Monitorovací systém Nagios a jeho využití ve firemní síti

Marek Voráč

Bakalářská práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav bezpečnostního inženýrství

Akademický rok: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Marek Voráč**
Osobní číslo:	**A17591**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Monitorovací systém Nagios a jeho využití ve firemní síti**
Téma práce anglicky:	**The Monitoring System Nagios and Use in the Corporate Network**

Zásady pro vypracování

1. Analyzujte možnosti monitoringu a managementu zařízení a služeb v počítačových sítích.
2. Srovnejte dostupné nástroje.
3. Zaměřte se na monitorovací systém Nagios.
4. Popište dostupné možnosti a konfiguraci.
5. Nakonfigurujte a v praxi otestujte systém Nagios na zvolených konfiguracích.

Rozsah bakalářské práce:
Rozsah příloh:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. SOSINSKY, Barrie A. *Mistrovství – počítačové sítě: [vše, co potřebujete vědět o správě sítí]*. Brno: Computer Press, 2010. ISBN 9788025133637.
2. KUROSE, James F. a Keith W. ROSS. *Počítačové sítě*. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.
3. KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5., aktualiz. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.
4. VACCHE, Andrea Dalle a Stefano Kewan LEE. *Mastering Zabbix* [online]. Packt Publishing, 2013 [cit. 2019-11-28]. ISBN 978-1-78328-349-1. Dostupné z: http://www.omid-online.com/ebooks/MasteringZabbix.pdf
5. Nagios Core Version 3.x Documentation [online]. 2009, 358. Dostupné z: https://assets.nagios.com/downloads/nagioscore/docs/nagios-3.pdf
6. *Nagios Core: The Industry Standard In IT Infrastructure Monitoring* [online]. Nagios Enterprises, 2019 [cit. 2019-11-28]. Dostupné z: https://library.nagios.com/library/products/nagios-core/

Vedoucí bakalářské práce: **doc. Ing. Martin Sysel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **7. prosince 2019**
Termín odevzdání bakalářské práce: **25. května 2020**

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Ve Zlíně dne 7. prosince 2019

Jméno, příjmení: Marek Voráč

Název bakalářské práce: Monitorovací systém Nagios a jeho využití ve firemní síti

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 22.6.2020

Marek Voráč v.r.

.....

podpis diplomanta

ABSTRAKT

Bakalářská práce je zaměřena na monitoring aktivních prvků počítačových sítí pomocí open source programu Nagios. V teoretické části jsou analyzovány možnosti monitoringu a managementu zařízení a služeb počítačových sítí.

Praktická část prezentuje implementaci open source programu Nagios do reálného prostředí vybrané společnosti, která disponuje rozlehlou síťovou infrastrukturou.

Klíčová slova: počítačová síť, monitoring sítě, Nagios

ABSTRACT

The bachelor thesis is focused on the monitoring of active elements of computer networks using the open source program Nagios.

The theoretical part analyzes the possibilities of monitoring and management of computer network equipment and services.

The practical part presents the implementation of the open source Nagios program into the real environment of a selected company that has a large network infrastructure.

Keywords: computer network, network monitoring, Nagios

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

V dnešním světě je pojem monitorování sítě rozšířen skrze celé odvětví informačních technologií (dále jen IT). Sledování sítě je kritický proces IT, ve kterém jsou všechny síťové komponenty, jako směrovače, přepínače, servery a další, monitorovány z hlediska závad a výkonu. Tyto hodnoty jsou průběžně vyhodnocovány tak, aby byla zachována a optimalizována jejich dostupnost. Účinné proaktivní monitorování může zabránit výpadkům nebo selhání sítě, které by mohly ohrozit chod, případně bezpečnost podniku. Toto lze eliminovat včasnou detekcí, a proto je nezbytné nepřetržité monitorování síťových zařízení. V bakalářské práci jsem řešil problém monitoringu firemní počítačové sítě pomocí open source systému Nagios, s jehož pomocí je možné zmíněným problémům předejít. Systém Nagios není jediným programem na trhu, který se tímto problémem zabývá. Těchto programů je vícero jak v bezplatné, tak placené podobě. Jelikož se v bakalářské práci zabývám open source variantou, vyzdvihnu zde několik dalších ze stejné sféry. Mezi nejznámější open source nástroje pro monitorování počítačové sítě, mimo již zmíněný Nagios, patří Zabbix, Icinga, Cacti, OpenNMS a Netdata. Když jsem se rozhodoval, který monitorovací nástroj zvolit, tak jsem studoval možnosti jednotlivých z nich. Po přečtení různých materiálů a zkušeností uživatelů jsem se rozhodl právě pro Nagios. Ze všech porovnávaných mi přišlo jeho prostředí a možnosti oproti konkurenci nejlepší. Musím ale říci, že všechny tyto systémy jsou velice propracované a jsou si velmi podobné. Ve výsledku tak spíše záleží na subjektivním pocitu uživatele, pro který z nich se rozhodne. Určitě volbou kteréhokoliv z nich neudělá krok špatným směrem a budou mu dobře sloužit, tak jako mně Nagios. V teoretické části bakalářské práce chci čtenáře seznámit se základními principy funkce počítačových sítí. Prezentuji zde informace, které jsou nezbytné pro pochopení, jak počítačové sítě fungují. Krátce shrnu základní informace o dalších, již zmíněných open source monitorovacích systémech. Dále detailně rozeberu systém Nagios a možnosti jeho konfigurace. V rámci praktické části jsem provedl implementaci systému Nagios do reálného prostředí společnosti. Řeším zde postup při implementaci, konfiguraci jednotlivých parametrů a problémy, se kterými jsem se v průběhu setkal.

I. TEORETICKÁ ČÁST

1 ANALÝZA MOŽNOSTÍ MONITORINGU A MANAGEMENTU ZAŘÍZENÍ A SLUŽEB V POČÍTAČOVÝCH SÍTÍCH

„Monitoring má mnoho podob a můžeme využít řadu technologií a protokolů. Celý monitorovací systém můžeme postavit na vlastních skriptech či na bezplatných řešeních, kdy investujeme pouze svůj čas a znalosti. Nebo využít některý z rozsáhlé nabídky komerčních produktů.

Pokud nebudeme spoléhat na cizí aplikace, ale vytvoříme vlastní skripty či programy, tak budeme mít detailní přehled o tom, jak monitoring probíhá a naše řešení bude přesně odpovídat našim potřebám. Musíme však mít hlubší znalosti skriptování či programování, spolu se znalostí síťových protokolů a technologií. Navíc je tvorba takového řešení časově náročná.

Produkty zdarma jsou často značně univerzální se širokými možnostmi konfigurace. Vyžadují však také hlubší znalosti pro nastavení, protože některé konfigurace znamenají psaní vlastních skriptů. Výhoda je, že máme komplexní prostředí (které zahrnuje třeba konfiguraci, dashboard, zpracování grafů) a na míru nastavujeme pouze určité šablony pro získávání dat.

Oproti tomu komerční produkty většinou nainstalujeme na pár kliknutí a monitorování rozchodíme během pár minut. Stačí znát adresy zařízení, a jaké údaje na nich chceme monitorovat. Většinou jsou zde připraveny šablony pro jednotlivé oblasti. To nám ovšem zároveň omezuje možnosti použití.

Samozřejmě nic není pouze bílé nebo černé, takže i do komerčních aplikací můžeme dopisovat vlastní skripty. Nalezneme i volně šiřitelné systémy, které jsou připravené na nejběžnější nasazení.

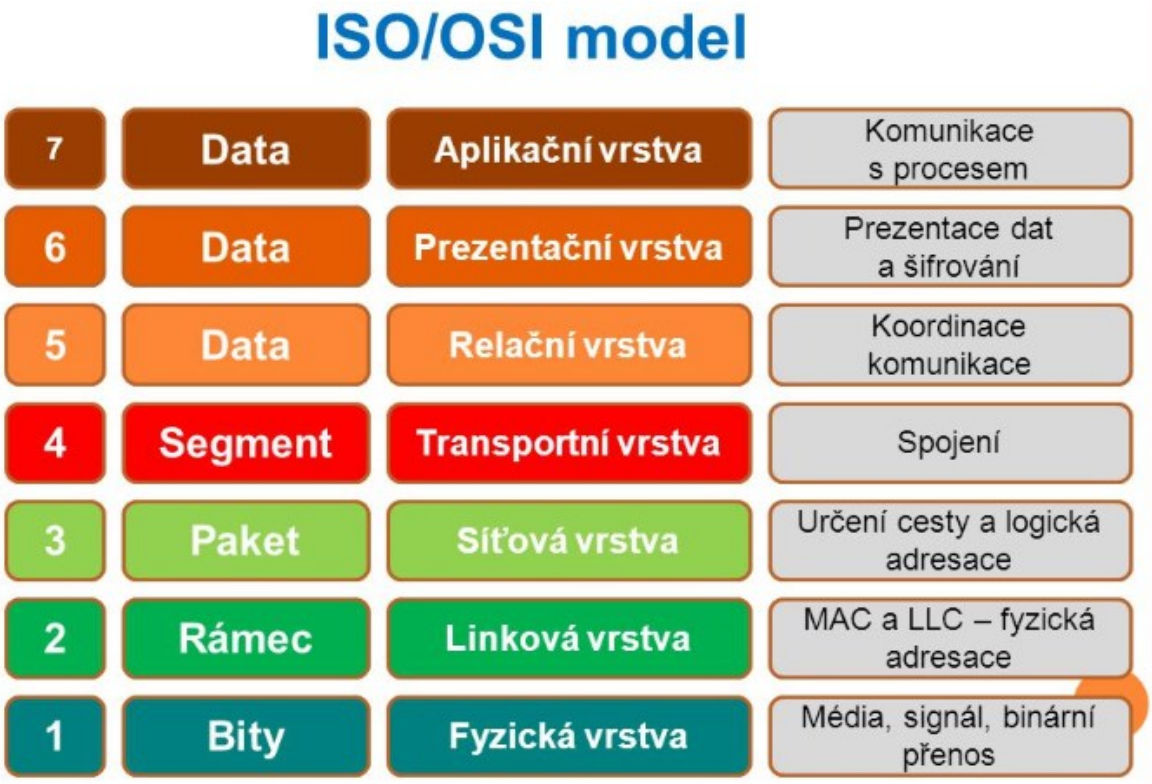
Než začneme vlastní monitoring plánovat, je třeba si uvědomit, co přesně chceme sledovat a jaké výstupy z monitoringu jsou pro nás prioritní. Podle toho je třeba následně zvolit použité technologie. I když existují rozsáhlé systémy s řadou komponent, tak asi nenalezneme monitorovací nástroj, který by obsáhl všechny oblasti, které potřebujeme sledovat ve větší firmě. Musíme tedy kombinovat více produktů.

Na monitoring se můžeme dívat ze dvou pohledů. Chceme se dozvědět, že někde došlo k problému. Tedy, že něco přestalo fungovat či byl překročen nějaký kritický limit. Nebo chceme získávat aktuální (ale i historické) informace o určitém systému. To může být pohled

na vytížení serveru, abychom plánovali jeho další využití. Přehled, kde v síti (do jakého portu jakého switche) je připojen klient s jakou IP a MAC adresou. Či sledování vytížení datových linek.“ [1]

1.1 Referenční model ISO/OSI

Pro pochopení, jak fungují počítačové sítě, je nutné znát základy v podobě sedmivrstvého open systems interconnect (dále jen OSI) modelu, který standardizuje klíčové funkce sítě pomocí síťových protokolů. To umožňuje různým typům zařízení od různých výrobců vzájemně komunikovat v síti. V modelu OSI jsou síťové komunikace seskupeny do sedmi logických vrstev. Dvě zařízení spolu komunikují pomocí protokolů standardizovaných OSI v každé vrstvě. [2] [3]



Obrázek 1. Model sedmi vrstev OSI, zdroj: [4]

„Popis jednotlivých vrstev:

1. Aplikační (poskytování aplikacím přístup ke komunikačnímu systému).
2. Prezentační (transformuje data do tvaru, který používají aplikace).
3. Relační (organizuje a synchronizuje dialog mezi relačními vrstvami).

4. Transportní (zajišťuje přenos dat mezi koncovými uzly).
5. Síťová (stará se o směrování v síti a síťové adresování).
6. Linková (Poskytuje spojení mezi dvěma sousedními systémy).
7. Fyzická (Aktivuje, udržuje a deaktivuje fyzické spoje mezi koncovými systémy). „ [4]

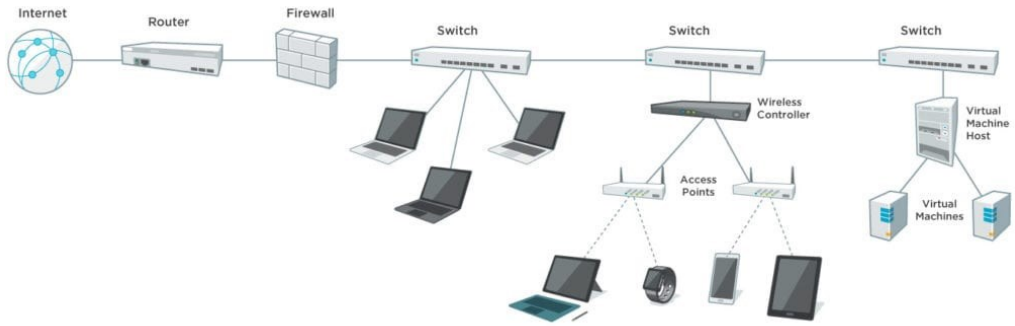
K monitorování se nejčastěji používají vrstvy 2, 3 a 7. Systémy monitorování sítě používají tyto vrstvy k vyhledávání zařízení v síti a zjišťování způsobu jejich připojení. [2] [3]

1.2 Jak data procházejí sítí

Většina soukromých sítí je připojena k internetu, který připojuje vzdálené uživatele k ústředím. Spojuje zákazníky s webovými stránkami. Soukromé sítě jsou připojeny k internetu pomocí směrovačů. Informace jsou zasílány přes internet ve formě datových paketů. Každý datový paket obsahuje cílovou adresu internetového protokolu (dále jen IP), kterou směrovače používají k odesílání informací z jednoho místa na druhé. Když router přijme datový paket z internetu, tak ho předá do soukromé sítě. Ve většině sítí musí datové pakety nejprve projít bránou firewall. Účelem je zabránit nechtěnému provozu a zabezpečit soukromou síť. Firewall to provádí filtrováním provozu mezi internetem a soukromou sítí. Pokud je příchozí datový paket označen pravidly brány firewall, je blokován a není puštěn do soukromé sítě.

Firewally také řídí přístup uživatelů mezi internetem a soukromou sítí. Firewall lze například nakonfigurovat tak, aby zabránil uživatelům v soukromé síti používat specifické protokoly, jako je peer to peer. Toto je jeden ze způsobů, jak brány firewall zabezpečují soukromé sítě před neoprávněným přístupem, malwarem a jinými bezpečnostními hrozbami.

Datové pakety procházející bránou firewall jsou přijímány přepínačem v soukromé síti. Přepíná připojení notebooků, serverů, tiskáren a dalších zařízení k soukromé síti. Tato zařízení jsou připojena k přepínači pomocí síťové karty. [2] [3]



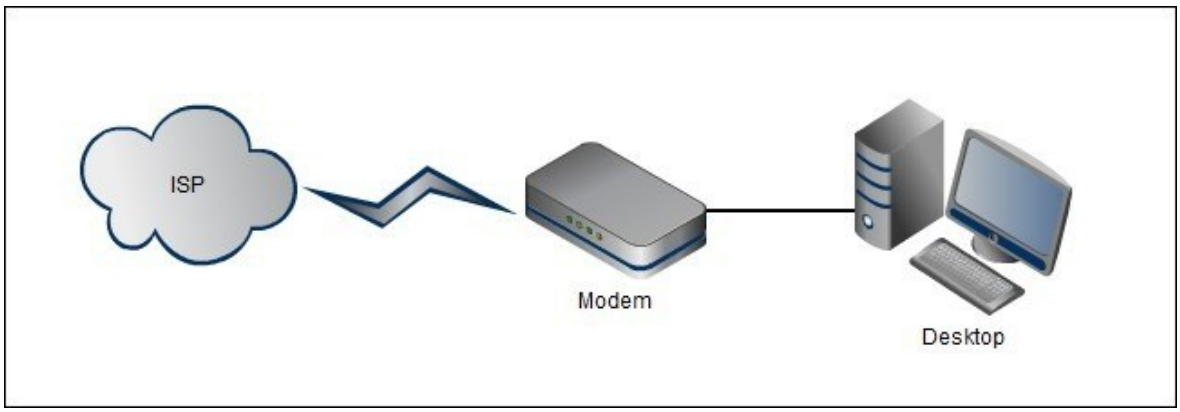
Obrázek 2. Data procházející počítačovou sítí, zdroj: [2]

1.3 Základní síťová zařízení

Mezi základní a nejběžnější síťová zařízení patří síťová karta, přepínač (anglicky switch), směrovač (anglicky router), server, opakovač (anglicky repeater) a modem.

1.3.1 Modem

Modem přijímá informace od poskytovatele internetového připojení (dále jen ISP) prostřednictvím telefonních linek, bezdrátového signálu, optických vláken nebo koaxiálního kabelu ve vaší domácnosti (v závislosti na poskytovateli služeb) a převádí je na digitální signál. Úkolem routeru je vyslat tento signál do připojených zařízení, buď prostřednictvím kabelových ethernetových kabelů nebo Wireless Fidelity (dále jen Wi-Fi), aby všechna vaše zařízení mohla naskočit na palubu a získat přístup k internetu. Váš směrovač a poskytovatel internetových služeb nemůže mezi sebou komunikovat přímo, protože mluví různými jazyky. Vysílají různé typy signálů, a proto je role modemu jako překladače tak důležitá. [5] [6]



Obrázek 3. Zapojení modemu v síti, zdroj: [7]

1.3.2 Síťová karta

Síťová karta je hardware (dále jen HW), bez kterého nelze počítač připojit k síti. Síťová karta komunikuje na více vrstvách modelu OSI. Na fyzické vrstvě zasílá signály, na linkové vrstvě datové pakety a na fyzické vrstvě funguje na úrovni síťového rozhraní.

Jedná se o desku s obvody nainstalovanou v počítači, která zajišťuje vyhrazené síťové připojení. Nazývá se také řadič síťového rozhraní, síťový adaptér nebo adaptér lokální sítě (dále jen LAN). Síťová karta umožňuje kabelovou i bezdrátovou komunikaci. Dále umožňuje komunikaci mezi počítači připojenými prostřednictvím LAN a také komunikaci přes rozsáhlou síť prostřednictvím IP. Síťové karty dělíme na interní a externí.

V interních síťových kartách má základní deska počítače slot pro síťovou kartu, kam ji lze vložit. Interní síťové karty jsou dvou typů. První typ používá připojení peripheral component interconnect (dále jen PCI), zatímco druhý typ používá industry standard architecture (dále jen ISA).

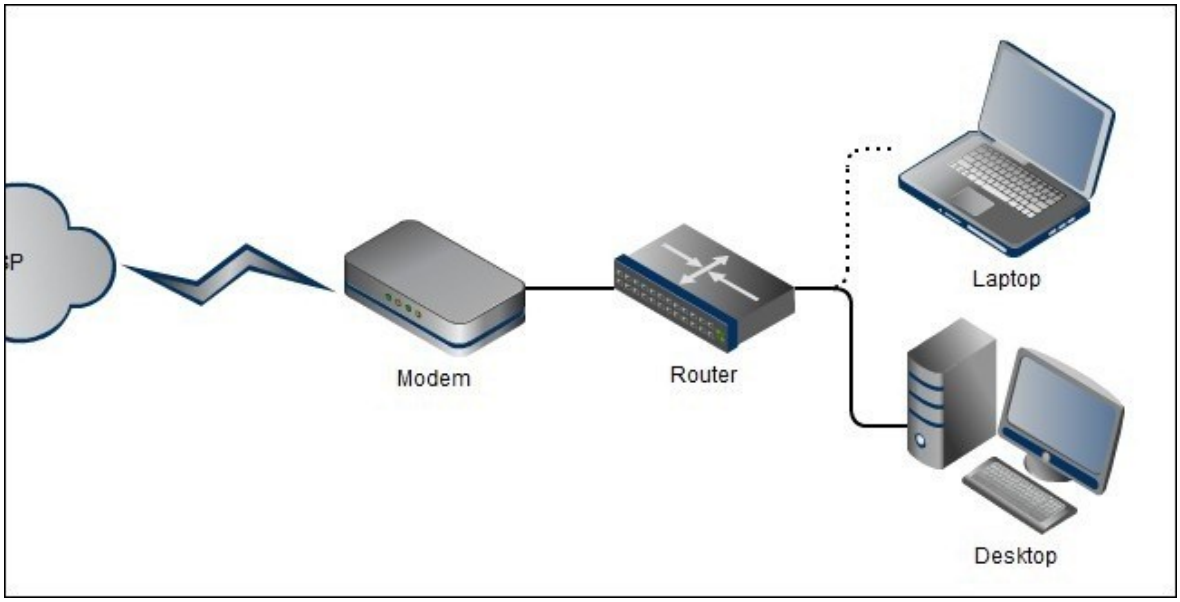
Externí síťové karty se používají u stolních počítačů a notebooků, které nemají interní síťovou kartu. Externí síťové karty jsou bezdrátové a jsou připojeny buď pomocí PCI nebo pomocí universal serial bus (dále jen USB). [5] [8]

1.3.3 Router

„Router je spojovací zařízení mezi jednotlivými segmenty sítě LAN. Pracuje na síťové vrstvě modelu OSI a řídí za pomocí síťových protokolů provoz datových paketů mezi jednotlivými sítěmi. Rozlišujeme jednoprotokolový, multiprotokolový a hybridní směrovač. Za použití různých kritérií, jako jsou vytížení sítě, průchodnost, poplatky, čekací doba, určuje směrovač pro každý datový paket optimální cestu počítačovou sítí k cílové adrese. K nalezení nejvýhodnější trasy využívá takzvanou směrovací tabulku, která podchycuje veškerá data o struktuře počítačové sítě. Rozlišujeme dvě základní metody směrování, statické a dynamické. Směrovač musí vykazovat následující základní vlastnosti:

- metodu identifikace jiné stanice,
- algoritmus zpracování převzatých paketů pro jejich přesměrování na jiný směrovač,
- hlavičku s informacemi o cílové adrese a životnosti paketu, jeho rozčlenění a následném spojení.

Na rozdíl od síťových mostů přesměruje směrovač pouze datové pakety se známou cílovou adresou. Na základě těchto analyzovaných vlastností je směrovač vhodný pro síťové spojení od LAN až po globální počítačovou síť (dále jen WAN).“ [9]

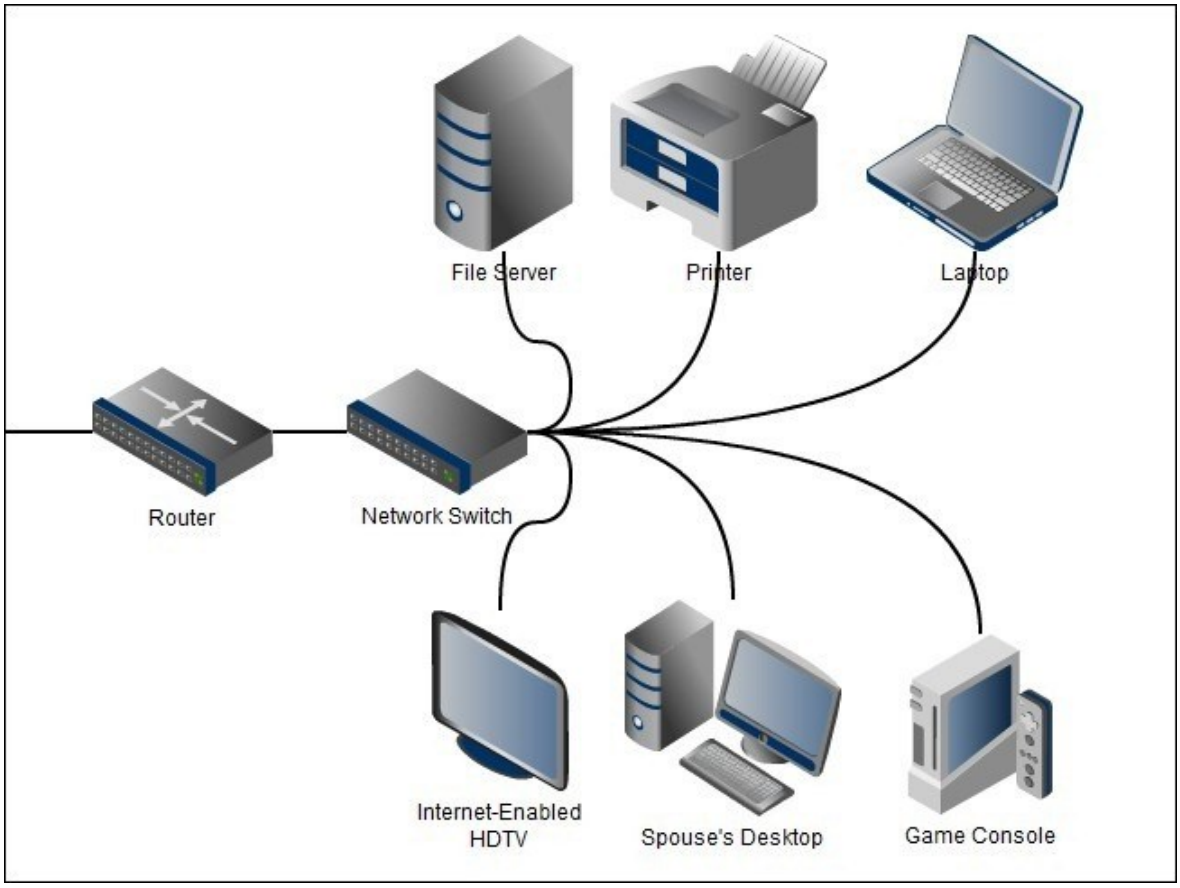


Obrázek 4. Zapojení routeru v síti, zdroj: [7]

1.3.4 Switch

Switch je síťové zařízení, které pracuje na linkové vrstvě modelu OSI. Příjme příchozí datové pakety a přesměruje je na místo určení v síti LAN. Switch v síti LAN založené na ethernetu čte příchozí datové pakety obsahující informace o cíli, když přecházejí do jednoho nebo více vstupních portů. Informace o cíli v paketech se používají k určení, které výstupní porty budou použity k odeslání dat na zamýšlené místo určení.

Přepínače jsou podobné rozbočovačům, pouze chytřejší. Rozbočovač jednoduše spojuje všechny uzly v síti. Komunikace probíhá v podstatě náhodným způsobem s jakýmkoli zařízením, které se snaží kdykoli komunikovat, což vede k mnoha kolizím. Na druhé straně přepínač vytvoří elektronický tunel mezi zdrojovými a cílovými porty na zlomek vteřiny, do kterého nemůže vstoupit žádný jiný provoz. Výsledkem je komunikace bez kolizí. [5] [10]



Obrázek 5. Zapojení switche v síti, zdroj: [7]

1.3.5 Repeater

„Repeatery neboli opakovače se používají k zesílení signálu především u rozsáhlých počítačových sítí, neboť u signálu dochází k útlumu a jeho hodnota klesá. Repeater patří do fyzické vrstvy modelu OSI. Může spojit pouze dva síťové segmenty, a to za předpokladu, že oba používají stejný síťový protokol.“ [9]

1.4 Síťový monitorovací nástroj

Síťový monitorovací nástroj (dále jen NMS) dotazuje síťová zařízení a servery na výkonnostní data pomocí standardních protokolů, jako jsou:

- Simple Network Management Protocol (dále jen SNMP),
- Windows Machine Interface (dále jen WMI),
- Secure Shell pro Unix a Linux server (dále jen SSH).

Dva nejpoužívanější monitorovací protokoly jsou SNMP a WMI. Poskytují síťovým administrátorům tisíce monitorů k posouzení stavu jejich sítí a zařízení v nich. [2] [5] [9]

1.4.1 SNMP

SNMP je standardní protokol, který shromažďuje data z téměř jakéhokoli zařízení připojeného k síti, včetně:

- směrovačů,
- přepínačů,
- bezdrátových LAN kontrolerů,
- bezdrátových přístupových bodů,
- serverů,
- tiskáren a dalších.

SNMP funguje za pomoci dotazu „Objects“. Objekt je něco, o čem NMS shromažďuje informace. Například využití procesoru (dále jen CPU) je objekt SNMP. Dotaz na objekt využití CPU by vrátil hodnotu, kterou NMS používá pro upozornění a hlášení.

Objekty, na které se SNMP dotazuje, jsou udržovány v bázi Management Information Base (dále jen MIB). MIB definuje všechny informace, které jsou vystaveny spravovaným zařízením. Například MIB pro směrovač Cisco bude obsahovat všechny objekty definované společností Cisco, které lze použít ke sledování tohoto směrovače, například využití CPU, využití paměti a stav rozhraní.

Objekty v MIB jsou katalogizovány pomocí standardizovaného systému číslování. Každý objekt má svůj vlastní jedinečný identifikátor objektu.

Některé NMS poskytují prohlížeč MIB. Prohlížeč MIB umožňuje správcům sítě procházet MIB, najít další objekty, které chtějí sledovat na zařízení. [2] [5] [9]

1.4.2 WMI

WMI je protokol používaný pro monitorování serverů a aplikací založených na Windows. WMI je specifické pro Windows a nemonitoruje síťová zařízení nebo servery jiných výrobců.

WMI má velkou knihovnu s tisíci čítačů výkonu. Pomocí protokolu SNMP můžete sledovat na serveru Windows téměř cokoliv.

Negativem WMI je náročnost na zdroje pro NMS, které zpracovávají více výkonu CPU a paměti než SNMP. [2] [5] [9]

2 SROVNÁNÍ DOSTUPNÝCH PROGRAMŮ SÍŤOVÉHO MONITORINGU

Pro potřeby monitoringu počítačových sítí existuje mnoho dostupných open source nástrojů. Mezi nejznámější open source software mimo Nagios patří Zabbix, Icinga, Cacti, OpenNMS a Netdata. V následujících podkapitolách představím jednotlivé z nich.

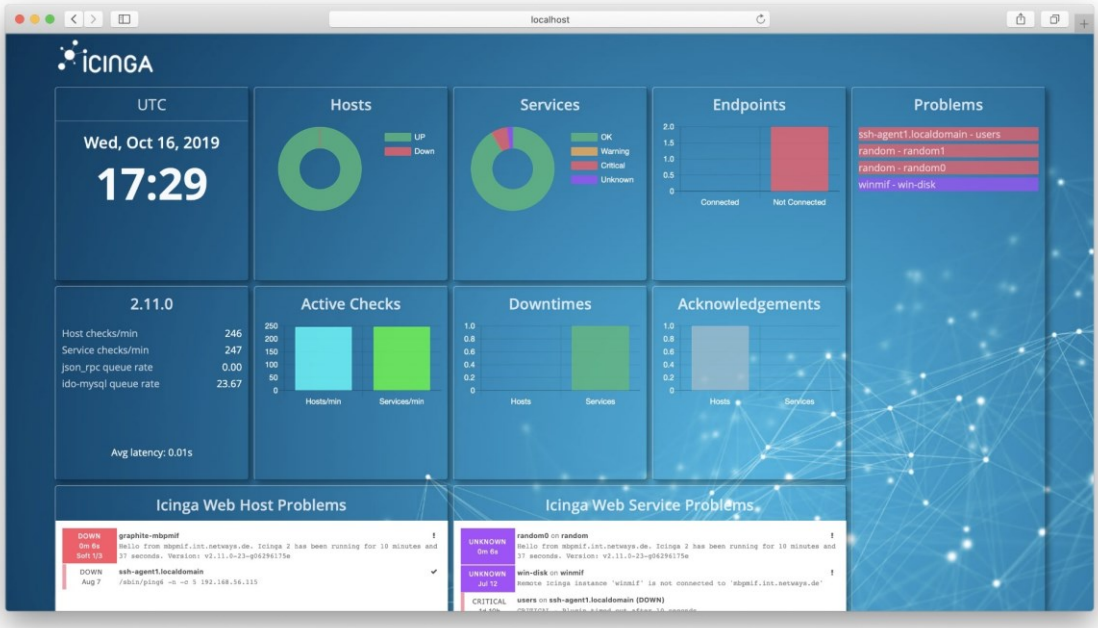
2.1 Zabbix

Zabbix je open source softwarový nástroj pro monitoring počítačových sítí, serverů, virtuálních strojů a cloudových služeb. Zabbix se za pomoci nativních agentů může spouštět na různých podporovaných platformách operačních systémů jako je Linux, Mac OS a Windows. Pomocí těchto nativních agentů shromažďuje ze zařízení data o dostupnosti zařízení, využití procesoru, paměti a dalších. Agent následně tato data předá na server, který tyto informace vizuálně zobrazí ve webovém uživatelském rozhraní. Zabbix umožňuje vlastní nastavení webového rozhraní pomocí přizpůsobitelných dashboardů, které jsou založeny na widgetech, grafech, síťových mapách, prezentacích a zprávách. [11]

Obrázek 6. Zabbix dashboard, zdroj: [12]

2.2 Icinga

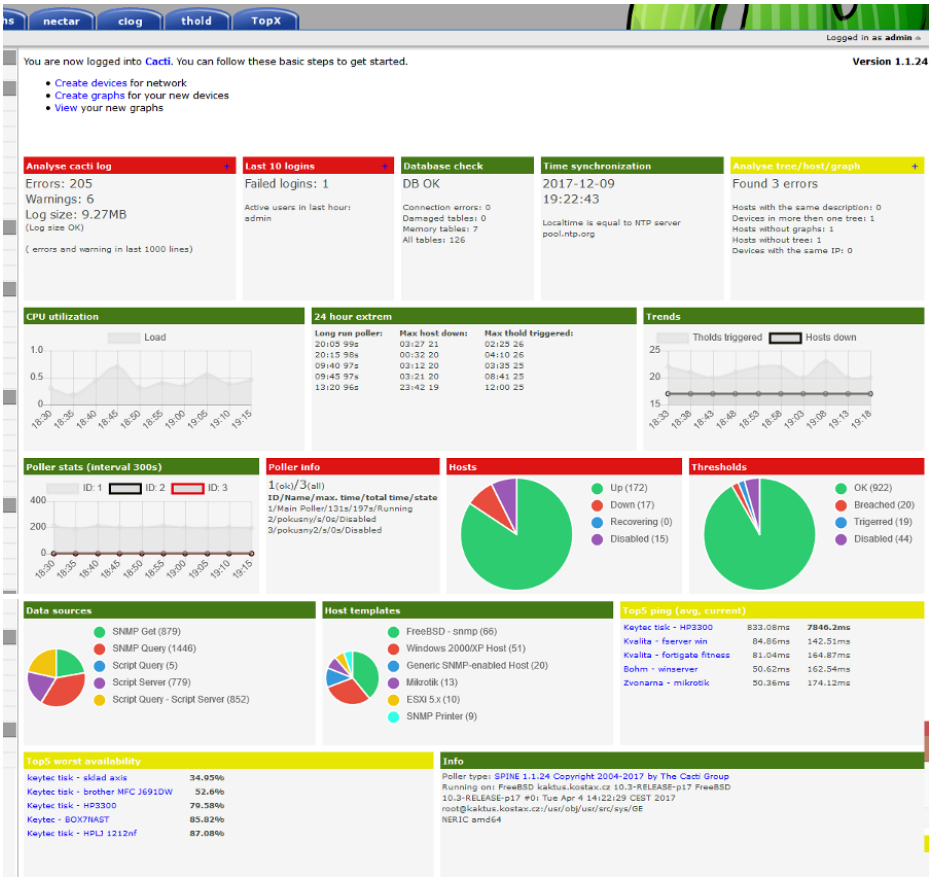
Icinga je open source monitorovací systém, který monitoruje dostupnost síťových prvků a následně upozorňuje uživatele na případné výpadky. Díky škálovatelnosti systému Icinga můžeme monitorovat rozsáhlé a složité síťové infrastruktury. Můžeme sledovat dostupnost hostů a služeb, kde hosty a službami může být cokoliv, co lze dotazovat, jako například HTTP, SMTP, SSH, tiskárny, přepínače, snímače a další. [13]



Obrázek 7. Icinga 3.0.0 dashboard, zdroj: [14]

2.3 Cacti

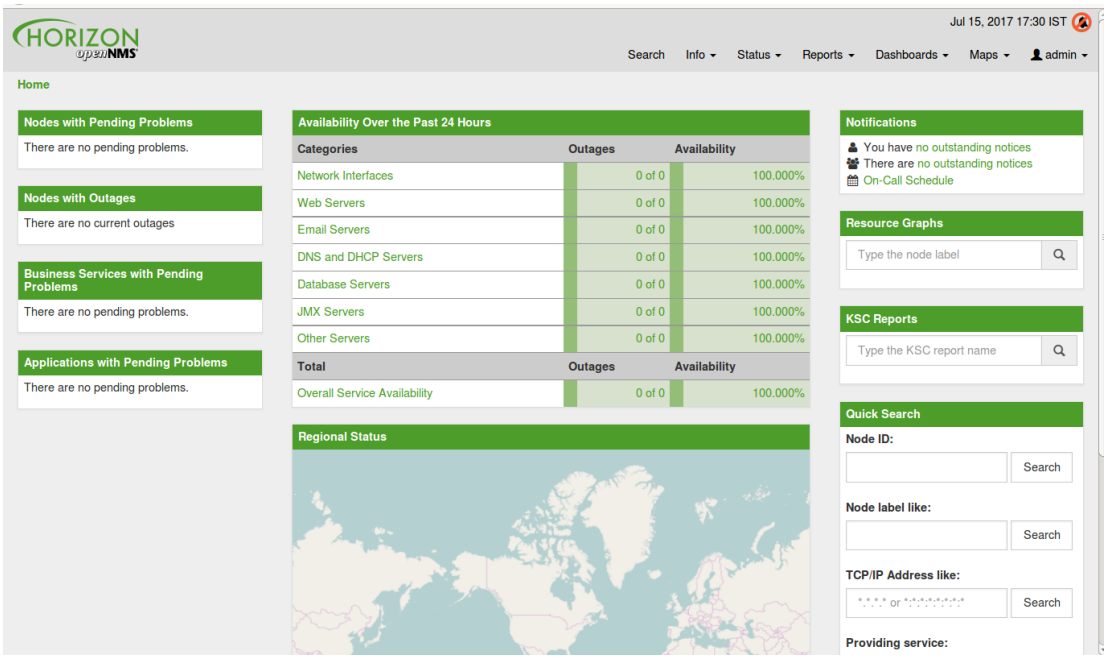
Cacti je open source webový nástroj monitorování počítačových sítí. Jde o kompletní řešení poskytující výkonný poller, vícero metod sběru dat, pokročilé grafy a funkce správy uživatelů. Cacti můžeme využít pro monitoring jak malých lokálních, tak rozlehlých sítí. Je navrženo tak, aby využilo možnosti ukládání dat a grafických funkcí RRDTool. Můžeme pomocí něj měřit dostupnost hostů, služeb, kapacitu jednotek, zatížení procesoru a další. [15]



Obrázek 8. Cacti dashboard, zdroj: [16]

2.4 OpenNMS

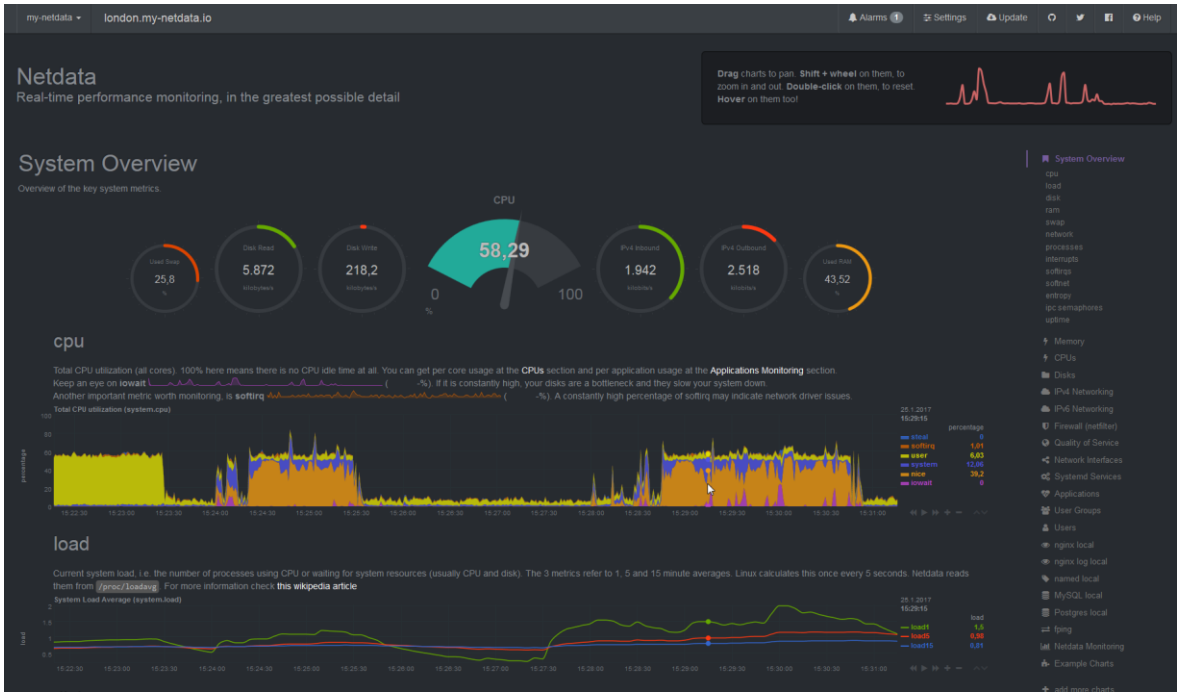
OpenNMS je open source platforma pro monitoring aktivních prvků a služeb počítačových sítí. OpenNMS je velice flexibilní a nabízí velké možnosti škálovatelnosti, díky čemuž je vhodný jak pro monitoring lokálních, ale i velice rozhlehlých sítí. Zjištěné problémy v počítačové síti jsou zobrazovány pomocí přehledných dashboardů. V současné době se skládá ze tří hlavních oblastí, a to monitorování služeb, sběr dat pomocí SNMP, správa událostí a oznámení. [17] [18]



Obrázek 9. OpenNMS dashboard, zdroj: [19]

2.5 Netdata

Netdata je open source systém pro sledování stavu počítačové sítě v reálném čase. Jeho samotná konfigurace je ve srovnání s předchozími zmíněnými velice jednoduchá a již ve výchozím nastavení zobrazuje zajímavé dashboardy s různými statistikami. [20]



Obrázek 10. Netdata dashboard, zdroj: [21]

3 MONITOROVACÍ SYSTÉM NAGIOS

Nagios je open source software, který slouží k automatizovanému monitorování síťové infrastruktury. Umožňuje monitoring všech kritických komponent infrastruktury včetně aplikací a služeb. Historie Nagiosu sahá do roku 1999, kdy byl představen jako NetSaint. V následujících letech byl jeho otevřený zdrojový kód doplněn spoustou přispěvatelů do dnešní podoby. Nyní je vydáván pod obecnou veřejnou licencí pro svobodný software (dále jen GPL). Je podporován všemi platformami jako například Windows, Linux a Unix. Jeho velkou předností je variabilita, kde lze základní řešení rozšířit o další moduly a pluginy. Díky nasazení monitorovacího systému jsou správci počítačových sítí schopni pohotově reagovat na případné výpadky nebo bezpečnostní výstrahy a minimalizovat tak jejich případný dopad na provoz. [22]

Obrázek 11. Logo Nagios, zdroj: [22]

3.1 Základní objekty

Objekty jsou definovány jako flexibilní šablony, které usnadňují konfiguraci a je možné při jejich definici využít dědičnosti vlastností jiných objektů. Nagios pracuje s několika základními objekty:

- zařízení neboli hostitelé (hosts),
- služby (services),
- kontakty (contacts),
- skupiny (groups),
- časové periody (time periods).

[23]

3.1.1 Hostitelé

Hostitelé jsou obvykle fyzická zařízení jako například switche, přístupové body, servery, počítače, disková pole, tiskárny a další. Hostitelé mají k dispozici vždy alespoň jednu nebo případně více služeb. Každý host musí mít svoji IP adresu, přes kterou je pomocí síťového nástroje ping testována jeho dosažitelnost. Při definování hostů využíváme hierarchie za pomoci rodičů, čímž můžeme efektivněji určit případné místo nového problému. Kontrolovaná zařízení se mohou nacházet v jednom ze tří hostitelských stavů:

- UP
    - Zařízení je dostupné.
- DOWN
    - Zařízení je nedostupné a alespoň jeden rodič je dostupný.
- UNREACHABLE
    - Zařízení je nedostupné a není dostupný ani žádný rodič. Nagios se tak nemůže dostat na dotazované zařízení a nedokáže určit, zda žije či nikoliv.

Na základě rozlišování stavů DOWN a UNREACHABLE lze efektivně monitorovat dostupnost sítě a jediným pohledem identifikovat místo, které způsobilo výpadek v síti. [23]

3.1.2 Služby

Služby jsou funkce nebo vlastnosti zařízení, které mají být monitorovány. Na jednom zařízení může být monitorováno i vícero služeb. Sledovat lze vše, u čeho je pomocí softwarových prostředků možné zjistit stav, jako například:

- program běžící na serveru (operační systém, databáze, aplikace),
- síťové služby (SMTP, POP3, HTTP, ICMP, SNMP, FTP, SSJ),
- dostupnost webové stránky,
- vytížení CPU,
- výkon diskového pole,
- stav tiskárny,
- chyby a varování hardwaru,
- protokoly záloh,

- statistika síťových prvků,
- a další…

Mezi službami lze definovat závislost jedné služby na druhé, případně vícero dalších. Závislosti se využívají především při aktivním plánování. Závislosti lze definovat nejen na úrovni jednotlivých služeb, ale i zařízení. Stejně jako hostitelé se můžou také služby nacházet v jednom z následujících stavů:

- OK
    - Vše v pořádku.
- WARNING
    - Výjimka, služba pravděpodobně běží, ale něco je v nepořádku.
- CRITICAL
    - Služba neběží nebo je v kritickém stavu.
- UNKNOWN
    - Test služby neproběhl.

V konfiguraci služeb a stejně tak i zařízení můžeme definovat počet pokusů testu dosažitelnosti. Díky tomu můžou všechny zmíněné stavy být typu:

- SOFT
    - Test selhal, ale ještě neproběhly všechny definované počty pokusů testu dosažitelnosti.
- HARD
    - Stav HARD nastává po vyčerpání všech pokusů testu dosažitelnosti.

[23]

3.1.3 Kontakty

Pomocí objektu kontakty můžeme nadefinovat uživatele, kterým budou doručeny zprávy o změně stavu zařízení. Kontakt může být omezen podmínkami doručení zprávy, jako například časem a vybranými stavy. Kontakty můžeme rozdělit do jednotlivých skupin a zjednodušit tím administraci. Každé zařízení nebo služba musí mít definovaný kontakt nebo skupinu kontaktů. [24]

3.1.4 Skupiny

Všechny základní objekty můžeme rozdělit do jednotlivých skupin. Díky tomu se velice zjednoduší administrace, pokud máme vícero objektů se stejnými vlastnostmi. Například pro všechny tiskárny můžeme vytvořit skupinu „tiskárny“, kde se jednotlivé parametry monitoringu definují přímo pro skupinu. [25]

3.1.5 Časové periody

Definování časových intervalů umožňuje nastavit, kdy budou aktivní jednotlivé aspekty logiky monitorování a varování. Můžeme nastavit například, jak často a ve které dny bude zařízení nebo služba monitorována atd. [26]

3.2 Možnosti monitorování

Nagios nabízí aktivní a pasivní možnosti monitorování.

3.2.1 Aktivní monitorování

Aktivně vyvolává kontrolu zařízení nebo služeb. Definují se frekvence, periody a počty opakování. Nevýhodou aktivního monitorování je, že nedokáže zachytit mikro výpadky. Plán kontrol je možné administrovat pomocí webového rozhraní. [27]

3.2.2 Pasivní monitorování

Při pasivním monitorování Nagios přijme zprávu o stavu zařízení, u které můžeme definovat její čerstvost. Dokáže zachytit i mikro výpadky, pokud je zařízení hlásí. Nagios umožňuje, aby služba byla monitorována zároveň aktivně i pasivně. [28]

3.3 Potvrzování problémů

Nagios umožňuje zadávat potvrzení o převzetí problému. Díky tomu můžeme zefektivnit práci na odstranění nastalého problému mezi více administrátory. Po označení problému jako potvrzený rozešle Nagios zprávu o této skutečnosti a již neposílá zprávy o chybě. Po vyřešení problému je možné rozeslat zprávu o jeho vyřešení. [28]

3.4 Plánované odstávky

V Nagiosu je možné nastavení plánovaných odstávek. Definuje se časové období, ve kterém bude na zařízení nebo službě probíhat údržba. Následně během tohoto období nebudou

zasílány zprávy ani prováděny žádné testy. Nagios rozlišuje chyby během odstávek a během normálního provozu při vytváření reportu o dostupnosti. [29]

3.5 Proaktivní řešení problémů

Nagios umožňuje nadefinovat automatické reakce na události. Takto lze nadefinovat proaktivní řešení problému, kdy po detekci nestandardního stavu je automaticky spuštěna jeho oprava přes event handler. Při konfiguraci automatických reakcí na událost je třeba dát pozor na to, aby automatické opravy nenapáchaly při nestandardních situacích více škody než užitku. [30]

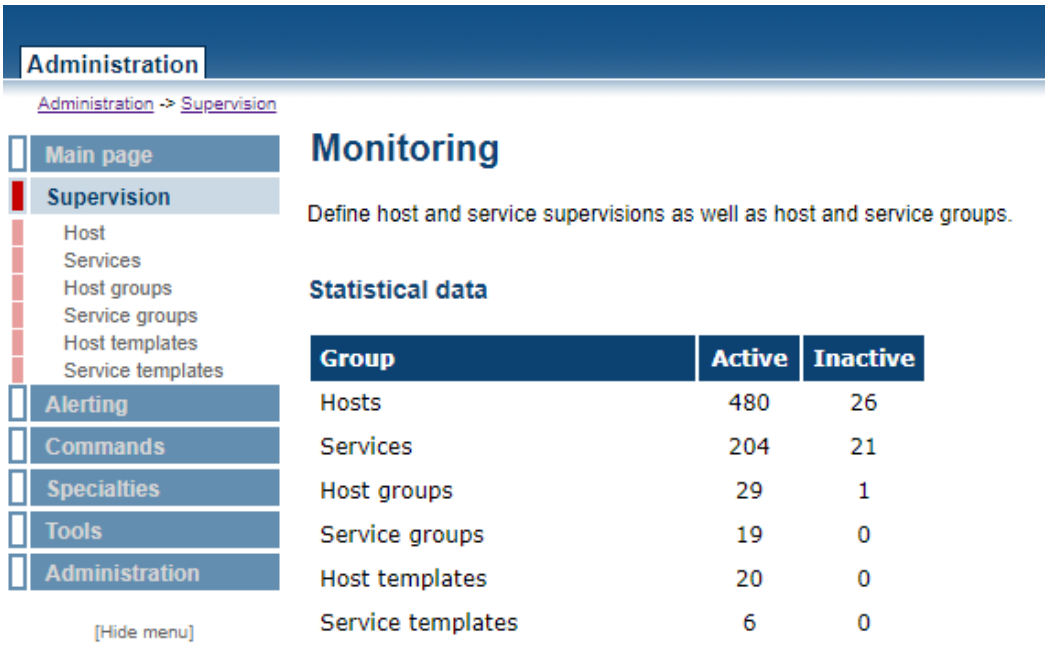
3.6 Reporty

- Tabulka dostupnosti služby a zařízení:
    - Absolutní i procentuální statistika stavů (OK, WARNING, ALERT).
    - Respektuje odstávky a časové periody kontrol.
    - Lze definovat časový rozsah.
- Graf dostupnosti:
    - Na časovém grafu jsou vyznačeny úseky, kdy byla služba nebo zařízení v různých stavech.
    - Lze definovat časový rozsah.
- SLA (Service Level Agreement) reporty:
    - Hromadný generovaný přehled o zařízeních a službách.
    - Může obsahovat tabulky dostupnosti, grafy dostupnosti a grafy s výkonovými parametry.

[31]

3.7 NagiosQL

NagiosQL je webové konfigurační rozhraní určené pro Nagios. Umožňuje velice jednoduchým a přehledným způsobem kompletní konfiguraci prostředí Nagios.



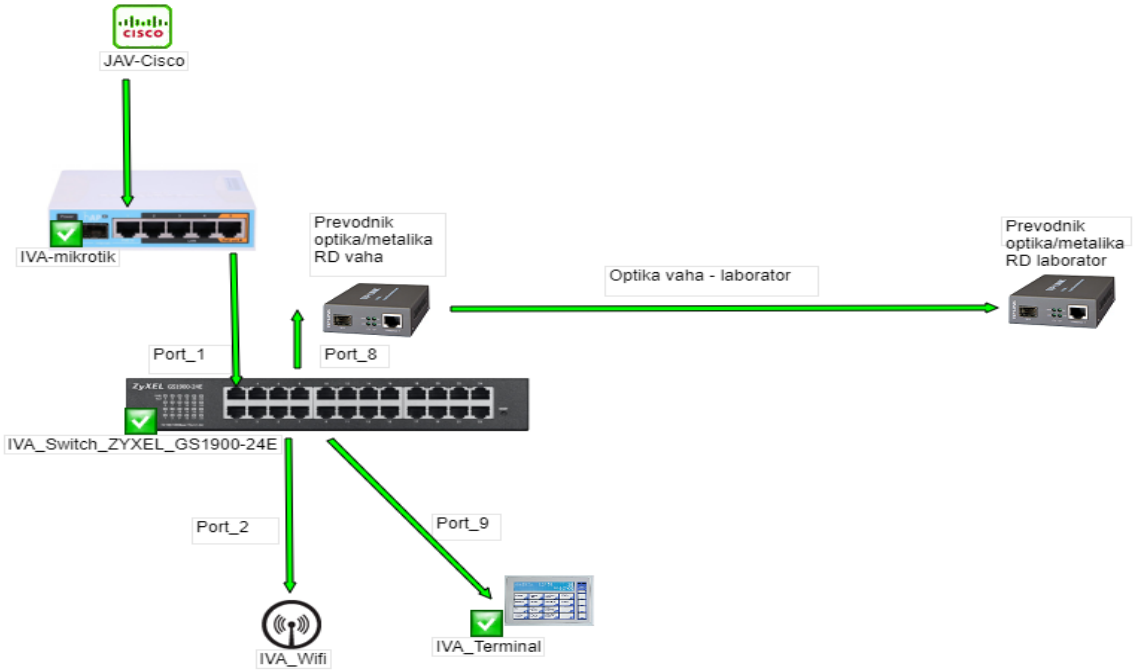
Obrázek 12. NagiosQL, zdroj: autor

3.8 Nagvis

Nagvis je vizualizační doplněk pro Nagios. Využívá se k vizualizaci dat Nagios a síťové infrastruktury. Mezi jeho klíčové vlastnosti patři:

- Zobrazení jednotlivých hostitelů a služeb.
- Zobrazení souhrnných stavů hostitelů a všech jeho služeb.
- Vizualizace kompletních IT procesů pomocí vlastní kresby.
- Online dokumentace IT prostředí včetně aktuálních stavů.
- Vizualizace síťového provozu pomocí linek.

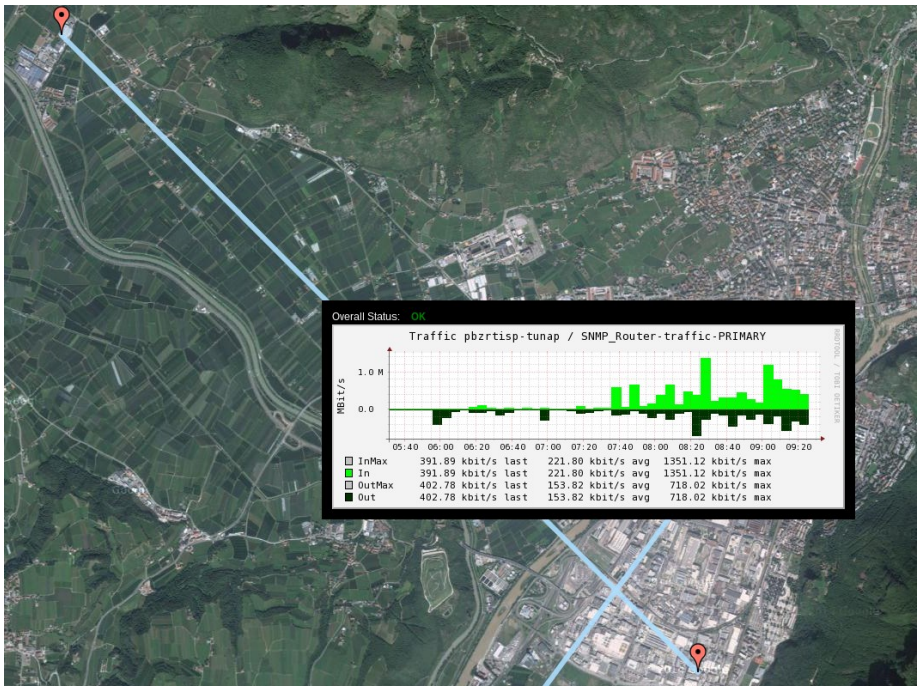
[32]



Obrázek 13. Nagvis, zdroj: autor

3.9 Nagmap

Nagmap je aplikace pro zobrazení topologie rozlehlé firemní sítě pomocí Google Maps Application Programming Interface (dále jen API). Ke zobrazení využívá data získaná z konfiguračních a stavových souborů Nagios.



Obrázek 14. Nagmap, zdroj: [33]

4 MOŽNOSTI A KONFIGURACE SYSTÉMU NAGIOS

Možnosti a konfigurace parametrů prostředí Nagios jsou velice rozsáhlé. V následujících podkapitolách si ukážeme možnosti konfigurace pomocí NagiosQL jednotlivých z nich. Souhrnný přehled konfigurovatelných objektů:

- Host,
- Services,
- Host groups,
- Service groups,
- Host templates,
- Service templates,
- Contact data,
- Contact groups,
- Time periods,
- Contact templates,
- Command definitions.

4.1 Host

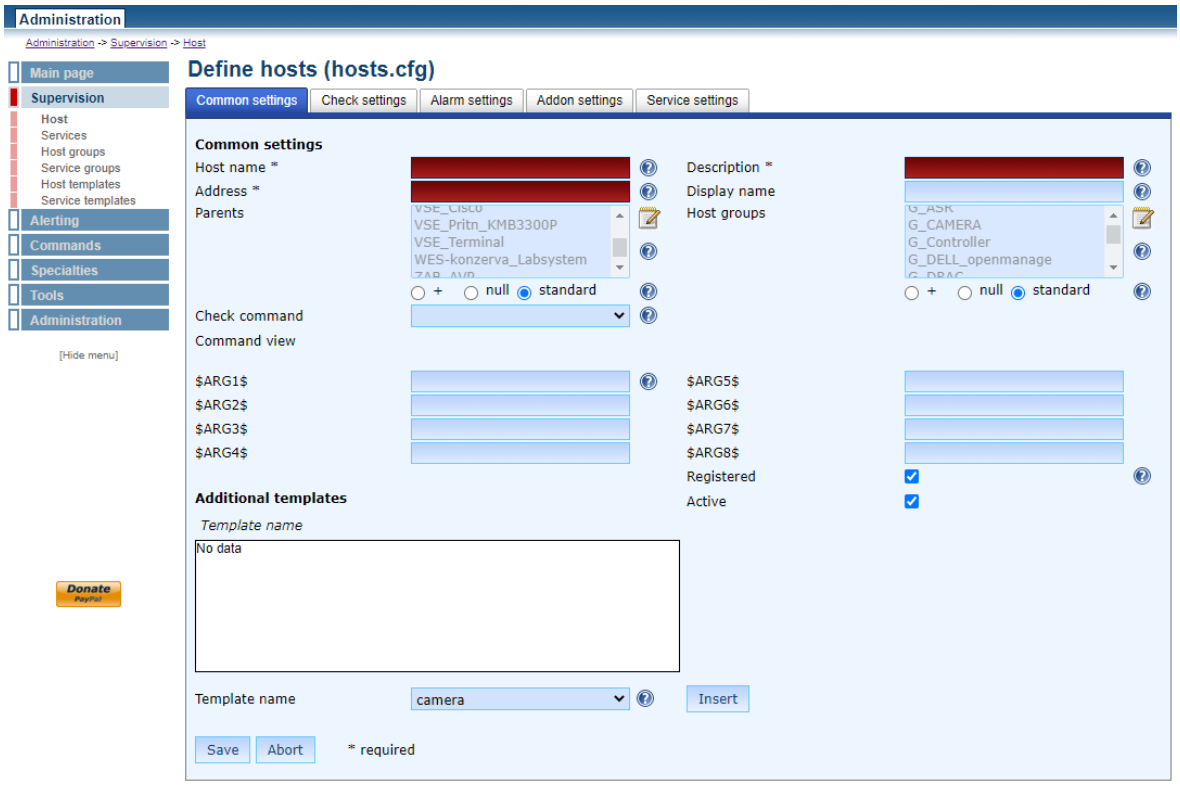
Možnosti konfigurace objektu host se dělí na pět samostatných kategorií, mezi které patří základní nastavení, nastavení kontroly, nastavení oznámení, nastavení doplňků a nastavení služeb.

4.1.1 Základní nastavení

Přehled základních konfigurovatelných parametrů:

- Host name:
    - název zařízení pro Nagios, jeho případná změna se bere jako založení nového zařízení.
- Adress:
    - IP adresa nebo hostname zařízení.

- Description:
    - název zařízení pro uživatele, může být totožný s host name.
- Parents:
    - zařízení (rodiče), přes které stávající zařízení komunikuje v rámci topologie sítě s Nagiosem.
- Host groups:
    - seznam skupin, do kterých zařízení patří.
- Template name:
    - nastavení šablony, od které přebírá předdefinované parametry.

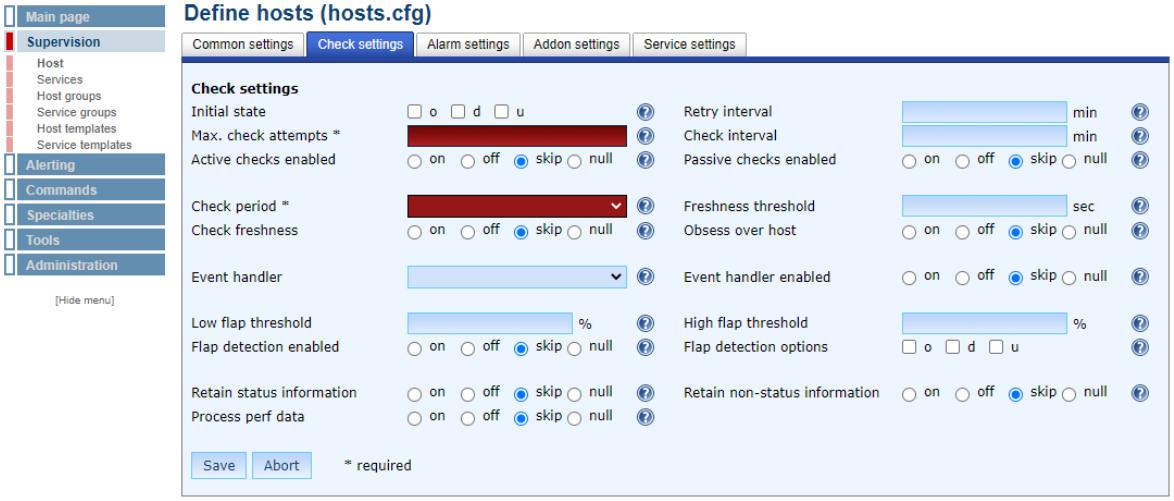


Obrázek 15. Základní nastavení Host, zdroj: autor

4.1.2 Nastavení kontroly

Pomocí nastavení kontroly zařízení definujeme časové periody, kdy má být zařízení testováno. Nastavení testů je možné přeskočit zaškrtnutím volby „skip“, kdy při této volbě bude probíhat test nastavení dle konfigurace přiřazené šablony v základním nastavení. Přehled základních konfigurovatelných parametrů nastavení testů, které se nejčastěji používají:

- Max. checks attempts:
    - počet opakování testu, než nastane HARD stav.
- Active checks enabled:
    - povolení nebo zakázání aktivních kontrol.
- Passive checks enabled:
    - povolení nebo zakázání pasivních kontrol.
- Check period:
    - časové období, kdy se sleduje dostupnost služby. Například 24 hodin denně, časový interval od 7 hodin ráno do 5 hodin odpoledne atd.
- Check freshness:
    - povolení nebo zakázání kontrol čerstvosti u pasivních kontrol.
- Freshness threshold:
    - nastavení časové periody prahu čerstvosti. Například pokud je prahová hodnota pro službu 100, tak Nagios vyhodnotí kontrolu jako neaktuální a vynutí aktivní kontrolu.
- Flap detection enabled:
    - povolení detekce rychlého přepínání stavů.
- Retry interval:
    - prodleva mezi opakováním testu u SOFT stavu.
- Check interval:
    - prodleva mezi testy.



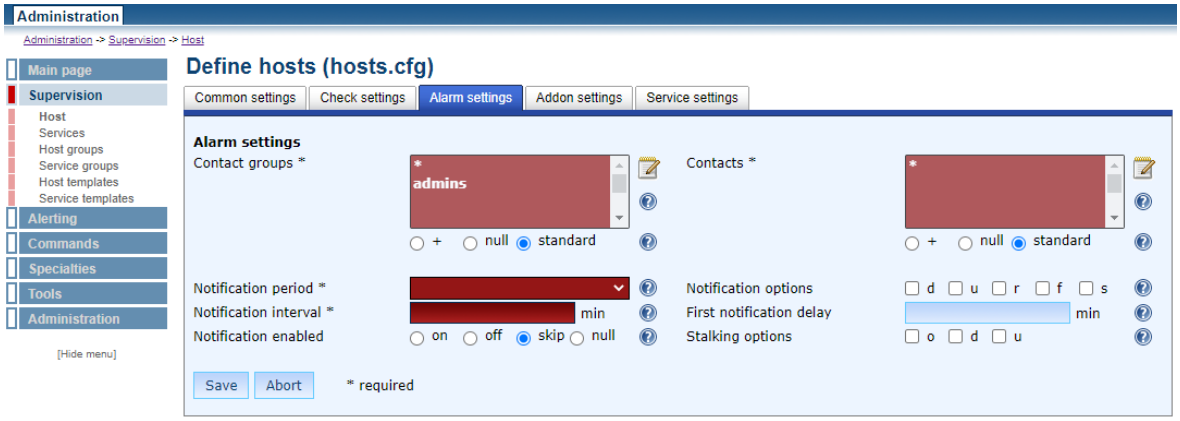
Obrázek 16. Nastavení kontroly Host, zdroj: autor

4.1.3 Nastavení oznámení

Nastavení kontaktní osoby nebo kontaktní skupiny, která má být upozorněna v případě problému. Je možné nastavit notifikační periody a intervaly, kdy mají být oznámení zasílána. Nastavení oznámení je možné přeskočit zaškrtnutím volby „skip“, kdy při této volbě bude probíhat zasílání oznámení dle konfigurace přiřazené šablony v základním nastavení. Přehled základních konfigurovatelných parametrů nastavení oznámení, které se nejčastěji používají:

- Contact groups:
  - seznam skupin kontaktů, na které se mají posílat oznámení.
- Contacts:
  - seznam kontaktů, na které se mají posílat oznámení.
- Notification period:
  - časové období, kdy se posílají oznámení.
- Notification interval:
  - prodleva mezi opakovaným zasíláním oznámení.
- Notification enabled:
  - povolení nebo zakázání oznámení.

- Notification options:
    - seznam stavů, které se posílají:
        - d – DOWN,
        - u – UNREACHABLE,
        - r – RECOVERY (stav UP),
        - f – FLAPPING (hostitel se opakovaně spustí a zastaví),
        - s – odesílá oznámení o zahájení a ukončení výpadku hostitele nebo služby.
- First notification delay:
    - odložení poslání prvního oznámení v minutách.

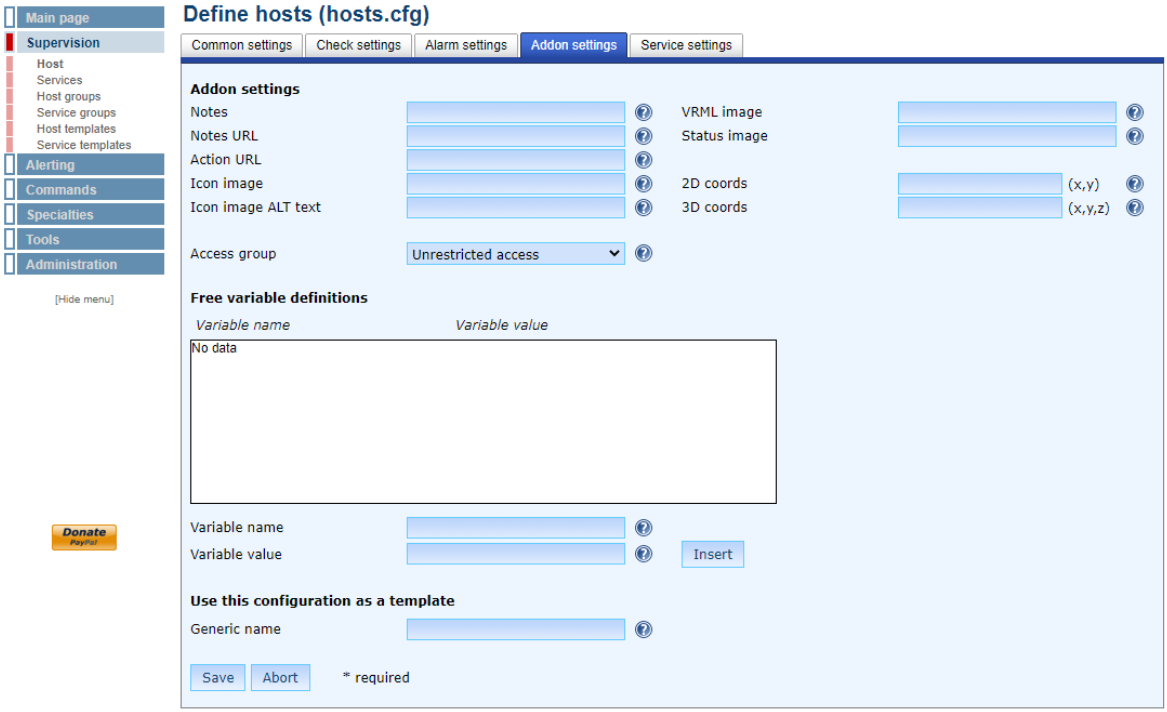


Obrázek 17. Nastavení oznámení Host, zdroj: autor

4.1.4 Nastavení doplňků

Přehled základních konfigurovatelných parametrů nastavení doplňků, které se nejčastěji používají:

- Notes:
  - textová poznámka.
- Notes URL (Uniform Resource Locator):
  - URL poznámka.
- Action URL:
  - další URL k zařízení.
- Icon image:
  - ikona zařízení, která bude použita v Nagmap.
- Icon image ALT text:
  - alternativní název k ikoně.
- Status image:
  - ikona zařízení ve status mapě.

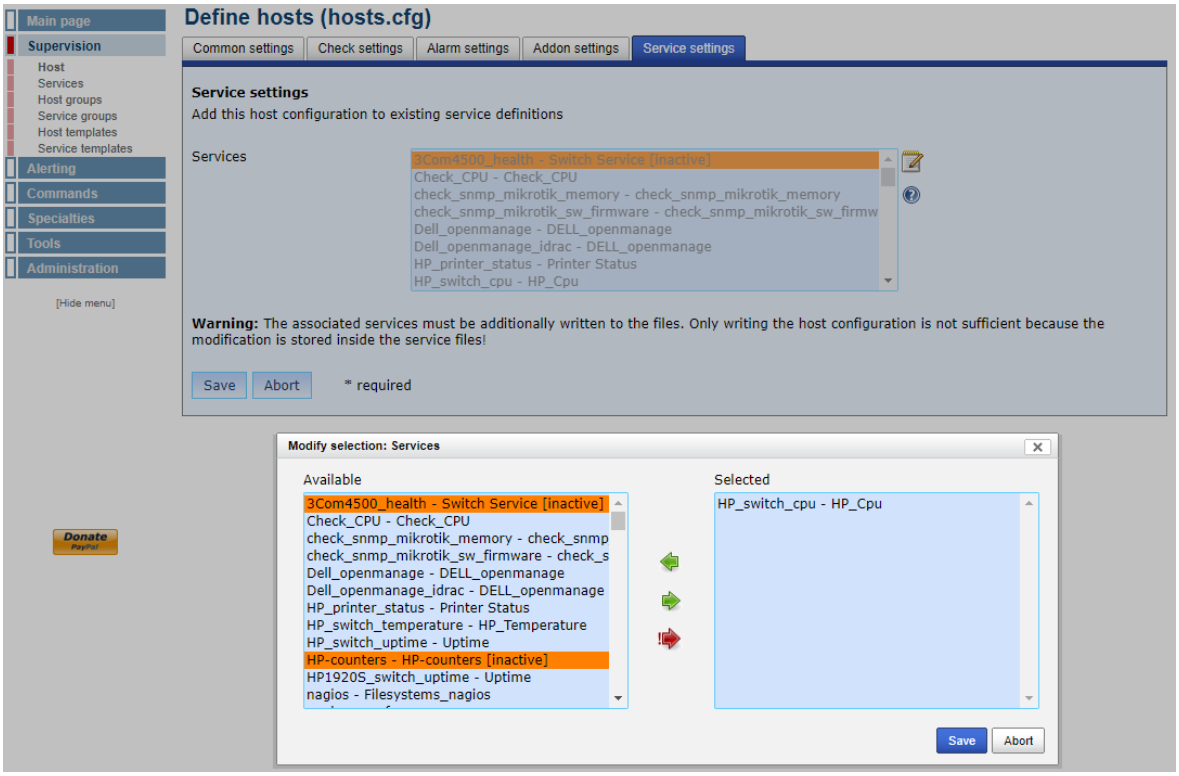


Obrázek 18. Nastavení doplňků Host, zdroj: autor

4.1.5 Nastavení služeb

Přehled základních konfigurovatelných parametrů nastavení služeb, které se nejčastěji používají:

- Services:
    - nastavení služeb, které mají být na zařízení spouštěny.



Obrázek 19. Nastavení služeb Host, zdroj: autor

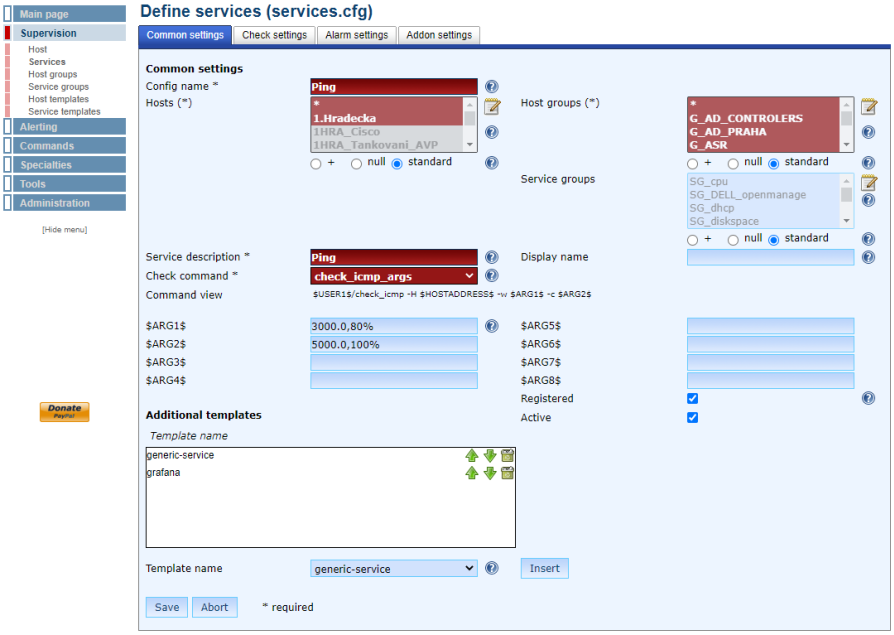
4.2 Services

Možnosti konfigurace objektu services se dělí na čtyři samostatné kategorie, mezi které patří základní nastavení, nastavení kontroly, nastavení oznámení a nastavení doplňků.

4.2.1 Základní nastavení

- Config name:
    - název služby.
- Hosts:
    - nastavení hostů, na kterých má být služba spouštěna.

- Host groups:
    - nastavení skupin, na kterých má být služba spuštěna.
- Template name:
    - nastavení šablony, od které přebírá definované parametry.
- Service description:
    - popis služby.
- Check command:
    - nastavení příkazů, které kontrolují dostupnost zařízení.



Obrázek 20. Základní nastavení Services, zdroj: autor

4.2.2 Nastavení kontroly

Pro nastavení kontroly platí totožná pravidla jako v případě objektu Host, více v kapitole 4.1.2.

4.2.3 Nastavení oznámení

Pro nastavení oznámení platí totožná pravidla jako v případě objektu Host, více v kapitole 4.1.3.

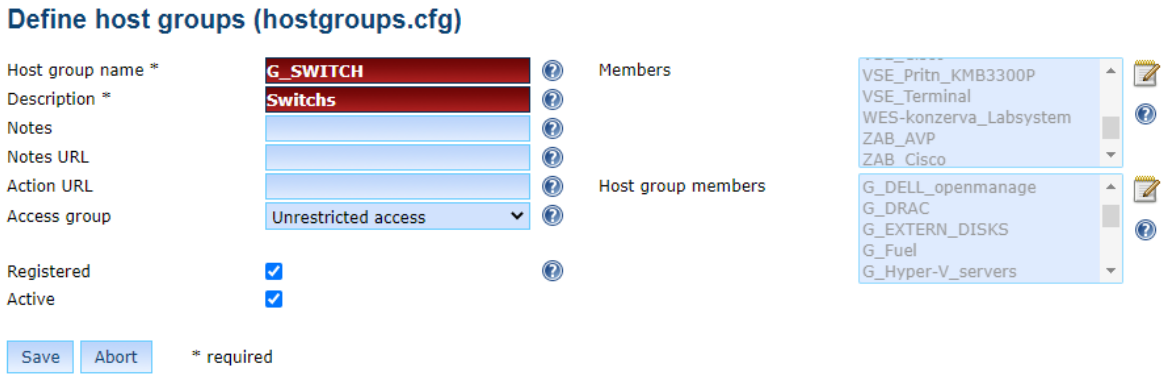
4.2.4 Nastavení doplňků

Pro nastavení oznámení platí totožná pravidla jako v případě objektu Host, více v kapitole 4.1.4.

4.3 Host a Service groups

Pro konfiguraci host groups a service groups platí totožná pravidla. Groups slouží k seskupení zařízení se stejnými vlastnostmi, například switche. Přehled základních konfigurovatelných parametrů skupin:

- Host group name:
  - definování názvu, který je použit k identifikaci skupiny.
- Description:
  - alternativní název skupiny, slouží pro snadnější identifikaci.
- Notes:
  - textová poznámka.
- Notes URL:
  - URL odkaz, který lze použít pro získání více informací o skupině.
- Action URL:
  - další URL odkaz.
- Members:
  - seznam zařízení oddělený čárkou.
- Host group members:
  - seznam skupin zařízení oddělený čárkou.



Obrázek 21. Konfigurace skupin, zdroj: autor

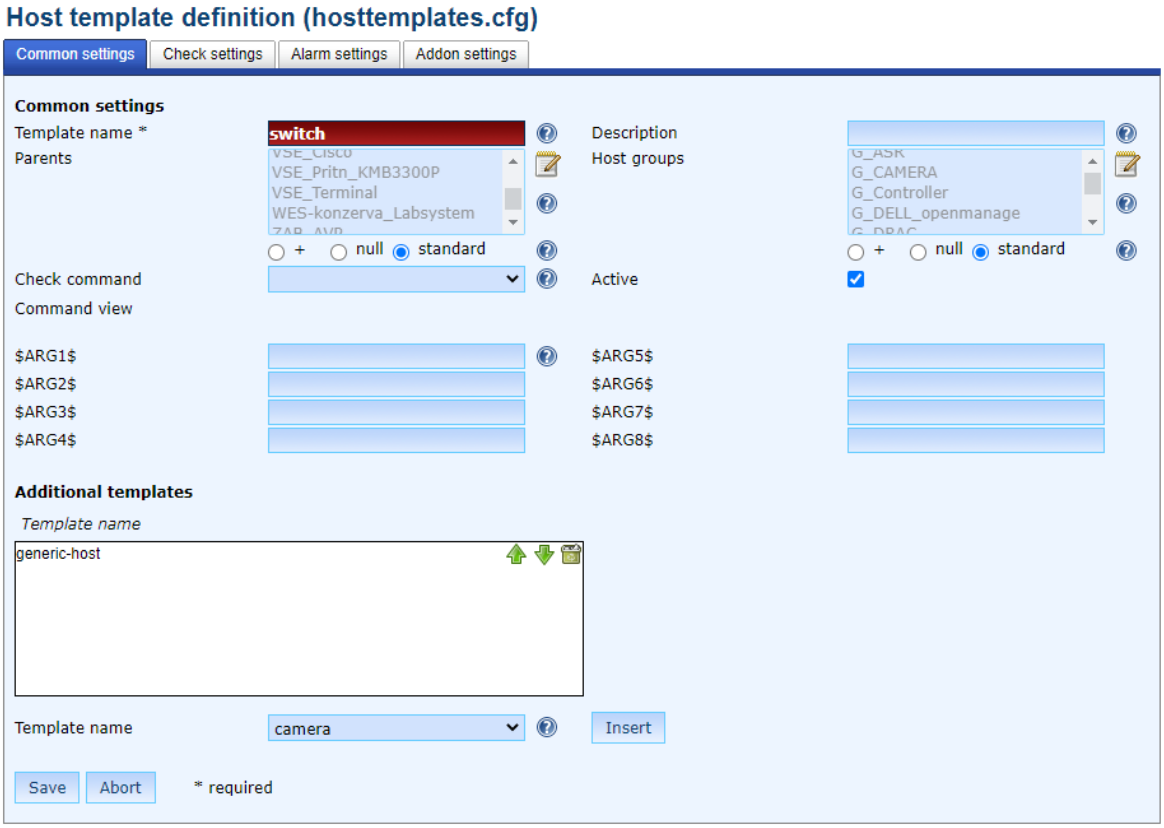
4.4 Host a Service templates

Pro konfiguraci host a service templates (šablon) platí totožná pravidla. Šablony slouží k definici vícero parametrů, jako je nastavení kontroly a nastavení oznámení. Šablonu je pak možné vždy přiřadit k danému zařízení, které se řídí nastavenými pravidly. Díky tomu odpadá nutnost definovat u každého zařízení jednotlivé parametry individuálně a stačí pouze přiřadit vhodnou šablonu. Možnosti konfigurace se dělí na čtyři samostatné kategorie, mezi které patří základní nastavení, nastavení kontroly, nastavení oznámení a nastavení doplňků.

4.4.1 Základní nastavení

Přehled základních konfigurovatelných parametrů šablon:

- Template name:
  - definování názvu, který je použit k identifikaci šablony.
- Description:
  - alternativní název šablony, který slouží pro snadnější identifikaci.
- Host groups:
  - nastavení skupin, na kterých má být šablona aplikována.
- Additional templates – template name:
  - nastavení nadřazené šablony, od které přebírá definované parametry.



Obrázek 22. Základní nastavení šablony, zdroj: autor

4.4.2 Nastavení kontroly, oznámení a doplňků

Nastavení kontroly, oznámení a doplňků je totožné jako u objektu Host, více v kapitole 4.1.

4.5 Contact data

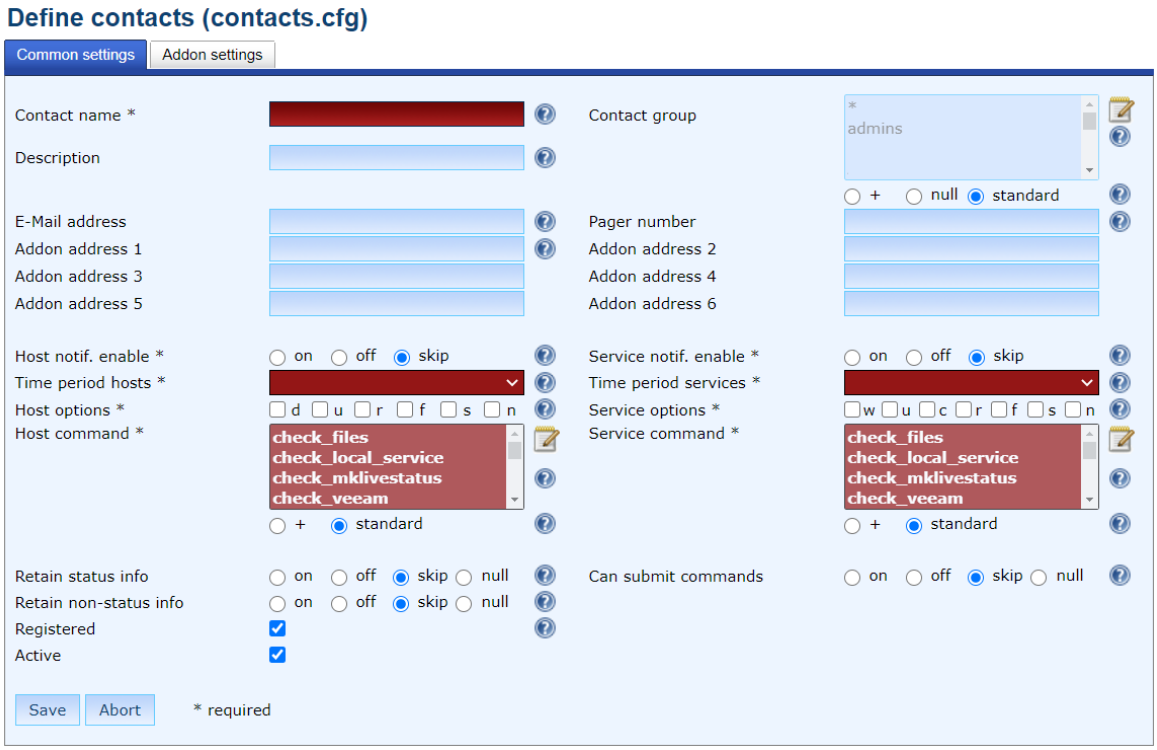
Objekt kontaktní údaje slouží pro definici parametrů zasílání oznámení a nastavení přístupu. Možnosti konfigurace se dělí na dvě samostatné kategorie, mezi které patří základní nastavení a nastavení doplňků.

4.5.1 Základní nastavení kontaktu

Přehled základních konfigurovatelných parametrů:

- Contact name:
    - definování názvu, který je použit k identifikaci kontaktu.
- Description:
    - alternativní název kontaktu, který slouží pro snadnější identifikaci. Může být stejný jako contact name.

- Contact group:
    - seznam skupin kontaktů, do které daný kontakt patří.
- E-mail adress:
    - emailová adresa, na kterou budou zasílána upozornění.
- Host notifications enabled:
    - nastavení, zda kontakt bude dostávat upozornění ze zařízení.
- Service notifications enabled:
    - nastavení, zda kontakt bude dostávat upozornění ze služeb.
- Host notification period:
    - časové období, kdy má kontakt dostávat upozornění ze zařízení.
- Service notification period:
    - časové období, kdy má kontakt dostávat upozornění ze služeb.
- Host notification options:
    - seznam stavů, které se mají posílat ze zařízení:
        - d – stav DOWN
        - u – stav UNREACHABLE
        - r – stav obnovení hostitele UP
        - f – stav FLAPPING (hostitel se opakovaně spustí a zastaví)
        - s – stav zahájení a ukončení plánovaného výpadku
- Service notification options:
    - seznam stavů, které se mají posílat ze služeb, parametry totožné jako v případě hostitele.
- Host command a service command:
    - název příkazu pro zasílání oznámení z hostitelů a služeb.



Obrázek 23. Základní nastavení kontaktu. zdroj: autor

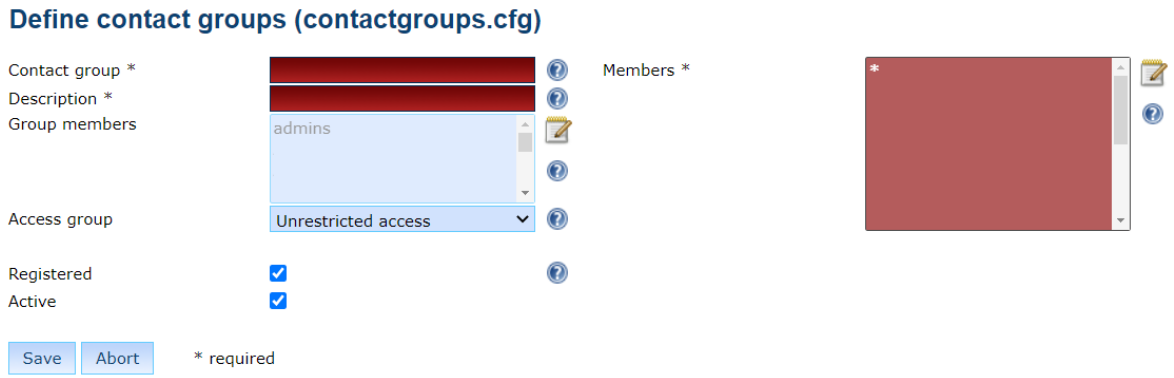
4.5.2 Nastavení doplňků kontaktu

Nastavení doplňků kontaktu je totožné jako v případě hostitele, více v kapitole 4.1.4.

4.6 Contact groups

Contact groups slouží k seskupení kontaktů se stejnými vlastnostmi, například správci sítě. Přehled základních konfigurovatelných parametrů kontaktních skupin:

- Contact group:
  - definování názvu, který je použit k identifikaci skupiny.
- Description:
  - alternativní název skupiny, který slouží pro snadnější identifikaci. Může být stejný jako contact groups.
- Members:
  - seznam kontaktů ve skupině.
- Group members:
  - seznam skupin kontaktů ve skupině.

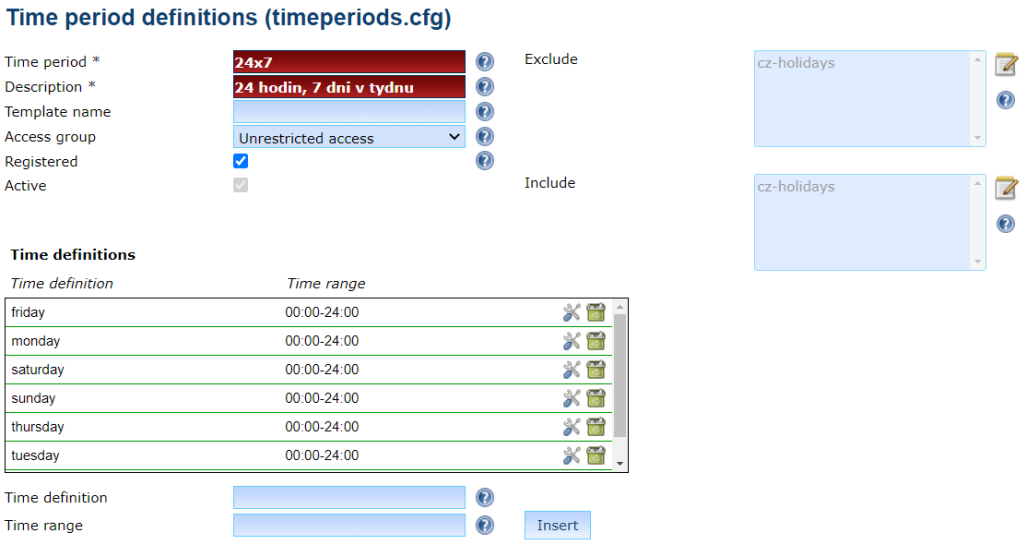


Obrázek 24. Konfigurace kontaktních skupin, zdroj: autor

4.7 Time periods

Objekt time periods obsahuje definici časových period, které se používají pro filtraci oznámení, časů testování apod. Přehled základních konfigurovatelných parametrů časových period:

- Time period:
  - definování názvu, který je použit k identifikaci časové periody.
- Description:
  - alternativní název časové periody, který slouží pro snadnější identifikaci.
- Template name:
  - nastavení šablony, od které přebírá definované parametry.
- Exclude a include:
  - dny a časy vyjmuté a vložené z periody.
- Time definition:
  - definice dnů v týdnu, pondělí až neděle.
- Time rande:
  - definice časového rozsahu v 24 hodinovém formátu HH:MM:SS.



Obrázek 25. Definice časových period, zdroj: autor

4.8 Contact templates

Šablony kontaktů slouží k definici vícero parametrů, jako je nastavení kontroly a nastavení oznámení. Šablonu je pak možné přiřadit k danému kontaktu, který se řídí nastavenými pravidly. Díky tomu odpadá nutnost definovat u každého zařízení jednotlivé parametry individuálně a stačí pouze přiřadit vhodnou šablonu. Možnosti konfigurace jsou totožné jako v kapitole 4.5.1.

II. PRAKTICKÁ ČÁST

5 KONFIGURACE A TESTOVÁNÍ SYSTÉMU NAGIOS

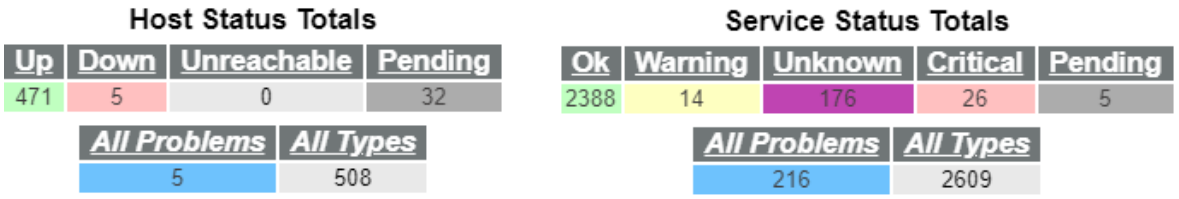
V praktické části bakalářské práce jsem se zaměřil na konfiguraci monitorovacího systému Nagios v praxi. Pro implementaci systému jsem si vybral společnost, která se zabývá obchodní činností v oblasti zemědělských komodit, průmyslových hnojiv a pohonných hmot. U dané společnosti pracuji na pozici IT specialisty, díky čemuž mám neomezený přístup k síťové infrastruktuře. Společnost se skládá z více než 60 samostatných středisek, která jsou rozmístěna po území České republiky. Disponuje tedy velice rozsáhlou počítačovou sítí, která čítá stovky aktivních prvků a pracovních stanic. Právě díky svojí velikosti nastala potřeba nasazení monitorovacího systému, který zvýší přehlednost a umožní rychleji reagovat na případné problémy. Všechna střediska jsou propojena pomocí multiprotokolového přepojování podle návěstí (dále jen MPLS) od společnosti O2. Díky tomu spolu můžou všechna zařízení komunikovat, jako by byla v jedné síti. V rámci MPLS má každé středisko svoji vlastní podsíť s daným rozsahem.

5.1 Požadavky na monitoring

Před realizací si bylo potřeba nejdříve říci, která zařízení budou monitorována. Po úvaze, která zařízení jsou pro bezproblémový chod společnosti klíčová a která nikoliv, vypadl následující model. Budou monitorovány následující skupiny zařízení, mezi které patří servery, drac karty, routery, switche, controllery, docházkové systémy, kamerové systémy (dále jen CCTV), poplachové zabezpečovací a tísňové systémy (dále jen PZTS), tankomaty, výrobní technologie a velké multifunkční tiskárny. Z monitoringu budou vyřazeny veškeré pracovní stanice a malé tiskárny v jednotlivých kancelářích. Tato zařízení nejsou pro provoz společnosti důležitá. Dalším problémem bylo určit v jakých časových periodách budou zařízení monitorována. Zde nastává problém s nepravidelnou pracovní dobou, která zahrnuje i občasný, nečekaně nahodilý nepřetržitý provoz. Díky této skutečnosti jsem se rozhodl, že budou všechna zařízení monitorována nepřetržitě, pokud nebude uvedeno jinak. Další otázkou je, jaké parametry u jednotlivých zařízení monitorovat. Zde byla odpověď jednoduchá, u všech zařízení je prioritní jejich dostupnost. Případné další monitorované parametry jednotlivých zařízení budou specifikovány při jejich konfiguraci.

5.2 Analýza počítačové sítě

V prvním kroku při realizaci, jsem musel provést detailní analýzu počítačové sítě. Tato část byla velice časově náročná. Nejprve bylo nutné rozsahy jednotlivých podsítí oskenovat. K tomuto účelu jsem využil bezplatný nástroj Advanced IP Scanner. Dále bylo nutné všechna střediska osobně navštívit a fyzicky se přesvědčit, zda sken zachytil všechna zařízení připojená do sítě a ujasnit si topologii síťové infrastruktury jednotlivých středisek. Po kompletní analýze počítačové sítě jsem do monitoringu zařadil celkem 508 zařízení, na kterých běží 2609 služeb.



Obrázek 26. Přehled hostů a služeb, zdroj: autor

Pro konkrétní ukázku jsem si vybral středisko Kroměříž. Stejným způsobem jako středisko Kroměříž jsem analyzoval i všechna ostatní. Středisko v Kroměříži se skládá z několika samostatně stojících budov uvnitř rozlehlého areálu. Středisko, stejně tak jako ostatní, je k internetu a MPLS připojeno pomocí Cisco routeru od O2. Zařízení, u kterých je vyžadován monitoring, jsou soustředěna do budov A, B, C a D. Jednotlivé budovy jsou mezi sebou propojeny pomocí optických kabelů. Optické kabely jsou zakončeny v optických vanách, které jsou umístěny uvnitř uzamykatelných rack skříní. Vany jsou dále pomocí optických patch cordů propojeny s optickými převodníky a ty následně s aktivními prvky. Část optických převodníků je v podobě Small Form-factor Pluggable (dále jen SFP) modulů a část v podobě starších typů média konvertorů. Zde vidím problém v rámci monitoringu. Ani jeden ze zmíněných optických převodníků nemá svoji IP adresu, a tak není možné kontrolovat jejich dostupnost. SFP moduly a média konvertory jsou zapojeny do pokročilých inteligentně řízených přepínačů Hewlett-Packard (dále jen HP). Díky tomuto faktu jsem našel řešení zmíněného problému. Tyto přepínače HP umožňují monitoring jednotlivých portů. Stačí znát čísla portů, do kterých jsou převodníky připojeny, a pomocí nich můžu monitorovat jejich dostupnost. Celý areál je monitorován a střežen za pomoci CCTV a PZTS. CCTV se skládá ze systematicky rozmístěných kamer a záznamového síťového videorekordéru (dále jen NVR). Součástí PZTS je ústředna, pasivní infračervená čidla (dále

jen PIR) a ovládací panel. PZTS a CCTV je napojeno na pult centralizované ochrany (dále jen PCO) bezpečnostní agentury. V budově A se nachází serverovna s rack skříní o výšce 42U. Rack je osazen následujícím HW:

- patch panel s 24 porty 4 ks,
- switch HP s 48 porty 3ks,
- cisco router,
- routerboard MikroTik,
- datové uložiště Synology,
- zdroj nepřerušovaného napájení (dále jen UPS),
- přídavná baterie UPS
- lan controller,
- server Dell 3 ks,
- CCTV,
- PZTS.

Na všech poschodích budovy A je umístěna velká multifunkční tiskárna. Dále ovládací panel PZTS a Wi-Fi router.

V budově B se nachází následující HW:

- docházkový terminál,
- switch,
- PZTS,
- CCTV.

V budově C se nachází následující HW:

- velká multifunkční tiskárna,
- switch 2ks,
- Wi-Fi router.

V budově D se nachází následující zařízení:

- řídící počítač technologie,
- řídící systém automatizace Siemens,
- automatizace,
- switch.

U budovy D jsem při analýze sítě narazil na problém. Na budově D běží výrobní technologie a není připojena k internetu pomocí O2, ale přes místního poskytovatele internetového připojení. Toto nastavení je zavedeno z bezpečnostních důvodů. Výroba musí mít přístup k internetu, ale zároveň nesmí být součástí provozního subnetu. To znamená, že není v MPLS a znemožňuje monitoring. Přemýšlel jsem, jak tento problém vyřešit, a nabídly se dvě možnosti. Buďto se připojovat ke stávající síti pomocí VPN nebo vytvořit novou síť pod O2. Z důvodu dobré zkušenosti s O2 a s nabídkou vytvoření podsítě zdarma v rámci poskytovaných služeb, jsem se rozhodl právě pro tuto variantu. U O2 jsem nechal vytvořit novou podsíť, která je součástí MPLS. Dále jsem ji nechal nakonfigurovat na druhý port Cisco routeru, kde na prvním portu běží stávající podsíť. Následně jsem provedl konfiguraci aktivních prvků a přepojil kabely z routeru místního providera do druhého portu Cisco routeru O2. Tímto krokem jsem připojil budovu D k MPLS na vlastním rozsahu a umožnil tak monitoring.

5.2.1 Podrobný seznam zařízení

Po detailní analýze počítačové sítě jsem definoval 508 zařízení. Z těchto 508 zařízení se 43 nachází na středisku Kroměříž. Každé zařízení jsem pojmenoval následujícím způsobem. Pokud se jedná o výrobní zařízení, je na první místě prefix ASR. Zkratka pro středisko, která je v tomto případě KMC. Skupina zařízení a případně další upřesňující popis. Pro příklad uvedu switch, který je umístěn na budově D. Jelikož se jedná o zařízení ve výrobě, bude název obsahovat prefix a jeho výsledná podoba bude ASR_KMC_Switch. Tento způsob pojmenování jsem zvolil z důvodu přehlednosti. Takto je na první pohled jasné, o jaké zařízení se jedná. V následující tabulce je uveden kompletní seznam monitorovaných zařízení na středisku Kroměříž a jejich popis.

Název zařízení:	**Popis:**
ASR_KMC_0MXL	Automatizace Siemens Simatic budova D
ASR_KMC_0MXP	Automatizace Siemens Simatic budova D
ASR_KMC_0MXS	Automatizace Siemens Simatic budova D
ASR_KMC_11MX	Automatizace Siemens Simatic budova D
ASR_KMC_12MXL	Automatizace Siemens Simatic budova D
ASR_KMC_12MXP	Automatizace Siemens Simatic budova D
ASR_KMC_12MXS	Automatizace Siemens Simatic budova D
ASR_KMC_13MX	Automatizace Siemens Simatic budova D
ASR_KMC_1MX	Automatizace Siemens Simatic budova D
ASR_KMC_3MX	Automatizace Siemens Simatic budova D
ASR_KMC_4MX	Automatizace Siemens Simatic budova D
ASR_KMC_6MX	Automatizace Siemens Simatic budova D
ASR_KMC_7MX	Automatizace Siemens Simatic budova D
ASR_KMC_8MX	Automatizace Siemens Simatic budova D
ASR_KMC_Cisco	Automatizace Siemens Simatic budova D
ASR_KMC_Dell_7070	Automatizace Siemens Simatic budova D
ASR_KMC_IN	Automatizace Siemens Simatic budova D
ASR_KMC_OUT	Automatizace Siemens Simatic budova D
ASR_KMC_Simatic_S7-1500	Automatizace Siemens Simatic budova D
ASR_KMC_Switch	Přepínač budova D
KMC_AGT_Switch_HP1910-8G	Přepínač budova C
KMC_AGT_Switch_HPE1920S-48G	Přepínač budova C
KMC_Cisco	Router O2
KMC_Controller_NXC2500	Lan Controller
KMC_Drac_Backup	Drac karta
KMC_ExtDisk_Synology	Externí disk Synology
KMC_iDRAC-NODE1	Drac karta serveru NODE1
KMC_iDRAC-NODE2	Drac karta serveru NODE2
KMC_MikroTik	Mikrotik
KMC_Switch_1	Přepínač budova A
KMC_Switch_2	Přepínač budova A
KMC_Switch_3	Přepínač budova A
KMC_Switch_Laborator	Přepínač budova B
KMC_Switch_SG200-18	Přepínač SFP budova A
KMC_Switch_SG300-10SFP	Přepínač SFP budova A
KMC_Synology	Externí disk Synology
KMC_Terminal	Docházkový terminál
KMC_Wifi_KMCWIFI	Wifi router budova A
KMC_Wifi_KMCWIFIAGT	Wifi router budova C
KMC_Wifi_KMCWIFIKLUB	Wifi router budova B
KMC_CCVT	Kamerový systém
KMC_NODE1	Server
KMC_NODE2	Server

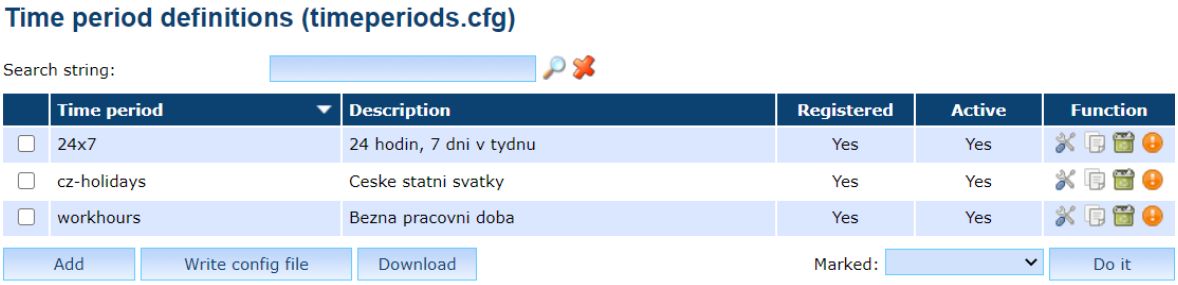
Tabulka 1. Seznam zařízení středisko Kroměříž, zdroj: autor

5.3 Konfigurace systému Nagios

Pomocí analýzy počítačové sítě jsem si udělal detailní přehled o síťové infrastruktuře společnosti. Dále jsem provedl konfiguraci jednotlivých hostitelů, služeb, skupin, časových period a dalších parametrů.

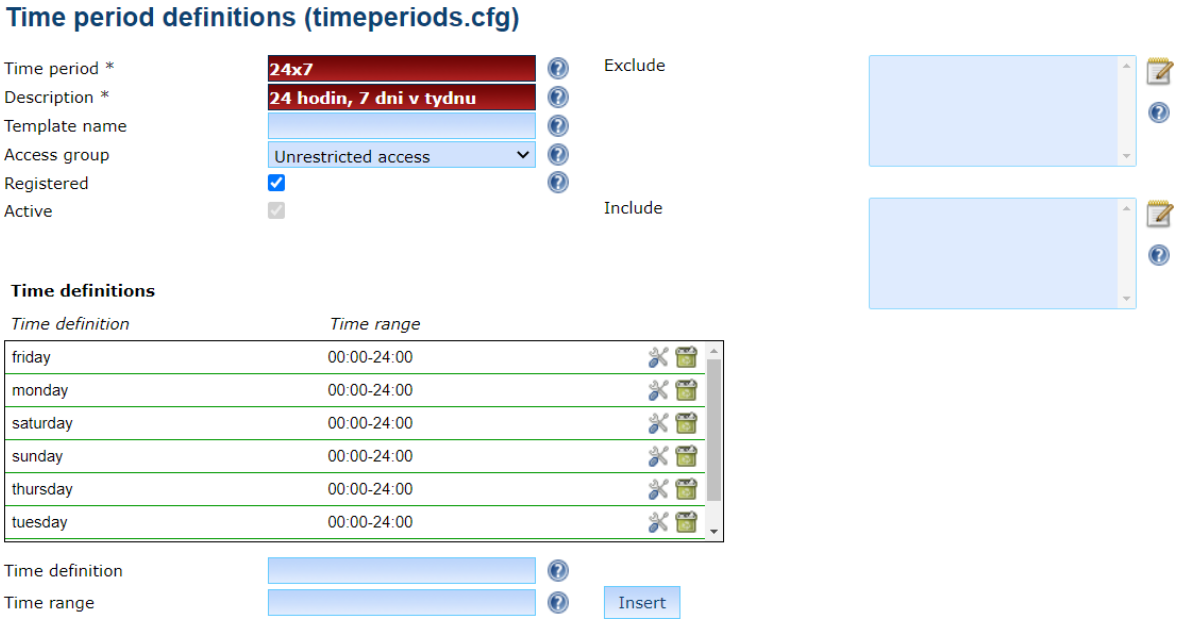
5.3.1 Definice časových period

Pro potřeby monitoringu jsem vytvořil tři časové periody nazvané 24x7, cz-holidays a workhours. Dle mého uvážení by tyto 3 periody měly dostatečně pokrýt potřeby monitoringu.



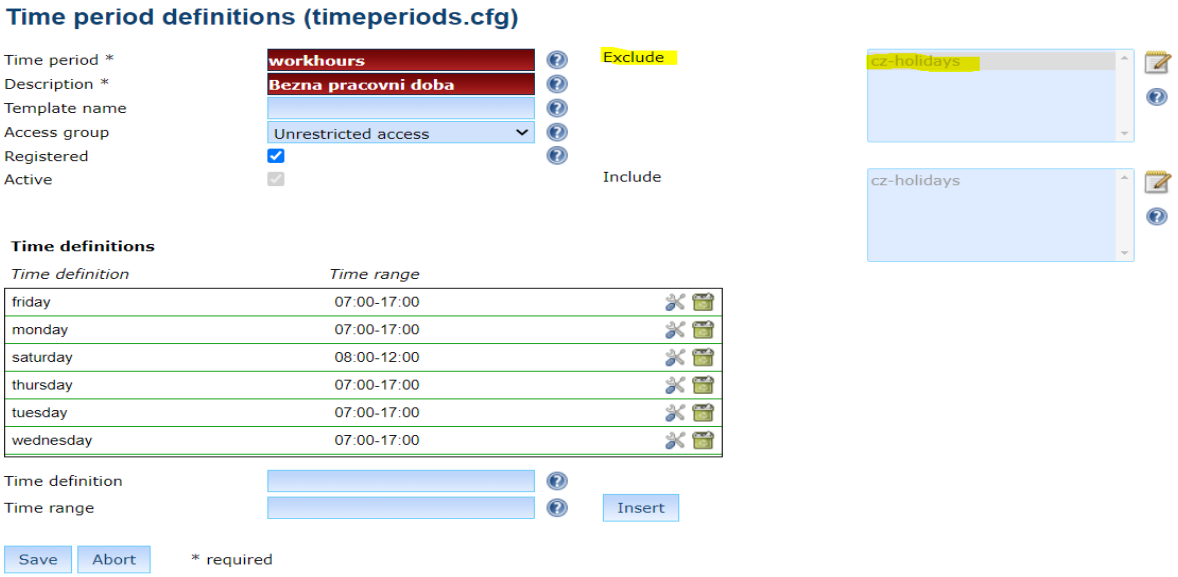
Obrázek 27. Přehled časových period, zdroj: autor

První časovou periodu 24x7 jsem vytvořil pro potřeby nepřetržitého monitoringu. Dny jsem nastavil pomocí time definition od pondělí do neděle. Časový rozsah pomocí time range od 00:00 do 24:00.



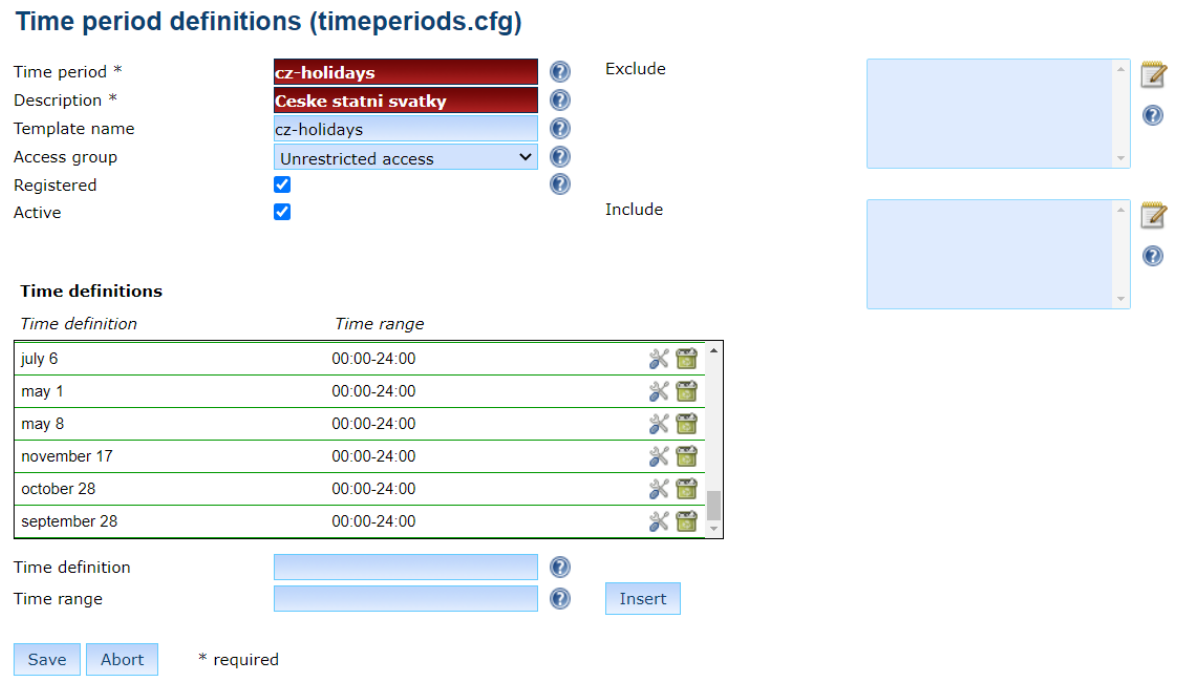
Obrázek 28. Definice časové periody 24x7, zdroj: autor

Druhou časovou periodu workhours jsem vytvořil pro potřeby monitoringu pouze během pracovní doby. Pracovní doba je ve všední dny od 7 do 17 hodiny.



Obrázek 29. Definice časové periody workhours, zdroj: autor

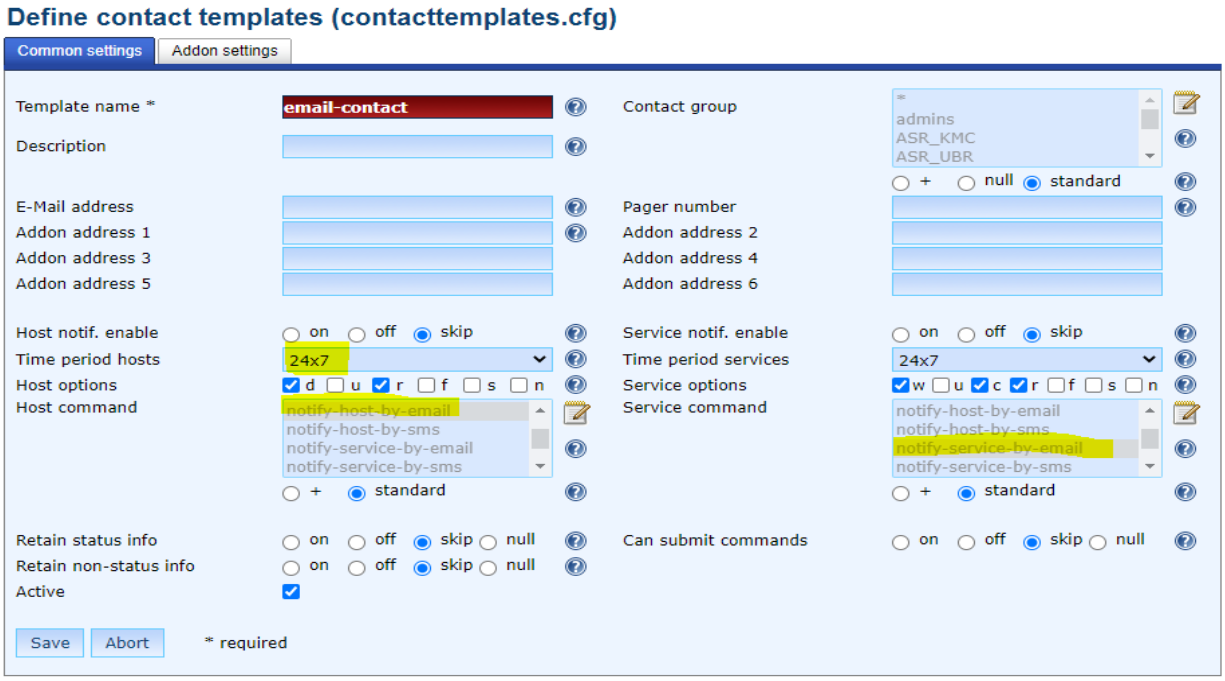
Třetí časová perioda se nazývá cz-holidays a uvedl jsem do ní všechny státní svátky České republiky. České státní svátky cz-holidays jsem následně pomocí příkazu „Exclude“ vyloučil z periody workhours. Díky tomu nebudou u daných zařízení zasílány notifikace, například během Štědrého dne, kdy je firma uzavřena.



Obrázek 30. Definice časové periody cz-holidays, zdroj: autor

5.3.2 Definice kontaktních šablon

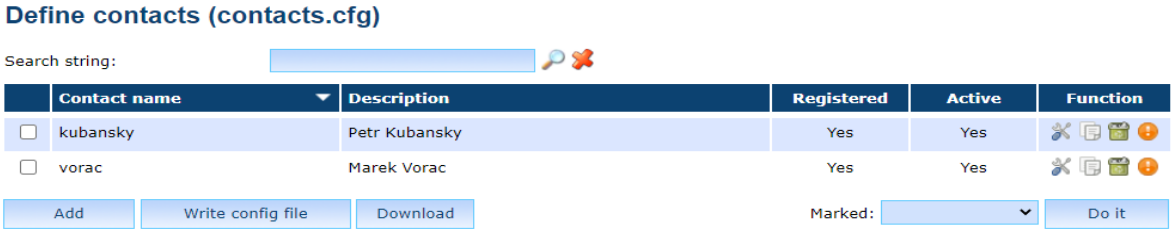
Pro kontaktování dotčených osob v případě výskytu problému bude sloužit dle domluvy výhradně emailová komunikace. V případě nepřetržitého monitoringu by bylo vhodné zasílat notifikace i pomocí textových zpráv na mobilní zařízení souběžně s emaily. Toto řešení bylo ovšem zamítnuto. Vytvořil jsem tak šablonu pro zasílání emailů pod názvem email-contact s nastavenou časovou periodou 24x7. Pro upozornění v případě problému s hostitelem jsem nastavil příkaz „notify-host-by-email“. Pro upozornění v případě problému se službou jsem nastavil příkaz „notify-service-by-email“.



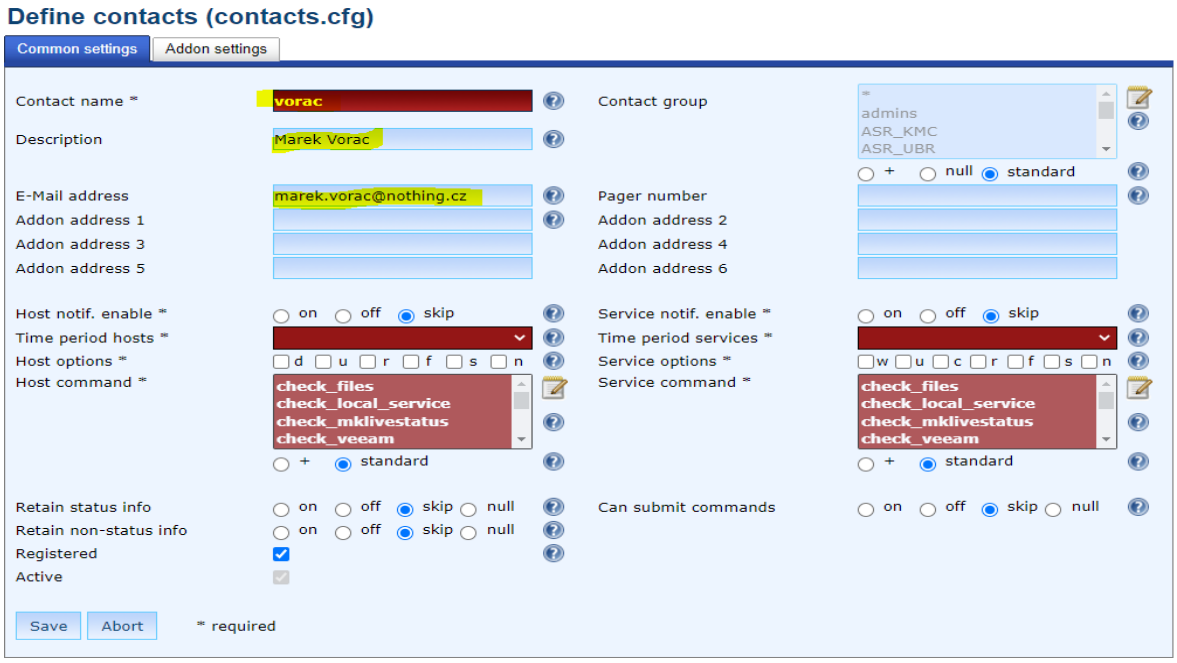
Obrázek 31. Definice kontaktních šablon, zdroj: autor

5.3.3 Definice kontaktů

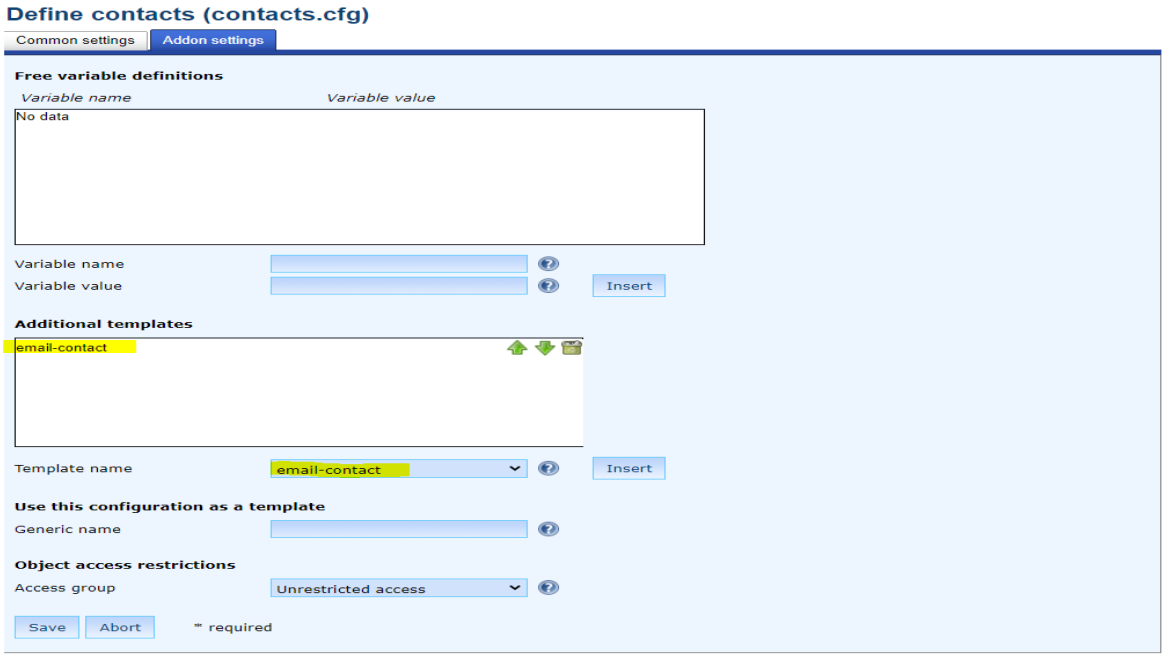
Pro středisko Kroměříž byly dle domluvy určeny dvě kontaktní osoby. Pro tyto osoby jsem definoval dva účty. První kontakt je na správce řídících technologií, který spravuje výrobní automatizaci. Druhý kontakt je na správce sítě, který má na starosti danou počítačovou síť. Dle mého názoru by bylo vhodné určit i sekundární kontakty, které by v případě nedosažitelnosti primárních kontaktů fungovaly jako zástup. Toto řešení je ovšem z personálních důvodů nerealizovatelné.



Obrázek 32. Přehled kontaktů, zdroj: autor



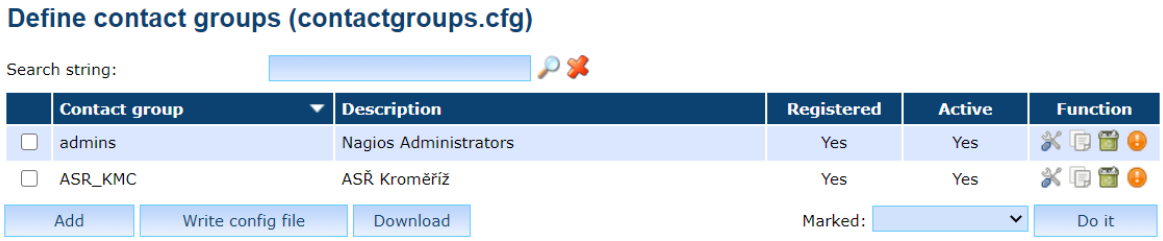
Obrázek 33. Definice kontaktu Common settings, zdroj: autor



Obrázek 34. Definice kontaktu Addon settings, zdroj: autor

5.3.4 Definice kontaktních skupin

V návaznosti na definované kontakty jsem vytvořil dvě skupiny. První je nazvaná admins a slučuje kontakty odpovědné za správu sítě. Druhá je nazvaná ASR_KMC a slučuje kontakty zodpovědné za technologie. V případě, že budou v budoucnu další správci sítě či řídících technologií, budou taktéž zařazeni do těchto skupin. V případě, že budou definováni i zastupující pracovníci, tak jim budou vytvořeny další kontaktní skupiny. Více skupin zpřehlední, kdo je kdo. Zda se jedná o primárního správce či sekundárního atd.



Obrázek 35. Přehled kontaktních skupin, zdroj: autor

5.3.5 Definice šablon služeb

Pro služby bylo potřeba vytvořit šablony, které budou pokrývat všechny potřebné možnosti provádění kontrol a zasílání oznámení. To by znamenalo vytvořit desítky jednotlivých šablon pro různá zařízení. Udělal jsem si rozbor jednotlivých potřeb kontroly a zasílání oznámení všech zařízení na středisku. Po zamyšlení, zda by nešlo vytvořit nějakou obecnou šablonu, která by byla průsečíkem těchto požadavků, jsem dospěl k následujícímu řešení. Vytvořil jsem šablonu nazvanou generic-service.

Obrázek 36. Přehled servisních šablon, zdroj: autor

U šablony generic-service jsem definoval nastavení kontroly a oznámení s parametry nejčastěji používaných hodnot. Tyto nastavené hodnoty jsem si dále v případě potřeby individuálně upravil přímo při konfiguraci hostitele. Díky tomu mi odpadla nutnost tvorby bezpočtu šablon.

V nastavení kontroly šablony generic-service jsem nastavil počet opakování testu, než nastane HARD stav na hodnotu 2. Tato hodnota mi přijde jako vhodný kompromis mezi variantou 1 a více než 2. Při hodnotě 1 byl hlášen HARD stav i při mikro výpadcích, které byly zapříčiněny chvilkovým vytížením sítě v době testu. Toto vedlo k zasílání zbytečných notifikací. Při hodnotě 3 a více už zase byla mezi testy dlouhá časová prodleva. Když jsem nastavil interval opakování testu například na hodnotu 5 minut, tak v případě 3 a více pokusů opakování testu byla notifikace o nedostupnosti zařízení zaslána až za více než 15 minut. Což je podle mého už velice dlouhá doba. Proto jsem zvolil již zmíněnou hodnotu 2.

Povolil jsem aktivní a pasivní kontroly. Pokud to monitorovací systém umožňuje, tak je tato varianta nejlepším řešením, jak popisuji v kapitole 3.2. Pro časové období, kdy se má sledovat dostupnost služby, jsem zvolil předdefinovanou časovou periodu 24x7. Prodlevu mezi opakováním testu u SOFT stavu jsem nastavil na 5 minut a prodlevu mezi testy pravidelné kontroly služby na 10 minut. Samozřejmě názory na hodnoty těchto intervalů se budou lišit člověk od člověka. Dle mých osobních zkušeností jsou tyto zvolené hodnoty časových intervalů nejlepší variantou.

Dále jsem povolil detekci rychlého přepínání stavů. Detekce rychlého přepínání pomáhá odhalit problémy s konfigurací a případné problémy se sítí. Je zde ovšem na zvážení, jakou hodnotu zvolit. Jaký počet změn stavu už je moc a jaký málo. Zde jsem se snažil najít různá řešení tohoto problému. Nakonec jsem zvolil dle doporučení Nagiosu nejlepší možnou hodnotu a tou je hodnota 0. Při uvedení této hodnoty se provádí detekce z hodnot posledních 21 testů. Obsluhu událostí, uchování nonstatus informací, uchování informací o stavu a zpracování údajů o výkonu.

V nastavení oznámení jsem povolil jeho zasílání a pro období, kdy se má zasílat, vybral předdefinovanou časovou periodu 24x7. Definoval jsem stavy, které se mají posílat. Jedná se o stavy WARNING, CRITICAL a OK. Tyto hodnoty jsou dle mých zkušeností nejvhodnější variantou. Další možnosti zasílaných stavů jsou pro mě v rámci monitoringu irelevantní.

5.3.6 Definice hostitelských skupin

Dle analýzy počítačové sítě jsem definoval celkem 508 hostitelů. Pro tyto hostitele jsem vytvořil 22 hostitelských skupin, do kterých byli hostitelé rozřazeni na základě typu zařízení.

Host group:	Description:
G_ASR	ASR
G_Camera	Kamera
G_Controller	Controller
G_DRAC	Drac Card
G_EXTERN_DISKS	Extern Disks
G_Fuel	Fuel
G_KAMEROVE_SYSTEMY	Kamerové systémy
G_Kotel	Kotel
G_MIKROTIK	Mikrotik
G_MS_servers	Windows Servers_Fyzické
G_MS_servers_Virtuals	Windows Servers_Virtuals
G_Pc	Computer
G_Pokladna	HP pokladna
G_Prevodnik	Prevodnik
G_Printers	Printers
G_Routers	Routers
G_SWITCH	Switchs
G_TECHNOLOGY	Technologie
G_Terminal	Docházkový terminál
G_UPS	UPS
G_Ustredna	Telefonni ustredna
G_WIFI	WIFI

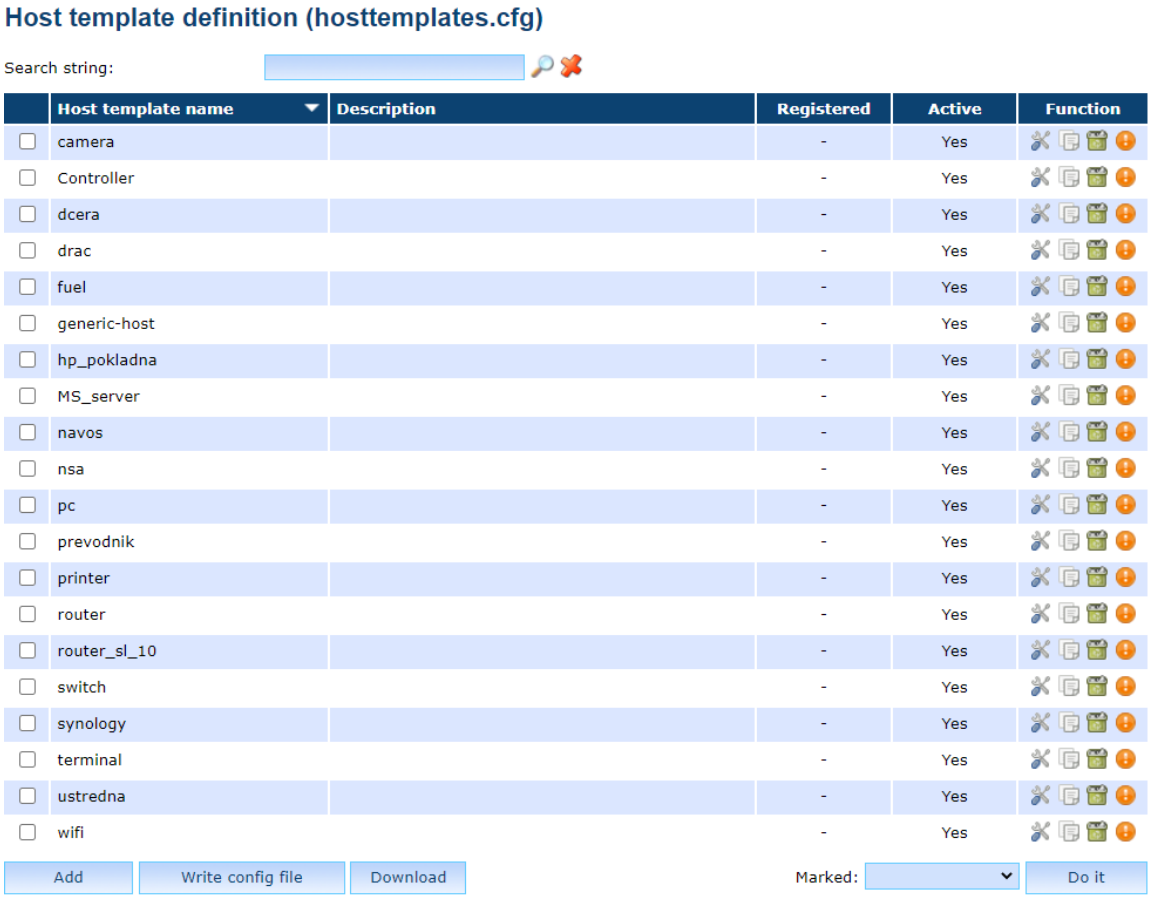
Tabulka 2. Hostitelské skupiny, zdroj: autor

Tento počet hostitelských skupin je více než dostatečný a pokrývá všechny skupiny zařízení, která jsou ve společnosti používána.

Obrázek 37. Detail definice hostitelské skupiny, zdroj: autor

5.3.7 Definice hostitelských šablon

Pro hostitele jsem dále vytvořil šablony. Každá šablona má dle typu zařízení individuálně nastaveny parametry základního nastavení, kontroly a oznámení.



Obrázek 38. Přehled hostitelských šablon, zdroj: autor

5.3.8 Definice služeb

Podle kategorie zařízení jsem definoval individuální požadavky monitoringu na jednotlivých skupinách hostitelů. Možnosti monitoringu jsou u každého typu zařízení velice různorodé. Liší se nejen typ od typu zařízení, ale také výrobce od výrobce. Například jeden výrobce kamerového sytému umožňuje monitorovat vícero parametrů a další pouze dostupnost zařízení. Proto jsem byl nucen najít v tak velkém počtu zařízení kompromis a vždy k typu zařízení najít společné parametry pro všechna zařízení v kategorii. Z důvodu časové náročnosti nepřipadalo v úvahu definovat zařízení od zařízení. U všech zařízení jsem tak po prostudování jejich možností monitoringu nalezl jeden společný parametr, který je možné sledovat. Tímto parametrem je vždy dostupnost zařízení. Dále jsem u jednotlivých skupin definoval další společné parametry, které je možné monitorovat. Tyto parametry jsem uvedl v tabulce 3.

Skupina:	Parametr:	Služba:
G_ASR	Dostupnost zařízení	Ping
G_Camera	Dostupnost zařízení	Ping
G_Controller	Dostupnost zařízení	Ping
G_DRAC	Dostupnost zařízení	Ping
G_EXTERN_DISKS	Dostupnost zařízení	Ping
G_Fuel	Dostupnost zařízení	Ping
G_KAMEROVE_SYSTEMY	Dostupnost zařízení	Ping
G_Kotel	Dostupnost zařízení	Ping
G_MIKROTIK	Dostupnost zařízení	Ping
	Kontrola paměti	Check_snmp_memory
	Kontrola firmware	Check_snmp_sw_firmware
G_MS_servers	Dostupnost zařízení	Ping
	Dostupnost drac karty	Dell_openmanage_idrac
	Dostupnost NS klienta	Windows_klient - Nsclient
	Využití procesoru	Windows_WMI_CPU - CPU
	NTP	Windows_NTP_time
	Zálohování	Windows_WMI_backup
	Windows aktualizace	Win_klient_service_windows_updates
	Souborový systém	Windows_WMI_Filesystems
	Teplota procesoru	Dell_cpu_temperature
	Teplota okolí	Dell_ambient_temperature
	Fyzická paměť	Windows_WMI_physical_memory
	Čas posledního restartu	Windows_WMI_Uptime
G_MS_servers_Virtuals	Dostupnost zařízení	Ping
	Dostupnost NS klienta	Windows_klient - Nsclient
	Využití procesoru	Windows_WMI_CPU - CPU
	NTP	Windows_NTP_time
	Čas posledního restartu	Windows_WMI_Uptime
	Fyzická paměť	Windows_WMI_physical_memory
	Windows aktualizace	Win_klient_service_windows_updates
G_Pc	Dostupnost zařízení	Ping
G_Pokladna	Dostupnost zařízení	Ping
G_Prevodnik	Dostupnost zařízení	Ping
G_Printers	Dostupnost zařízení	Ping
G_Routers	Dostupnost zařízení	Ping
G_SWITCH	Dostupnost zařízení	Ping
	Čas posledního restartu	Switch_uptime
	Provoz na portech	Trafficts_ports_01 - 52
G_TECHNOLOGY	Dostupnost zařízení	Ping
G_Terminal	Dostupnost zařízení	Ping
G_UPS	Dostupnost zařízení	Ping
	Porucha nabíjení	UPS_battery_charger_fault
	Teplota okolí	UPS_ambient_temperature
	Úroveň nabití baterie	UPS_battery_level

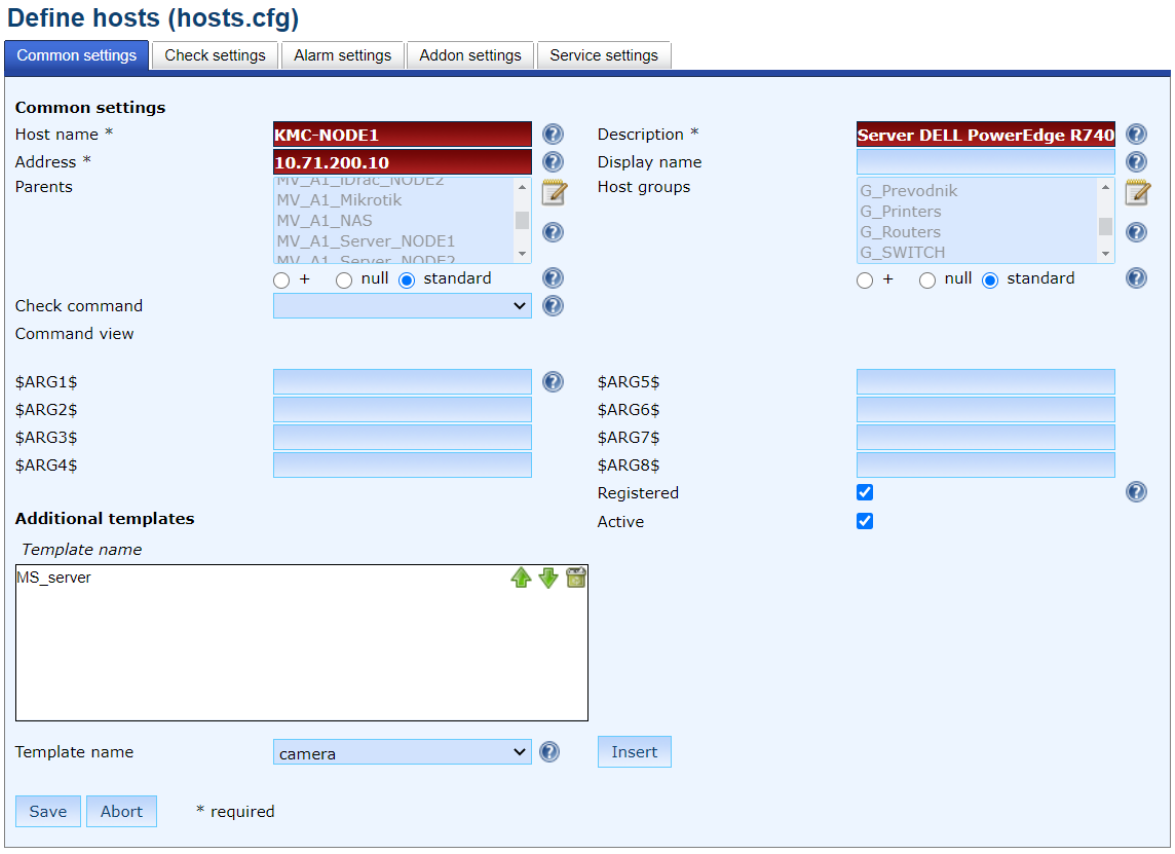
Skupina:	Parametr:	Služba:
	Napětí baterie	UPS_battery_voltage
	Teplota baterie	UPS_battery_temperature
G_Ustredna	Dostupnost zařízení	Ping
G_WIFI	Dostupnost zařízení	Ping

Tabulka 3. Specifikace monitorovaných parametrů skupin hostitelů, zdroj: autor

5.3.9 Definice hostitelů

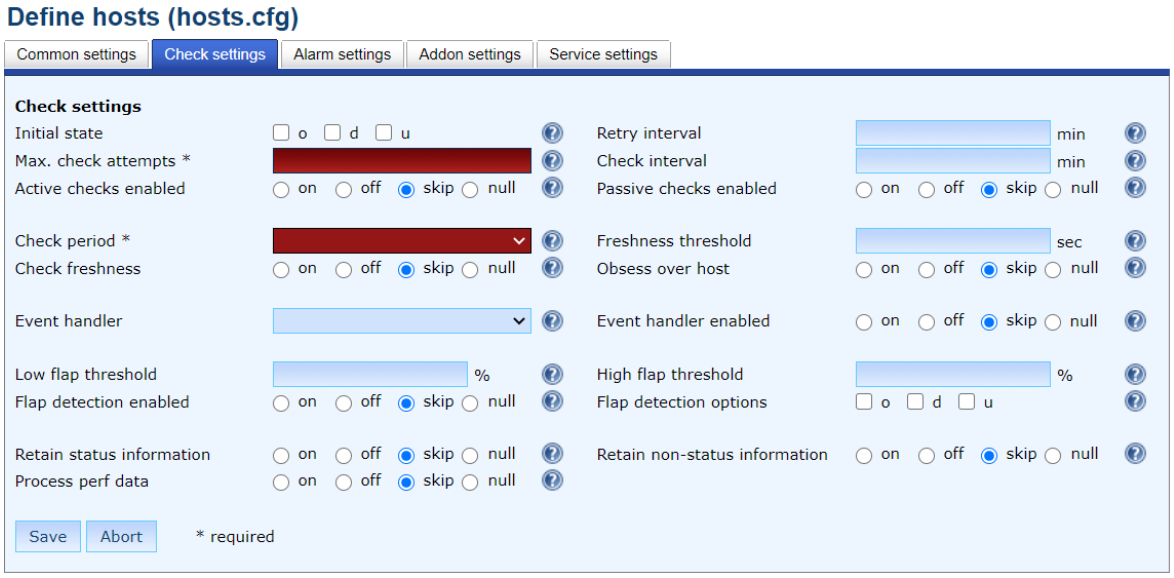
Dle analýzy počítačové sítě jsem vytvořil celkem 43 hostitelů, které jsem následně rozdělil do hostitelských skupin dle typu zařízení. Podrobný seznam hostitelů je uveden v tabulce 1. a odpovídá skutečnému stavu zařízení na středisku. U každého hostitele jsem při vytvoření definoval parametry základního nastavení, nastavení kontroly, nastavení oznámení, nastavení doplňků a nastavení služeb.

Pro představu názorně předvedu konfiguraci hostitele KMC-NODE1. V tomto případě se jedná o fyzický server od firmy Dell s operačním systémem Windows. V základním nastavení hostitele definuji jeho název, popis, IP adresu, rodiče, hostitelskou skupinu a hostitelskou šablonu.



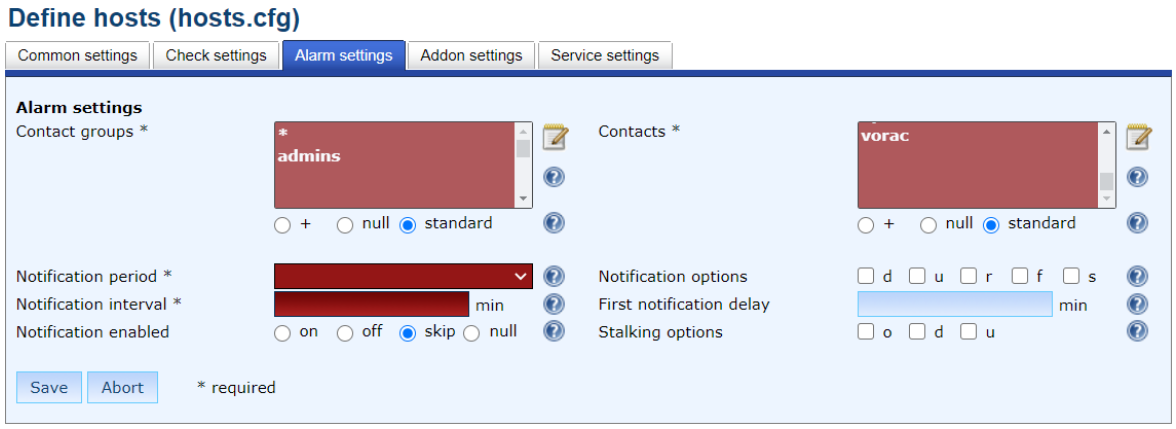
Obrázek 39. Detail definice základního nastavení hostitele, zdroj: autor

V nastavení kontroly jsem všechny možnosti nastavil na „skip“. Tímto nastavením přebírá hostitel nastavení kontroly z definované šablony.

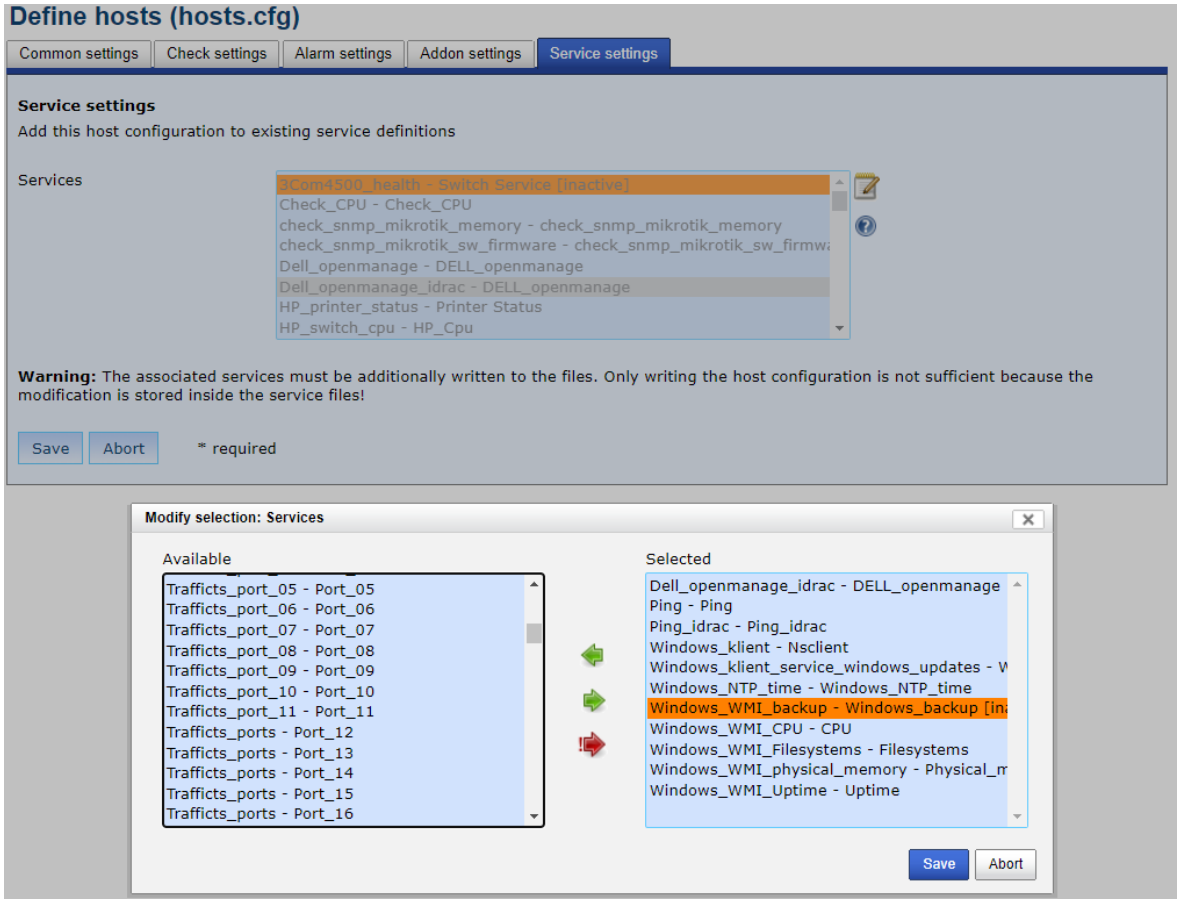


Obrázek 40. Detail definice nastavení kontroly hostitele, zdroj: autor

Stejně tak v nastavení oznámení jsem zvolil možnost „skip“.



Obrázek 41. Detail definice nastavení oznámení hostitele, zdroj: autor

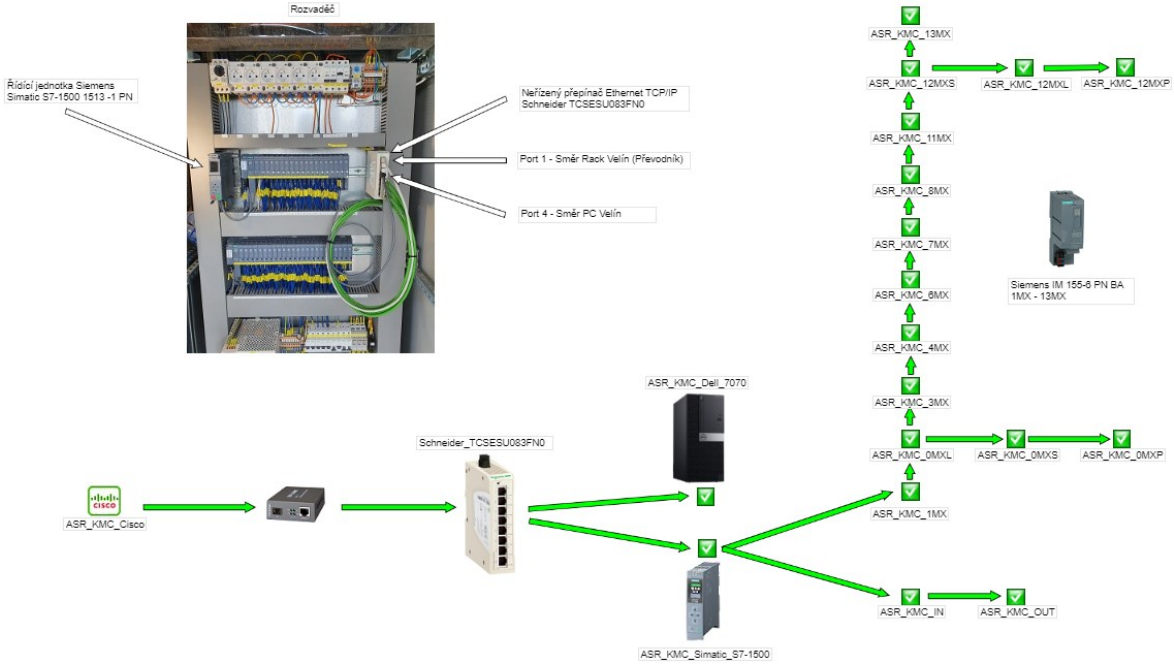


Obrázek 42. Detail definice nastavení služeb hostitele, zdroj: autor

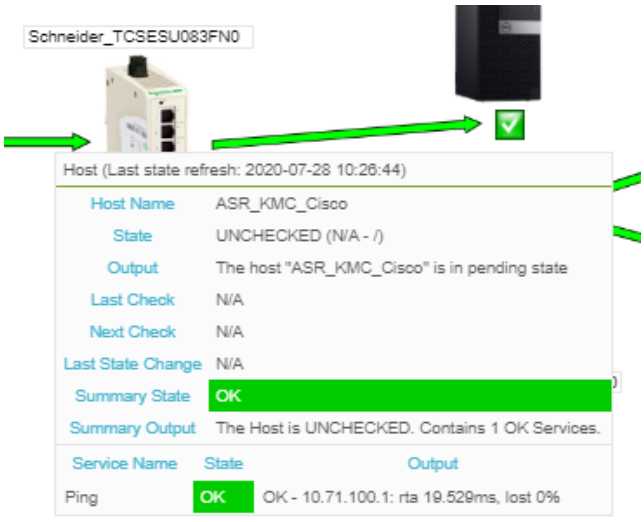
Všechna nastavení jsem provedl s ohledem na maximální efektivitu a jednoduchost systému. V jednoduchosti se nachází síla. Veškeré parametry, které jsem zvolil, jsou dle mého nejlepší možnou variantou.

5.4 Nagvis

Nagvis slouží k vizualizaci dat, jak už jsem uvedl v teoretické části. V případě střediska Kroměříž jsem jej využil k zobrazení topologie zapojení jednotlivých komponent síťové infrastruktury. Vytvořil jsem podrobnou mapu budovy D, ve které probíhá výroba. V případě výpadku je pomocí mapy možné zjistit, o které zařízení se jedná a kde je umístěno.



Obrázek 43. Nagvis – technologie budova D, zdroj: autor



Obrázek 44. Nagvis - detail zařízení, zdroj: autor

Stejným způsobem jsem nakonfiguroval mapy ostatních budov na středisku Kroměříž i všech ostatních.

5.5 Testování systému Nagios

Po úspěšné konfiguraci všech hostitelů, skupin, šablon a služeb jsem provedl na středisku Kroměříž test funkčnosti. Testování probíhalo v cyklu jednoho týdne, tj. od pondělí do neděle. Během testovacího cyklu jsem simuloval různé stavy zařízení a nedostupnosti jednotlivých služeb. Testování proběhlo bez jakýchkoliv problémů a systém byl zaveden do ostrého režimu. Stejným způsobem jsem postupoval na všech ostatních střediscích. Na ukázku jsem níže uvedl notifikaci, kterou zaslal systém Nagios.

Na obrázku 47. je notifikace ze zařízení mikrotik, které je vedeno pod hostitelským názvem KOT-mikrotik. Jedná se o upozornění zaslané pomocí služby:

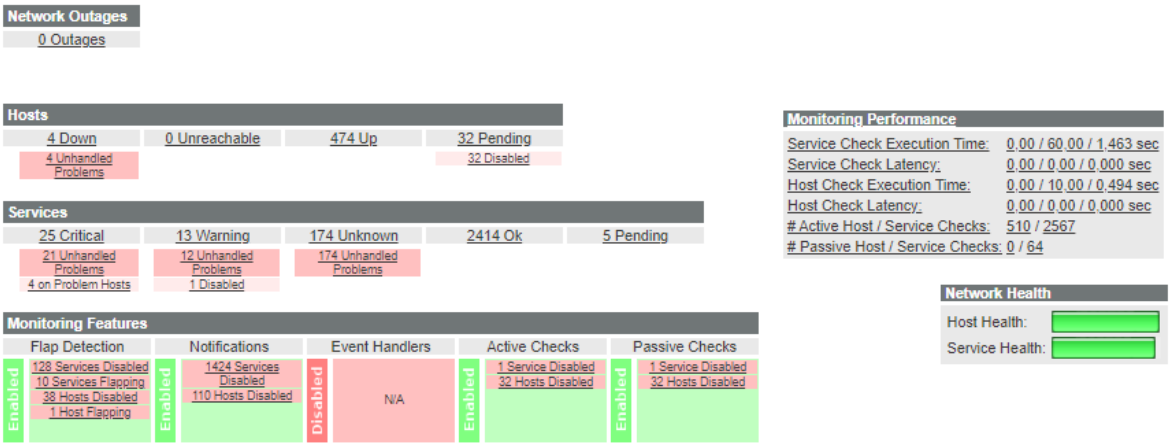
- Check_snmp_sw_firmware.

Tato služba upozorňuje na zastaralý firmware zařízení s uvedením stávající a aktuální verze.

Nagios message

Hostname	KOT-mikrotik
Service	check_snmp_mikrotik_sw_firmware
Timestamp	2020.07.27 18:57:52
State	CRITICAL
Type	PROBLEM
Message	Critical : RouterOS is up to date (6.47.1). Firmware Requires Upgrade (6.47 -> 6.47.1).

Obrázek 45. Nagios – upozornění na upgrade



Obrázek 46. Taktický přehled stavu a monitorovacího výkonu, zdroj: autor

ZÁVĚR

Cílem bakalářské práce bylo seznámit čtenáře s možnostmi monitorování počítačové sítě pomocí open source systému Nagios a jeho následná implementace do reálného prostředí vybrané společnosti.

V úvodní části jsem čtenáře uvedl do problematiky monitorování počítačových sítí. Prezentoval jsem základní principy funkčnosti počítačových sítí tak, aby byly pochopitelné i laické veřejnosti. Ukázal jsem základní sedmivrstvý model OSI, který standardizuje klíčové funkce sítě pomocí síťových protokolů. To umožňuje různým typům zařízení od různých výrobců vzájemně komunikovat v síti.

Dále jsem rozebral, jak data procházejí sítí, jaká máme základní síťová zařízení a co je to síťový monitorovací nástroj. Zde jsem podrobněji rozebral dva nejpoužívanější monitorovací protokoly SNMP a WMI. Následně jsem uvedl další varianty open source monitorovacích systémů mimo Nagios, mezi které patří Zabbix, Icinga, Cacti, OpenNMS a Netdata.

Zaměřil jsem se na systém Nagios a zmínil možnosti monitoringu a konfigurace, které nabízí. Z důvodu zachování anonymity jsem v praktické části pozměnil použité názvy a hodnoty, protože mám obavu ze zneužití. Provedl jsem implementaci systému Nagios do reálného provozu vybrané společnosti. Vybraná společnost se skládá z více než 60 samostatných středisek, která jsou rozmístěna po celém území České republiky. Tato střediska jsou mezi sebou propojena pomocí MPLS. Díky tomuto faktu disponuje velice rozsáhlou počítačovou sítí a potřeba síťového monitoringu byla více než nutná. U dané společnosti působím několik let na pozici IT specialisty, a tak mám možnost neomezeného přístupu k síti.

Při realizaci jsem nejdříve musel provést detailní analýzu počítačové sítě. Tato část byla velice časově náročná a zabrala nejvíce času. Mimo skenování rozsahů jednotlivých subnetů jsem musel střediska navštívit i osobně. To proto, abych si ujasnil detaily topologie sítě daných středisek. Po analýze jsem zařadil do monitoringu celkem 508 zařízení. Z toho bylo 43 zařízení na středisku Kroměříž, které jsem si vybral pro detailní ukázku.

Při konfiguraci Nagiosu jsem nejprve definoval časové periody, dále kontaktní šablony, kontakty, kontaktní skupiny, šablony služeb, hostitelské skupiny, služby a na konec samotné hostitele. Toto pořadí mělo svůj smysl, jelikož na sebe některé objekty navazují. Při konfiguraci jsem se setkal s problémy, jejichž řešení je popsáno v práci. Například výrobní

prostory střediska Kroměříž byly mimo MPLS a bylo zde internetové připojení realizováno pomocí místního providera. Tato skutečnost komplikovala monitoring a bylo nutné najít řešení. Dále některá klíčová zařízení v podobě optických převodníků neumožňovala dotazovat jejich dostupnost a další.

SEZNAM POUŽITÉ LITERATURY

[1] Samuraj.cz [online]. [cit. 2020-07-05]. Dostupné z: https://www.samuraj-cz.com/clanek/zaciname-s-monitoringem-site/

[2] Whats up gold [online]. [cit. 2020-07-05]. Dostupné z: https://www.whatsupgold.com/what-is-network-monitoring

[3] SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Brno: Computer Press, 2010. ISBN 978-802-5133-637.

[4] Maturitní helpdesk [online]. [cit. 2020-07-05]. Dostupné z: http://matureplus.4fan.cz/pos/3-model-isoosi-vrstvy/

[5] KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

[6] Link SYS [online]. [cit. 2020-07-05]. Dostupné z: https://www.linksys.com/us/r/resource-center/what-is-a-modem/

[7] How-To Geek [online]. [cit. 2020-07-05]. Dostupné z: https://www.howtogeek.com/99001/htg-explains-routers-and-switches/

[8] Computer Hope [online]. [cit. 2020-07-05]. Dostupné z: https://www.computerhope.com/jargon/n/nic.htm

[9] WINKLER, Peter. Velký počítačový lexikon: co je co ve světě počítačů. Brno: Computer Press, 2009. ISBN 978-80-251-2331-7.

[10] Tech Terms [online]. [cit. 2020-07-05]. Dostupné z: https://techterms.com/definition/switch

[11] Techtarget.com [online]. [cit. 2020-06-10]. Dostupné z: https://searchitoperations.techtarget.com/definition/Zabbix

[12] Zabbix.com [online]. [cit. 2020-06-10]. Dostupné z: https://assets.zabbix.com/img/5.0/zabbix_dashboard_v50_dark.jpg

[13] Icinga.com [online]. [cit. 2020-06-10]. Dostupné z: https://icinga.com/docs/

[14] Icinga.com [online]. [cit. 2020-06-10]. Dostupné z: https://community.icinga.com/t/dashing-for-icinga-3-0-0/2523

[15] Cacti.net [online]. [cit. 2020-06-10]. Dostupné z: https://www.cacti.net/what_is_cacti.php

[16] Github.com [online]. [cit. 2020-06-10]. Dostupné z: https://github.com/Cacti/cacti/issues/458

[17] Opennms.org [online]. [cit. 2020-06-10]. Dostupné z: https://docs.opennms.org/opennms/releases/latest/guide-development/guide-development.html

[18] Financesonline.com [online]. [cit. 2020-06-10]. Dostupné z: https://reviews.financesonline.com/p/opennms/

[19] Websetnet.net [online]. [cit. 2020-06-10]. Dostupné z: https://websetnet.net/cs/server-monitoring-opennms-ubuntu-16-04/

[20] Netdata [online]. [cit. 2020-06-10]. Dostupné z: https://www.netdata.cloud/

[21] Turris.cz [online]. [cit. 2020-06-10]. Dostupné z: https://forum.turris.cz/t/monitoring-omnia-with-netdata/3179

[22] Nagios.com [online]. [cit. 2020-07-02]. Dostupné z: https://www.nagios.com/

[23] Nagios Core Documentation [online]. [cit. 2020-07-02]. Dostupné z: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/configobject.html

[24] The geek Stuff [online]. [cit. 2020-07-03]. Dostupné z: https://www.thegeekstuff.com/2009/06/4-steps-to-define-nagios-contacts-with-email-and-pager-notification/

[25] Packt [online]. [cit. 2020-07-03]. Dostupné z: https://subscription.packtpub.com/book/networking_and_servers/9781785889332/1/ch01lvl1sec14/creating-a-new-hostgroup

[26] Nagios Core Documentation [online]. [cit. 2020-07-03]. Dostupné z: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/timeperiods.html

[27] Nagios Core Documentation [online]. [cit. 2020-07-03]. Dostupné z: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/activechecks.html

[28] Nagios Core Documentation [online]. [cit. 2020-07-03]. Dostupné z: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/pasivechecks.html

[29] Nagios Core Documentation [online]. [cit. 2020-07-03]. Dostupné z: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/downtime.html

[30] Nagios Core Documentation [online]. [cit. 2020-07-03]. Dostupné z: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/

[31] Exchange.nagios.org [online]. [cit. 2020-07-08]. Dostupné z: https://exchange.nagios.org/directory/Tutorials/Nagios-XI-Tutorials/Reporting-and-Graphing-Series/Nagios-XI-%E2%80%93-Reporting-%26-Graphing-%E2%80%93-Overview-of-Reporting-in-Nagios-XI/details

[32] Nagvis [online]. [cit. 2020-07-08]. Dostupné z: http://www.nagvis.org/home

[33] NetEye [online]. [cit. 2020-07-08]. Dostupné z: https://www.neteye-blog.com/2014/11/nagmap-new-features/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IT	Informační technologie
OSI	Open Systems Interconnect
IP	Internet Protocol
HW	Hardware
LAN	Lokální síť
PCI	Peripheral Component Interconnect
ISA	Industry Standard Architecture
USB	Universal Serial Bus
ISP	Poskytovatel internetového připojení
Wi-fi	Wireless fidelity
WAN	Globální počítačová síť
NMS	Síťový monitorovací nástroj
SNMP	Simple Network Management Protocol
CPU	Procesor
MIB	Management Information Base
GPL	Licence pro svobodný software
API	Application Programming Interface
URL	Uniform Resource Locator
PZTS	Poplachový zabezpečovací a tísňový systém
CCTV	Kamerový systém
PIR	Pasivní infračervené čidlo
NVR	Síťový video rekordér
PCO	Pult centralizované ochrany
USP	Zdroj nepřerušovaného napájení
SFP	Small Form-factor Pluggable

HP	Hewlett-Packard
MPLS	Multiprotokolové přepojování podle návěstí

SEZNAM OBRÁZKŮ

SEZNAM TABULEK