSystem c7000 enclosure zajišťuje veškeré napájení, chlazení a I/O infrastrukturu modulárním serverům, které jsou do tohoto BladeSystemu zasunuty. Enclosure zabírá 10U na výšku v rozvaděči a dokáže pojmout až 16 zásuvných serverů a volitelné redundantní síťové a diskové propojovací moduly. Toto řešení zajišťuje redundantní připojení serverů do jádra sítě a na sdílená disková úložiště. Napájení je zajištěno pomocí sdílené napájecí sběrnice a u vstupního napájení je na výběr z jednofázového AC vstupu, tří fázového AC vstupu, -48 V DC vstupu a vysoko napěťového DC vstupu.

Tohle řešení sjednocuje servery, úložiště, síťová rozhraní, napájecí management a chlazení do jednotného řešení, které může být spravováno jako celek. Pomocí iLO vzdálené správy můžete konfigurovat a kontrolovat servery bez ohledu na operační systém na serverech. [2]

3.2.2 Blade servery

Blade system v serverovně A obsahuje čtveřici zasunutých serverů. První z nich je Integrity BL860c i2, na kterém běží Oracle 11 a centrální instance SAP ERP 6.04. Na výšku zabírá dva sockety. Disponuje dvojicí Intel Itanium 9300 procesorů, až 384 GB operační paměti DDR3 zasunutých ve 24 DIMM slotech a čtyřmi Flex-10 10 Gigabit Ethernet porty. Je zde nainstalovaný operační systém HP-UX 11.31. Je to nejkritičtější server ve firmě. [3]



Obrázek 1: Čelní pohled na servery v HPE BladeSystem c7000 enclosure

Druhý server je ProLiant BL460c G7, který zabezpečuje službu BackupExec 10. Je vybaven dvojicí Intel Xeon procesorů. Maximální operační paměť je 384 GB DDR3. Připojení do sítě zajišťuje 10 Gigabit rozhraní. Je zde nainstalovaný VMware ESXi 6. [4]

Třetí server v Bladu je opět ProLiant BL460c G7, který je v tuto chvíli nevyužit, protože sloužil jako hlavní server pro VMware vSphere 6, ale byl nahrazen novějším modelem. Momentálně je využíván pro testovací účely.

Poslední připojený server je ProLiant BL460c Gen9, na kterém aktuálně běží služba VMware vSphere 6. Nabízí Intel Xeon E5-2600 procesor a až 2 TB DDR4 operační paměti. Opět je zde nainstalovaná tenká virtualizační vrstva VMware ESXi 6. [5]

V serverovně B je BladeSystem osazen stejnými klíčovými servery. Rozložení zátěže mezi těmito BladeSystemy je při standardní situaci 50/50. V případě výpadku jednoho serveru přebírá jeho roli shodný server ve druhé serverovně.

Na Integrity BL860c i2 serveru běží Oracle 11 + Pomocné Instance SAP ERP 6.04, na ProLiant BL460c G7 VMware vCenter Server a na ProLiant BL460c Gen9 opět VMware vSphere 6.

Jak si můžeme povšimnout, většina výpočetního výkonu je virtualizována. Je to dnešní trend a administrátorovi to nabízí mnohem širší možnosti při přidělování prostředků jednotlivým virtuálním serverům na míru. Pro představu, na těchto pěti fyzických serverech běží 48 různých virtuálních serverů pro různé účely. Navzájem sdílí systémové prostředky. Nesporná výhoda je v možnosti spravování jednotlivých virtuálních strojů. Můžeme si uložit obraz stroje během několika sekund (pořídit snapshot), provést nutné modifikace, instalace, aktualizace a v případě neúspěchu se jednoduše vrátit k tomuto pořízenému snapshotu.

3.3 Síťová infrastruktura

3.3.1 Jádro sítě

Jádro sítě tvoří dvojice Cisco L3 4506-E spřepínačů. Poskytují vysoký výkon, mobilní a bezpečné uživatelské prostředí skrze přepínání vrstev 2-4. Zajišťují bezpečnost, mobilitu, aplikační výkon, virtualizaci, automatizaci a energetické úspory napříč infrastrukturou. Vyznačují se vysokou odolností proti chybám. Cisco Catalyst 4506-E má centralizovanou architekturu, která umožňuje spolupráci, virtualizaci a provozní správu prostřednictvím zjednodušených operací. S dopřednou a zpětnou kompatibilitou nabízí tento switch výjimečnou flexibilitu nasazení, tak aby splňoval měnící se potřeby firmy. Rozšiřují kontrolu k hranicím sítě s inteligentní síťovou službou, která zahrnuje sofistikovaný QoS, předvídatelný výkon, rozšířenou bezpečnost, komplexní řízení a integrovanou odolnost. Škálovatelnost těchto inteligentních síťových služeb je možná s vyhrazením specializovaných zdrojů známých jako obsahově-adresovatelná paměť (TCAM). Dostatek TCAM umožňuje směrování a přepínání paketů rychlostí rozhraní nezávisle na QoS. Nedochází tedy k žádnému zpomalení při přechodu z jedné sítě do druhé. [6]

Každý ze dvou přepínačů disponuje čtveřicí 10 Gigabit optických rozhraních (2 na propojení mezi sebou, 2 k připojení Blade přepínačů). Dále pak obsahuje 12 Gigabitových optických portů pro připojení přístupových přepínačů, 48 Gigabitových metalických portů pro další konektivitu. Jeden přepínač je umístěn v serverovně A a druhý je umístěn v serverovně B. Navzájem jsou propojeny dvojicí 10 Gigabit single mode optickým spojem. Vůči okolí se tváří jako jeden logický přepínač díky technologii VSS.

3.3.2 Přístupové přepínače

Přístupové přepínače zde zastupují Cisco 2960-S zařízení. Jsou to 1U vysoké Gigabit Ethernet přepínače s fixní konfigurací, které poskytují přepínaní na 2. vrstvě pro areál a pro přístup k aplikacím. Umožňují spolehlivé a bezpečné obchodní operace prostřednictvím řady inovativních funkcí, včetně FlexStack pro propojení více switchů, Power Over Ethernet Plus (PoE +) a Cisco Catalys SmartOperations. Nabízí 48 Gigabit Ethernet portů, ve většině případů jsou zde propojeny dva switche pomocí 20 Gbps FlexStack technologie. [7]

V našem případě je vždy propojen jeden 48 portový přepínač poskytující PoE + s jedním 48 portovým přepínačem bez PoE. Logicky tvoří jeden přepínač s 96 porty. Do portů PoE + jsou připojeny bezdrátové přístupové body, které pak nepotřebují jiné napájení. Hlavní rozdíl mezi PoE (802.3af standard) a PoE + (802.3at standard) je v maximálním množství energie, kterou poskytují přes Cat5 kabeláže. Maximum u 802.3af (PoE) je 15,4 W. U 802.3at (PoE +) činí maximální hodnota dodávané energie 25,5 W.

Ve firmě nalezneme 13 těchto logických přístupových přepínačů viz Tabulka 1. Jejich název odpovídá umístění, ve kterém se nachází. Každý přepínač má dvě Gigabitové přípojky do centrálního přepínače. Vždy fyzicky vedeny jinou trasou po firmě a do jiného ze dvou fyzických centrálních přepínačů. Tohle radundantní zapojení poskytuje vysokou ochranu jednak proti vý-

padku jednoho z centrálních přepínačů, ale také ochrana proti poškození jedné trasy vedení kabelů.

Tabulka 1: Rozdělení přístupových přepínačů

Název přepínače	**Počet přepínačů**	**Z toho PoE+**
Servers	2	1
Metrology	2	1
Logistics	2	1
PTC	2	1
Presstool 1	2	1
Presstool 2	1	1
Energetics	1	1
PHS 1	1	1
PHS 2	1	1
Cutting dep	2	1
Gallery	2	1
Grinding	2	1
Admin Building	4	2

3.3.3 Blade propojovací přepínače

Důležitou součástí sítě je propojení serverů, přístup uživatelů k serverům a informacím uloženým na diskových polích. Jelikož jsou servery řešeny pomocí BladeSystemu, tak se také BladeSystem stará o tuto síťovou konektivitu. První skupinou Blade přepínačů je dvojice SAN přepínačů v každém BladeSystemu. Tuto funkci zde zastupují zařízení Brocade 5480. SAN přepínač je zařízení, umožňující komunikaci serverů se sdílenými úložnými systémy. V případě firmy Pramet Tools, s.r.o. se SAN využívá pro komunikaci serverů se sdílenými diskovými poli a sdílenou magnetopáskovou knihovnou. Brocade 5480 má 24 8 Gbit portů.

Druhou skupinou jsou LAN přepínače, které jednak umožňují komunikovat Blade serverům mezi sebou navzájem a zároveň umožňují komunikaci s ostatními objekty firemní infrastruktury. Tento typ switchů zde zastupují zařízení ProCurve 6120XG. ProCurve jsou Ethernetové switche, takže zajišťují napojení na firemní LAN.

Všechny tyto switche jsou 24 portové, mají vždy 16 interních portů pro servery a 8 externích portů pro napojení vnějšího světa. Přepínače jsou zde záměrně vždy ve dvojicích, aby byla zajištěna vysoká dostupnost konektivity. Proto i servery mají vždy minimálně dva ethernet a dva fibre channel porty vyvedené vždy každý na jiný přepínač. Případný výpadek jednoho přepínače z dané dvojice neznamená totální ztrátu konektivity pro servery.

3.3.4 Wide Area Network

Je zde zajištěno VPN spojení se všemi lokalitami mateřské společnosti po celém světě, včetně vlastních zahraničních poboček. Základem je směrovací technologie MPLS postavená na páteřní

infrastruktuře světového síťového operátora Verizon Enterprise Solutions. Pro bezpečný přístup na internet se využívá globální cloudová služba Zscaler. Připojení je fyzicky zajištěno dvěma různými Cisco routery, které jsou vzájemně propojeny clusterovým protokolem HSRP tudíž je jedna virtuální IP adresa jako výchozí brána.

Každý router je umístěn v jiné části firmy a každý využívá jinou fyzickou externí konektivitu. Jeden používá optickou síť, druhý bezdrátovou technologii.

3.4 Ostatní zařízení

3.4.1 Disková pole

Úložiště souborů zde zajišťuje 2 x HPE 3PAR StoreServ 7200 diskové pole, každé v jiné serverovně se stejnou kapacitou a stejným výkonem. Je napojeno do firemní optické SAN pro komunikaci se servery i mezi poli navzájem. Rovněž je připojeno do firemní ethernet LAN pro management, monitoring a komunikaci s Quorum Witness.

Disková pole poskytují sdílený diskový prostor pro servery HP-UX a VMware. Diskové svazky klíčových systémů jsou synchronně replikovány (zrcadleny) mezi poli a současně prezentovány vůči serverům z obou polí najednou (vždy z jednoho pole v režimu Active a z druhého pole v režimu Standby). Ve třetí lokalitě (serverovně) běží Quorum Witness (virtuální server), který je, spolu se synchronními replikami, nutnou podmínkou konfigurace Peer Persistence.

Tato konfigurace umožňuje tzv. Transparent Failover, což v důsledku znamená, že běh klíčových aplikací není jakkoli ovlivněn případným výpadkem jednoho z polí.

3.4.2 Wireless kontroléry

Pro řízení wifi přístupu jsou zde k dispozici dva Cisco 5508 Wireless Controllery, opět každý v jiné serverovně. Jsou navázány na Active Directory. Obhospodařují 37 fyzických Cisco přístupových bodů po celé firmě včetně poboček. Poskytují souběžně několik SSID.

3.4.3 Tiskové řešení

Tiskové řešení Y Soft SafeQ spočívá v posílání tiskových úloh na virtuální síťovou tiskárnu (SafeQ tiskový port -> SafeQ tiskový server). Tiskový server spravuje 20 velkých multifunkčních zařízení a 25 menších stolních tiskáren, vše značky Konica Minolta. Uživatelé tisknou pomocí přímých, nebo zabezpečených front (autorizace osobní ID kartou nebo PINem). Uživatelské účty jsou napojeny na Active Directory. Správa uživatelských tiskových front je přes webové rozhraní.

3.4.4 Docházkový systém

Docházkový server COMINFO spravuje soustavu bezdrátových NFC čteček a zámků, které jsou umístěny jak na vstupních turniketech do firmy, tak na dveřích všech zabezpečených prostor. Pracovníci jsou vybaveni osobními ID kartami. Elektronická evidence docházky je podklad

pro mzdový systém. Je zde možnost prohlížení docházky na osobních počítačích, příp. v tzv. kioscích pro dělníky.

3.4.5 Kamerový systém

Kamerový server Genetec Omnicast spravuje 23 ethernet IP kamer vně i uvnitř areálu firmy. Jsou zde dvě monitorovací centra. Několikadenní záznam se ukládá na pevný disk.

3.4.6 Telefonní systém

Je zde telefonní ústředna NexSpan. Využívá se zde strukturovaná kabeláž. Spravuje analogové, digitální a IP telefony.

3.5 Shrnutí

V následující tabulce je souhrn a počet všech zařízení, které se nějakým významným způsobem začleňují do fungování IT služeb podniku viz Tabulka 2. Všechna tyto zařízení by tedy bylo dobré nějakým způsobem monitorovat a mít o nich všeobecný přehled, případně být včas upozorněn na vzniklou chybu, nebo závadu. Jednotlivá koncová zařízení uživatelů nejsou kritická pro fungování firmy, proto nejsou brána v potaz. Schéma počítačové sítě nalezneme v příloze A.

Tabulka 2: Souhrn a počet významných zařízení

Kategorie	**Počet zařízení**
Blade enclosure	2
Fyzické blade servery	7
Virtuální servery	48
L3 přepínače	2
Přístupové přepínače (stacky)	13
Blade přepínače	8
Směrovače	2
Disková pole	2
Bezdrátové řadiče	2
Přístupové body	37
Tiskárny	45
Docházkový systém	1
IP kamery	23
Telefonní ústředna	1
Celkem	**193**

4 Monitorovací systém

V celé této kapitole se budeme věnovat monitorovacímu systému síťové a výpočetní infrastruktury. Jako výchozí informace o potřebě a počtu monitorovaných zařízení použijeme předchozí kapitolu, která se věnovala průzkumu a popisu výpočetní techniky a síťových zařízení. Provedeme zde celý proces zavádění systému od výběru vhodného monitorovacího systému, výběr vhodného umístění instalace monitorovacího systému, implementaci a následné testování zatížení sítě a výpočetní techniky způsobené zavedením monitorovacího systému. Pokud to bude možné, zvolíme Open Source systém, který nám nabídne dostatečnou funkcionalitu a robustnost.

4.1 Výběr monitorovacího systému

Jako první zde uvedu 8 monitorovacích aplikací, které jsou pro nás teoreticky vhodné a splňují minimální požadavky. Následně z nich vyberu jednu vhodnou pro naši situaci.

- **OpenNMS**

  OpenNMS je open source podnikové řešení pro správu a monitorování sítě, které nabízí automatické zkoumání sítě, správu událostí a oznámení, měření výkonu a zabezpečování služeb. OpenNMS obsahuje klientskou aplikaci pro iPhone a iPad pro on-to-go přístup.

- **Pandora FMS**

  Pandora FMS je nástroj pro sledování výkonu, monitorování sítě, dohled nad servery, aplikacemi a komunikací. Má pokročilý systém pro korelaci událostí, který vám umožní vytvářet upozornění založené na událostech od různých zdrojů a oznámí to správci ještě před vyvrcholením problému.

- **Zenoss Core**

  Zenoss Core je open source IT monitorovací platforma, která monitoruje aplikace, servery, datová úložiště, síť k zajištění dostupnosti a výkonnostních statistik. Má také vysoce výkonný systém zpracování událostí a pokročilý systém oznámení.

- **The Dude**

  The Dude je síťoví monitorovací nástroj, který monitoruje zařízení a hlásí problémy. Umožňuje také automatické prozkoumání veškerá zaplá zařízení na dané podsíti a na základě těchto informací vykreslit mapu dané podsítě.

- **Icinga 2**

  Icinga je open source systém založený na Linuxu, který ověřuje dostupnost síťových zdrojů a okamžitě upozorňuje správce, pokud některé zařízení přestane pracovat. Icinga poskytuje data pro hlubokou analýzu a výkonné rozhraní příkazového řádku.

- **Total Network Monitor**

  Total Network Monitor neustále monitoruje zařízení a služby na lokální síti. Upozorní vás na případné problémy, které vyžadují pozornost administrátora. Výsledek každého měření je ozančen barvou (zelená, červená, černá) pro rychlé rozpoznání výsledku měření, jestli proběhlo v pořádku, nebo negativní výsledek, či vůbec nebylo měření dokončeno.

- **NetXMS**

  NetXMS je multi-platformní systém pro správu a monitorování sítě, který poskytuje správu událostí, sledování výkonu, hlášení, vykreslování grafů pro celou IT infrastrukturu. Hlavní rysy NetXMS zahrnují podporu pro více operačních systémů a databázových systémů, distribuované monitorování sítě, automatické objevování zařízení v síti a nástroj pro analýzu obchodních dopadů. NetXMS vám dává možnost správy přes webové rozhraní, nebo pomocí příkazové řádky.

- **Zabbix**

  Zabbix je ultimátní software pro podnikové účely pro monitorování miliónů metrik získaných od desítek tisíc serverů, virtuálních počítačů a síťových zařízení. Zabbix je open source systém a je nabízen bez dalších poplatků. Jeho instalace je vhodná na mnoho platforem, včetně distribucí Linuxu. Nabízí správu událostí, hlášení chyb a upozornění mnoha komunikačními cestami.

Jak je možná z výše uvedeného výčtu jasné, naše požadavky splňuje více monitorovacích aplikací. Při výběru vhodného kandidáta musíme uvažovat, že se snažíme nalézt systém, který dokáže monitorovat nejen síťová zařízení, ale i výpočetní zařízení a různé aplikace. Potřebujeme robustní systém pro stovky monitorovaných zařízení a hlubokou možnost nastavení monitorovaných zařízení. Při výběru je nutné zvážit, že se ve firmě používá v hojné míře virtualizace hardwaru. Proto je vhodné s tímto faktem počítat. Jako kritérium stanovíme nutnost podpory instalace monitorovacího systému na serverovou variantu OS Ubuntu, který se ve firmě hojně používá pro různé aplikace. Výhodou tohoto OS je fakt, že je to open source systém a nabízí dlouhodobou podporu. Je robustní a nabízí modifikovanou instalační variantu jako virtuální stroj, což zajisté využijeme.

Na základě těchto kritérií jsem se rozhodl implementovat monitorovací systém Zabbix ve verzi 3.0 LTS. Poběží na OS Ubuntu Server 16.04 LTS. Oba dva systémy nejsou nejnovější edice, ale edice LTS. Za předpokladu, že monitorovací systém bude běžet dlouhodobě, je volba systému s dlouhou podporou rozumnější. Bude to virtuální stroj umístěn na bladovém serveru ProLiant BL460c G7 v serverovně A, který je v tuto chvíli nevyužíván a slouží pro testovací účely. Tento stroj nabídne dostatečný výkon, paměť RAM, ukládací prostor a vysokorychlostní napojení do počítačové sítě.

4.2 Popis systému Zabbix

Firma Zabbix SIA byla založena v roce 2005 Alexeiem Vladishevem v Lotyšsku. Od té doby otevřela jednu pobočku v Japonsku. Myšlenkou této firmy je vytvořit profesionální open source monitorovací systém nejvyšší kvality, který bude řešit skutečné problému uživatelů. Hlavní funkce produktu je shromažďování dat, ukládání a správa dat, upozornění na nebezpečí prostřednictvím e-mailu, SMS apod. a vizualizace údajů pomocí grafů, map a obrázků. Výhody tohoto systému:

- Provádí analýzu současného stavu IT infrastruktury a předvídá potencionální nebezpečí.
- Hledá korelační závislosti mezi daty z různých aplikací a zařízení.
- Umožňuje monitorování podle specifických parametrů.
- Webové rozhraní se zabezpečeným ověřováním uživatelů.
- Poskytuje agenty pro všechny známé OS
- Dokáže monitorovat i bez agenta pomocí SNMP protokolu
- Dokáže sledovat VMware virtuální stroje
- Automatické skenování sítě
- Rozšiřující skripty mohou být psány ve více programovacích jazycích

Nevýhody:

- Online technická profesionální podpora není zdarma

4.2.1 Monitorování pomocí Zabbixu

Sledování parametrů stroje probíhá pomocí nainstalovaného agenta, který je dostupný pro systémy Windows, Linux, UNIX.

Přístup k frontendu zabezpečuje SSL. Jednotlivé komponenty spolu vzájemně komunikují a přijímají zprávy pouze z autorizovaných IP adres.

Zabbixx posílá upozornění na problémy e-mailem, SMS zprávou, nebo pomocí protokolu XMPP (Jabber). Je zde možnost nastavení automatického vytváření ticketů. Pokud jdou některé problémy jednoduše vyřešit (restartování stroje), Zabbix může sám tento proces spustit. Pokud se problém nevyřeší pomocí jednoho postupu, Zabbix umožňuje eskalaci problému a přesune problém další skupině uživatelů.

Systém umožňuje aktivní i pasivní kontroly. Pasivní kontroly spočívají v tom, že si server vyžádá informace od zařízení. Při aktivní kontrole sám server zasílá informace. Agent prochází i logovací soubory zařízení a při nalezení problému informuje server.

Zabbix umožňuje sledovat zařízení pomocí SNMP a IPMI agenta. SNMP agent se hlavně využívá při sledování síťových zařízení. V neposlední řadě máte také možnost naprogramovat

si vlastního agenta. Máte zde také možnost základní kontroly dostupnosti zařízení bez agenta pomocí ICMP protokolu. [8]

4.3 SNMP protokol

SNMP je jednoduchý, široce rozšířený, standardizovaný protokol. Slouží pro získávání, nebo nastavování hodnot na určitém zařízení zařízení. Protokol SNMP podporuje velká řada zařízení, například aktivní síťové prvky, počítačová čidla, tiskárny, přístupové body. Osobní počítače a servery mohou získat podporu SNMP po doinstalování potřebných balíčků a ovladačů. Hodnoty můžeme získávat v pravidelných intervalech, ukládat je do databáze a z nich pak vykreslit graf sledované veličiny v závislosti na čase. Přehledně tak můžeme zobrazit graf vytížení procesoru, teploty, nebo provozu na síťovém rozhraní.

4.3.1 Princip fungování SNMP

Komunikace pomocí protokolu SNMP probíhá mezi dvěma stranami. Jeden vystupuje v roli správce (manager) a druhý je agent.

Rozlišujeme dva režimy činnosti:

- Správce posílá dotazy na agenta a přijímá odpovědi.
- Agent zasílá oznámení (trapy) na adresu správce.

Protokol SNMP se v současné době provozuje ve třech verzích. SNMPv1 a SNMPv2c používají pro autentizaci community string (textové heslo). SNMPv3 je sofistikovanější a autentizace probíhá pomocí zašifrovaného jména a hesla.

SNMP pro komunikaci využívá protokol UDP, díky čemuž je velmi rychlý, ale může dojít ke ztrátě datagramu. Od verze 2 je implementovaná kontrola doručení, takže by ke ztrátám docházet nemělo. Standardně se pro SNMP využívá port 161 na straně agenta pro dotazy a port 162 na straně serveru pro příjem trapů. Ostatní porty použité při komunikaci jsou voleny dynamicky.

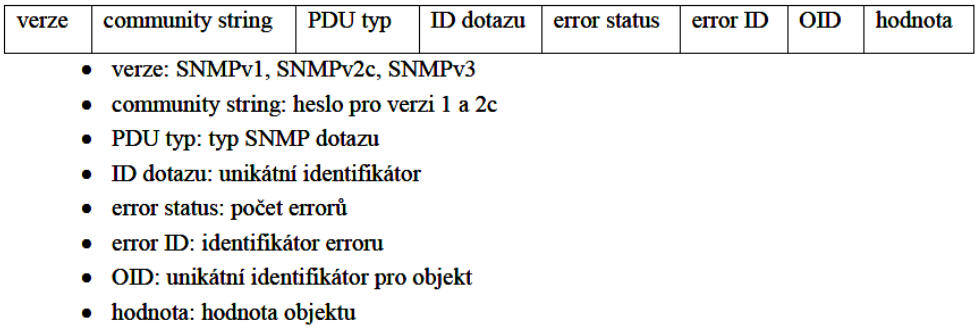
4.3.2 SNMP paket

Rozlišujeme dva typy datagramů. Jeden je pro SNMP komunikaci typu dotaz a odpověď, viz Obrázek 2. Druhý typ je pro zasílání trapů.

SNMP datagram pro zasílání trapů je rozšířením předchozího datagramu o následující pole: enterprise, agent IP, gen trap, spec trap, čas.

4.3.3 SNMP dotazy

Při klasické komunikaci odešlu dotaz na jednu hodnotu a následně přijímám odpověď. Provede se nastavení na typ GET, zadá se OID pro zjišťovanou hodnotu a nastaví se na NULL. Při odpovědi je typ nastaven na RESPONSE (2), OID je stejné jako při dotazu a v kolonce hodnota je odpověď na náš dotaz. Máme možnost využít i další typy dotazů:



Obrázek 2: Struktura SNMP datagramu pro dotaz a odpověď

- GET (0): vrátí jednu hodnotu
- GET NEXT (1): vrátí další hodnotu (následující OID za zadaným)
- GET-BULK: od verze 2, vrátí více hodnot najednou
- TRAP: pro zaslání trapu
- NOTIFICATION: speciální typ zprávy
- INFORM: speciální typ zprávy
- REPORT: speciální typ zprávy

Kromě zasílání dotazů pro zjištění nějaké hodnoty, máme možnost i hodnoty nastavit. K tomu se využívá typ zprávy SET.

4.3.4 MIB databáze

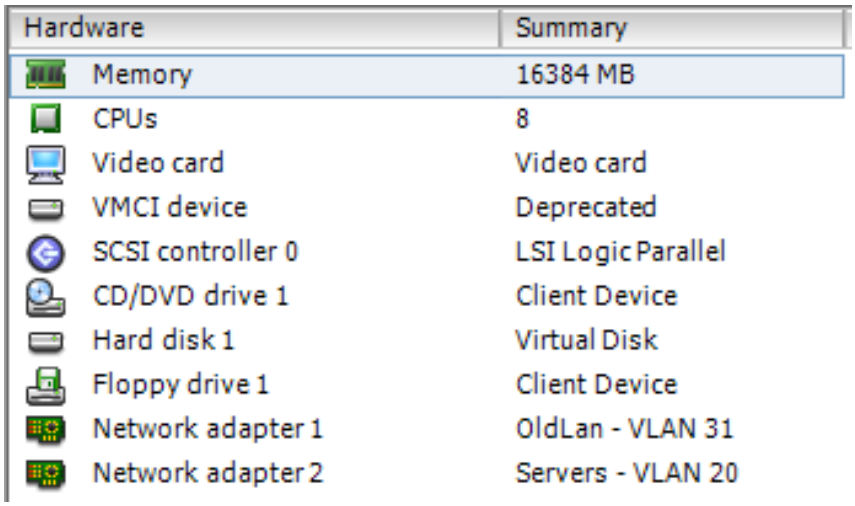
Každá hodnota v SNMP je jednoznačně identifikovaná pomocí unikátního identifikátoru OID. Ten se skládá z čísel oddělených tečkou. Jedná se o stromovou strukturu, kde vlevo od tečky je nadřazený prvek a vpravo podřazený. Například OID 1.3.6.1.2.1.2.2.1.6.1 odpovídá textové verzi iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifPhysAddress.

Pro vlastní fungování SNMP MIB databázi nepotřebuje. Ale pokud neznáme správné OID, můžeme jej dohledat v příslušné MIB databázi. Existují různé programy pro snadné prohledávání MIB databází. [10]

4.4 Instalace Ubuntu 16.04 LTS

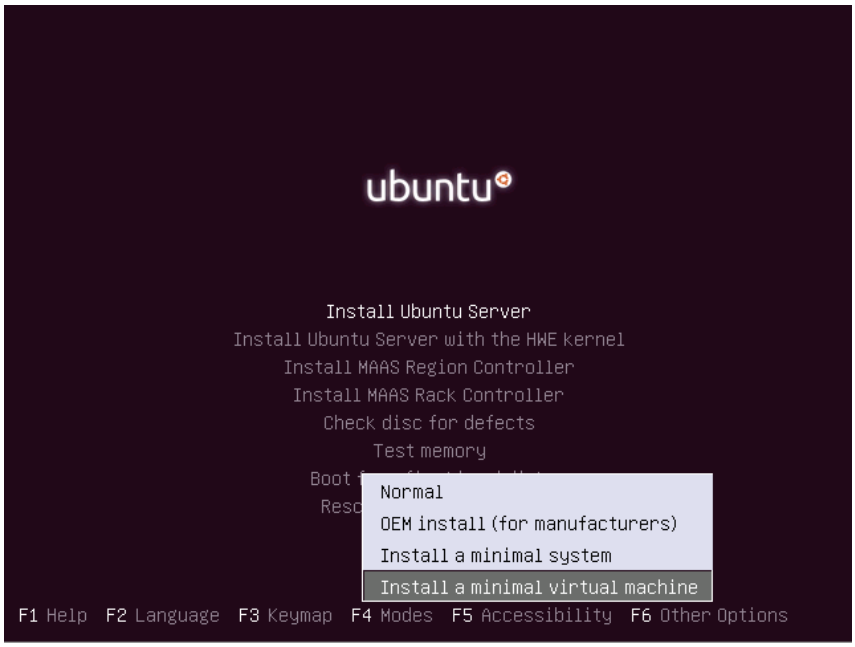
Operačním systémem, na kterém bude monitorovací systém Zabbix 3.0 LTS nainstalován je Ubuntu Server 16.04 LTS. Jeho podpora a aktualizace skončí až v roce 2021. Poté bude vhodné upgradovat verzi OS.

Instalaci provedeme pomocí nástroje VMware Vsphere Client. Jako první vytvoříme nový virtuální stroj. Zvolíme, že se jedná o linux 64-bit. Následně přiřadíme systémové prostředky viz Obrázek 3.



Obrázek 3: Zvolené systémové prostředky virtuálního stroje

Do virtuální mechaniky připojíme iso obraz instalačního média Ubuntu Server 64-bit. Virtuální stroj zapneme. Po zapnutí zvolíme jazyk instalace. V následujícím okně vybereme minimální virtuální stroj viz Obrázek 4. Následující kroky je potřeba jen potvrdit a dokončit instalaci bez dalších přídavných funkcionalit. Nyní máme nainstalovaný čistý operační systém bez grafiky, na kterém můžeme začít pracovat.



Obrázek 4: Instalace minimálního virtuálního stroje

Pro síťovou komunikaci je nutné správně nastavit IP adresaci. Jelikož se jedná o server, provedeme tuto konfiguraci ručně a adresy přidělíme staticky viz Výpis 1. Pro server je to vhodná a bezpečná varianta, protože přidělené ip adresy pak nejsou závislé na další službě, např. DHCP. Konfiguraci provedeme v terminálu následujícími příkazy. Konektivitu do vnitřní sítě i internetu ověříme příkazem ping viz Výpis 2.

```
sudo ip link set dev ens160 up
sudo ip address add X.X.1.205/16 dev ens160
sudo ip link set dev ens192 up
sudo ip address add X.X.2.85/25 dev ens192
sudo ip route add default via X.X.1.1
sudo sysctl -w net.ipv4.conf.all.forwarding=1
```

Výpis 1: Nastavení síťové konektivity v Ubuntu

```
ping X.X.1.10
ping www.seznam.cz
```

Výpis 2: Ověření síťové konektivity v Ubuntu

V tomto stavu máme připravený operační systém s dostatkem systémových prostředků a zajištěnou síťovou dostupnost.

4.5 Implementace Zabbix 3.0 LTS

Instalace systému Zabbix je dle oficiálního manuálu rozdělena do několika etap. Provedeme tedy instalaci systému Zabbix Server ve verzi 3.0 LTS a potřebný databázový systém MySQL.

4.5.1 Instalace repozitáře

Pomocí následujících příkazů nejdříve stáhneme a rozbalíme konfigurační balíček pro repozitář. Následně aktualizujeme dostupné instalační zdroje viz Výpis 3.

```
wget http://repo.zabbix.com/zabbix/3.0/ubuntu/pool/main/z/zabbix-release/zabbix
    -release_3.0-1+xenial_all.deb
dpkg -i zabbix-release_3.0-1+xenial_all.deb
apt-get update
```

Výpis 3: Instalace Zabbix repotitáře

4.5.2 Instalace Zabbix serveru s databází MySQL

Nejdříve nainstalujeme monitorovací systém s databází a webový server Apache viz Výpis 4. Následně vytvoříme databázi a provedeme její základní konfiguraci viz Výpis 5 a 6.

```
apt-get install zabbix-server-mysql zabbix-frontend-php
apt-get install apache2
```

Výpis 4: Instalace Zabbix serveru s MySQL a Apache serveru

```
shell> mysql -uroot -p<root_password>
mysql> create database zabbix character set utf8 collate utf8_bin;
mysql> grant all privileges on zabbix.* to zabbix@localhost identified by '<
    password>';
mysql> quit;
```

Výpis 5: Nastavení MySQL databáze

```
zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -uzabbix -p
    zabbix

vi /etc/zabbix/zabbix_server.conf
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=<password>
```

Výpis 6: Nastavení Zabbix serveru

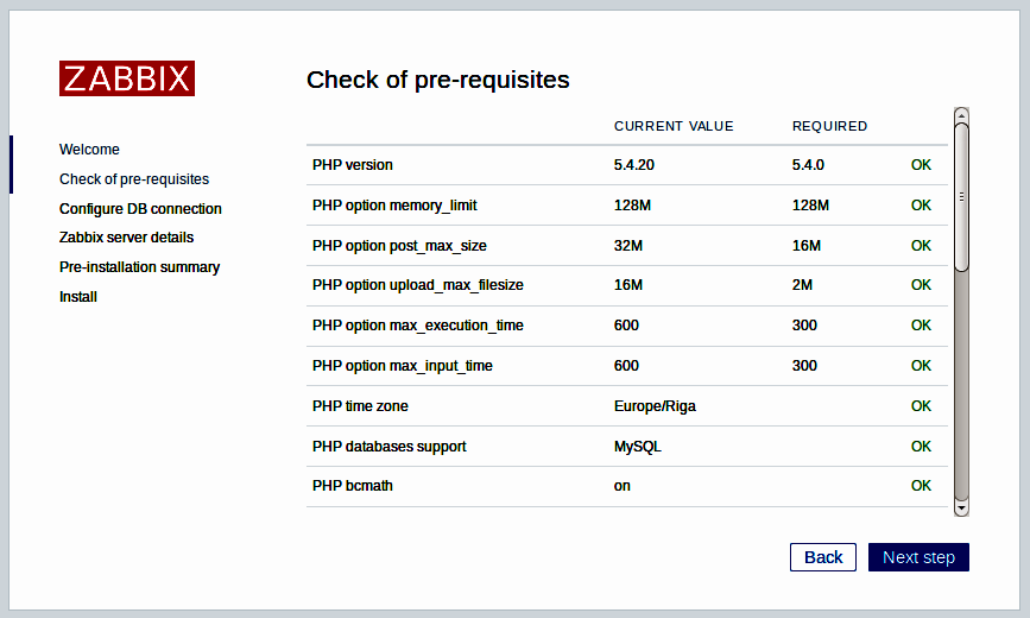
Nyní stačí služby spustit, popřípadě restartovat. U systému Zabbix nastavíme spuštění po zapnutí stroje viz Výpis 7.

```
service zabbix-server start
update-rc.d zabbix-server enable
service apache2 restart
```

Výpis 7: Spuštění Zabbix serveru

4.5.3 Instalace frontend

Ve webovém prohlížeči zadáme URL adresu serveru a můžeme vidět uvítací stránku Zabbixu. Na dalším snímku se ujistíme, že všechen potřebný software máme nainstalovaný, popřípadě provedeme jeho instalaci viz Obrázek 5. Následně nakonfigurujeme přístup do již vytvořené databáze a zahájíme instalaci. Po jejím úspěšném ukončení se uvítací stránka změní na přihlašovací formulář. Instalaci systému Zabbix server 3.0 LTS máme hotovou. [11]



Obrázek 5: Přehled potřebného softwaru pro správný chod Zabbix serveru

4.6 Přidání monitorovaných zařízení

Jak již bylo zmíněno, Zabbix dokáže monitorovat zařízení několika způsoby. My budeme využívat dva z nich. První způsob bude monitorování pomocí protokolu SNMP, který se využívá mimo jiné ke sledování síťových zařízení. Je to velmi jednoduchý, ale velice mocný a nenáročný protokol. Pro správné fungování je nutné, aby OS, na kterém Zabbix server běží, měl nainstalovaný snmp balíček. Instalaci provedeme příkazem viz Výpis 8.

```
sudo apt-get install snmp
```

Výpis 8: Instalace SNMP na Ubuntu

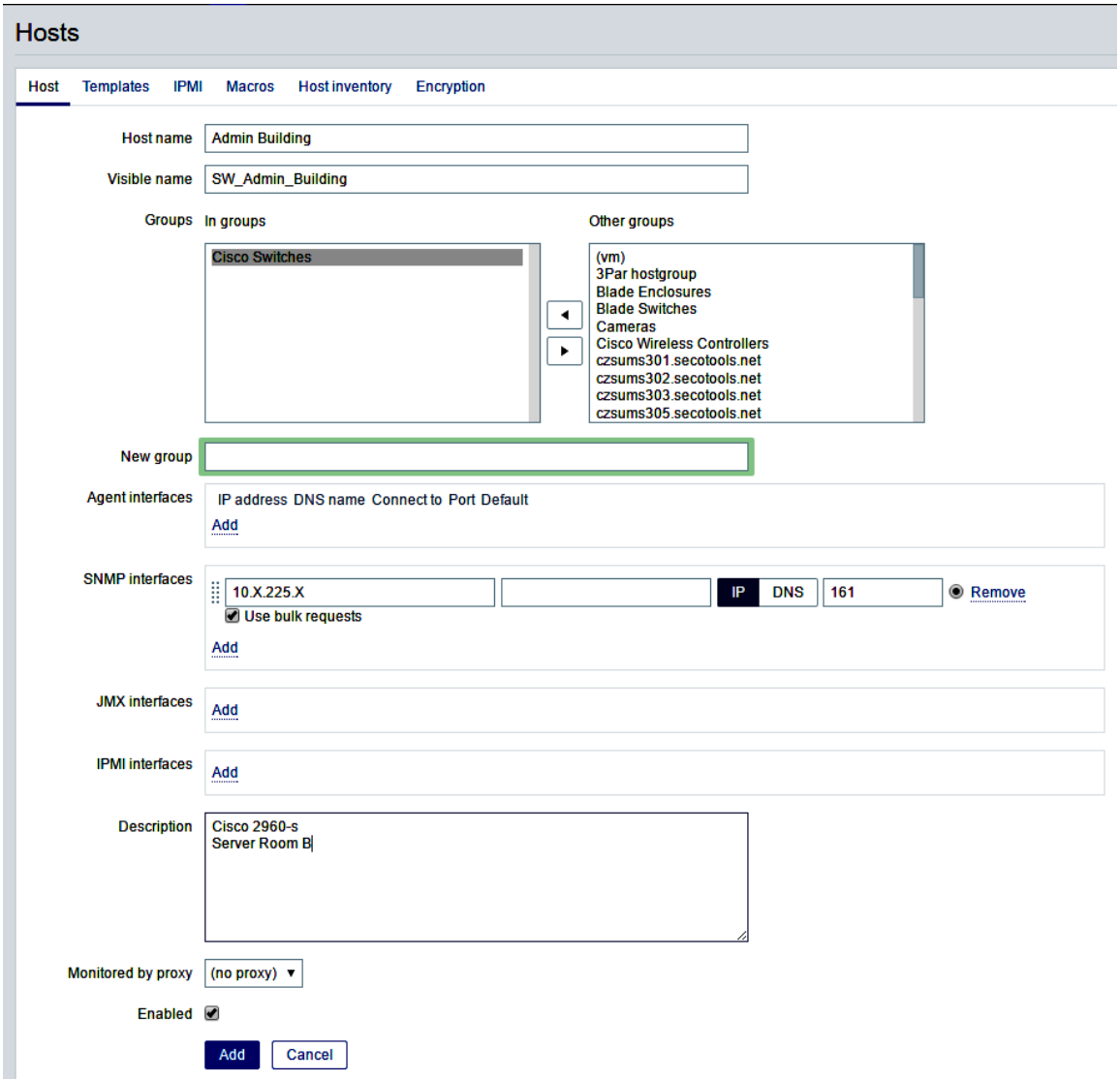
Druhý způsob monitorování je pomocí agenta přímo od Zabbixu. Je to vhodný způsob sledování pro zařízení, kde máme přístup k OS a jsme schopni provést instalaci tohoto agenta. My instalaci provedeme na sledovaných serverech s operačními systémy Windows, Linux a HP UX.

4.6.1 SNMP zařízení

Ve webovém rozhraní Zabbix serveru přejdeme do záložky Configuration -> Hosts. Zde vidíme výpis monitorovaných zařízení.Při hledání nějakého konkrétního můžeme použít filtr s mnoha možnostmi. Pro přidání nového zařízení vybereme v pravém horním rohu možnost Create Host. Nyní musíme v podzáložce Host nadefinovat následující parametry viz Obrázek 6:

- Host name: název zařízení
- Visible name: název zařízení pro Zabbix

- Groups: přiřazená skupina
- SNMP interface: IP adresa sledovaného zařízení (jméno zařízení) a port
- Description: Popis zařízení (model, umístění, . . .)



Obrázek 6: Parametry v záložce Host

V další podzáložce Templates vybereme vhodnou šablonu. Tato šablona je v podstatě souhrn sledovaných OID pro dané zařízení s dalším nastavením. Máme možnost použít obecnou šablonu předdefinovanou Zabbixem (SNMP Device), ovšem budeme získávat méně informací, než dané zařízení podporuje. Druhou možností je stažení připravené šablony pro daný typ zařízení. Nemusí nám však plně vyhovovat. Třetí možností je vytvoření vlastní šablony. Zde využijeme MIB databáze, dohledáme příslušná OID a přidáme je do dané šablony. Každé sledované OID

s nastavenými parametry (snmp string, datový typ, ukládání do historie, časové intervaly získávání, ...) Zabbix nazývá Item viz Obrázek 7. Tato šablona obsahuje i vzor pro grafy, které se nám budou následně vykreslovat, spouštěče událostí (hlášení chyb).

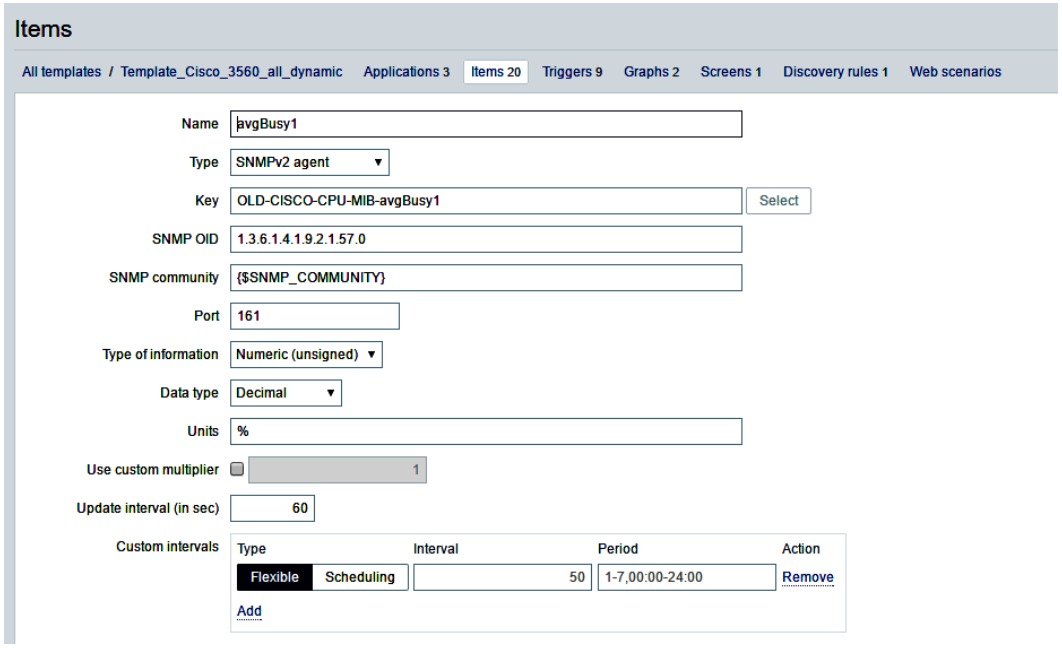
Poslední podzáložku, kterou musíme nastavit, je Macros. Stačí nám zadat community string pro ověření. Vyplníme název makra a jeho hodnotu.

V monitorovaném zařízení musíme povolit SNMP a nastavit community string. U cisco zařízení můžeme snmp konfiguraci vyčíst z výpisu running config viz Výpis 9. U ostatních zařízení konfigurujeme SNMP většinou pomocí webového rozhraní daného zařízení.

```
show running config

snmp-server community xxxx RO
snmp-server community XXXX RW
snmp-server location Pramet Tools Admin-Building
snmp-server chassis-id Admin-Building
snmp-server enable traps envmon fan shutdown supply temperature status
```

Výpis 9: Zjištění konfigurace SNMP u Cisco zařízení



Obrázek 7: Příklad nastavení itemu v šabloně

4.6.2 Zabbix agent

Pro sledování zařízení pomocí Zabbix agenta musíme provést instalaci tohoto agenta na příslušný OS. Pro instalaci na OS Linux zadáme příkaz apt-get install zabbix-agent. Na OS Wndows

stáhneme instalační soubor a provedeme instalaci. U obou nastavíme start aplikace po zapnutí PC.

Přidat zařízení do Zabbixu je obdobné jako v případě přidání SNMP zařízení. Změníme pouze typ agenta (port) a vybereme šablonu pro příslušný OS.

4.6.3 Sledování bez agenta

U zařízení, která nepodporují SNMP a nemáme možnost nainstalovat Zabbix agenta a chceme kontrolovat alespoň jejich dostupnost, můžeme využít monitorování pomocí protokolu ICMP. Klasicky přidáme hosta, vyplníme IP adresu hosta do kolonky Zabbix agent, ale v záložce Templates vybereme šablonu ICMP Ping. Tímto způsobem získáváme alespoň základní informaci o dostupnosti zařízení.

Pro sledování virtuálních strojů využijeme funkci automatického prohledávání. Ručně nastavíme pouze zařízení, která obsahují virtuální stroje. Pomocí šablony Virt VMware budeme získávat informace o virtuálních stojích.

4.6.4 Souhrn sledovaných zařízení

V následující Tabulce 3 vidíme přehled skupin zařízení s počtem zařízení a typem pro monitorování.

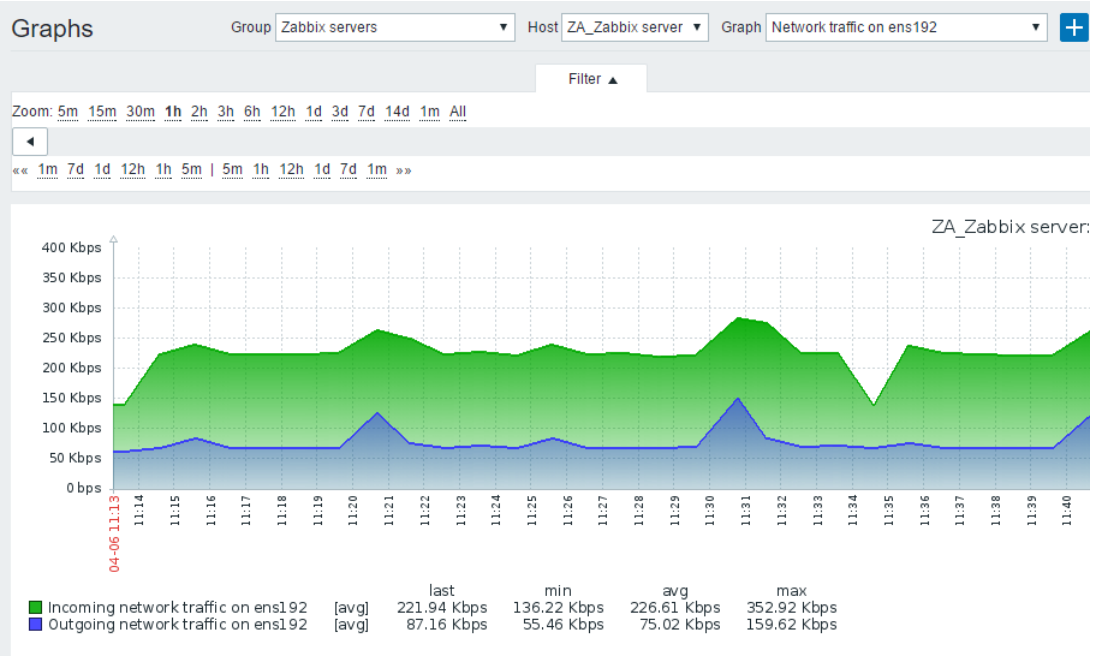
Tabulka 3: Souhrn monitorovaných zařízení

Skupina	Typ agenta	Šablona	Počet zařízení
Cisco Switches	SNMP	Template Cisco 3560 all dynamic	14
Blade Switches	SNMP	Template SNMP Device	8
Cisco Wireless Controllers	SNMP	Template SNMP Device	1
Wireless Access Points	NONE	ICMP Ping	28
Blade Enclosures	SNMP	Template HP Chassis	2
Disk Arrays	SNMP	Template SNMP Disks	2
Firewalls	SNMP	Template SNMP Device	1
Hardware Managements	SNMP	Template SNMP Device	2
Printers Big	SNMP	Template SNMP Printer	21
Printers Small	SNMP	Template SNMP Printer	25
Routers	SNMP	Template SNMP Cisco Router	5
Storages	SNMP	Template SNMP Device	1
Linux Servers	Zabbix	Template OS Linux	2
Windows Servers	Zabbix	Template OS Windows	2
Zabbix Servers	Zabbix	Template App Zabbix Server	1
Discover VMware VMs	NONE	Template Virt VMware	94
Hypervisors	NONE	Template Virt VMware	6

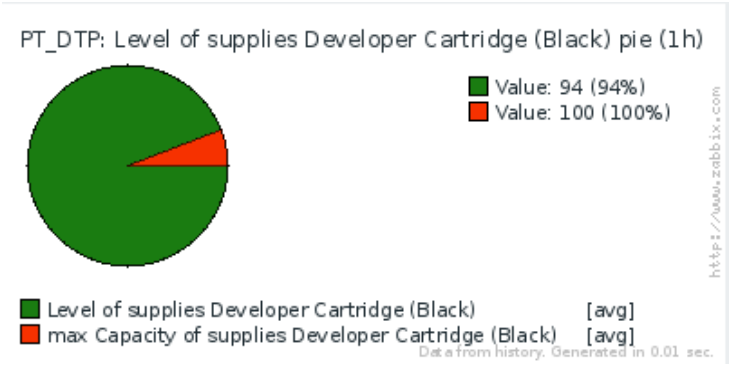
4.7 Výstupní informace

K výstupním informacím přistupujeme pomocí webvého prohlížeče. Na úvodní obrazovce front-endu můžeme vidět souhrn všech monitorovaných skupin zařízení, počet a závažnost vyskytujících se problémů v těchto skupinách. Úvodní obrazovka také obsahuje výpis posledních dvaceti problémů. Orientace na této stránce je velmi intuitivní a během okamžiku máme přehled o všech zařízeních a problémech.

Velkou skupinou výstupních informací jsou vykreslované grafy všech sledovaných čidel viz Obrázek 8. Můžeme si zobrazit grafy síťového provozu na rozhraních, grafy teplotního vývoje na zařízení viz Obrázek 9, graf stavu tonerů na tiskárně a sposty další.



Obrázek 8: Ukázka grafu zatížení síťového rozhraní



Obrázek 9: Ukázka grafu stavu toneru na tiskárně

Posledním typem výstupních informací jsou přehledné interaktivní mapy a obrazovky. Na ně si můžeme umístit třeba jen část sledovaných zařízení a specfických čidel a mít tak rychlý přehled o nejčastěji sledovaných čidlech viz přílohy B a C.

4.8 Hlášení chyb

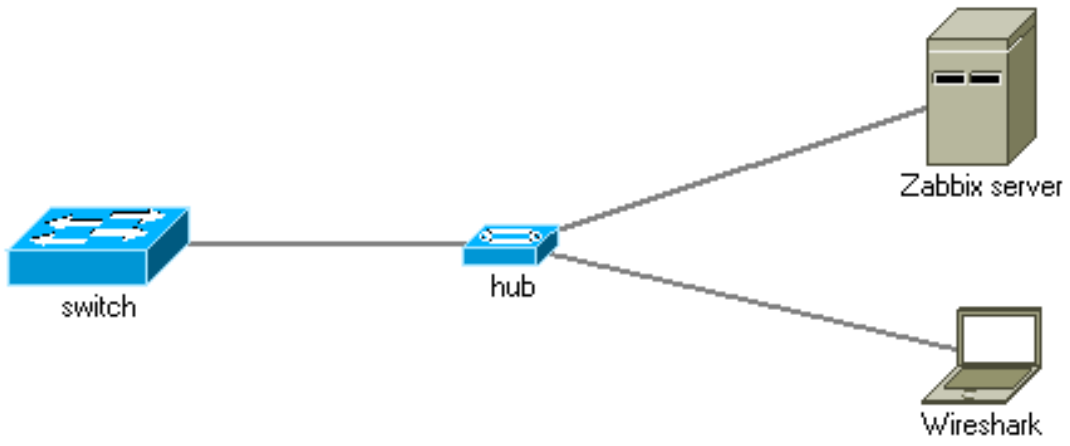
V této aplikaci se hlášení problémů nastavuje velmi snadno. V záložce Media Types se nastaví příslušná služba. My použijeme e-mail. Zadá se adresa SMTP serveru a nastaví se výchozí tvar zprávy. Nyní stačí jednotlivým uživatelům nastavit zasílání chybového hlášení. Různým uživatelům můžeme nastavit různé typy hlášení.

4.9 Měření zátěže

V poslední části věnované monitorovacímu systému se budu věnovat zatížení, které zavedení monitorovacího systému způsobilo. Budu zkoumat 3 typy zatížení: způsobený provoz na síti, zátěž na výpočetní výkon a zátěž na paměť.

4.9.1 Zátěž na síť

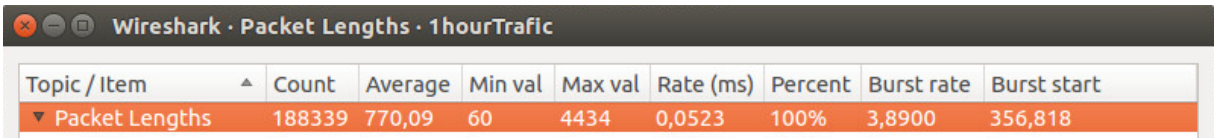
Pro zjištění zátěže sítě jsem se rozhodl použít program Wireshark. Vytvořil jsem další virtuální stroj čistě pro testování zátěže. Je umístěn na stejné podsíti, jako stroj se Zabbix serverem. Oba stroje budou připojeny do sítě přes virtuální hub, což nám zaručí, že veškerý provoz mířící na rozhraní Zabbix serveru i od něj, budeme schopni zachytávat na rozhraní nově vytvořeného stroje s Wiresharkem viz Obrázek 10. Budu zachytávat veškeré pakety na tomto rozhraní po dobu 1 hodiny. Následně dostaneme informaci o provozu a velikosti přenesených paketů Zabbix serverem za 1 hodinu.



Obrázek 10: Schéma zapojení měřícího stroje

Celková velikost zachycených paketů činí 18,128 MB. Jedná se o 188339 paketů o průměrné velikosti 770 b. Z toho je 62195 paketů o průměrné velikosti 837 b protokolu SNMP viz Obrázek 11.

Z měření vyplývá, že monitorovací systém žádným významným způsobem nezatěžuje síťové prostředky. Pokud uvážíme fakt, že nejpomalejším propojením v této firmě jsou gigabitové linky, síťový provoz 18,128 MB za hodinu je zanedbatelný.



Obrázek 11: Výpis z Wiresharku

4.9.2 Zátěž procesoru

Pro změření zátěže procesu si zvolíme jedno síťové zařízení. Zatížení na ostatních zařízeních bude velmi podobné. Konkrtétně se jedná o přístupový přepínač PHS 2. K tomuto přepínači se mohu připojit pomocí konzole. Je tedy možné změřit zatížení při spuštěném Zabbix serveru, následně Zabbix server vypnout a měření provést znovu.

Jak vyplývá z následujících výpisů konzole přístupového přepínače, Zabbix nemá vliv na zatížení procesoru sledovaného přepínače. Zatížení CPU se v obou měřeních pohybovalo okolo hodnoty 30% viz Výpis 10 a 11.

```
show processes cpu history

    222222222222222222223422222222222222223222222222232222222
    955442554699555555445387944457456257666206466563568445565
 70
 60
 50                    *
 40                    *                          *
 30 ***   ** *####### **##*  ** ** ***** ** **** *** *****
 20 ############################################################
 10 ############################################################
   0....5....1....1....2....2....3....3....4....4....5....5....
            0    5    0    5    0    5    0    5    0    5
              CPU% per minute (last 60 minutes)
             * = maximum CPU% # = average CPU%
```

Výpis 10: Hodinová zátež procesoru při zaplém Zabbixu

```
show processes cpu history

   2222222222222222222222222222222232222222222222222222222222
   6554553554576755554457566554555556065166355653455357254995
 50
 40
 30 *** ** ** ******** ******* ********* ** **** ** ** * ***
 20 ############################################################
 10 ############################################################
  0....5....1....1....2....2....3....3....4....4....5....5....
           0    5    0    5    0    5    0    5    0    5
             CPU% per minute (last 60 minutes)
            * = maximum CPU% # = average CPU%
```

Výpis 11: Hodinová zátež procesoru při vyplém Zabbixu

4.9.3 Zátěž paměti

Pro změření zátěže paměti zvolím stejný postup jako v případě měření zátěže procesoru. Opět můžeme říct, že Zabbix neklade paměťové nároky na sledované zařízení. V obou měřeních se hodnota volné paměti pohybovala okolo 60% viz Výpis 12 a 13.

```
show memory statistics history

   6666666666666666666666666666666666666666666666666666666666
   2222222222222222222222222222222222222222222222222222222222
 70
 60 ############################################################
 50 ############################################################
 40 ############################################################
 30 ############################################################
 20 ############################################################
 10 ############################################################
  0....5....1....1....2....2....3....3....4....4....5....5....
           0    5    0    5    0    5    0    5    0    5
             Free memory per minute (last 60 minutes)
            * = maximum # = average
```

Výpis 12: Hodinová zátež paměti při zaplém Zabbixu

```
show memory statistics history

   6666666666666666666666666666666666666666666666666666666666
   2222222222222222222222222222222222222222222222222222222222
 70
 60 ############################################################
 50 ############################################################
 40 ############################################################
 30 ############################################################
 20 ############################################################
 10 ############################################################
  0....5....1....1....2....2....3....3....4....4....5....5....
           0    5    0    5    0    5    0    5    0    5
             Free memory per minute (last 60 minutes)
            * = maximum # = average
```

Výpis 13: Hodinová zátež paměti při vyplém Zabbixu

5 Rozšíření sítě

Druhým větším úkolem mé praxe bylo vymyslet a otestovat propojení dvou přepínačů dvojicí metalických STP kabelů, které by dokázalo pracovat současně a využít tak potenciál obou kabelů. Vznikla by tak ochrana proti výpadku jedné linky a navýšila by se přenosová rychlost.

Tento požadavek vznikl při plánované expazni sítě z důvodu stavby nové budovy. V této budově ja plánovaný nový přepínač Cisco 2960-S. Jako ostatní přístupové přepínače má být připojen dvojicí optických vláken do páteřních L3 přepínačů. Bohužel páteřní přepínače mají optické konetktory již plně využity pro připojení stávajících přístupových přepínačů. Při jejich koupi se s rozšířením sítě nepočítalo.

Navrhované řešení je tedy následující: Uvolnit dvojici optických konektorů pro nový přepínač, najít dva stávající nejméně vytížené přepínače, mezi kterými existuje nevyužité vedení STP, tyto dva přepínače propojit.

Vhodní kandidáté jsou přepínače PHS1 a PHS2. Vertikální umístění v budově mají shodné, horizontálně jsou od sebe dvě patra. Mezi těmito přepínači existuje nevyužitá dvojice STP kabelů. Provoz na přepínači PHS 2 je minimální.

Při hledání možnosti propojení těchto přepínačů STP kabeláží se jeví jako nejlepší technologie EtherChannel.

5.1 Technologie EtherChannel

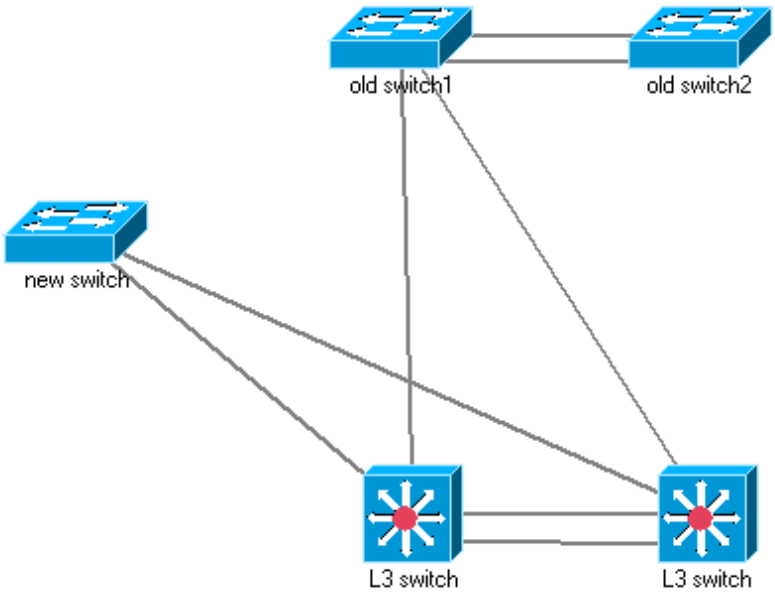
EtherChannel je technologie portů, která slouží ke spojování linek. Primárně se používá na Cisco přepínačích. Dovoluje spojit několik fyzických ethernetových linek do jedné logické z důvodu zabezpečení proti výpadku jedné linky a také navýšení přenosové rychlosti. EtherChannel může být vytvořen mezi dvěma až osmi (100 Megabit až 10 Gigabit) aktivními linkami a až osmi neaktivními záložními linkami. EtherChannel se primárně využívá na páteřní síti, ale může být využit i k připojení koncového zařízení. [12]

5.2 Konfigurace přepínače

Konfiguraci na přepínači provedeme pomocí následujících příkazů.

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable non-silent
Switch(config-if-range)# end
```

Výpis 14: Konfigurace EtherChannel na přepínači



Obrázek 12: Schéma zapojení nového přepínače

5.3 Testování EtherChannel

Pro otestování technologie EtherChannel proti výpadku linky jsem provedl základní test. Na obou testovaných přepínačích jsem nastavil IP adresu. K jednomu přepínači jsem připojil notebook a přiřadil mu IP adresu ze stejného rozsahu jako přepínačům. Spustil jsem příkaz ping na IP adresu vzdálenějšího přepínače. Postupně jsem odpojoval propojovací kabely přiřazené do skupiny EtherChannel. Nedostupnost vzdáleného přepínače opravdu nastala až při úplném přerušení všech linek. Po připojení komunikace ihned pokračovala.

6 Závěr

V této bakalářské práci jsem shrnul absolvování individuální odborné praxe ve společnosti Pramet Tools, s.r.o. na oddělení informatiky a pozici správce sítě.

Na začátku práce jsem zmapoval síťovou a výpočetní infrastrukturu podniku a převedl ji do vizuální podoby pomocí programu Network Notepad. Vizuální podobu topologie můžeme vidět v příloze A.

Většina bakalářské práce je věnována zavedení monitorovacího systému. Na základě určených kritérií jsem zvolil monitorovací systém Zabbix 3.0 LTS běžící na OS Ubuntu 16.04 LTS. Je zde popsán kompletní proces implementace. Uvedl jsem různé použité způsoby monitorování. Nejvíce jsem využil monitorování pomocí protokolu SNMP. Příklady přehledných grafických výstupů nalezneme v přílohách B, C, D. Změřil jsem a dokázal nenáročnost monitorovacího systému působící na síťové prostředky, CPU a paměť monitorovaného zařízení. V tuto chvíli je monitorováno 250 zařízení. Řada závad již byla díky tomuto systému odhalena a opravena. Jsou zde další veliké možnosti v budoucím rozšiřování sledovaných zařízení (případně dalších senzorů na zařízeních) a v grafické prezentaci naměřených dat. Do budoucna není vyloučeno použít Zabbix pouze jako systém pro sbírání informací a pro prezentaci dat použít jiný software, například systém Grafana.

V poslední části jsem otestoval řašení propojení dvou Cisco přepínačů pomocí technologie EtherChannel. Ověřil jsem robustnost této technologie pomocí základního testu odpojování linek od přepínače.

Během praxe jsem řešil i jiné problémy a úkoly. Čas na jejich řešení byl ovšem mnohonásobně menší, než na již zmíněné úkoly. Jednalo se například o testování nového konferenčního SIP telefonu s možností přenosu obrazu, nebo problému neprůchodnost telefonní dvojlinky technologií VDSL.

Během praxe jsem využil znalosti získané v předmětech zabývajících se problematikou počítačových sítí, prácí s OS Ubuntu a programem Wireshark a v malé míře i z předmětů elektrotechnických.

Literatura

[1] Profil společnosti, http://www.dormerpramet.com/cs-cz/company/who-we-are, 18.4.2017.

[2] HPE BladeSystem c7000 Enclosures, https://www.hpe.com/us/en/product-catalog/storage/disk-enclosures/pip.hpe-bladesystem-c7000-enclosures.1844065.html, 18.4.2017.

[3] HPE Integrity BL860c i2 Server Blade, https://www.hpe.com/cz/en/product-catalog/servers/integrity-servers/pip.hpe-integrity-bl860c-i2-server-blade.4186428.html, 18.4.2017.

[4] HP ProLiant BL460c G7 Server - Overview, http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c02535780, 18.4.2017.

[5] HPE ProLiant BL460c Gen9 Server Blade, https://www.hpe.com/cz/en/product-catalog/servers/proliant-servers/pip.hpe-proliant-bl460c-gen9-server-blade.7271227.html, 18.4.2017.

[6] Cisco Catalyst 4500 Series Switch Data Sheet, http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-series-switches/product_data_sheet0900aecd801792b1.html, 18.4.2017.

[7] Cisco Catalyst 2960-S Series Switches Data Sheet, http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-s-series-switches/data_sheet_c78-726680.html, 18.4.2017.

[8] Kateřina Hanušová. *Monitoring mobilních klientů*. Univerzita Hradec Králové, Hradec Králové, 2015

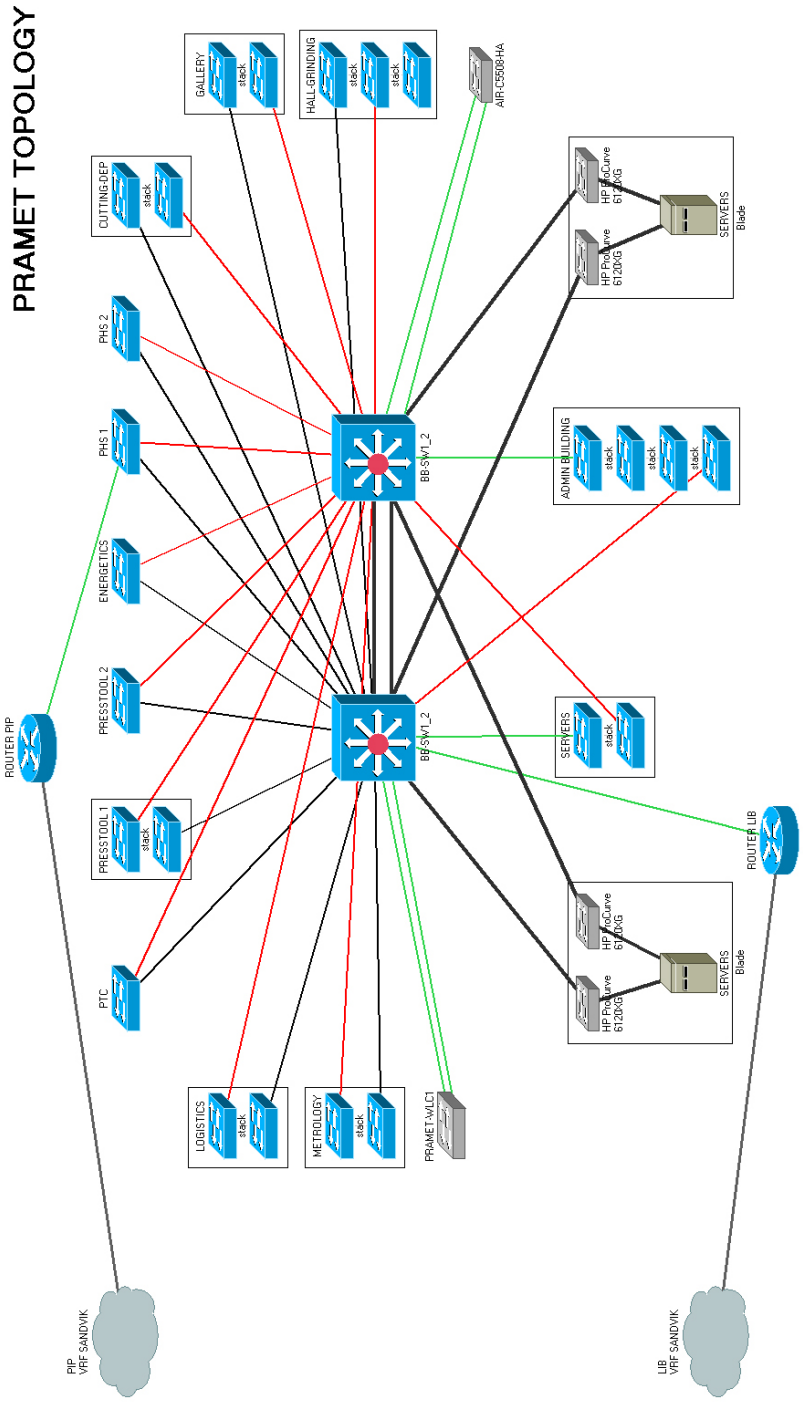
[9] Andrew Tabona. *The top 20 free Network Monitoring and Analysis Tools for sysadmins*, https://techtalk.gfi.com/the-top-20-free-network-monitoring-and-analysis-tools-for-sys-admins/, 15.5.2015.

[10] Petr Bouška. *SNMP - Simple Network Management Protocol*, http://www.samuraj-cz.com/clanek/snmp-simple-network-management-protocol/, 20.12.2006.

[11] Zabbix Documentation 3.0, https://www.zabbix.com/documentation/3.0/manual, 18.4.2017.

[12] EtherChannel, https://en.wikipedia.org/wiki/EtherChannel, 6.4.2017.

A Topologie Pramet Tools, s.r.o.



Obrázek 13: Pramet topologie

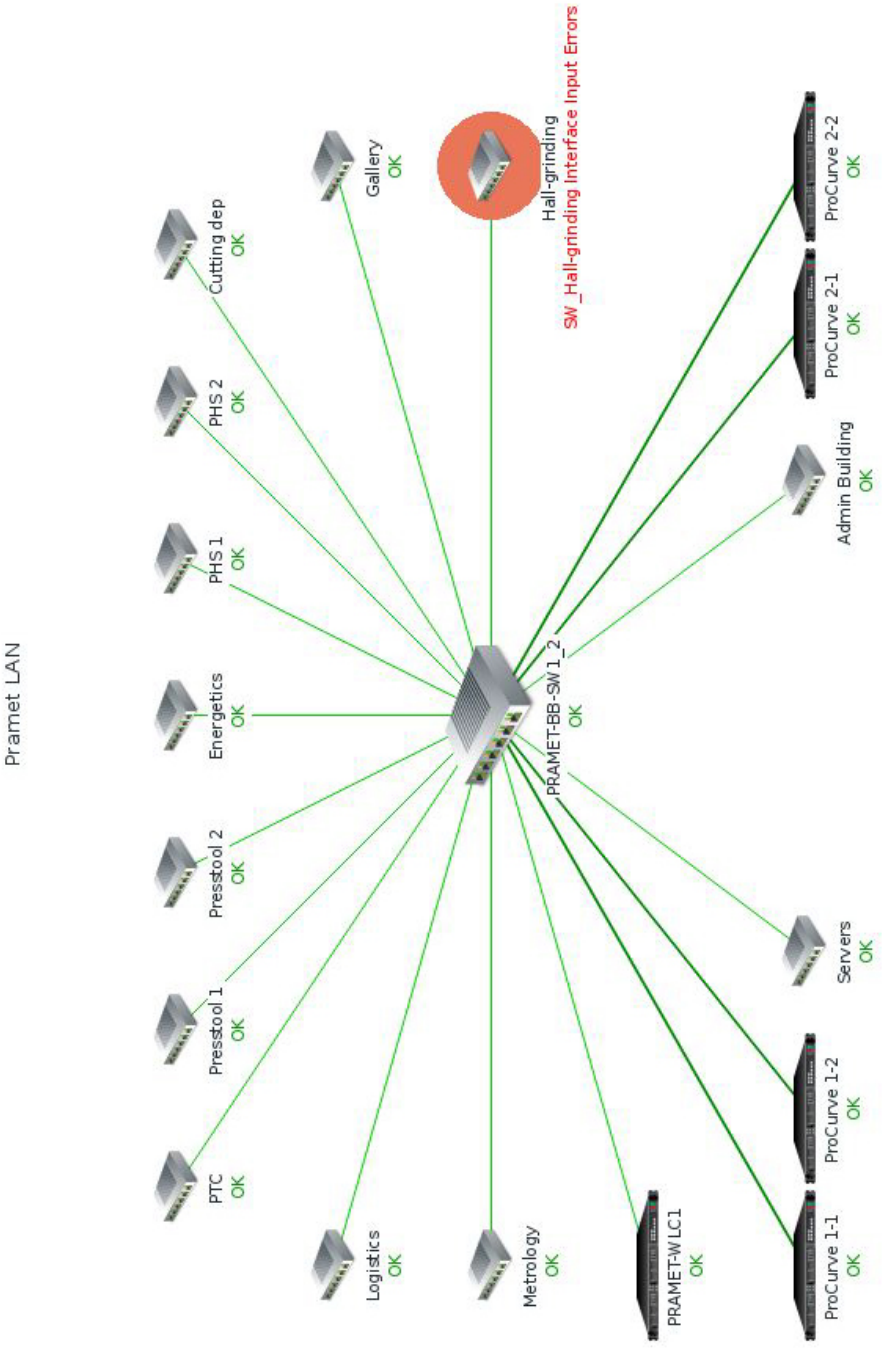
B Stav monitorovaných zařízení

System status

Host group	Disaster	High	Average	Warning	Information	Not classified
(vm)	0	0	0	0	0	0
Blade Enclosures	0	0	0	0	0	0
Blade Switches	0	0	0	0	0	0
Cameras	0	0	0	0	0	0
Cisco Switches	0	1	0	0	0	0
Cisco Wireless Controllers	0	0	0	0	0	0
czsums301.secotools.net	0	0	0	0	0	0
czsums302.secotools.net	0	0	0	0	0	0
czsums303.secotools.net	0	0	0	0	0	0
czsums305.secotools.net	0	0	0	0	0	0
czsums308.secotools.net	0	0	0	0	0	0
czsums309.secotools.net	0	0	0	0	0	0
Discovered hosts	0	0	0	0	0	0
Disk Arrays	0	0	0	0	0	0
Firewalls	0	0	0	0	0	0
Hardware Managements	0	0	0	0	0	0
Hypervisors	0	0	0	0	0	0
Linux servers	0	0	0	0	0	0
Printers_Big	0	0	0	0	7	0
Printers_Small	0	0	0	0	6	0
Routers	0	0	0	0	0	0
Server Blades	0	0	0	0	0	0
Server Blades (vm)	0	0	0	0	0	0
Storages	0	0	0	0	0	0
Uninterruptible Power Supplyes	0	0	0	0	0	0
Virtual machines	0	0	0	0	0	0
Windows Servers	0	0	0	3	0	0
Wireless Acess Points	0	0	0	0	0	0
Zabbix servers	0	0	0	0	0	0

Obrázek 14: Stav monitorovaných zařízení

C Interaktivní mapa sítě



Obrázek 15: Interaktivní mapa sítě