

Jihočeská univerzita v Českých Budějovicích
Pedagogická fakulta

Bakalářská práce

Nagios a jeho využití
na Zemědělské fakultě JU

Ing. Radek Černý

Katedra informatiky

České Budějovice 2007

Vedoucí bakalářské práce: Ing. Ladislav Beránek, CSc., MBA

Poděkování

Děkuji vedoucímu mé bakalářské práce Ing. Ladislavu Beránkovi za připomínky, odborné konzultace a vstřícnost při psaní této práce a během mého studia.

Děkuji kolegovi a kamarádovi Mgr. Radimovi Remešovi za rady a připomínky v oblasti sazby mé bakalářské práce v sázecím programu T_EX.

Prohlášení

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

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě, elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách.

V Českých Budějovicích 25. dubna 2007

Ing. Radek Černý

Anotace

Cílem této bakalářské práce bylo ukázat instalaci, konfiguraci a implementaci monitorovacího systému Nagios v prostředí Zemědělské fakulty Jihočeské univerzity. Poukázat na praktickém příkladě důležitost využití monitorovacího systému pro monitorování provozu informačních sítí.

Teoretická část práce seznamuje čtenáře s monitorovacími systémy, které jsou v současné době dostupné na trhu. Dále podrobně popisuje postup při instalaci, konfiguraci a programování vlastních modulů monitorovacího systému. Praktická část bakalářské práce zahrnuje implementaci monitorovacího systému Nagios na jedné z fakult JU včetně konfigurace, programování specifických monitorovacích modulů a správu systému.

The aim of this bachelor's thesis is to demonstrate the installation, configuration and implementation of the monitoring system Nagios in the environment of the Faculty of Agriculture at the University of South Bohemia. The importance of such a monitoring system for monitoring data network operation will be shown on a practical example.

The theoretic part acquaints the reader with monitoring systems available on the current market. It also illuminates the procedure of installation, configuration and programming concrete modules of the monitoring system in detail. The practical part of this work embraces the implementation of the monitoring system Nagios at one of the faculties at the University of South Bohemia including configuration, programming specific monitor modules and system administration.

Obsah

1	Úvod	9
2	Proč monitorovací systém?	11
3	Nástroje pro monitorování sítě	12
3.1	Monitorovací systém „Nagios“	13
3.2	Monitorovací systém „Akk@da“	15
3.3	Monitorovací systém „Zenoss“	16
3.4	Monitorovací systém „Zabbix“	17
3.5	Monitorovací systém „NetDisco“	19
4	Monitorovací systém Nagios	21
4.1	Architektura systému Nagios	21
4.2	Hardwarové požadavky na systém	22
4.3	Instalace Nagiosu	22
4.4	Instalační proces ze zdrojových kódů	23
4.5	Instalační proces z balíčků	24
4.6	Konfigurace webové konzole	25
4.6.1	Konfigurace webového serveru - varianta č. 1	26
4.6.2	Konfigurace webového serveru - varianta č. 2	26
5	Konfigurace základních objektů	28
5.1	Definice a testování zařízení	30
5.1.1	Definice zařízení (host)	30

5.1.2	Testování zařízení (host)	31
5.2	Definice a testování služby (service)	33
5.3	Definice kontaktu (contact)	34
5.4	Definice skupin (hostgroups)	35
5.5	Definice časového intervalu (timeperiod)	35
6	Základní operace v Nagiosu přes WWW	36
6.1	Sekce „Monitoring“	36
6.1.1	Tactical Monitoring Overview	37
6.1.2	Service Detail	38
6.1.3	Host Detail	38
6.1.4	Ostatní odkazy v sekci „Monitoring“	38
6.2	Sekce „Reporting“	39
6.2.1	Report „Availability“	39
6.2.2	Event Log Report	40
6.3	Sekce „Configuration“	40
7	Monitorování provozu sítě a lokálních služeb	41
7.1	Monitorování provozu sítě	41
7.1.1	Monitorování zařízení	42
7.1.2	Monitorování služeb	43
7.1.3	Lokální monitorování	43
7.1.4	Síťové monitorování	44
7.2	Vzdálené monitorování lokálních služeb	45
7.2.1	Monitorování pomocí NRPE služby	45
7.2.2	Vzdálené monitorování pomocí SSH	46
7.2.3	Monitorování pomocí SNMP	48
8	Vytváření vlastních skriptů	49
9	Monitorované servery a služby	51
9.1	Monitorovaná zařízení v prostředí JU	52
9.1.1	Zařízení na Zemědělské fakultě JU	52

<i>OBSAH</i>	8
9.1.2 Zařízení rektorátu JU	53
9.1.3 Zařízení na Teologické fakultě JU	54
9.1.4 Zařízení Zdravotně sociální fakulty JU	54
9.2 Monitorovaná zařízení v komerční sféře	55
9.2.1 Radio Faktor s.r.o.	55
9.2.2 Marten-Louis s.r.o.	56
9.2.3 Jazyková škola EDUCO	56
9.2.4 1K Design s.r.o.	56
10 Konfigurace Nagiosu v praxi	57
10.1 Vložení pracovníka do systému	58
10.2 Vložení serveru a služeb do systému	58
11 Zkušenosti s provozem	60
12 Závěr	66
Literatura	68
Rejstřík	69
Seznam obrázků	71
Seznam tabulek	72

Kapitola 1

Úvod

Téma „Nagios a jeho využití na Zemědělské fakultě“ jsem si vybral z toho důvodu, že jsem již 6 let zaměstnán jako správce sítě na této fakultě a právě monitorování sítě v současné době považuji za naprostou nutnost a již si nedovedu představit správu serverů a služeb bez těchto nástrojů.

Trendy v této oblasti jsou jednoznačné. Příčinou je skutečnost, že hardwarové vybavení je stále levnější a mzdové nároky na zaměstnance se neustále zvyšují. Pokud porovnáám situaci před 8 lety na Jihočeské univerzitě v počtech serverů a současnou situaci, lze mluvit o nárůstu ve stovkách procent. Nicméně management univerzity a poté fakult, se snaží udržet z ekonomických důvodů stejný počet zaměstnanců, které se o tyto servery starají. Rovněž je kladen větší důraz na spolehlivost služeb, kdy i kratší výpadek u některé ze služeb může mít citelné následky. Tuto skutečnost nejlépe vystihuje slogan, který je uváděn ve spojení s monitorovacím systémem Nagios a zní: *„Nagios je program pro monitorování počítačů, služeb, navržený tak, aby Vás informoval o případných výpadcích dříve než to udělají zákazníci, uživatelé či Vaši šéfové...“* [1].

Systém Nagios je velmi silný monitorovací nástroj, který je možno využít pro dohled síťových prostředků (serverů, počítačů, aktivních prvků, tiskáren) a služeb jimi poskytovaných (elektronická pošta, www stránky atd.). V případě výpadku některé z dohledových služeb umí systém poslat varování

správčům systému či provést jiné definované akce. Celý systém je jednoduše rozšiřitelný a umožňuje monitorovat velké množství různých typů zařízení. Neumí-li systém se standardně dodávanými testy monitorovat Vaše zařízení, je možné do systému přidat vlastní testy či nastavit jiné možnosti monitorování. Do systému lze integrovat také již stávající monitorovací systémy, např. programy UPS od společnosti APC.

Při současném značném množství serverů a služeb není možné, aby preventivně administrátor kontroloval veškeré služby na všech serverech stále dokola. Je nutné, aby byl co nejrychleji detailně informován o kolizích a výpadcích, k nimž v síti dojde, a aby následně vyhledal a analyzoval příčiny těchto kolizí. Nagios samozřejmě není jediným monitorovacím nástrojem na trhu. Myslím si však, že je jedním z nejrozšířenějších, což je způsobeno tím, že je dostupný zcela zdarma.

Cílem práce je, shrnout informace o monitorovacím systému Nagios, poskytnout praktické poznatky, výsledky a zkušenosti s ročním provozem. Čtenář bude informován o vhodné volbě instalace monitorovacího systému, základní konfiguraci nastavení, jak nejvhodněji vkládat a modifikovat skupiny, uživatele, časové intervaly, monitorované servery a jejich služby, dále bude seznámem se základními možnostmi programování vlastních modulů a správou či údržbou monitorovacího systému.

Kapitola 2

Proč monitorovací systém?

V současné době se asi žádná společnost či organizace neobejde bez výpočetní techniky. Počítače mohou být používány jako komunikační prostředek nebo jako výrobní a podpůrné nástroje.

Počítače a jejich podpůrné vybavení se stává čím dál více složitější. Při nasazení počítačů dochází proto často k problémům, ať už technickým (shoří důležitá součástka; po vypnutí elektrického proudu nenaběhne server korektně) či následkem selhání lidského faktoru (správce počítače omylem nastaví špatná přístupová práva). Tyto problémy způsobují částečnou a někdy i celkovou nedostupnost systémů a s tím spojené ztráty.

Je-li v síti nasazen nějaký monitorovací systém, většinou vědí správci o nastalém problému téměř okamžitě včetně jeho lokalizace (ve velké části případů odpadá dohadování s uživateli, kteří většinou nebývají odborníky v IT) a mohou jej případně rychleji odstranit. Je zřejmé, že nasazením monitorovacího systému se drasticky snižuje doba nedostupnosti a také škoda nedostupností způsobená. Části problémů lze pomocí monitorovacích systémů předejít, např. zastavení serveru způsobené přeplněním disku je možné vysledovat ještě dříve, než nastane.

Při vhodném nasazení monitorování je možné hlídat i nekritická zařízení – moderní tiskárny, které umí na požádání sdělit informace o zbývajícím obsahu náplně v toneru, zdali nejsou ve stavu, kdy vyžadují opravu apod [1].

Kapitola 3

Nástroje pro monitorování sítě

Jak jsem již zmínil výše, je důležité vědět, co se kde ve vlastní síti přihodí. Není to pouze otázkou profesionální hrdosti administrátora, ale jde o klíčovou položku pro bezpečnost i pro samostatné zabezpečení spolehlivého chodu sítě. Pro její monitorování existují desítky nástrojů od jednoduchých skriptů v Perlu až po rozsáhlé aplikace, které podporují stovky zařízení a poskytují zajímavé statistické výstupy. V této kapitole jsem se pokusil shrnout nejznámější opensourcové monitorovací nástroje, které jsou v současné době dostupné.

Každá síť je do jisté míry jedinečná, takže při volbě vhodného nástroje se lze vydat různými cestami. Na jedné straně existují komplexní řešení s předkonfigurovanými rozhraními pro většinu známých zařízení a služeb. Na straně druhé nejsou moc robustní nebo existují univerzálnější a méně náročné systémy, jež nabízejí jen základní kolekci služeb, přičemž speciální síťová zařízení je nutno doplnit ručně.

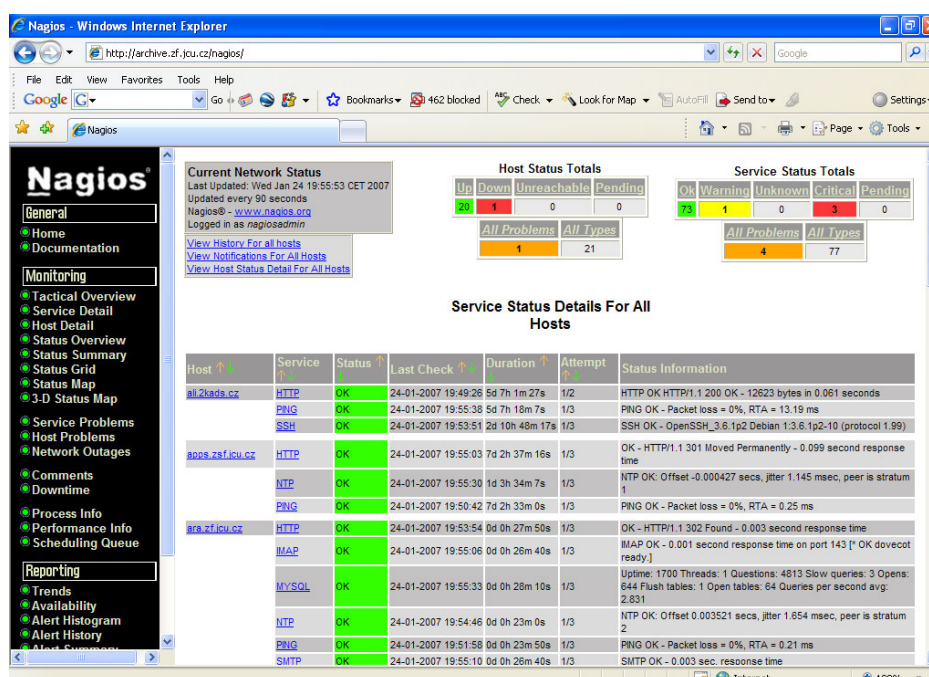
Zatímco komerční aplikace volí první variantu a většinou vyžadují i specifický hardware nebo alespoň dedikované servery, opensourcové programy jsou často méně náročné a díky otevřenému kódu i snáze upravitelné. Je ovšem důležité zvážit, zda jsme ochotni věnovat potřebný čas úvodní konfiguraci a seznámení se systémem, k němuž bývá většinou k dispozici pouze textová dokumentace a nikoliv rozšířený servis jako u komerčních balíků. Opensour-

cová řešení sice nebývají tak robustní, dávno ale však nejde jen o základní nástroje spojující několik diagnostických utilit. Typickým příkladem mohou být právě systémy typu Nagios nebo částečně komerční řešení Zenoss, které nabízejí širokou paletu funkcí v jednotném rozhraní za doprovodu komplexních statistik [5].

Ať už se jedná o jednoduchý nebo komplexní systém, základní monitorovací funkce bývají často společné. Hlavní rozdíl spočívá v interpretaci výsledků. Jednodušší výpisy formou klasického textového logu jsou vhodné pro malé sítě a nejsou-li doplněny alespoň základními funkcemi pro ohlašování chyb (nejčastěji e-mailem, SMS či jinou cestou), stávají se velmi nepružnými a prakticky nepoužitelnými. Níže vybrané nástroje vždy nabízejí i souhrnné statistiky a přehledy, i když ne všude se setkáme s grafickou prezentací. Dalším kritériem byla přítomnost rozhraní v podobě webové administrace nebo samostatné aplikace s on-line přehledem aktuálního stavu celé sítě i jednotlivých prvků. Všechny popisující nástroje jsou určeny pro provoz pod operačním systémem Linux, případně jiným Unixových systémem a shodně ke své činnosti vyžadují služby webového serveru, kterým je většinou Apache s podporou Perlu a databáze MySQL [5].

3.1 Monitorovací systém „Nagios“

Nagios patří patrně k nejznámějším a nejrozšířenějším monitorovacím nástrojům, které mají GPL licenci. Vzhledem k nabídce funkcí a dlouhému vývoji, by se hledalo velice těžko komplexnější řešení, a to i mezi komerčními aplikacemi. Pod jednotným webovým rozhraním nalezneme monitorovací funkce prakticky pro všechna sledovatelná zařízení a služby v síti. Vedle podpory SNMP (verze 1 až 3) systém nabízí velké množství dalších modulů pro aktivní sledování síťových služeb a aplikací (např. SSH, SMTP, HTTP, POP3, DNS, MySQL), zobrazování hodnot externích čidel (např. teplota) nebo sledování systémových prostředků jednotlivých zařízení (zatížení procesoru, využití paměti, disková kapacita, běžící služby a aplikace atd.)



Obrázek 3.1: Ukázka monitorovacího systému „Nagios“

Pokud program požadovanou službu nenabízí, lze ji doplnit pomocí jednoduchého skriptovacího jazyka nebo využít některý z řady volně dostupných doplňků. Síla Nagiosu nespočívá pouze v množství služeb, které lze sledovat, ale zejména v jejich integraci a možnostech rozhraní. Jednou z nejužitečnějších vlastností je definování hierarchie jednotlivých zařízení a služeb, kdy testování probíhá postupně, takže nedochází ke zbytečným chybovým hlášením – např. spadne-li webový server Apache, nemá význam testovat databázi, či nepracuje-li router, nemá smysl testovat zařízení za ním. Pro snazší přehled o stavu sítě a definování těchto závislostí nabízí Nagios přehlednou 2D a 3D mapu. Samozřejmostí jsou také souhrnné statistiky (s jednoduchou trendovou funkcí), omezení testování podle času (např. pouze během pracovní doby) a široké možnosti upozorňování (e-mail, IM, SMS, WAP atd.). I když je testování velmi rychlé, ve velkých sítích se ocení škálovatelnost a distribuovatelnost Nagiosu.

Nagios je bezpochyby jedním z nejlepších nástrojů pro komplexní moni-

toring. Na druhou stranu je nutné předpokládat složitější instalaci a zejména konfiguraci, jak jednotlivých modulů, tak hlavně při celkovém uzpůsobování systému konkrétní síti [5].

3.2 Monitorovací systém „Akk@da“

The screenshot shows the Akk@da web interface for a Cisco router. The top navigation bar includes 'general', 'alarms', 'stat', 'log', 'options', 'services', 'options', 'utilities', and 'rights'. The main content area is divided into two sections: 'collected information' and 'services'.

collected information:

- ip address: 10.1.9.3
- name: dcr-9-3
- descr: Cisco Internetwork Operating System Software IOS (tm) 3650 Software (C3650-IS-M), Version 12.2(26), RELEASE SOFTWARE (FC) Copyright (c) 1996-2004 by cisco Systems, Inc. Compiled Sat 31-Jul-04 02:56 by eakamas
- up time: timebicks: (L109243797) 128 days, 09:13:96.37
- contact: jsmth@foo.pl
- location: Long 19, Warszawa
- ip forwarding: forwarding

services:

name	error	last change	last check
ATM2/0	usage in: (397.08 bps); usage out: (185.08 bps); gts (test)	06/06/06 23:48:28	06/26/06 17:04:42
ATM2/0-aal5 layer		06/06/06 23:48:39	06/26/06 17:04:39
ATM2/0-atm layer		06/06/06 23:48:28	06/26/06 17:05:17
ATM2/0-0-aal5 layer	usage in: (0.00 bps); usage out: (0.00 bps); gts (test)	06/06/06 23:48:29	06/26/06 17:05:17
ATM2/0-0-atm subif	usage in: (0.00 bps); usage out: (0.00 bps); gts (test)	06/06/06 23:48:35	06/26/06 17:05:15
ATM2/0-011-aal5 layer	usage in: (436.05 bps); usage out: (187.87 bps); link to the Internet (gts, test)	06/06/06 23:48:42	06/26/06 17:04:43
ATM2/0-011-atm subif	usage in: (0.00 bps); usage out: (0.00 bps); link to the Internet (gts, test)	06/06/06 23:48:38	06/26/06 17:05:06
ethernet2/0	usage in: (209.53 bps); usage out: (243.80 bps); Corporate public LAN (62.65.43.32-47)	06/06/06 23:48:40	06/26/06 17:05:07
ethernet2/0/0	usage in: (3.74k bps); usage out: (5.79k bps); FrontEnd public LAN	06/06/06 23:48:38	06/26/06 17:05:06
Null0	usage in: (0.00 bps); usage out: (0.00 bps)	06/06/06 23:48:30	06/26/06 17:05:08
Spw	usage: (0.00 bps)	06/10/06 20:05:03	06/26/06 17:05:10
I/O	used: 83398705.00MB; 38.08%	06/20/06 15:33:24	06/26/06 17:05:06
Processor	used: 164.37960000.334.14%	06/06/06 23:48:26	06/26/06 17:04:31
Fan 1	state: normal	06/25/06 17:07:39	06/26/06 17:04:43
Fan 2	state: normal	06/25/06 17:09:09	06/26/06 17:04:44
Fan 3	state: normal	06/25/06 17:07:36	06/26/06 17:05:15
Fan 4	state: normal	06/25/06 17:07:59	06/26/06 17:04:44
Fan 5	state: normal	06/25/06 17:07:28	06/26/06 17:04:43
Fan 6	state: normal	06/25/06 17:07:58	06/26/06 17:04:43
Power Supply 1	state: normal; source: AC	06/25/06 17:08:02	06/26/06 17:04:50
Power Supply 2	state: normal; source: AC	06/25/06 17:07:52	06/26/06 17:05:03
10.1.9.2	remote AS: 32002; bgp state: established	06/26/06 08:11:57	06/26/06 17:04:31
10.1.9.4	remote AS: 32002; bgp state: established	06/24/06 07:32:28	06/26/06 17:04:42
217.17.34.29	remote AS: 15279; bgp state: established	06/06/06 23:48:56	06/26/06 17:05:12
TCP/IP	RTO: vanj; min 300; max 60000; TCP max connections: -1; default TTL: 255	06/06/06 23:49:17	06/26/06 17:04:29
NTP server	remote: 10.1.9.2; refid: 150.254.183.15; stratum: 2; delay: 0.780; offset: -0.283; jitter: 45.210	06/16/06 12:53:06	06/26/06 17:04:28

Obrázek 3.2: Ukázka monitorovacího systému „Akk@da“

Akk@da je relativně jednoduchý monitorovací systém pro malé a střední sítě založený na jazyce Perl, který využívá protokol SNMP i aktivní prohledávání pro zjišťování stavu v síti. Jedná se o relativně mladý projekt, který byl spuštěn koncem roku 2005 a dosud se nachází v beta verzi. Jeho instalace není zcela jednoduchá a některé funkce jsou zatím implementovány jen v omezené míře. Na druhou stranu zase přichází se zajímavými postupy, překvapivě rychlým a nenáročným získáváním údajů a zejména výborně propracovanou automatickou detekcí zařízení a služeb. Obdobně moderně působí i webové rohraní aplikace, využívající záložky a plovoucí okna,

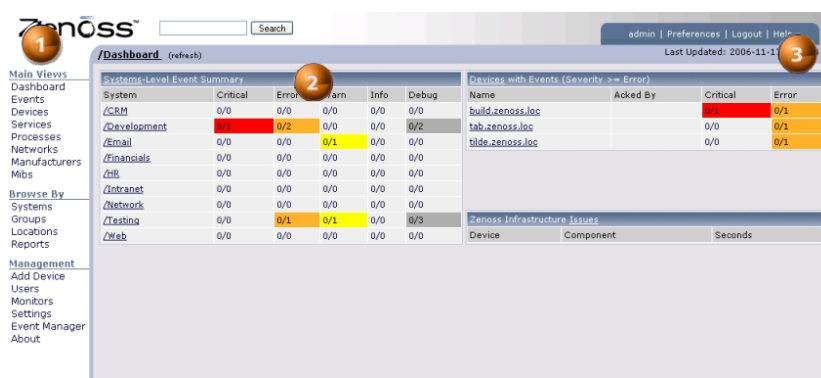
což podstatně přispívá k přehlednosti a umožňuje implementovat další funkce a doplňky bez změn stávajícího prostředí. Jednotlivé služby, zařízení a prostředky jsou řazeny ve stromové struktuře, kde lze libovolně definovat jejich skupiny a také využít automatického rozřazování například podle podsítě atd. Detailní nebo souhrnné informace se následně zobrazují v samostatném panelu, který je opět rozdělen na několik záložek. Statistiky si opět zaslouží velkou pochvalu - využívají dynamické grafy a patří k nejpřehlednějším mezi zmíněnými programy.

Akk@da je velmi moderní, i když zatím jednodušší systém s řadou zajímavých funkcí, přehledným rozhraním a výborně vyřešenými statistikami. Nevýhodou je složitější doplňování chybějících funkcí a zatím nepříliš přívětivá instalace [5].

3.3 Monitorovací systém „Zenoss“

Jedná se o projekt, který vychází z Nagiosu a dnes s ním velmi silně soupeří o nejvybavenější opensourcový monitorovací systém. I přesto, že zdědil všechny možnosti Nagiosu a je plně kompatibilní s jeho pluginy, řada funkcí byla kompletně přepsána, rozšířena a v neposlední řadě došlo k značné změně uživatelského rozhraní. Vylepšený vzhled je na první pohled nejvýraznější změnou, i když zdaleka ne nejdůležitější.

Po funkční stránce byl produkt značně rozšířen a kromě vlastností Nagiosu přináší například kompletně přepracovanou službu Auto-discovery, umožňující jednoduché automatické přidávání nových zařízení v síti, přičemž se nemezuje jenom na základní sledování. Dokáže přidat nejen jednotlivé stroje, ale i jejich komponenty (HDD, CPU atd.) a služby, které na nich běží. Další silnou stránkou jsou detailní přehledy, generování grafů a statistik i souhrnné výpisy. Zenoss dokáže nejen provádět vlastní měření a sledování, ale zpracuje logy a přehledy jiných systémů a zařízení, které dokonce ani nemusejí mít standardní formát, protože je možné definovat vlastní parsování pro libovolné výpisy. Velká část procesů je plně automatická, testy lze seskupovat



Obrázek 3.3: Ukázka monitorovacího systému „Zenoss“

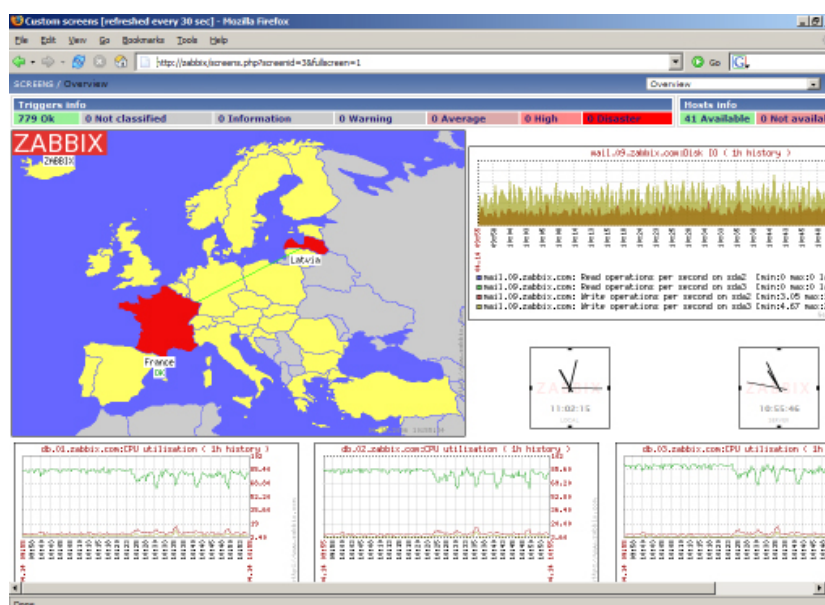
do skriptů, naplánovat jejich spuštění podle časnebo stavu dohlížených zařízení.

Zajímavostí je i licenční politika Zenossu, kdy celý systém a většina modulů jsou poskytovány jako open source, ale je možné si zaplatit podporu a některé specifické moduly. To umožňuje, aby jeho vývoj šel neustále velmi rychle kupředu [5].

3.4 Monitorovací systém „Zabbix“

Systém s komplexností mezi Akkadou a Zenossem, zaměřený především na větší sítě sází na jednoduché rozhraní, grafickou jednoduchost a extrémně rychlou práci. Mezi jeho zajímavými výsledky najdeme bezproblémové nasazení v síti s více než 5000 stanicemi a servery nebo schopnost pracovat na FreeBSD či MAC OS. Nabídka funkcí sice za Zenossem zaostává a chybí mu například i automatické detekce zařízení v síti, na druhou stranu ale jeho jednoduchost, nenáročnost a schopnost dohledu stanic s libovolným operačním systémem jistě kompenzuje tyto nedostatky.

Na rozdíl od ostatních řešení nevyužívá primárně aktivní zjišťování stavu vzdálených zařízení a zprávy SNMP, ale práci agentů – rezidentní hlídači jsou k dispozici pro 14 platforem, přičemž kompilace pro libovolnou uni-



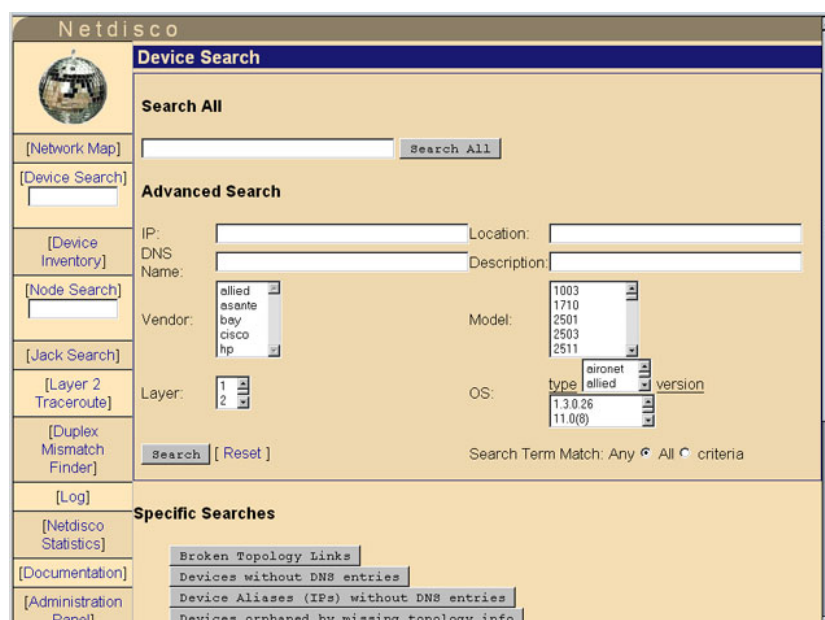
Obrázek 3.4: Ukázka monitorovacího systému „Zabbix“

xovou distribucí tento počet ještě rozšiřuje. Mezi podporovanými systémy najdeme například Solaris 9 na UltraSparc nebo True64 na Alpha. Zabbix zatím nepodporuje automatickou detekci zařízení v síti, ale přichází se zajímavým konceptem šablon, určeným pro přidání většího množství shodně konfigurovaných stanic – zadá se pouze obecné schéma spolu s rozsahem IP adres a Zabbix na tyto adresy „doručí“ své agenty. Ti se následně zaregistrují na serveru se systémem a odesílají pravidelná hlášení. Zabbix má samozřejmě i nástroje pro aktivní monitorování, ale jedná se spíše o základní úlohy typu ping a podobně. Naopak rozhraní a jeho přehlednost i při zobrazení stovek zařízení patří k jednoznačným kladům.

K největším výhodám systému patří jeho nenáročnost (vše potřebné zajišťují jeho agenti) a tím též schopnost centrálně monitorovat značně rozsáhlou síť. Pokud následující verze přinese slibované funkce (automatizace, distribuované monitorování, monitorování webových aplikací aj.), bude se jednat o ještě zajímavější řešení. I zde existuje komerční varianta s podporou a přídatnými moduly, celek je ale stále open source [5].

3.5 Monitorovací systém „NetDisco“

Projekt NetDisco je vhodný pro střední a velké sítě na akademické půdě a primárně je určen k monitorování aktivních síťových prvků typu switch či router, které dokáže i vzdáleně spravovat (zejména povolování a zakazování portů patří k velmi přehledným a propracovaným). Využívá technologii SNMP a podporuje všechny tři verze tohoto protokolu. Ve spojení s CDP (Cisco discovery protocol) lze využít automatickou detekci v síti. NetDisco zvládá také automatickou organizaci jednotlivých prvků do skupin, ať již podle typu zařízení, modelu nebo použitého operačního systému. NetDisco rozdělí síť na jednotlivé nody a ke každému uzlu následně vede kompletní historii. Veškerá data se získávají pomocí SNMP dotazů na DNS, takže systém je schopen pracovat se stovkami uzlů bez drastických nároků na hardware. Kromě funkcí pro dohled obsahuje i funkce bezpečnostní (např. Wireless Access Point locator) a samozřejmě souhrnné statistiky. Velmi přehledná a interaktivní je mapa sítě, z níž lze jednotlivé prvky přímo ovládat.



Obrázek 3.5: Ukázka monitorovacího systému „NetDisco“

V případě NetDisca se nejedná o univerzální ale více zaměřený nástroj, který nestaví na kompletním přehledu o každé položce v síti, ale zaměřuje se primárně na přehled o stavu celé sítě a její klíčové prvky. Spolu s možnostmi vzdálené správy se stává vhodný právě pro akademické sítě a velké sítě ještě s větším množstvím uživatelů [5].

Kapitola 4

Monitorovací systém Nagios

Nagios je open source monitorovací software založen na UNIXové platformě s webovým rozhraním a konzolí. Nagios může monitorovat převážnou část výpočetní techniky např. servery, síťová zařízení a aplikace, které využívají TCP/IP protokol. Nagios může být provozován pod operačními systémy Microsoft Windows, Unix/Linux, Novell NetWare a dalšími operačními systémy [2].

4.1 Architektura systému Nagios

Hlavní částí Nagiosu je proces nagios. Tento proces po spuštění načte z konfiguračním souborů nastavení a začne monitorovat. Informace o výsledcích testů ukládá do souboru, z jiného souboru načítá příkazy. Pro zobrazení informací o stavu slouží webové rozhraní, které je realizováno několika CGI skripty. Tyto CGI skripty přistupují do souboru se stavy a zobrazují je v rozumné formě jako HTML stránky – pro přístup k Nagiosu proto lze využít HTML prohlížeč. Z webového rozhraní je možné do Nagiosu zasílat i jednodušší příkazy.

Nevyhovuje-li koncovému uživateli z jakéhokoliv důvodu webové rozhraní, je možné webové rozhraní přizpůsobit či napsat celé prezentační rozhraní dle vlastních požadavků. Samotný systém byl navržen na Linuxu, mo-

monitorovat však lze téměř cokoliv od počítačů s UNIXy, Windows, přes telefonní ústřednu. Celý systém je navržen logicky a pochopitelně a je dobře škálovatelný a distribuovatelný [2].

4.2 Hardwarové požadavky na systém

Jak již bylo zmíněno Nagios byl primárně navržen pro operační systém Linux. Není závislý na konkrétní distribuci Linuxu a je možné jej implementovat na preferované distribuci. Výkonnost serveru a diskového prostoru je přímo úměrná požadavkům na monitorování sítě. Obrázek č. 4.1 pro představu demonstruje vzorové hardwarové požadavky ve spojení s množstvím monitorovacích služeb [2].

# of Hosts Monitored	# of CPUs	CPU Speed	Memory	Disk Space
< 100	1	800MHz+	512MB+	5GB+
100–500	1	1GHz+	1GB+	10GB+
500–1000	1+	3GHz+	1GB+	20GB+
> 1000	1+	3GHz+	2GB+	40GB+

Obrázek 4.1: Porovnání hardwarových požadavků na systém

4.3 Instalace Nagiosu

Před samotnou instalací Nagiosu je nutné mít nainstalovány podpůrné programy, kterými jsou především Apache, GD knihovny a další utility Nagiosem využívané. Předpokládám, že tyto programy již jsou součástí operačního systému. Nejdříve je nutné zvolit alternativu ukládání dat v Nagiosu. Mezi nejčastější možnosti patří ukládání informací v textových souborech (nagios-text), ukládání dat v MySQL databázi (nagios-mysql) či PostgreSQL databázi (nagios-psql). V této práci bude Nagios spuštěn s ukládáním do textových souborů. Dále máme možnost výběru instalace z předpřipravených balíčků nebo kompilací zdrojových kódů [6].

```

archive:~#
archive:~# wget http://easynews.dl.sourceforge.net/sourceforge/nagios/nagios-2.0rc1.tar.gz
--13:08:54-- http://easynews.dl.sourceforge.net/sourceforge/nagios/nagios-2.0rc1.tar.gz
=> `nagios-2.0rc1.tar.gz.1'
Resolving easynews.dl.sourceforge.net... done.
Connecting to easynews.dl.sourceforge.net[69.16.168.245]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1,731,687 [application/x-tar]

100%[=====>] 1,731,687 427.15K/s ETA 00:00

13:08:58 (427.15 KB/s) - `nagios-2.0rc1.tar.gz.1' saved [1731687/1731687]

archive:~# md5sum nag
nag nagios-2.0rc1.tar.gz.1 nagios_skripts
nagios-2.0rc1.tar.gz nagios_by_ssh.txt
archive:~# md5sum nagios-2.0rc1.tar.gz
a3d37eal9bb4cfe353c247de941775 nagios-2.0rc1.tar.gz
archive:~# tar -xvzf nagios-2.0rc1.tar.gz
archive:~# groupadd nagios
archive:~#
archive:~# useradd -g nagios -M nagios
archive:~#

```

Obrázek 4.2: Ukázka stáhnutí zdrojových kódů Nagiosu

```

./configure --prefix=/usr/local/nagios --with-htmlurl=/nagios/
--with-cgiurl=/nagios/cgi-bin --with-nagios-user=nagios
--with-nagios-group=nagios --with-command-group=ncmd

```

Obrázek 4.3: Ukázka kompilace zdrojových kódů Nagiosu

4.4 Instalační proces ze zdrojových kódů

Zdrojové kódy monitorovacího systému lze stáhnout z oficiálních www stránek Nagiosu <http://www.nagios.org/download/>. V současné době je poslední verze Nagiosu 2.0. Z oficiální www stránky budete odkázáni na Sourceforge (www.sourceforge.net), kde si můžete vybrat neoptimálnější download zdrojových kódů Nagiosu. Po jejich stáhnutí a rozpakování je nutné vytvořit skupinu a uživatele Nagios viz obrázek č. 4.2.

Parametr `-g -u useradd` vloží nově vytvořeného uživatele do skupiny nagios a parametr `-M` způsobí, že se uživateli nagios nevytvoří domovský adresář. V tomto okamžiku můžeme přejít ke kompilaci monitorovacího systému. Kompilaci spustíme příkazem `./configure` přesná definice je na obrázku č. 4.3.

Prefix nám specifikuje adresář základního nastavení pro Nagios server, který se nachází v `/usr/local/nagios`. Druhý a třetí parametr nám specifikuje nastavení pro webovou konzoli Nagiosu. Parametr `-with-htmlurl` specifikuje URL pro Nagios, která je přednastavena na `/nagios/`, tzn. že pokud se budeme připojovat pomocí webového prohlížeče do konzole Nagiosu,

```
*** Compile finished ***

If the main program and CGIs compiled without any errors, you
can continue with installing Nagios as follows (type 'make'
without any arguments for a list of all possible options):

make install
- This installs the main program, CGIs, and HTML files

make install-init
- This installs the init script in /etc/rc.d/init.d

make install-commandmode
- This installs and configures permissions on the
  directory for holding the external command file

make install-config
- This installs *SAMPLE* config files in /usr/local/nagios/etc
  You'll have to modify these sample files before you can
  use Nagios. Read the HTML documentation for more info
  on doing this. Pay particular attention to the docs on
  object configuration files, as they determine what/how
  things get monitored!
```

Obrázek 4.4: Úkazka úspěšného zkompileování Nagiosu

budeme udávat URL v tomto tvaru `http://hostname/nagios`. Třetí parametr `-with-cgicurl` specifikuje URL pro CGI skripty. Toto je defaultně nastaveno do `/nagios/cgi-bin/`. Poslední dva parametry nám specifikují uživatele a skupinu, kteří mají oprávnění spouštět Nagios server proces. Následně spustíme příkaz `make all` a pokud kompilace proběhne bez chyb, měli bychom obdržet informaci shodnou s obrázkem č. 4.4 [2].

4.5 Instalační proces z balíčků

Druhou možností, jak nainstalovat monitorovací systém je z předpřipravených balíčků. Nagios je součástí drtivé většiny distribucí Linuxu. Samotná instalace může proběhnout buďto pomocí příkazu `apt-get install` (viz obrázek č. 4.5) nebo pomocí `dselect` konfiguratoru (viz obrázek č. 4.6).

Při instalaci z předpřipravených balíčků systém uživatele informuje o závislostech, které je rovněž nutno nainstalovat. Podrobný průvodce instalace z instalačních balíčků je uveden v praktické části této bakalářské práce. Jed-

```

apps:~#
apps:~# apt-get install nagios-text
Reading Package Lists... Done
Building Dependency Tree... Done
The following extra packages will be installed:
  libnet-smmp-perl libradius1 nagios-common nagios-plugins qstat radiusclient1 snmp
Suggested packages:
  libdigest-hmac-perl libio-socket-inet6-perl ntp
Recommended packages:
  perl-modules
The following NEW packages will be installed:
  libnet-smmp-perl libradius1 nagios-common nagios-plugins nagios-text qstat radiusclient1 snmp
0 upgraded, 8 newly installed, 0 to remove and 444 not upgraded.
Need to get 3591kB of archives.
After unpacking 9212kB of additional disk space will be used.
Do you want to continue? [Y/n] █

```

Obrázek 4.5: Ukázka začátku instalace Nagiosu pomocí příkazu `apt-get`

```

apps.zsf.jcu.cz - PuTTY
dselect - recursive package listing
mark:+/*/- verbose:v help:?
EIO M Pri Section Package Description
--
* Opt net nagios-nrpe- Nagios Remote Plugin Executor Plugin
* Opt net nagios-pgsql A host/service/network monitoring and management system
* Opt net nagios-mysql A host/service/network monitoring and management system
* Opt net nagios-text A host/service/network monitoring and management system
* Opt net nagios-common A host/service/network monitoring and management system
* Xtr net nagios-plugins Plugins for the nagios network monitoring and management system
* Opt games qstat Command-line tool for querying quake (and other) servers
* Opt net snmp NET SNMP (Simple Network Management Protocol) Apps
* Xtr admin radiusclient /bin/login replacement which uses the RADIUS protocol for authentication.
* Opt perl libnet-smmp- Script SNMP connections
* Xtr libs libradius1 /bin/login replacement with RADIUS. Shared lib to used by programs.
* Opt perl libcrypt-des Perl DES encryption module
* Opt perl libdigest-hm create standard message integrity checks

nagios-text not installed ; install (was: purge). Optional
nagios-nrpe-plugin depends on nagios
nagios-text provides nagios

interrelationships affecting nagios-text:

```

Obrázek 4.6: Ukázka začátku instalace Nagiosu pomocí příkazu `dselect`

ním z nepostradatelných balíčků je `nagios-plugins` a `nagios-common`, doporučuji rovněž instalovat `nagios-nrpe-plugin` (viz kapitola Možnosti vzdáleného monitorování služeb) [2].

4.6 Konfigurace webové konzole

Posledním krokem instalace Nagiosu je konfigurace webové konzole. Existují dvě možnosti jak nakonfigurovat webový server Apache pro potřeby Nagiosu. První a doporučenou metodou je konfigurace, která je umístěna v prostoru webového serveru Apache. Po nakonfigurování touto variantou lze přistupovat k webové konzoli přes URL `http://pc.yourdomain.cz/nagios` (viz konfigurace webového serveru varianta č. 1). Druhou alternativou je konfigurace virtuálního serveru. Přístup na webovou konzoli poté bude přes URL

<http://nagios.yourdomain.cz/> (viz konfigurace webového serveru varianta č. 2).

4.6.1 Konfigurace webového serveru - varianta č. 1

Veškerá potřebná editace bude probíhat v souboru `httpd.conf`. Nejprve je potřeba umístit do konfiguračního souboru informace o CGI skriptech viz obrázek č. 4.7. Dále je nutné vložit do konfiguračního souboru informace o umístění souborů monitorovacího systému viz obrázek č. 4.8.

```
ScriptAlias /nagios/cgi-bin /usr/local/nagios/sbin
<Directory "/usr/local/nagios/sbin">
    AllowOverride None
    Options ExecCGI
    Order allow,deny
    Allow from all
</Directory>
```

Obrázek 4.7: Ukázka modifikace souboru `/etc/apache/httpd.conf`

```
Alias /nagios /usr/local/nagios/share
<Directory "/usr/local/nagios/share">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
</Directory>
```

Obrázek 4.8: Druhá modifikace souboru `/etc/apache/httpd.conf`

V tomto okamžiku je nutné restartovat webový server a překontrolovat logovací soubory, zda nedošlo k nesrovnalostem [2].

4.6.2 Konfigurace webového serveru - varianta č. 2

Při konfiguraci monitorovací webové konzole jako virtuální domény je nutné rovněž modifikovat soubor `/etc/apache/httpd.conf`. Nejprve je nutné povolit virtuální domény a poté umístit do konfiguračního souboru shodné

informace jako u varianty č. 1. Potřebná kompletní konfigurace je znázorněna na obrázku č. 4.9. Po dokončení konfigurace a restartu bychom na zvoleném URL měli dostat podobnou úvodní stránku jako na obr. č. 4.10 [2].

```
<VirtualHost nagios.yourdomain.com>
  ServerAdmin admin@puppy.yourdomain.com
  DocumentRoot /usr/local/nagios/share
  ServerName nagios.yourdomain.com

  ScriptAlias /nagios/cgi-bin/ /usr/local/nagios/sbin/
  <Directory "/usr/local/nagios/sbin/">
    AllowOverride None
    Options ExecCGI
    Order allow,deny
    Allow from all
  </Directory>

  Alias /nagios/ /usr/local/nagios/share/
  <Directory "/usr/local/nagios/share">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
  </Directory>
</VirtualHost>
```

Obrázek 4.9: Modifikace souboru `httpd.conf` pro virtuální doménu



Obrázek 4.10: Ukázka úvodní stránky systému Nagios

Kapitola 5

Konfigurace základních objektů

Aby mohl Nagios správně fungovat, je nutné nadefinovat jednotlivá zařízení. Nagios pojmenovává tato zařízení slovem **host**. Rovněž je nutné definovat určité atributy a funkce jednotlivým hostům. Funkce a atributy Nagios pojmenovává slovem **services**. Takto může být označen např. FTP server, e-mail server, různé aplikace či databáze. Services mohou rovněž zahrnovat některé atributy zařízení či aplikací, kterými jsou např. volné místo na pevném disku nebo počet spuštěných procesů konkrétní aplikace. Dále zde můžeme rovněž definovat pracovníky k jednotlivým zařízením a jak mají být případně kontaktováni. Pracovníci, kteří mají být informováni o událostech spojených se zařízeními (hosts) nebo službami (services) se nazývají **contact**. Dále v textu budou používány termíny **host**, **service** a **contact**, nikoliv jejich ekvivalenty v českém jazyce, protože anglické výrazy lépe vystihují jednotlivé prvky systému Nagios.

Nejdříve musíme definovat zařízení, jeho atributy a pracovníky spojené s ním a až poté definujeme mechanismy pro monitorování těchto zařízení a služeb. Kontaktování zařízení nebo služby využívající nějaký příkaz se nazývá **check**. Otestováním (check) nelze chápat výsledek testu např. pokud budeme testovat, zda nedochází místo na serveru, nechápeme **checkem** vrácenou hodnotu v procentech. Také nechápeme **checkem** určení stavu zařízení nebo služby. Pokud na pevném disku dochází místo, tak se status služby

může změnit. Tuto skutečnost nazýváme **notification** (oznámení). Jedná se o zprávu, kterou Nagios sdělí změnu v zařízení nebo službě např. e-mailem, SMS zprávou atd.

Nagios server, webová konzole a samotná konfigurace monitorování je kontrolována několika konfiguračními soubory, které jsou obvykle v adresáři `/etc/nagios` nebo `/usr/local/nagios/etc/`. V tomto adresáři jsou tři skupiny konfiguračních souborů. První skupinou jsou soubory týkající se Nagios serveru a webové konzole. Jedná se o soubory `nagios.cfg` a `cgi.cfg`. Druhou skupinou jsou soubory, které zahrnují informace týkající se databázových připojení a maker. Konfigurační soubory jednotlivých zařízení jsou třetí skupinou souborů. V následující tabulce č. 5.1 jsou definovány objektové typy, jež mohou být v Nagiosu použity.

host	host je skutečné zařízení (např. servery, routery, firewally)
hostgroup	skupina zařízení, které mají společnou vlastnost (např. umístění)
service	služby provozované na zařízení např. SMTP, HTTP, SSH atd.
servicegroup	skupina služeb, které mají nějakou společnou vlastnost
contact	prvek, který bude kontaktován při splnění určitých podmínek
contactgroup	skupina prvků, která má nějakou společnou vlastnost
timeperiod	definice časových intervalů např. otevírací doba, víkendy atd.
command	příkazy, které spouštějí nějaké nedefinované akce
servicedependency	umožní službě nebo službám být závislé na jiných službách
serviceescalation	zprostředkovává proces oznámení pro službu
hostdependency	umožní zařízení nebo zařízením být závislé na jiných zařízeních
hostescalation	zprostředkovává proces oznámení pro zařízení
hostextinfo	upravuje způsob jakým se zařízení prezentuje přes webovou konzoli
serviceextinfo	Upravuje způsob jakým se služba prezentuje přes webovou konzoli

Tabulka 5.1: Tabulka objektových typů využívající Nagios

Veškeré konfigurační soubory se definují v základním souboru `nagios.cfg`, na každém řádku se definuje jeden konfigurační soubor. Po instalaci budou v souboru `nagios.cfg` definovány odkazy na soubory viz obrázek č. 5.1 [3].

```
cfg_file=/usr/local/nagios/etc/checkcommands.cfg
cfg_file=/usr/local/nagios/etc/misccommands.cfg
cfg_file=/usr/local/nagios/etc/minimal.cfg
#cfg_file=/usr/local/nagios/etc/contactgroups.cfg
#cfg_file=/usr/local/nagios/etc/contacts.cfg
#cfg_file=/usr/local/nagios/etc/dependencies.cfg
#cfg_file=/usr/local/nagios/etc/escalations.cfg
#cfg_file=/usr/local/nagios/etc/hostgroups.cfg
#cfg_file=/usr/local/nagios/etc/hosts.cfg
#cfg_file=/usr/local/nagios/etc/services.cfg
#cfg_file=/usr/local/nagios/etc/timeperiods.cfg
#cfg_file=/usr/local/nagios/etc/hosttextinfo.cfg
#cfg_file=/usr/local/nagios/etc/serviceextinfo.cfg
```

Obrázek 5.1: Ukázka souboru `nagios.cfg` a odkazu na konfig. soubory

5.1 Definice a testování zařízení

Jak již bylo uvedeno dříve, `hosts` jsou fyzická zařízení v síti jako např. servery, routery, switche a další části síťové infrastruktury. Další definice může být, že se jedná o veškeré prvky v síti, které disponují s vlastní IP adresou a MAC (Media Access Control) adresou.

5.1.1 Definice zařízení (host)

Každé zařízení je specifikováno několika definicemi, z nichž některé jsou povinné a jiné volitelné. Ukázka č. 5.2 zobrazuje zařízení se všemi povinnými parametry.

Nejprve je definováno jméno zařízení, dále stručný popis a přidělená IP adresa. Dále je definováno, že server má být testován v časovém intervalu 24x7 tj. 24 hodin denně, 7 dní v týdnu. Pokud server přestane plnit své povinnosti, které jsou monitorovány, informuje o této skutečnosti správce a techniky v jakoukoliv hodinu. Tyto informace bude zasílat každých 30 minut bez ohledu na to, zda je noc či den. Poslední definice nám udává za jakých okolností má být informace zaslána, v tomto případě `down`, `unreachable`, `recovery`.

Volitelné parametry jsou např. `parents`, což nám specifikuje, zda je po-

```

define host {
    host_name          server.yourdomain.cz
    alias              Hlavní server
    address            192.168.0.1
    check_period       24x7
    max_check_attempts 1
    contact_groups     spravci, technici
    notification_interval 30
    notification_period 24x7
    notification_options d,u,r

```

Tabulka 5.2: Ukázka definice zařízení v Nagiosu

pisované zařízení na jiném závislé (např. pokud bude nedostupný server a zároveň i switch, který je mu nadřizený, bude se upozornění zasílat pouze na switch) a `hostgroups`, které nám specifikuje skupinu, do níž zařízení patří (např. routery).

5.1.2 Testování zařízení (host)

V tomto okamžiku, kdy máme zařízení nastaveno, můžeme přistoupit k definování pravidel u testovaného zařízení. Tabulka č. 5.3 shrnuje parametry spojené s testováním zařízení.

<code>check_command</code>	příkaz, který má otestovat zařízení	nepovinné
<code>check_period</code>	specifikuje kdy má být zařízení testováno	povinné
<code>max_check_attempts</code>	počet testovacích pokusů, po kterých má být odeslána informace	povinné
<code>check_interval</code>	časový interval mezi jednotlivými testy	nepovinné
<code>active_checks_enabled</code>	specifikuje aktivní testy pro zařízení	nepovinné
<code>passive_checks_enabled</code>	specifikuje pasivní testy pro zařízení	nepovinné

Tabulka 5.3: Parametry spojené s testováním zařízení

První parametr Nagiosu sděluje, jaký příkaz má být použit pro testování zařízení. Většina testů je založena na potvrzení, že zařízení je aktivní a odpoví na testování. Typickým příkladem je příkaz `ping`. Pokud nepoužijeme tento parametr Nagios považuje zařízení za stále aktivní. Praktické využití je např. u tiskáren či kopírovacích strojů. Dalším parametrem je `check_periods`, který nám udává okamžik, kdy má být zařízení testováno. Můžeme požadovat, aby zařízení bylo testováno pouze v pracovní době a není nutné jej testovat o víkendech. Parametr `max_check_attempts` udává počet opakujících se testů do doby od chybového hlášení. Jinak řečeno, než Nagios vygeneruje informaci o problému.

Při každém definování testů je nutné uvést konkrétní typy oznámení, jež jsou vysvětleny v tabulce č. 5.4.

d	odešle oznámení, když zařízení je DOWN
u	odešle oznámení, když zařízení je UNREACHABLE
r	odešle oznámení, když zařízení je RECOVERY
n	neodešle žádné oznámení (No)
f	odešle oznámení, když zařízení začne nebo ukončí „Flapping“

Tabulka 5.4: Možnosti parametru `notification_options` u zařízení

První volba udává vygenerování a zaslání oznámení v případě, kdy je status zařízení registrován jako `DOWN`. Druhý typ oznámení je `UNREACHABLE`, který je vyvolán v případě, když je zařízení nedostupné. Tento stav nastane v situacích, kdy máme definován server, jehož `parent` je např. aktivní prvek, který má status `DOWN`. Poté každé další zařízení umístěné za tímto aktivním prvkem bude vyhodnoceno se statusem `UNREACHABLE`. Status `RECOVERY` nastává v situaci, kdy zařízení začalo opět komunikovat a předcházející stav byl non-OK (tento stav je buďto `DOWN` nebo `UNREACHABLE`). Volbu `n` využijeme v případě, pokud si nepřejeme být informováni o změnách stavu zařízení. Tato volba musí být uvedena samostatně a nesmí být v kombinaci s ostatními volbami. Poslední volbou je oznámení při `flappingu`. Nagios `flappingem` označuje situaci, kdy zařízení rapidně mění svůj stav [2].

5.2 Definice a testování služby (service)

Dalším krokem po nadefinování zařízení v Nagiosu je definice služby, kterou chceme monitorovat. Služby jsou složeny z širokého škály možností a velkého počtu pluginů, jež nám Nagios nabízí. Mezi nejjednodušší síťové služby patří např. monitoring SMTP či HTTP služeb. Nicméně lze také monitorovat služby vzdálených zařízení, databáze, logy atd. V tabulce č. 5.5. je ukázka definice služby.

```
define service {
    service_description    SMTP
    host_name              server.zf.jcu.cz
    check_command          check_smtp
    max_check_attempts    3
    normal_check_interval 5
    retry_check_interval  1
    check_period           24x7
    notification_interval 60
    notification_period   24x7
    notification_options  w,u,c
    contact_groups        spravci, technici
}
```

Tabulka 5.5: Ukázka nadefinování služby v Nagiosu

Parametry uvedené při nastavení služby jsou obdobné jako u definice zařízení. Je zde navíc specifikován typ vykonávaného příkazu `check_smtp` a testovací intervaly.

Také po nadefinování služby je nutné doplnit parametry nutné ke správnému testování služby. Drtivá část parametrů se opět překrývá s parametry zařízení. Konkrétní typy stavů, které mohou nastat při testování služeb, jsou vysvětleny v tabulce č. 5.6 [2].

c	odešle oznámení, když je služba v kritickém stavu CRITICAL
f	odešle oznámení, když služba začne nebo ukončí Flapping
n	neodešle žádné oznámení No
r	odešle oznámení, když služba je RECOVERY
w	odešle oznámení, když je služba ve varovném stavu WARNING
u	odešle oznámení, když služba je UNREACHABLE

Tabulka 5.6: Možnosti parametru `notification_options` u služeb

5.3 Definice kontaktu (`contact`)

Poté je nutné nadefinovat kontakty pracovníků, kterým má být odesláno oznámení o aktuálním stavu sítě. Tabulka č. 5.7 zobrazuje nadefinování kontaktu.

```

define contact {
    contact_name           radek
    alias                  Radek Cerny
    contact_groups         spravci
    service_notification_period 24x7
    host_notification_period 24x7
    service_notification_options w, u, c, r
    host_notification_options d, u, r
    service_notification_command notify-by-email
    host_notification_command host-notify-by-email
    email                  radek@domain.com
    pager                  12345@pager.com
    address                 555-1234-888

```

Tabulka 5.7: Ukázka definování kontaktu

Výše uvedená ukázka definuje osobu ze skupiny `spravci` jménem `radek`, který je informován o stavu sítě 24 hodin denně včetně víkendů. Na email jsou zasílána oznámení v případě, že některé zařízení není dostupné, začne-li

komunikovat nebo je-li problém u nadřazeného zařízení [2].

5.4 Definice skupin (hostgroups)

Praktickou funkcí je rovněž vytváření skupin zařízení podle námi definovaných pravidel. V praxi většinou dochází k vytváření skupin podle typu zařízení či podle subjektu, který je se zařízením spojen. Výhodou takto vytvořených skupin je především efektivnější vyhodnocování statistik, různých trendů či jiných parametrů, posuzovaných nejen na určitých zařízeních, ale také na skupinách. Ty rovněž zvyšují přehlednost monitorovacího systému. Definice skupiny znázorňuje ukázka č. 5.8.

```
define hostgroup {  
    hostgroup_name    Pclinux  
    alias             Linux servers  
    members          server.domain.com, server1.domain.com
```

Tabulka 5.8: Ukázka definování skupin

První parametr udává pojmenování skupiny a druhý alias této skupiny. Do posledního parametru definujeme výčtem veškeré zařízení, které do této skupiny zahrnujeme. Obdobným způsobem je možné definovat i skupiny služeb [2].

5.5 Definice časového intervalu (timeperiod)

Poslední důležitou informací, kterou nemusíme definovat, je vytvoření časových intervalů, v nichž má monitorovací systém odesílat oznámení o vzniklých stavech. Defaultní nastavení zahrnuje několik intervalů, kterými jsou zejména 24x7 (vždy), mimo víkendy a pouze v pracovní době atd.

Kapitola 6

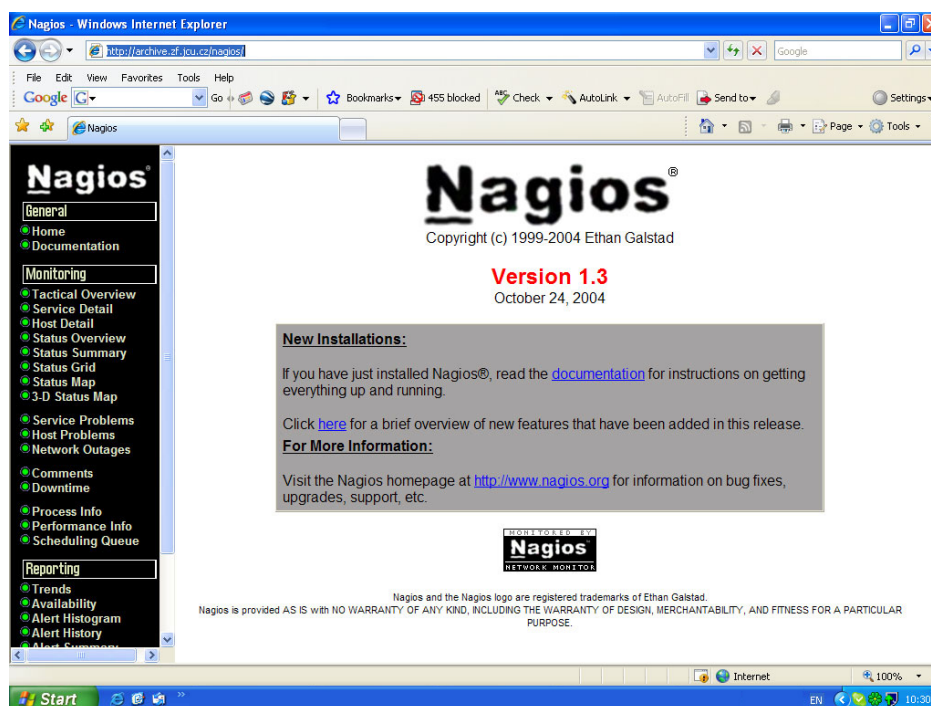
Základní operace v Nagiosu přes WWW

Webový přístup do monitorovacího systému je asi nejvhodnější nástroj pro správu, provedení změn a zjišťování aktuálních informací o stavu sítě. Mnoho organizací využívá tuto konzoli jako jedno ze základních monitorovacích center v počítačových pracovištích. Webová konzole je rozdělena do dvou částí. V první části je navigační panel a v druhé části je prostor pro zobrazování požadovaných informací vyvolaných z navigačního panelu. Tato výchozí obrazovka je znázorněna na obrázku č. 6.1.

Levé menu je rozděleno do několika oddělených sekcí. Těmito sekcemi jsou: „General“ pro návrat na úvodní obrazovku a možnost využití dokumentace; „Monitoring“ zahrnující řadu nástrojů pro přehled aktuálního stavu; „Reporting“ zahrnující veškeré statistické informace z historie a „Configuration“ umožňující shlédnutí aktuální konfigurace monitorovaných zařízení a služeb.

6.1 Sekce „Monitoring“

Sekce monitorování v hlavním menu je složena ze mnoha možných pohledů na monitorovací prostředí. Kromě toho také obsahuje odkazy na infor-



Obrázek 6.1: Úvodní obrazovka monitorovacího systému

mace o procesech, chování jednotlivých zařízení, testovaných služeb a grafickou reprezentaci monitorovaných prvků.

6.1.1 Tactical Monitoring Overview

První pohled je nazván „Tactical Monitoring Overview“ viz obrázek č. 11.1 a zobrazuje uživateli nejstručněji stav monitorované sítě. Prostor je rozdělen do 6 samostatných částí. První část nás informuje o aktuálním čase a aktuálně přihlášeném uživateli. Druhou částí je „Monitoring Performance“ zahrnující statistiky o průběhu testování zařízení a služeb. Rovněž znázorňuje celkový počet aktivního a pasivního testování. Části „Network Health“ a „Network Outage“ slouží pro grafickou reprezentaci „zdraví“ monitorované sítě. Ostatní sekce umístěné ve spodní části obrazovky nás souhrnně informují o jednotlivých stavech zařízení, služeb a zakázaných či povolených testovacích prvků.

6.1.2 Service Detail

Další položkou v menu jsou detailní informace o monitorovaných službách viz. obrázek č. 11.2. Jedná se převážně o nejčastější odkaz, který uživatele informuje podrobně o zařízení a jeho službách, jejich stavu, čase posledního testování, jak dlouho je služba testována a výstupu testování. Po kliknutí na odkaz u každé služby, můžeme vykonávat různé operace, kterými je pozastavení testování, opětovné aktivování, nastavení časových intervalů atd.

6.1.3 Host Detail

Dalším odkazem je „Host Detail“ viz obrázek č. 11.3, který je podobný odkazu Service Detail s tím rozdílem, že se více zaměřuje na zařízení než na služby. Znárodnuje seznam všech monitorovaných zařízení. V záhlaví jsou znázorněny souhrnné informace o stavech zařízení a službách. Samotný výpis zařízení je rozdělen do několika sloupců, které obsahují název zařízení, aktuální stav, čas posledního testování a časový interval, po který je zařízení systémem monitorováno. Tyto informace je možné řadit podle preferovaných kritérií. Shodně jako u služeb je možné po kliknutí na zařízení vykonávat operace spojené s tímto zařízením např. pozastavení testování, pozastavení zasílání oznámení kontaktní skupině atd.

6.1.4 Ostatní odkazy v sekci „Monitoring“

Sekce „Monitoring“ obsahuje řadu dalších pohledů od různých kombinací monitorovaných zařízení a služeb, výpisu služeb či zařízení s problémovým stavem, grafického znázornění, zobrazení zařízení seskupených do skupin, informací o procesech samotného monitorovacího systému, až po časové rozvržení testování apod.

6.2 Sekce „Reporting“

Sekce „Reporting“ zahrnuje řadu výstupů o monitorovaných zařízeních a službách, ale také informace o upozornění, událostech a oznámení, které monitorovací systém vygeneroval. Výstupy zahrnují detailní informace o dostupnosti služeb či skupin služeb a trendy s nimi spojené. Jednotlivé odkazy jsou vysvětleny v tabulce č. 6.1.

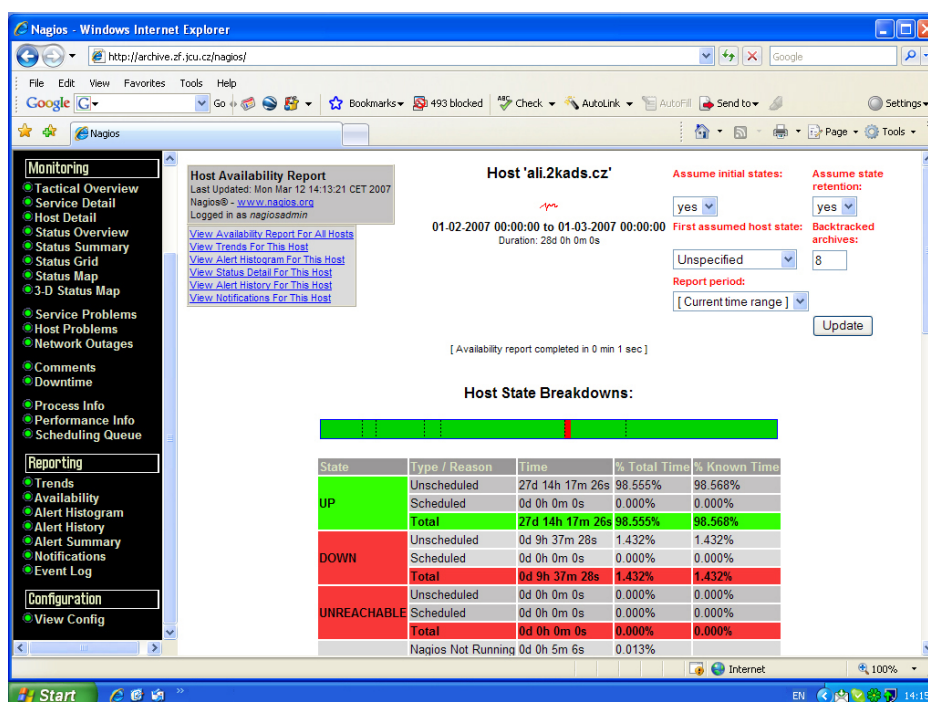
Trends	trend historických stavů pro zařízení nebo služby
Availability	procentní dostupnosti jednotlivých skupin nebo jednotlivých zařízení a služeb
Alert Histogram	diagram zobrazující upozornění spojené se zařízením nebo službou
Alert History	historie všech upozornění pro všechny zařízení a služby
Alert Summary	volitelně konfigurovatelný report zahrnující upozornění
Notification	volitelně konfigurovatelný report zahrnující oznámení
Event Log	report zobrazující veškeré události

Tabulka 6.1: Popis odkazů sekce „Reporting“ webové konzole

Blíže se zaměřím pouze na dva reporty, a to report „Availability“ a „Event Log Report“. Ostatní reporty převážně vycházejí ze stejného základu a v rozsahu této práce není prostor pro jejich bližší nastínění.

6.2.1 Report „Availability“

Pravděpodobně nejvíce využívaný výstup ze sekce reportů je „Availability Report“. Po vybrání tohoto reportu je nutné zvolit oblast, o jaké si přejeme být informováni. System dává na výběr možnost jednotlivé služby, zařízení nebo skupiny služeb. Po výběru budeme dále dotázáni na konkrétní zařízení a v posledním kroku vybereme časový interval, pro který si přejeme report vygenerovat. Následně obdržíme grafické i statistické informace o jeho korektním běhu, výpadcích, nerozpoznaných stavech, včetně samostatného rozčlenění pro každou službu a kompletní log týkající se námi vybraného serveru [2].



Obrázek 6.2: Ukázka vygenerovaného „Availability Reportu“

6.2.2 Event Log Report

Druhým velmi využívaných výstupem je report všech událostí viz obrázek č. 11.7, k nimž v monitorovacím systému došlo. Report je seříděn od nejnovějších informací ke starším. Historie je ukládána v hodinových intervalech. Pokud si přejeme znázornit report z kteréhokoliv dne v historii, je možné jej vyhledat v archivu. Veškeré logy jsou systémem archivovány.

6.3 Sekce „Configuration“

Poslední položkou v levém menu v sekci „Configuration“ je odkaz „View Config“. Tento odkaz umožňuje znázornit aktuální konfiguraci zařízení a služeb. Pro znázornění tohoto odkazu musí být uživatel autorizován. V souboru `cgi.cfg` v položce `authorized_for_configuration_information` jsou definováni autorizovaní uživatelé viz obrázek č. 11.8 [2].

Kapitola 7

Monitorování provozu sítě a lokálních služeb

Při monitorování nevyužíváme pouze metod síťového charakteru, i přesto že tyto metody převládají. V praxi administrátor požaduje nejen informace o stavu zařízení a provozovaných službách ale často také podrobné informace o každém serveru, kterými mohou být např. vytížení procesoru, teplota, využití diskového prostoru, počet spuštěných procesů atd. Tato kapitola tyto dva přístupy podrobně popisuje.

7.1 Monitorování provozu sítě

Srdce monitorovacího systému Nagios je v mechanismu metod, který je schopen efektivně monitorovat provoz sítě. Typy monitorování jsem rozdělil do čtyř částí, na monitorování zařízení a služeb, na monitorování lokálního charakteru (např. počet přihlášených uživatelů, vytížení zařízení, nedostatek diskového prostoru atd.) a síťového charakteru (např. zda je spuštěna databáze, zda funguje index Virtuální server virtuální server atd.). V kapitole č. 8 vysvětlím i problematiku monitorování lokálních služeb na vzdáleném zařízení.

7.1.1 Monitorování zařízení

Ve většině případů požadujeme, aby byly monitorovány služby námi provozovaného zařízení. Pokud zařízení pouze definujeme a monitorujeme služby na něm spuštěné, monitorovací systém předpokládá, že zařízení je rovněž v pořádku. Nejzákladnější metoda k otestování zařízení je `check-host-alive`. Tabulka č. 7.1 nám tuto metodu znázorňuje.

```
define command {
    command_name    check-host-alive
    command_line    $USER1$/check_ping -H $HOSTADDRESS$ -w 3000.0,80%
                   -c 5000.0,100% -p1
```

Tabulka 7.1: Metoda `ping` k monitorování dostupnosti zařízení

Metoda spustí příkaz `check_ping` do proměnné `$HOSTADDRESS$` bude standardně doplněna IP adresa monitorovaného zařízení. Parametr `--w` a `--c` udává interval, kdy bude zařízení ve stavu `WARNING` či `CRITICAL` a parametr `--p` udává počet odeslaných paketů na zařízení. Interval je složen ze dvou částí, které jsou odděleny tečkou. První udává odezvu na příkaz `ping` v milisekundách a druhá část nám udává kolik % paketů může být ztraceno. Spárování metody `check-host-alive` je v těle definice zařízení, viz tabulka č. 7.2 [2].

```
define host {
    host_name        name.intranet.cz
    check_command    check-host-alive
    .....
}
```

Tabulka 7.2: Uvedení metody `check-host-alive` v definici zařízení

7.1.2 Monitorování služeb

Základní konfigurace pro testování služeb je velmi podobná testování zařízení. Tabulka č. 7.3 je ukázkou typické metody pro testování služby. Tato metoda (plugin) se připojí na TCP port testovaného zařízení a vrátí výsledek. Například vrátí OK, jestliže spojení bylo úspěšné a CRITICAL pokud bylo spojení přerušeno.

```
define command {
    command_name    check_tcp
    command_line    $USER1$/check_tcp -H $HOSTADDRESS$ -p $ARG1$
}
```

Tabulka 7.3: Metoda pro testování služby

Většina metod má možnost nastavení parametrů. V tomto případě mohou být parametry dva. U vlastních metod je možné využít až 32 parametrů [4].

7.1.3 Lokální monitorování

```
define command {
    command_name    check_local_disk
    command_line    $USER1$/check_disk -w $ARG1$ -c $ARG2$ -p $ARG3$
}

define service {
    service_description    check_local_disk
    command_line            check_local_disk!10%!5%!
    .....
}
```

Tabulka 7.4: Definice metody a testování v lokálním monitorování

Prvním typem monitorovacích skriptů jsou lokální metody, které testují služby a hodnoty na lokálním zařízení. Tyto služby zahrnují testování diskové

KAPITOLA 7. MONITOROVÁNÍ PROVOZU SÍTĚ A LOKÁLNÍCH SLUŽEB44

kapacity, paměti, využití procesoru, stavu aplikací či procesů. Pro ukázkou je použita funkce na testování diskové kapacity. Definice metody a testování je uvedeno v tabulce č. 7.4.

```
define command {  
    command_name    check_ssh  
    command_line    $USER1$/check_ssh -H $HOSTADDRESS$  
}
```


Tabulka 7.5: Ukázka síťového monitorování sshd služby.

Výše uvedená ukázka testuje diskovou kapacitu. Pokud je volné místo menší než 10%, metoda vrátí stav **WARNING**, pokud bude méně než 5% volného místa, návratový řetězec bude **CRITICAL** [4].

7.1.4 Síťové monitorování

Jedním z nejjednodušších úkonů je vzdálené monitorování síťových služeb, kterými jsou např. LDAP, SSH, FTP, SMTP atd. Návratové hodnoty síťového monitorování jsou stejné jako u lokálního monitorování. Tabulka č. 7.5 zobrazuje síťové monitorování sshd služby.

Metoda `check_ssh` se připojí na IP adresu v proměnné `$HOSTADDRESS$` a návratová hodnota bude podobná jako u příkladů lokálního monitorování. Obrázek č. 7.1 zobrazuje spuštění skriptů `check_ssh`, `check_fping`, `check_smtp` a jejich návratových hodnot [8].



```
archive.zf.jcu.cz - PuTTY  
archive:~#  
archive:~# /usr/lib/nagios/plugins/check_ssh -H ara.zf.jcu.cz  
SSH OK - OpenSSH_3.4p1 Debian 1:3.4p1-1 (protocol 1.99)  
archive:~#  
archive:~# /usr/lib/nagios/plugins/check_fping -H ara.zf.jcu.cz  
FPING OK - ara.zf.jcu.cz (loss=0%, rta=0.270000 ms)|loss=0%;;0;100 rta=0.000270s;;;0.000000  
archive:~#  
archive:~# /usr/lib/nagios/plugins/check_http -H ara.zf.jcu.cz  
OK - HTTP/1.1 302 Found - 0.028 second response time |time=0.027927s;;;0.000000 size=248B;;;0  
archive:~#  
archive:~# /usr/lib/nagios/plugins/check_smtp -H ara.zf.jcu.cz  
SMTP OK - 0.004 sec. response time|time=0.003585s;;;0.000000  
archive:~#  
archive:~#  
archive:~#
```

Obrázek 7.1: Ukázka aktuální konfigurace zařízení a služeb

7.2 Vzdálené monitorování lokálních služeb

Nagios nabízí dvě možnosti monitorování lokálních služeb. Pomocí pluginů, které nám umožňují monitorovat lokální služby, těmi mohou být kontrola procesů, zatížení serveru, počet přihlášených uživatelů, informace o plných discích a síťových služeb, jimiž jsou HTTP, FTP, DNS, LDAP, POP3 atd.

První typ monitorování je užitečný, ale jako plugin může být spustitelný pouze na lokálním serveru. Pro jeho univerzální využití i na vzdálených serverech je nutné nakonfigurovat mechanismus, který nám umožní spouštět akce na vzdálených serverech a následně vyhodnotit odpověď. Druhý typ je více efektivní, lze jej využít pouze pro síťové služby.

Existuje více variant, jak problém monitorování lokálních služeb vzdáleně provádět. Otázka různé alternativy řešení se samozřejmě odvíjí od složitosti sítě. Hlavním kritériem je však bezpečnost. Mezi nejznámější patří monitorování lokálních služeb přes NRPE, šifrovaný SSH tunel a monitorování přes SNMP.

7.2.1 Monitorování pomocí NRPE služby

Dle mého názoru neoptimálnější variantou pro vzdálené monitorování je služba, kterou vytvořil Ethan Galstad nazvaná NRPE. NRPE má dvě komponenty, plugin pojmenovaný `check_nrpe` a služba `nrpe`. Plugin je instalován na server, kde je spuštěn Nagios a NRPE služba je nainstalována na vzdáleném počítači. Zásuvný modul `check_nrpe` funguje na pasivním principu, kdy je jméno příkazu spuštěno pomocí NRPE služby běžící na vzdáleném serveru. V Nagiosu je definován seznam příkazů, které je možné spustit pomocí NRPE služby. NRPE služba je definována v konfiguračním souboru `nrpe.cfg`, kde je rovněž definován seznam služeb, jež si přejeme na vzdáleném serveru spouštět.

Příkaz v ukázce č. 7.6 se bude snažit spojit NRPE službou na vzdáleném serveru pomocí TCP/IP spojení na portu 5666 a poté spustí lokálně

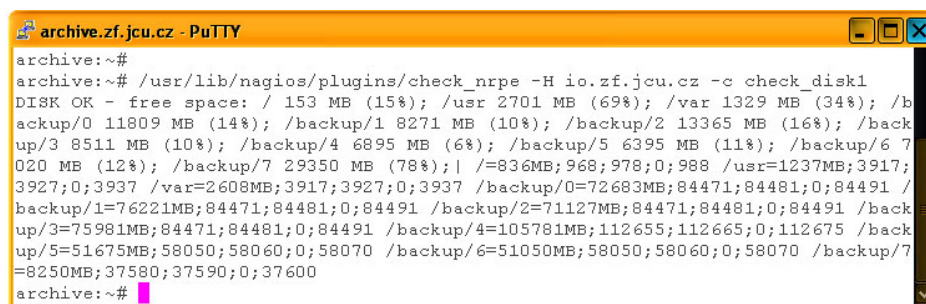
```

define service {
    service_description    disk
    host_name              owlet
    check_command          check_nrpe!check_disk
}

```

Tabulka 7.6: Definice metody k testování disk. prostoru službou NRPE

příkaz `check_disk`. Příkaz `check_disk` je samozřejmě definován v `nrpe.cfg` konfiguračním souboru. Obrázek č. 7.2 zobrazuje spuštění příkazu z Nagiosu pro zjištění volného kapacity disku na vzdáleném serveru `io.zf.jcu.cz` a jeho odpověď [8].



```

archive.zf.jcu.cz - PuTTY
archive:~#
archive:~# /usr/lib/nagios/plugins/check_nrpe -H io.zf.jcu.cz -c check_disk1
DISK OK - free space: / 153 MB (15%); /usr 2701 MB (69%); /var 1329 MB (34%); /b
ackup/0 11809 MB (14%); /backup/1 8271 MB (10%); /backup/2 13365 MB (16%); /back
up/3 8511 MB (10%); /backup/4 6895 MB (6%); /backup/5 6395 MB (11%); /backup/6 7
020 MB (12%); /backup/7 29350 MB (78%); | / =836MB;968;978;0;988 /usr=1237MB;3917;
3927;0;3937 /var=2608MB;3917;3927;0;3937 /backup/0=72683MB;84471;84481;0;84491 /
backup/1=76221MB;84471;84481;0;84491 /backup/2=71127MB;84471;84481;0;84491 /back
up/3=75981MB;84471;84481;0;84491 /backup/4=105781MB;112655;112665;0;112675 /back
up/5=51675MB;58050;58060;0;58070 /backup/6=51050MB;58050;58060;0;58070 /backup/7
=8250MB;37580;37590;0;37600
archive:~#

```

Obrázek 7.2: Spuštění příkazu pro zjištění disk. prostoru pomocí NRPE

7.2.2 Vzdálené monitorování pomocí SSH

Tato metoda ke vzdálenému monitorování využívá standardní SSH spojení, přes které jsou na vzdáleném serveru spouštěny příkazy. Nejprve je nutné, aby byla na serverech spuštěna SSH služba včetně výjimek definovaných např. v `/etc/hosts.allow` pro přístup na server. Rovněž musí být povolen port 22 na firewallech či jiných aktivních zařízeních. Základní otázkou zůstává, jak se má SSH spojení autentifikovat. Standardně je SSH spojení autentifikováno definováním jména a zadáním hesla viz 7.3.

Zadávání hesla při každém testu je značně nepraktické až nepoužitelné. Tento problém lze vyřešit pomocí kombinace privátního a veřejného SSH klíče,

KAPITOLA 7. MONITOROVÁNÍ PROVOZU SÍŤE A LOKÁLNÍCH SLUŽEB47

```
puppy$ check_by_ssh -H 10.0.0.15
-C "/usr/local/nagios/libexec/check_disk -w 10 -c 5 -p /"
admin@10.0.0.15's password:*****
DISK OK - free space: / 77 MB (52%); | /=70MB;137;142;0;147
```

Obrázek 7.3: Spuštění vzdáleného příkazu přes SSH spojení

jako kompromisu pro autorizovaný přístup na server. Otázkou zůstává, jak je toto řešení robustní a hlavně bezpečné především v případě, že se tímto způsobem autentifikujeme na více serverů. Pokud se i přesto pro toto řešení rozhodneme, je nutné nejdříve vygenerovat SSH klíč. Tento klíč je možné vygenerovat příkazem `ssh-keygen`. Pro generování jsem zvolil DSA klíč, což znamená využití SSH Protokolu verze 2. Protokol je definován pomocí parametru `-t dsa`.

```
puppy$ check_by_ssh -H 10.0.0.15 -l nagios -i /home/nagios/.ssh/id_dsa
-C "/usr/local/nagios/libexec/check_disk -w 10 -c 5 -p /"
DISK OK - free space: / 77 MB (52%); | /=70MB;137;142;0;147
```

Obrázek 7.4: Spuštění vzdáleného příkazu přes SSH tunel

Po spuštění příkazu budeme požádáni o zvolení cesty, kam se má klíč uložit (defaultně se jedná o adresář `./ssh`) a následně budeme požádáni o zadání hesla a jeho ověření. V tomto případě je klíč generován pro uživatele `root`, což nebylo příliš vhodné, proto doporučuji SSH klíč generovat např. pro uživatele `nagios`. Dále je nutné veřejný klíč umístit na vzdálený server do adresáře `./ssh/authorized_keys`. Po této operaci by mělo být možné se pomocí SSH protokolu přihlásit na vzdálený server bez zadání uživatelského hesla. Po správném nastavení a opětovném spuštění příkazu dostaneme odpověď na obrázku č. 7.4 [8].

Toto řešení, ačkoliv není dokonalé, je jednoduše implementovatelné a funkční. Uživatel si nicméně musí být vědom rizik spojených s SSH tunely.

7.2.3 Monitorování pomocí SNMP

Poslední metodou pro vzdálené monitorování služeb je pomocí protokolu SNMP (Simple Network Management Protocol), který je běžný v převážné většině UNIXů a síťových zařízení. Tento protokol je spíše využíván pro monitorování zařízení, jako jsou routery, firewally či switche. Implementace této metody do Nagiosu a využívání pro vzdálené monitorování je jistě zajímavou volbou, však vzdálené monitorování pomocí NRPE či SSH je mnohem jednodušší pro implementaci a myslím si, že pro naši potřebu vhodnější [8].

Kapitola 8

Vytváření vlastních skriptů

Ačkoliv monitorovací systém obsahuje většinu běžně využívaných skriptů, může nastat situace, kdy je nutné monitorovat nějakou specifickou službu či aplikaci. Z tohoto důvodu bude nutné potřebný skript vytvořit. Nejvhodnější programovací jazyk pro programování vlastních skriptů je shell, Perl nebo jazyk C. Součástí distribuce monitorovacího systému jsou i šablony pro psaní skriptů. Ukázka skriptu pro kontrolu softwarového raidu je znázorněna na obrázku č. 8.1. Při vytváření je důležité se zaměřit na návratové hodnoty, které jsou zobrazené v tabulce č. 8.1.

0	OK
1	WARNING
2	CRITICAL
3	UNKNOWN

Tabulka 8.1: Návratové hodnoty pro vytváření vlastních skriptů


```

archive.zf.jcu.cz - PuTTY
TW /usr/lib/nagios/plugins/che Row 1 Col 1 7:02 Ctrl-K H for help
# /bin/sh

PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin

PROGNAME=`basename $0`
PROGPATH=`echo $0 | sed -e 's,[\\\/][^\\\/][^\\\/]*$,,'`
REVISION=`echo '$Revision: 1.8 $' | sed -e 's/[^0-9.]/g'`

. $PROGPATH/utils.sh

print_usage() {
    echo "Usage: $PROGNAME"
}

print_help() {
    print_revision $PROGNAME $REVISION
    echo ""
    print_usage
    echo ""
    echo "This plugin checks software raid volumes."
    echo ""
    support
    exit 0
}

case "$1" in
    --help)
        print_help
        exit 0
        ;;
    -h)
        print_help
        exit 0
        ;;
    --version)
        print_revision $PROGNAME $REVISION
        exit 0
        ;;
    -v)
        print_revision $PROGNAME $REVISION
        exit 0
        ;;
    *)
        raiddata=`cat /proc/mdstat`
        raiddata2=`cat /proc/mdstat`

        if echo ${raiddata} | egrep _U > /dev/null; then
            echo SW RAID CRITICAL - Detected fail disk in sw raid!
            exit 2

        elif echo ${raiddata} | egrep U_ > /dev/null; then
            echo SW RAID CRITICAL - Detected fail disk in sw raid!
            exit 2

        elif echo ${raiddata} | egrep UU > /dev/null; then
            echo SW RAID is OK
            exit 0

        else
            echo ${raiddata2}
            exit 1

        fi
        ;;
esac

```

Obrázek 8.1: Ukázka programovaného skriptu pro testování SW raidu

Kapitola 9

Monitorované servery a služby

V praktické části jsem se pokusil veškeré získané informace o možnostech monitorovacího systému ukázat na souboru sítě, kterou spravuji a z důvodu odlišnosti požadavků mezi jednotlivými organizačními celky, byl do tohoto souboru přidán i soubor serverů dalších fakult a také několika komerčních firem.

Před samotnou implementací monitorovacího systému bylo nejdříve důležité získat informace o serverech, aktivních prvcích a dalších požadavcích, které bylo potřeba v systému zohlednit.

Jednalo se například o požadavky:

- kdo je za jaké služby zodpovědný
- zda má být při výpadku některé ze služeb kontaktován pouze zodpovědný pracovník nebo celé IT oddělení
- zda mají být upozornění z monitorovacího systému odesílány elektronickou poštou nebo mohou být zaslány na mobilní telefon
- zda tyto zprávy mají být zasílány pouze v pracovní dobu nebo i v noci či o víkendech
- a mnoho dalších

9.1 Monitorovaná zařízení v prostředí JU

9.1.1 Zařízení na Zemědělské fakultě JU

Na Zemědělské fakultě v okamžiku zprovoznění monitorovacího systému bylo 8 serverů, které zajišťovaly provoz IT služeb v rámci této fakulty a částečně v rámci rektorátu.

Ara.zf.jcu.cz

Server `ara.zf.jcu.cz` má nejdůležitější úlohu. Mezi kritické služby patří především: primární doména pro Zemědělskou fakultu JU, Samba, diskový prostor pro veškeré uživatele ZF JU, mailový server Postfix, ProFTP daemon atd.

Taurus.zf.jcu.cz

Server `taurus.zf.jcu.cz` zajišťuje na ZF JU systémové služby především: DNS, MySQL databázi, DHCP, ProFTP daemon atd.

Cygnus.zf.jcu.cz

Server slouží pro zálohovací účely. Jsou zde zálohována data z ostatních serverů pro případ hardwarových problémů. Provozované služby NFS server, ProFTP daemon, Samba, Cron atd.

Lynx.zf.jcu.cz

Server obsahuje uživatelské projekty, které jsou na něm provozovány. Nároky a systémové požadavky jsou přibližně shodné se serverem `ara.zf.jcu.cz`.

Ecologica.zf.jcu.cz

Server zakoupený pro provoz komerčního softwaru Ecologica. Tento server spravují autoři aplikace, do monitorovacího systému je zapojen z důvodu kontroly výpadků konektivity.

9.1.2 Zařízení rektorátu JU

Smartq.zf.jcu.cz

Jedná se o server zajišťující provoz, autentifikaci a zúčtování tisku na síťových tiskárnách a kopírovacích strojích, které využívají studenti a zaměstnanci Jihočeské univerzity v Českých Budějovicích. Požadované služby jsou PostgreSQL, Tomcat, SSH, NFS server, Cron.

Crux.zf.jcu.cz

Server `crux.zf.jcu.cz` slouží jako aplikační a instalační server. Soustřeďuje potřebná data pro univerzitu k instalaci počítačů (např. veškerá data z Microsoft Select) a další specifické aplikace využívané rektorátem. Požadované služby jsou Apache, Samba, SSH, Maple, Cron.

Bootes.zf.jcu.cz

Na tomto serveru je spuštěna databázová agenda, která je využívána převážnou částí Jihočeské univerzity. Požadované služby jsou SSH, Apache, NFS server, PostgreSQL, Cron atd.

Obd.zf.jcu.cz

Server spravuje databázovou agendu OBD. Požadované služby databáze SyBase, SSH, NFS server, NTP, Apache.

Betty.lib.jcu.cz

Server knihovny Jihočeské univerzity sloužící jako mail server a file server pro pracovníky knihoven JU. Požadované služby jsou Apache, mailový server Postfix, MySQL databáze, NFS server, Samba, NTP, cron.

Fornax.bobik.jcu.cz

Server pro univerzitní počítačovou laboratoř Bobík sdílející data studentů a zaměstnanců JU. Požadované služby jsou Apache, MySQL databáze, NFS server, Samba, NTP, cron.

9.1.3 Zařízení na Teologické fakultě JU**Lumen.tf.jcu.cz**

Server zajišťující provoz Teologické fakulty Jihočeské univerzity z hlediska domény, mail serveru a file serveru. Požadované služby jsou Apache, MySQL databáze, NFS server, Samba, NTP, LDAP, cron.

Trin.tf.jcu.cz

Aplikační server Teologické fakulty JU. Požadované služby jsou Apache, MySQL databáze, NFS server, NTP, cron.

9.1.4 Zařízení Zdravotně sociální fakulty JU**Asterix.zsf.jcu.cz**

Jedná se o server zajišťující provoz pro Zdravotně sociální fakultu JU. Nároky na služby jsou shodné se serverem `lumen.tf.jcu.cz` Teologické fakulty JU.

Apps.zsf.jcu.cz

Jedná se o aplikační server Zdravotně sociální fakulty JU pro provoz specifických aplikací požadovaných na ZSF JU. Požadované služby jsou Apache, Samba, ProFTP, SSH, MySQL databáze, NTP, cron.

9.2 Monitorovaná zařízení v komerční sféře

Jako součást bakalářské práce jsem zahrnul rovněž monitorování serverů komerčních institucí. Je pravdou, že se mohou potřeby a požadavky komerčních a vzdělávacích institucí lišit, ať už se jedná o dobu sledování výpadků, nároků na okamžité odstranění, zastupitelnost správců IT systémů či zasílání výpadků nadřízeným pracovníkům.

9.2.1 Radio Faktor s.r.o.

Z tohoto důvodu jsem navázal spolupráci se společností Rádio Faktor, kde po vzájemné dohodě došlo k začlenění serverů do monitorovacího systému Nagios. Výpadky serverů mají pro společnost značné následky, které mohou odradit potenciální klienty v marketingových službách. Společnost Radio Faktor s.r.o. v současné době disponuje 3 hlavními servery dostupnými z internetu. Jedná se o servery v Českých Budějovicích, Táboře a na Jihočeské univerzitě v Českých Budějovicích.

Radio.faktor.cz

Server je umístěn přímo v objektu vysílacích pracovišť v Českých Budějovicích. Jeho hlavními činnostmi jsou firewall, zajištění mailového serveru, www serveru a dalších služeb dle požadavků. Mezi klíčové služby patří Apache, MySQL, mailový server Postfix, ProFTP, SSH, Samba, NTP a další.

Tabor.faktor.cz

Server umístěný v Táboře, odkud rovněž Rádio Faktor vysílá pro místní region, zajišťuje obdobné služby jako server v Českých Budějovicích. Tyto servery jsou mimo jiné propojeny šifrovaným tunelem pro komunikaci mezi pracovišti po lokálních adresách.

Live-ra.eldorado.cz

Poslední server, který využívá Radio Faktor na internetu, je umístěn na JU. Slouží k vysílání Rádia Faktor na internetu, což byl projekt realizovaný ve spolupráci se společností CESNET. Požadavky na tento server jsou SSH, NTP a speciální software pro streamování dat do internetu.

9.2.2 Marten-Louis s.r.o.**Cb.marten-louis.cz a Mail. marten-louis.cz**

Tyto servery zajišťují stejný rozsah služeb a požadavky jsou především databáze MySQL, Apache, ProFTP, SSH, NTP, cron.

9.2.3 Jazyková škola EDUCO

Další společností je Jazyková škola Educo, která disponuje jedním serverem typickým pro provoz malé společnosti s malými nároky. Hodinový výpadek na serveru nebude mít žádné katastrofické následky a v této situaci není nutné služby monitorovat 24 hodin denně po dobu 7 dní v týdnu.

Educo.educo-cb.cz

Na serveru je spuštěn základní soubor služeb potřebných pro provoz. Požadované služby jsou Apache, ProFTP, mailový server Postfix, SSH, NTP.

9.2.4 1K Design s.r.o.

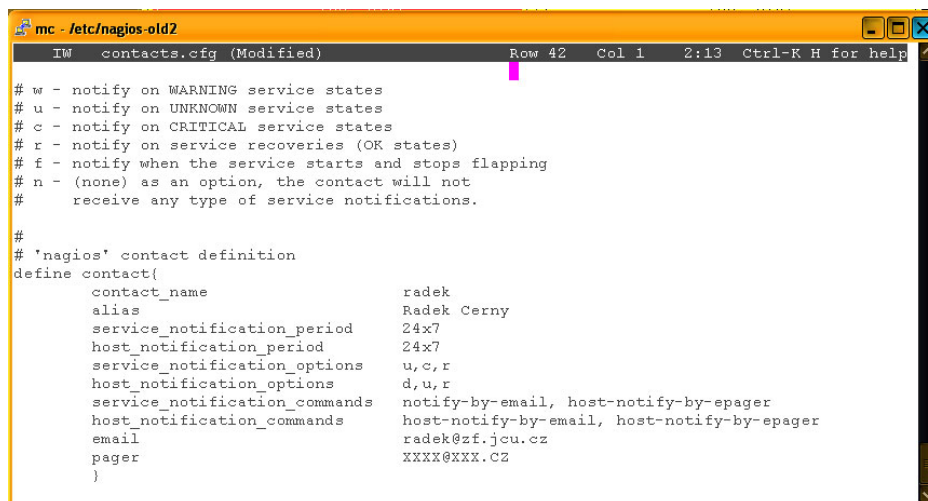
Poslední společností je 1K Design s.r.o., která se zabývá tvorbou www prezentací a hostingovými službami. Soubor požadovaných služeb se moc neliší od Jazykové školy Educo, jejich provozování je intenzivnější a nároky na bezproblémový chod jsou mnohem vyšší. Server této společnosti zajišťuje provoz služeb Apache, ProFTP, mailový server Postfix, SSH, NTP.

Kapitola 10

Konfigurace Nagiosu v praxi

Po shrnutí informací o jednotlivých serverech, službách provozovaných na serverech a pracovnících zodpovědných za tyto servery, můžeme jednotlivé servery se všemi ostatními informacemi zahrnout a vhodně nakonfigurovat v Nagiosu.

Již z teoretické části bakalářské práce bychom měli mít monitorovací systém úspěšně nainstalován.



```
mc - /etc/nagios-old2
contacts.cfg (Modified) Row 42 Col 1 2:13 Ctrl-K H for help

# w - notify on WARNING service states
# u - notify on UNKNOWN service states
# c - notify on CRITICAL service states
# r - notify on service recoveries (OK states)
# f - notify when the service starts and stops flapping
# n - (none) as an option, the contact will not
#     receive any type of service notifications.

#
# 'nagios' contact definition
define contact{
    contact_name           radek
    alias                  Radek Cerny
    service_notification_period 24x7
    host_notification_period 24x7
    service_notification_options u,c,r
    host_notification_options d,u,r
    service_notification_commands notify-by-email, host-notify-by-epager
    host_notification_commands host-notify-by-email, host-notify-by-epager
    email                  radek@zf.jcu.cz
    pager                  XXXX@XXX.CZ
}
```

Obrázek 10.1: Přidání uživatele do systému

10.1 Vložení pracovníka do systému

Ještě před tím než začneme do Nagiosu vkládat jednotlivé servery a jejich služby, bude nutné nadefinovat uživatele, viz obrázek č. 10.1 v souboru `contacts.cfg`.

Dále modifikujeme soubor `contactgroups.cfg`, do něhož uložíme informaci o názvu skupiny a jejích členech viz obrázek č. 10.2.



```
mc - /etc/nagios
IW contactgroups.cfg (Modified) Row 45 Col 1 2:23 Ctrl-K H for help
define contactgroup{
    contactgroup_name      ZF-admins
    alias                  Linux Administrators
    members radek, homola, friebel
}

define contactgroup{
    contactgroup_name      ZF-win-admins
    alias                  Windows Administrators
    members milota, radek
}

define contactgroup{
    contactgroup_name      switch-admins
    alias                  Switch Administrators
    members milota, radek, homola, friebel
}
```

Obrázek 10.2: Přidání uživatele do skupiny ZF-admins

10.2 Vložení serveru a služeb do systému

Pokud máme vložené uživatele starající se o dané servery a rovněž máme nadefinovány jejich skupiny, můžeme přistoupit ke vkládání jednotlivých serverů. Vzhledem k tomu, že informace o serveru a jeho službách jsou ve více souborech, preferoval jsem způsob, který se mi v praxi osvědčil. To znamená, že převážná část informací o serveru je umístěna do jednoho souboru (jsou zde společně informace o serveru i službách), viz obrázek č. 10.3 a tento konfigurační soubor je načten při startu Nagiosu z hlavního konfiguračního souboru viz obrázek č. 5.1. V opačném případě bychom museli tyto informace spravovat minimálně v souborech `hosts.cfg` pro definování serveru a `services.cfg` pro definice služeb. To však ještě není vše. Dále je nutné tuto informaci uložit do souboru `hostgroups.cfg`, kde definujeme

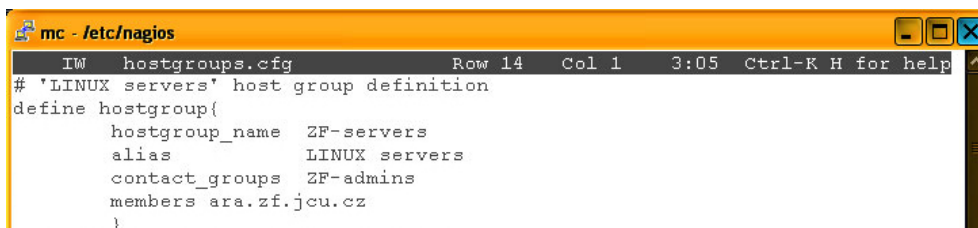


```
mc - /etc/nagios/servers/zf-vypoctak
IW ara.cfg (Modified) Row 4 Col 1 2:57 Ctrl-K H for help
# 'ARA.ZF.JCU.CZ' host definition
define host{
    use generic-host ; Name of host template
    host_name ara.zf.jcu.cz
    alias Linux Server ARA
    address 160.217.161.4
    parents a10zfvc
    check_command check-host-alive
    max_check_attempts 10
    notification_interval 240
    notification_period 24x7
    notification_options d,u,r
}

# Service definition
define service{
    use generic-service ; Name of servi
    host_name ara.zf.jcu.cz
    service_description PING
    is_volatile 0
    check_period 24x7
    max_check_attempts 3
    normal_check_interval 5
    retry_check_interval 1
    contact_groups ZF-admins
    notification_interval 240
    notification_period 24x7
    notification_options c,r
    check_command check_ping_ok!100.0,20%!500.0,60%
```

Obrázek 10.3: Přidání uživatele do skupiny ZF-admins

stejně jako u skupiny uživatelů i skupinu serverů včetně členů (jednotlivých serverů) a dále zde definujeme kontaktní skupinu, udávající seznam pracovníků, kteří budou informováni v případě výpadků viz obrázek č. 10.4.



```
mc - /etc/nagios
IW hostgroups.cfg Row 14 Col 1 3:05 Ctrl-K H for help
# 'LINUX servers' host group definition
define hostgroup{
    hostgroup_name ZF-servers
    alias LINUX servers
    contact_groups ZF-admins
    members ara.zf.jcu.cz
}
```

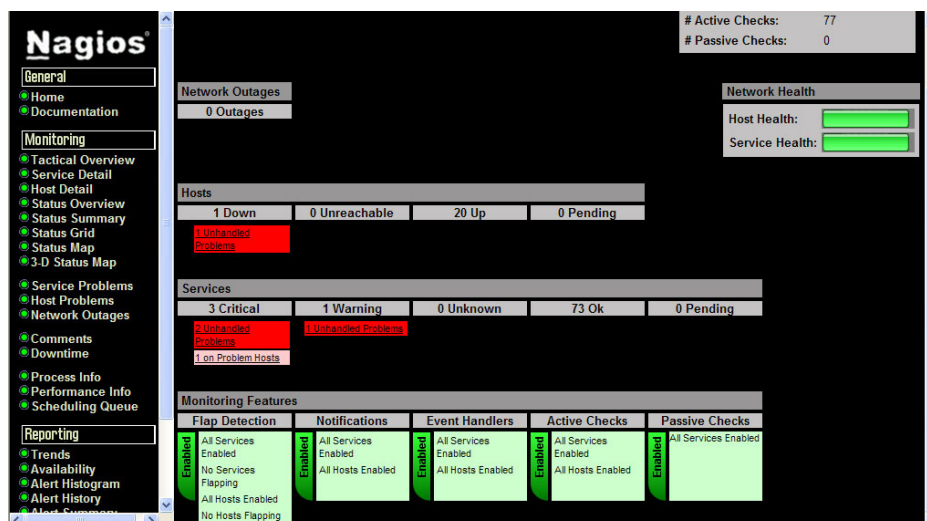
Obrázek 10.4: Přiřazení serverů ke kontaktní skupině ZF-admins

Pokud došlo k přidání uživatelů, skupin uživatelů, serverů a jejich služeb, můžeme Nagios restartovat a přes webové rozhraní se do něj přihlásit. Obdržíme informace zobrazené na obrázku č. 11.2.

Kapitola 11

Zkušenosti s provozem

Po definici testovaných zařízení a služeb na základě získaných informací o serverech a požadavcích na jejich provoz, byl Nagios v první polovině roku 2006 spuštěn do testovacího provozu. Od té doby bylo nutné upravit různá nastavení od prodloužení odezvy ICMP paketů na zařízeních umístěných na pomalém připojení, přes upravení limitů při testování diskové kapacity až po korekci ručně vytvořených skriptů.

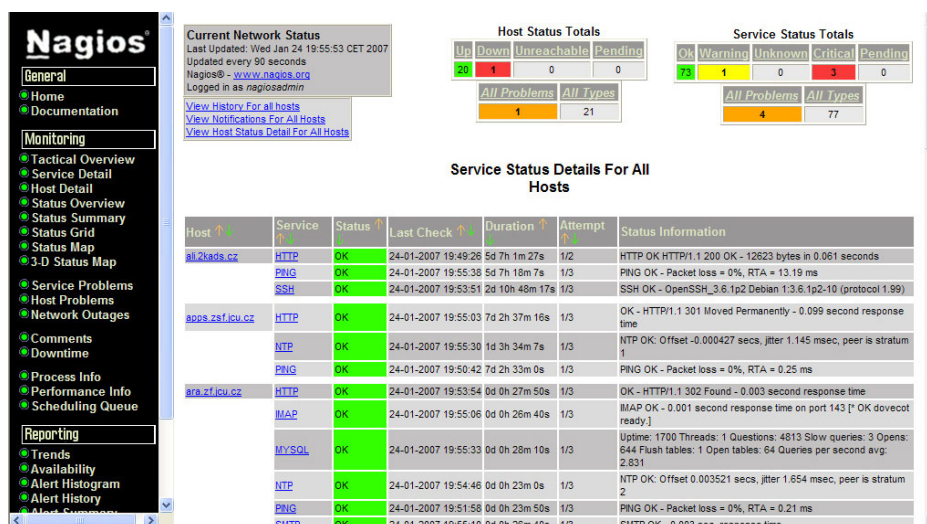


Obrázek 11.1: Sekce „Tactical Overview“

Monitorovací systém byl po těchto úpravách spuštěn do plného provozu

a informace o konfliktních situacích byly zasílány odpovědným osobám k jejich následnému řešení. Tento stav trvá dodnes s tím rozdílem, že se systém rozrostl o „několik desítek“ dalších zařízení. V této kapitole bych rád poukázal na praktické informace, které systém může uživateli poskytnout.

Po úspěšném přihlášení je, stejně jako na obrázku č. 11.1, znázorněna úvodní obrazovka, která nás stručně informuje o aktuální situaci. V `hosts` je patrné, že se jedno zařízení nalézá ve stavu `DOWN`. Rovněž v sekci `services` jsou tři problematické služby ve stavu `CRITICAL` a jedna ve stavu `WARNING`. O těchto stavech byli informováni odpovědní pracovníci. Ostatní sekce jsou zbarveny zeleně, což znamená, že vše ostatní je v pořádku.

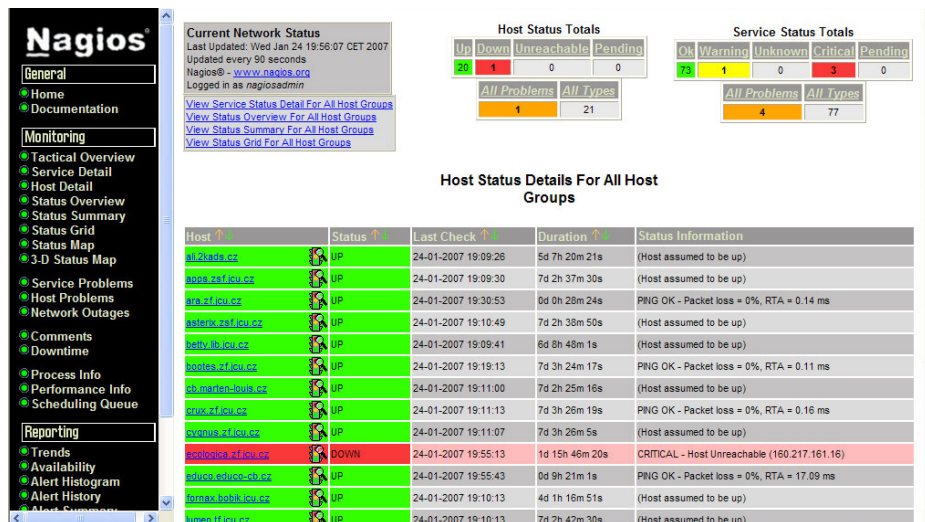


Obrázek 11.2: Sekce „Service Detail“

Pokud klikneme na odkaz „Service Detail“, budeme podrobně informováni o jednotlivých testovaných službách viz obrázek č. 11.2, kde jsou v horní části výpisu zobrazeny tři zařízení včetně služeb a dalších informací. Odkaz `Host` a `Service` je možné dále otevřít a vykonávat úkony spojené s těmito položkami.

Další ukázka na obrázku č. 11.3 zobrazuje pouze zařízení nikoliv služby, jejich stavy a bližší informace o monitorování. Zde je patrné, že zařízení se stavem `DOWN` z obrázku č. 11.1 je `ecologica.zf.jcu.cz`, která není dostupná

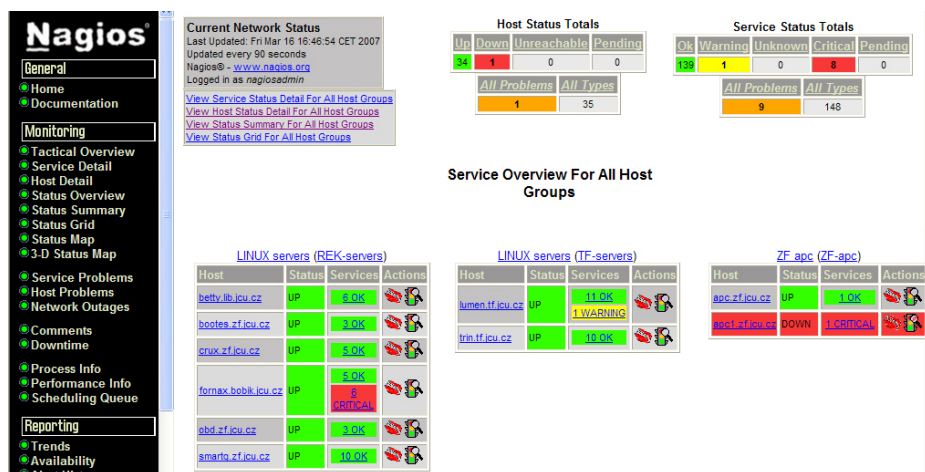
z důvodu hardwarových chyb.



Obrázek 11.3: Sekce „Host Detail“

Použití odkazu „Status Overview“ zobrazuje obrázek č. 11.4, který byl pořízen v jiný okamžik a informuje nás souhrnně o stavech zařízení rozdělených do jednotlivých skupin. Opět jsou jednotlivá zařízení barevně odlišena pro lepší přehlednost.

Do této chvíle nás monitorovací systém informoval pouze o aktuálním



Obrázek 11.4: Sekce „Status Overview“

stavu sítě. Značnou silou systému jsou také informace spojené s historií. Často uživatele může zajímat počet výpadků spojených s konkrétní službou, zařízením nebo spolehlivost celé skupiny zařízení či celé sítě. Tyto informace jsou dostupné v sekci „Reporting“.

Hostgroup 'REK-servers' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
belty.lib.jcu.cz	99.789% (99.801%)	0.199% (0.199%)	0.000% (0.000%)	0.013%
bootes.zf.jcu.cz	99.984% (99.996%)	0.004% (0.004%)	0.000% (0.000%)	0.013%
enux.zf.jcu.cz	99.987% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.013%
fomax.bobik.jcu.cz	99.186% (99.199%)	0.801% (0.801%)	0.000% (0.000%)	0.013%
obd.zf.jcu.cz	99.984% (99.997%)	0.003% (0.003%)	0.000% (0.000%)	0.013%
smardq.zf.jcu.cz	99.987% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.013%

Hostgroup 'TF-servers' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
lumen.tf.jcu.cz	99.987% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.013%
trn.tf.jcu.cz	96.888% (96.900%)	3.100% (3.100%)	0.000% (0.000%)	0.013%

Hostgroup 'ZF-apc' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
apc.zf.jcu.cz	99.987% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.013%
apc1.zf.jcu.cz	0.000% (0.000%)	99.987% (100.000%)	0.000% (0.000%)	0.013%

Hostgroup 'ZF-servers' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
ara.zf.jcu.cz	99.987% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.013%
archive.zf.jcu.cz	99.987% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.013%
cygnus.zf.jcu.cz	99.987% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.013%
ecologica.zf.jcu.cz	57.179% (57.186%)	42.808% (42.814%)	0.000% (0.000%)	0.013%

Obrázek 11.5: Sekce „Availability“

Obrázek č. 11.5 zobrazuje report vygenerovaný na základě požadavků uživatele. V tomto případě spolehlivost celé sítě rozdělené do jednotlivých skupin zařízení za měsíc srpen 2006. Čtenáře by mohlo zaujmout, proč není 100% dostupnost u většiny zařízení. Důvodem nedostupnosti některých zařízení byla skutečnost, že v několika částech fakulty docházelo ke stavebním pracem a tedy i k nutnému odpojení serverů od internetu.

Displaying most recent 25 of 731 total matching alerts

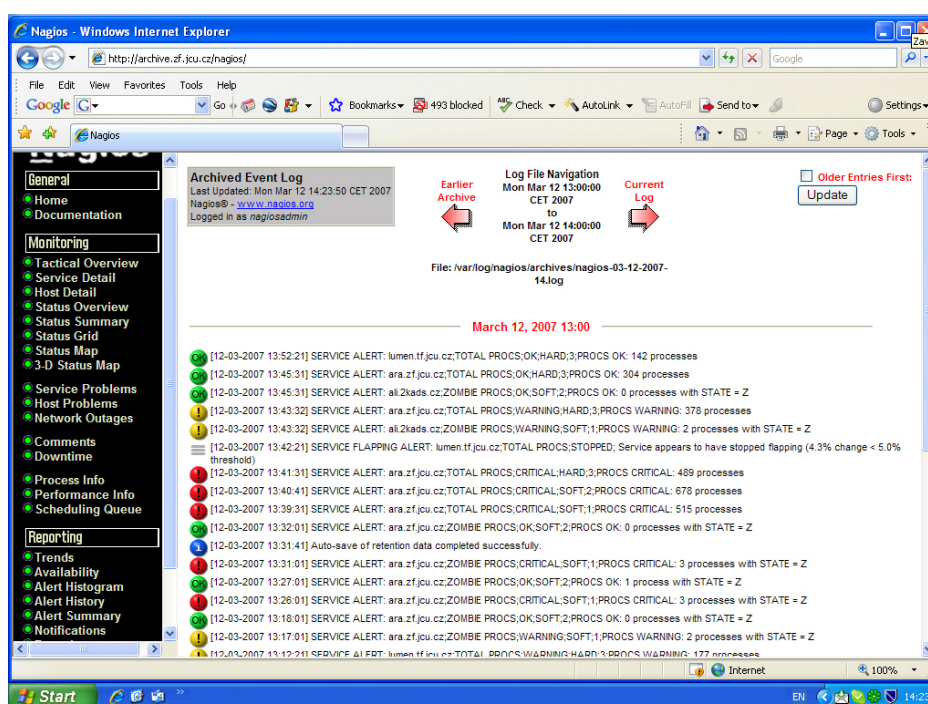
Time	Alert Type	Host	Service	State	State Type	Information
16-03-2007 16:03:21	Service Alert	ara.zf.jcu.cz	ZOMBIE PROCS	OK	HARD	PROCS OK: 0 processes with STATE = Z
16-03-2007 16:01:21	Service Alert	ara.zf.jcu.cz	ZOMBIE PROCS	CRITICAL	HARD	PROCS CRITICAL: 3 processes with STATE = Z
16-03-2007 15:06:51	Service Alert	belty.lib.jcu.cz	PING	OK	HARD	PING OK - Packet loss = 0%, RTA = 0.35 ms
16-03-2007 15:03:21	Host Alert	belty.lib.jcu.cz	N/A	UP	HARD	PING OK - Packet loss = 0%, RTA = 0.18 ms
16-03-2007 15:02:56	Service Alert	belty.lib.jcu.cz	PING	CRITICAL	HARD	CRITICAL - Plugin timed out after 10 seconds
16-03-2007 15:02:56	Host Alert	belty.lib.jcu.cz	N/A	DOWN	HARD	CRITICAL - Host Unreachable (160.217.164.2)
16-03-2007 14:18:21	Service Alert	ara.zf.jcu.cz	TOTAL PROCS	OK	HARD	PROCS OK: 315 processes
16-03-2007 14:16:21	Service Alert	ara.zf.jcu.cz	TOTAL PROCS	CRITICAL	HARD	PROCS CRITICAL: 409 processes
16-03-2007 14:14:21	Service Alert	ara.zf.jcu.cz	ZOMBIE PROCS	OK	HARD	PROCS OK: 0 processes with STATE = Z
16-03-2007 14:12:21	Service Alert	ara.zf.jcu.cz	ZOMBIE PROCS	WARNING	HARD	PROCS WARNING: 2 processes with STATE = Z
16-03-2007 14:12:11	Service Alert	lumen.tf.jcu.cz	TOTAL PROCS	OK	HARD	PROCS OK: 140 processes
16-03-2007 14:10:11	Service Alert	lumen.tf.jcu.cz	TOTAL PROCS	WARNING	HARD	PROCS WARNING: 158 processes
16-03-2007 14:04:21	Service Alert	ara.zf.jcu.cz	ZOMBIE PROCS	CRITICAL	HARD	PROCS CRITICAL: 5 processes with STATE = Z

Obrázek 11.6: Sekce „Alert Summary“

Pokud uživatelé zajímá report spolehlivosti konkrétního zařízení včetně gra-

fického zobrazení, využije stejný odkaz s tím rozdílem, že definuje pouze jedno zařízení a potřebný časový interval. V tomto případě obdrží informace podobné s obrázkem č. 6.2, kde byl zvolen server `ali.2kads.cz`.

Obrázek č. 11.6 ukazuje využití odkazu „Alert Summary“. Ten nám vygeneruje report obsahující informace o službách, které v definovaný časový interval změnil svůj stav. I tato funkce je dobře využitelná pro drobné korekce monitorovaných zařízení.



Obrázek 11.7: Ukázka vygenerovaného „Event Log Reportu“

Velice užitečným odkazem v sekci „Reporting“ je „Event Log“. O tomto reportu jsem se již zmínil v teoretické části práce, ale rád bych se k němu ještě vrátil a použil grafickou ukázkou. Do tohoto reportu ukládá monitorovací systém veškeré akce včetně jejich historie viz obrázek č. 11.7. Report umožňuje uživateli analýzu vzniklých stavů a reakci monitorovacího systému na tyto stavy. Obrázek č. 11.7 zobrazuje události, ke kterým došlo 12. března 2007 před 14 hodinou. Převážnými stavy jsou kritické hodnoty spuštěných procesů, což je zapříčiněno značnou náročností spamové analýzy mailového

serveru.

Sekce „Configuration“ obsahuje odkaz viz obrázek č. 11.8 zobrazující veškerou konfiguraci monitorovacího systému, která byla nadefinována. Výhodou tohoto odkazu je jednoduché a efektivní procházení jednotlivých nastavení s možností využití odkazů na ostatní související nastavení.

The screenshot shows the Nagios web interface in Internet Explorer. The main content area displays the 'Configuration' page, which includes a table of hosts. The table has the following columns: Host Name, Alias/Description, Address, Parent Hosts, Notification Interval, Notification Options, Notification Period, Max. Check Attempts, Host Check Command, Enable Checks, Event Handler, and Enable Event. The table lists several hosts, including a10zfvj.jcu.cz, a24zsf-dek, al12kads.cz, apc.zf.jcu.cz, and apc1.zf.jcu.cz. The interface also shows a sidebar with navigation options like Monitoring, Reporting, and Configuration.

Host Name	Alias/Description	Address	Parent Hosts	Notification Interval	Notification Options	Notification Period	Max. Check Attempts	Host Check Command	Enable Checks	Event Handler	Enable Event
a10zfvj.jcu.cz	a10zfvj.jcu.cz	160.217.8.239		4h 0m 0s	Down, Unreachable, Recovery	24x7	10	check-host-alive	Yes		Yes
a24zsf-dek	Switch ZSF	160.217.201.253	zsf-dek	12h 0m 0s	Down, Unreachable, Recovery	24x7	3	check-host-alive	Yes		Yes
al12kads.cz	Linux Server KOS	212.71.133.15		4h 0m 0s	Down, Unreachable, Recovery	24x7	10	check-host-alive	Yes		Yes
apc.zf.jcu.cz	apc.zf.jcu.cz	160.217.161.245		4h 0m 0s	Down, Unreachable, Recovery	24x7	10	check-host-alive	Yes		Yes
apc1.zf.jcu.cz	apc1.zf.jcu.cz	160.217.161.246		4h 0m 0s	Down, Unreachable, Recovery	24x7	10	check-host-alive	Yes		Yes

Obrázek 11.8: Ukázka aktuální konfigurace zařízení a služeb

Kapitola 12

Závěr

Cílem této bakalářské práce bylo ukázat instalaci, konfiguraci a implementaci monitorovacího systému Nagios v prostředí Zemědělské fakulty Jihočeské univerzity. Poukázat na praktickém příkladě důležitost využití monitorovacího systému pro monitorování provozu informačních sítí. Důležitost není dána pouze potřebou těchto systémů z hlediska auditu pracoviště nebo provozu služeb, ale implementace systému by měla pomoci i administrátorům se správou sítě a včasnému odstranění vzniklých problémů.

Práce seznamuje se současnými trendy, nabídkou opensourcových i částečně komerčních monitorovacích systémů dostupných v současné době na trhu. Rovněž byl v práci kladen důraz na výhody a nevýhody jednotlivých monitorovacích systémů pro případné porovnávání včetně grafických ukázek.

V dalších kapitolách byl čtenář podrobněji seznámen s funkčností systému, možnostmi instalace ze zdrojových kódů či předpřipravených balíčků včetně celého průběhu instalace. Po úspěšné instalaci byl čtenář detailně seznámen s konfigurací základního nastavení, definováním zařízení, služeb, kontaktů a dalších objektů a vzájemných závislostí. Následující kapitoly byly věnovány problematice lokálního a síťového monitorování včetně využití různých metod pro vzdálené monitorování lokálních služeb. Čtenář je rovněž informován o možnostech vytváření vlastních monitorovacích skriptů včetně ukázky skriptu pro monitorování softwarového raidu.

Druhá část bakalářské práce pojednává o praktické implementaci na Jihočeské univerzitě v Českých Budějovicích a rozšíření o servery v komerční sféře. Stručný popis jednotlivých serverů a služeb, které poskytují uživatelům. Poté byl čtenář seznámen s vložením těchto informací do monitorovacího systému a informován o konkrétních možnostech a reportech, které lze od systému očekávat včetně příkladů s popisem a grafickou ukázkou.

Literatura

- [1] Kaplan, V.: *Nagios®. monitorovací systém*, Tacoma, spol. s r.o., 2004.
- [2] Turnbull, J.: *Pro Nagios 2.0*. No Starch Press, 2006.
- [3] Galstad, E.: *Nagios® Version 2.0 Documentation*, <http://www.nagios.org/>.
- [4] Burgess, Ch.: *The Nagios Book*, 2005.
- [5] *Upgrade IT!*, ARTAX a.s., únor 2007.
- [6] Graham, S., Shah S.: *Administrace systému Linux*, Grada Publishing, 2003.
- [7] Kretchmar, J.: *Open Source Network Administration*, Prentice Hall PTR, 2003.
- [8] Josephsen, D.: *Building a Monitoring Infrastructure with Nagios*, Prentice Hall PTR, 2007.

Rejstřík

- Akkada, 15
- Alert Summary, 64
- Architektura, 21
- Availability, 39

- Check, 28
- Check-host-alive, 42
- Check_disk, 46
- Check_fping, 44
- Check_periods, 32
- Check_smtp, 33, 44
- Check_ssh, 44
- Configuration, 36, 40, 65
- Contactgroups, 58
- Contacts, 28, 58

- DHCP, 52
- DNS, 45, 52
- Down, 30
- DSA klíč, 47

- Event Log, 64
- Event Log Report, 39

- Flapping, 32
- FTP, 45

- Host, 28
- Host Detail, 38
- Hostgroups, 31, 35, 58
- Hosts, 58, 61
- HTTP, 33, 45

- Instalace, 22

- Konfigurace, 25

- LDAP, 44, 45

- Max_check_attempts, 32
- Monitoring, 36
- MySQL, 52

- Nagios, 13
- nagios.cfg, 29
- NetDisco, 19
- Network Health, 37
- Network Outage, 37
- Notification, 29
- NRPE, 45, 48

- Overview, 37

- Parents, 30, 32
- Performance, 37
- Perl, 12
- Ping, 32

POP3, 45

Recovery, 30

Reporting, 39, 63, 64

Service, 28

Service Detail, 38, 61

Services, 58, 61

SMTP, 33, 44

SNMP, 13, 48

SSH, 44, 46

SSH klíč, 47

Status Overview, 62

Timeperiod, 35

Unreachable, 30

View Config, 40

WWW konzole, 36

Zabbix, 18

Zdrojové kódy, 23

Zenoss, 16

Seznam obrázků

3.1	Ukázka monitorovacího systému „Nagios“	14
3.2	Ukázka monitorovacího systému „Akk@da“	15
3.3	Ukázka monitorovacího systému „Zenoss“	17
3.4	Ukázka monitorovacího systému „Zabbix“	18
3.5	Ukázka monitorovacího systému „NetDisco“	19
4.1	Porovnání hardwarových požadavků na systém	22
4.2	Ukázka stáhnutí zdrojových kódů Nagiosu	23
4.3	Ukázka kompilace zdrojových kódů Nagiosu	23
4.4	Ukázka úspěšného zkompileování Nagiosu	24
4.5	Ukázka začátku instalace Nagiosu pomocí příkazu <code>apt-get</code>	25
4.6	Ukázka začátku instalace Nagiosu pomocí příkazu <code>dselect</code>	25
4.7	Ukázka modifikace souboru <code>/etc/apache/httpd.conf</code>	26
4.8	Druhá modifikace souboru <code>/etc/apache/httpd.conf</code>	26
4.9	Modifikace souboru <code>httpd.conf</code> pro virtuální doménu	27
4.10	Ukázka úvodní stránky systému Nagios	27
5.1	Ukázka souboru <code>nagios.cfg</code> a odkazu na konfig. soubory	30
6.1	Úvodní obrazovka monitorovacího systému	37
6.2	Ukázka vygenerovaného „Availability Reportu“	40
7.1	Ukázka aktuální konfigurace zařízení a služeb	44
7.2	Spuštění příkazu pro zjištění disk. prostoru pomocí NRPE	46
7.3	Spuštění vzdáleného příkazu přes SSH spojení	47

7.4	Spuštění vzdáleného příkazu přes SSH tunel	47
8.1	Ukázka programovaného skriptu pro testování SW raidu	50
10.1	Přidání uživatele do systému	57
10.2	Přidání uživatele do skupiny ZF-admins	58
10.3	Přidání uživatele do skupiny ZF-admins	59
10.4	Přiřazení serverů ke kontaktní skupině ZF-admins	59
11.1	Sekce „Tactical Overview“	60
11.2	Sekce „Service Detail“	61
11.3	Sekce „Host Detail“	62
11.4	Sekce „Status Overview“	62
11.5	Sekce „Availability“	63
11.6	Sekce „Alert Summary“	63
11.7	Ukázka vygenerovaného „Event Log Reportu“	64
11.8	Ukázka aktuální konfigurace zařízení a služeb	65

Seznam tabulek

5.1	Tabulka objektových typů využívající Nagios	29
5.2	Ukázka definice zařízení v Nagiosu	31
5.3	Parametry spojené s testováním zařízení	31
5.4	Možnosti parametru <code>notification_options</code> u zařízení	32
5.5	Ukázka nadefinování služby v Nagiosu	33
5.6	Možnosti parametru <code>notification_options</code> u služeb	34
5.7	Ukázka definování kontaktu	34
5.8	Ukázka definování skupin	35
6.1	Popis odkazů sekce „Reporting“ webové konzole	39
7.1	Metoda <code>ping</code> k monitorování dostupnosti zařízení	42
7.2	Uvedení metody <code>check-host-alive</code> v definici zařízení	42
7.3	Metoda pro testování služby	43
7.4	Definice metody a testování v lokálním monitorování	43
7.5	Ukázka síťového monitorování <code>ssh</code> služby.	44
7.6	Definice metody k testování disk. prostoru službou <code>NRPE</code>	46
8.1	Návratové hodnoty pro vytváření vlastních skriptů	49