

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství



Diplomová práce

**Nasazení Zabbix monitorovacího systému
v korporátním prostředí**

Bc. Michal Áčko

© 2013 ČZU v Praze

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Nasazení Zabbix monitorovacího systému v korporátním prostředí" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil(a) autorská práva třetích osob.

V Praze dne 29. listopadu 2013

Bc. Michal Áčko

Poděkování

Rád bych touto cestou poděkoval svému vedoucímu diplomové práce panu Ing. Marku Píckovi, Ph.D., za výbornou komunikaci, nápadité úpravy moji diplomové práce a celkově aktivní přístup k vedení. Dále bych velmi rád poděkoval za spolupráci svým kolegům ze společnosti, kde byla vytvořena praktická část této diplomové práce, za ochotu poskytnout prostředky společnosti pro její vypracování, za jejich strávený čas a mé pozitivní naladění k vypracování této práce ve vypjatých chvílích. Dále za velmi kvalitní praktickou konzultaci z oboru informačních technologií a v neposlední řadě za ochotu věnovat se mé osobě a problémům spojených s touto diplomovou prací nejen v napjaté a časově náročné pracovní době. Jmenovitě bych rád uvedl kolegy Milana Gvoždíka, specialistu pro testování a administrátora testovacího prostředí, Václava Kolpeka, vedoucího oddělení administrátorů testovacích prostředí a nakonec Karla Svrčka, manažera kompletního teamu společnosti.

Nasazení Zabbix monitorovacího systému v korporátním prostředí

Deployment of Zabbix monitoring system in corporate environments

Souhrn

Tato práce úvodem pojednává obecně o monitorovacích systémech pro IT obor. Hlavní myšlenkou práce je však podrobně rozebrat monitorovací systém Zabbix.

K tomuto systému zde uvedeme další konkurenční systémy a porovnáme jejich klady a zápory, rozebereme obecné postoje k monitoringu a rozebereme základní otázky kolem monitorování sítí a jejich prvků.

Dále se dostaneme k praktické části práce, která nejdříve pojednává o obecných stanoviscích Zabbix systému a poté o instalaci Zabbix monitorovacího systému na Linux platformu. Zajistíme jeho kompletní zprovoznění a uvedeme si ukázkou naplnění Zabbix monitorovacího systému prvky pro praktickou ukázkou monitoringu.

Nakonec si ukážeme výstupy, které plynou ze sběru dat za pomoci monitorování sítě.

Summary

At first, this work deals with the general specifications of monitoring systems for IT sphere. The main idea of the work is to analyze in detail a monitoring system which is called Zabbix.

To this system there will be mentioned other competing systems and compare their pros and cons, discuss general attitudes to monitor and analyze fundamental questions about the monitoring networks and their elements.

Furthermore, we are getting to the practical part, which first discusses the general opinions of Zabbix system and then install the Zabbix monitoring system on Linux platform. We provide the complete launch and we will demo the fulfillment of Zabbix monitoring system elements for a practical demonstration of monitoring.

Finally, we show outputs that result from data collection using network monitoring.

Klíčová slova:

Monitorovací systém, server, agent, platforma, konfigurace, instalace, GUI, Zabbix

Keywords:

Monitoring system, server, agent, platform, configuration, installation, GUI, Zabbix

Obsah

1	Úvod.....	9
2	Cíl práce a metodika	9
3	Úvod do monitoringu	2
4	Základní otázky monitoringu.....	2
5	Způsoby monitoringu	3
5.1	Monitoring bez agenta.....	4
5.2	Monitoring s agentem.....	4
5.2.1	Monitoring s agentem – Passive Check	4
5.2.2	Monitoring s agentem – Active Check	5
5.3	Úrovně monitoringu	5
5.3.1	Komunikační protokol	5
6	Vlastnosti monitorovacího systému	6
7	Typy notifikace	7
8	Monitorované technologie.....	8
9	Přehled monitorovacích systémů	8
9.1	Zabbix.....	9
9.2	Nagios.....	10
9.3	Cacti	10
9.4	Zenoss.....	11
10	Platformy monitorovacího systému	12
11	Seznámení se s Zabbix	12
11.1	Zabbix – Historie	12
11.2	Zabbix – Co je to Zabbix	13

11.3 Zabbix – Myšlenka	14
11.4 Zabbix – Funkce	14
11.5 Zabbix – Monitorovací funkce	15
11.6 Zabbix – Podporované platformy	16
11.7 Zabbix – Slovníček	17
11.8 Zabbix – Potřebný software	19
11.9 Zabbix – Velikost databáze	21
11.10 Zabbix – HW a SW nároky	24
11.11 Zabbix – Jak jej získat	24
12 Zabbix – Instalace serveru	25
12.1 Zabbix – Instalace serveru - Zdroj	25
12.2 Zabbix – Instalace serveru - Uživatel	26
12.3 Zabbix – Instalace serveru – MySQL databáze	26
12.4 Zabbix – Instalace serveru – Konfigurace zdrojů	28
12.5 Zabbix – Instalace serveru – Instalace	28
12.6 Zabbix – Instalace serveru – Konfigurace po instalaci	29
12.7 Zabbix – Instalace serveru – Spuštění	29
13 Zabbix – Instalace webového rozhraní	31
13.1 Zabbix - Instalace GUI	32
13.1.1 Zabbix – instalace GUI - welcome	32
13.1.2 Zabbix – instalace GUI – Check of pre-requisites	33
13.1.3 Zabbix – instalace GUI – Configuration DB connection	33
13.1.4 Zabbix – instalace GUI – Zabbix server details	34
13.1.5 Zabbix – instalace GUI – Install	35
13.1.6 Zabbix – instalace GUI – Frontend is ready	35
13.2 Zabbix – Instalace Zabbix Agenta	36

14 Zabbix – Komunikace Server – Agent.....	39
15 Zabbix – GUI.....	40
15.1 Zabbix – GUI - Dashboard.....	40
15.2 Zabbix – GUI - Struktura.....	41
15.3 Zabbix – GUI – Popis prvků menu.....	42
16 Zabbix – GUI - Nejpoužívanější ovládací prvky.....	45
17 Zabbix – Započetí monitorování.....	45
17.1 Zabbix – Přidání Hosta	45
17.2 Zabbix – Přidání položky	47
17.3 Zabbix – Přidání triggeru	49
17.4 Zabbix – Konfigurace notifikace.....	51
17.4.1 Zabbix – Konfigurace notifikace - email	51
17.4.2 Zabbix – Konfigurace notifikace – Akce	52
17.5 Zabbix – Vytvoření template.....	54
18 Zabbix – IT Services	55
19 Zabbix – Výstupní informace	57
19.1 Zabbix – Výstupní informace - SLA	58
19.2 Zabbix – Výstupní informace - SLA	59
20 Závěr	60
21 Zdroje:	62
22 Seznam Obrázků:	64
23 Seznam Tabulek:.....	65
24 Přílohy:	66

1 Úvod

V dnešní době je funkčnost a spolehlivost informačních technologií nutností. Tyto vlastnosti by měly být zajištěny na sto procent po celý den, týden či rok. Proto je běžné, že větší společnosti vynakládají velké finanční prostředky na jejich denní údržbu, jistotu denního provozu a spolehlivost použitím kvalitního SW a HW.

Z pohledu sledování investic a sledování práce IT oddělení jsou výstupy monitoringu základním parametrem pro výslednou kontrolu nejen pro administrátory, ale i pro manažery.

V prostředích obrovských korporací, jak všichni víme, existuje velká byrokracie a chuť přehazování problémů z jednoho oddělení, na druhé a za každou cenu daný horký brambor nemít v ruce je bohužel denním chlebem.

Ze zkušeností z mé praxe, slouží monitoring serverů a sítě z pohledů manažera například k obhájení si výpadků systémů. Druhou stranou například bylo tvrzeno, že práce nemohla být provedena z důvodu výpadku systému. Ovšem po předložení výstupů monitoringu byl potvrzen fakt, že k výpadku systému nedošlo.

Sledovací systémy tedy jsou velmi užitečnou záležitostí ve sféře informačních technologií a jejich neustále zdokonalování a přizpůsobování nejnovějším trendům, přispívá k jejich neustále větší oblibě.

2 Cíl práce a metodika

Cílem této práce je praktická ukázka instalace monitorovacího systému Zabbix, jeho sledovacího serveru a agenta, náhled do komunikace mezi Zabbix serverem a agentem, popis monitorovacího systému Zabbix. Účelem je také názorně přiblížit monitorovací prostředí s popisem jednotlivých prvků a funkcí tohoto systému.

Dále v této práci rozebereme, jak se vytváří jednotlivé prvky sledování, ukážeme si grafický vývoj sledovaných prvků a definujeme si závěry z těchto grafů vyplývajících.

3 Úvod do monitoringu

V dnešní době je IT infrastruktura v obrovském rozmachu. Vše se přenáší do digitálních podob, neustále se zdokonaluje hardware i software. V podstatě je již problém najít ručně psaný dopis či tištěnou podobu tabulek s daty. Jednoduše řečeno snahou je uložit vše v digitální podobě v datových úložištích, nad daty pracují další aplikace, které spolu komunikují přes velmi důležitou síťovou infrastrukturu, a proto je funkční provoz s minimálními výpadky na prvním místě potřeb IT oddělení společností. Z těchto důvodů je dobré mít k dispozici monitorovací systémy, které budou dohlížet nad provozem těchto IT periférií a zároveň získávat data pro budoucí predikci chování společnosti nebo zpětnou kontrolu a vyvozování nových postojů společnosti.

Ve chvíli výpadku systému, serveru či prvku sítě, jsou administrátorovi kladeny různé typy otázek. „Jak dlouho tato aplikace neběžela?“, „Šlo předejít výpadku daného systému?“, „Jak zatěžuje nová dodávka softwaru daný server?“. Toto je jen pár otázek, na které by administrátor či manažer měl umět odpovědět. A právě odpovědi na tyto a podobné otázky poskytne monitorovací systém.

4 Základní otázky monitoringu

Základními otázkami monitoringu je myšleno zjistit důvody proč chceme něco monitorovat, jakým způsobem bychom chtěli monitorovat a konec konců chceme zhodnotit to, co bychom chtěli monitorovat tak, abychom se dostali k potřebným informacím zodpovídající naše otázky.

Důvodem proč monitorovat, jsou různé pro různé skupiny lidí, které požadují určité výstupy monitoringu. Některé skupiny potenciálních uživatelů monitorovacích systémů jsem již zmínil.

Například pro administrátory IT prostředí monitoring poskytuje informace o funkčnosti síťových prvků, aplikací, serverů, služeb atp. V případě výpadku či jiného problému je díky danému monitorovacímu systému administrátor ihned informovaný. Může daný problém začít řešit a do budoucna.

Další skupinou lidí, pro kterou je monitorovací systém výborným zdrojem informací, jsou manažeři společností. S jejich pomocí mají celé základny informací o tom, kolik bylo výpadků systémů, na jak dlouho, jakých prvků sítě atp. Tyto informace slouží například k určení SLA (Service Level Agreement) označující smlouvu sjednanou mezi poskytovatelem služby a jejím konzumentem nebo k tvorbě různých reportů.

Otázkou je, co monitorovat. Nejlepší pro efektivní řešení problému IT infrastruktury je začít s monitorováním aktivních síťových prvků. Pod tímto pojmem si můžeme představit například hub. Ve chvíli, kdy takovýto hlavní prvek sítě nefunguje, mohou se vyskytovat velkoplošné výpadky sítě, následně výpadky serverů a na nich běžících aplikací.

Dalším z ne méně důležitých prvků sítě pro monitoring jsou jednotlivé servery. Monitoruje se například jejich zatížení, výkonnost či zaplněnost datových disků, vytížení operační paměti, vytížení samotného procesoru atp. Na nich se potom mohou monitorovat služby a aplikace, které na daných serverech běží.

Mezi základní nejdůležitější aplikace fungujících na serverech můžeme řadit například webový server, SMTP server nebo DNS server, sloužící k vzájemnému překladu IP adres a doménových názvů.

5 Způsoby monitoringu

Volba způsobu monitoringu záleží převážně na tom, co chceme monitorovat. Určitě by šlo vytvořit detailnější rozdělení, ale pro základní přehlednost budou způsoby monitoringu rozděleny do dvou kategorií.

Tyto kategorie jsou:

- Monitoring bez agenta
- Monitoring s agentem

5.1 Monitoring bez agenta

Tato metoda se používá při monitorování síťově přístupných služeb. Například při kontrole, zda na daném serveru běží webový server. V takovém případě se sledovací systém pokusí připojit na port webového serveru (http, 80) a pokud by se nedokázal připojit, zahlásí monitorovací systém problém.

Typem této metody monitoringu může být například SimpleCheck metoda, která je zpracována sledovacím serverem.

5.2 Monitoring s agentem

Tato metoda poskytuje navíc informace například o zaplnění datových disků či vytížení procesoru, které jsou přístupné v rámci operačního systému daného serveru. Chceme-li tyto informace monitorovat, je potřeba mít takzvaného agenta (software pro stahování informací), který potřebné informace vytáhne z operačního systému a přepoše je sledovacímu serveru.

Dále můžeme tuto metodu pro monitoring s agentem rozdělit do dvou typů monitorování.

5.2.1 Monitoring s agentem – Passive Check

Tato metoda zasílání informací funguje principiálně tak, že monitorovací systém na sledovacím serveru zašle na daný sledovaný server danému agentovi požadavek na určitou hodnotu, například aby zjistil jak je určitý disk zaplněný či určitý procesor využitý. Ten tyto informace „vytáhne“ z operačního systému a zašle jej zpět na server s monitorovacím systémem, kde se informace uloží pro další jejich využití. Tento typ zasílání na základě dotazu je nazýván tzv. Passive Check. Uvedený způsob je více náročný na zatížení Zabbix serveru.

5.2.2 Monitoring s agentem – Active Check

Druhá metoda zasílání dat je tzv. Active Check. Ta funguje na principu, že agent jednou za určité období závislé na frekvenci obměny sledovaných prvků serveru obdrží seznam monitorovaných prvků serverů a agent je v pravidelných intervalech dle vlastní konfigurace posílá serveru zpět ke zpracování a vyhodnocení. Tento způsob je méně náročný na zatížení Zabbix serveru.

5.3 Úrovně monitoringu

Monitorované prvky můžeme kontrolovat na více úrovních. Jak jsme již demonstrovali na webovém serveru, základní kontrola je, že se agent připojí na port webového serveru obvykle označený číslem 80. Pokud se mu podaří na port připojit, agent pošle informaci zpět, že server běží a systém hlásí jeho správnou funkci.

Další úroveň kontroly je, že se agent připojí na server, server poskytne určitou HTML stránku, která by měla být při správném běhu webového serveru dostupná. Pokud agentovi bude tato stránka poskytnuta, pošle zpět monitorovacímu systému informaci o správném běhu služby.

Poslední úroveň kontroly je, že se server připojí opět na port webového serveru, poté si nechá vygenerovat HTML stránku a následně v textu bude vyhledávat slovní řetězce, které by měla stránka při generování bez chyb obsahovat. Ve chvíli, kdy tyto řetězce agent najde, pošle informaci monitorovacímu systému zpět o tom, že služba běží správně.

5.3.1 Komunikační protokol

Komunikační protokol je způsob, jak mezi sebou komunikují monitorovací systém se svým agentem či síťovými prvky přímo. Zde můžeme zmínit několik komunikačních protokolů.

Protokol SNMP neboli Simple Network Management Protocol. Je to standardizovaný protokol sloužící k monitorování aktivních síťových prvků v síti. Tento protokol byl vydán v několika verzích.

- SNMP v1 – Vznik v roce 1988 a jeho slabina byla v posílání hesla v otevřeném tvaru.
- SNMP v2 – V této verzi se odstranil problém s otevřenou podobou hesla.
- SNMP v3 – Přidáno navíc šifrování kvůli možnému sniffingu.

Další protokol, který je standardizován, je asi nejběžnější protokol TCP. Tento protokol je takzvanou nadstavbou protokolu UDP, který má tu nevýhodu, že zpětně nekontroluje přijatá data. TCP protokol odešle data a čeká na zprávu z druhé strany, zda všechny datové pakety přišly, kam měly.

Další protokol pro komunikaci použitelný v monitorování sítě je IPMI. Je to specifický protokol, kterým komunikuje pouze některý speciální hardware, proto je jeho použití ojedinělejší.

V neposlední řadě je potřeba zmínit protokol http, díky kterému mohou některé monitorovací systémy a jejich agenti navzájem komunikovat.

Jako poslední, zde uvedu možnost nakonfigurovat svůj vlastní protokol a definovat pravidla, dle kterých budou informace odesílány, přijímány, šifrovány atp. Některé monitorovací systémy mají své vlastní komunikační protokoly.

6 Vlastnosti monitorovacího systému

Na vlastnosti, které by měl mít monitorovací systém, lze nahlížet opět z několika hledisek.

Podíváme-li se z hlediska administrátorského, mohli bychom uvést tyto požadavky na monitorovací systémy:

- Přehled o infrastruktuře – nejen celkový pohled na hardwarovou skladbu IT infrastruktury společnosti, ale také přehled jednotlivých běžících aplikací či služeb.
- Zjišťování chybových stavů – v případě, že se některý prvek monitorovaných objektů dostane do chybového stavu, chceme, aby se monitorovací systém o tomto dozvěděl, a to v co nejkratším čase.

- Nahlášení chybových stavů – Nakonec v případě, že se vyskytne chybový stav na některém z monitorovaných prvků, je potřeba, aby jej monitorovací systém nahlásil odpovědným osobám, většinou administrátorům. Způsoby můžou být různé dle nastavení notifikace monitorovacího systému.

Další hledisko bude manažerské, kde můžeme uvést tyto požadavky:

- Reporty – Monitorovací systém by měl umět vygenerovat souhrnné zprávy či přehledy o výpadcích, jak dlouho jednotlivé výpadky trvaly atp.
- Grafy – Monitorovací systém by měl umět graficky zobrazit nasbírané data za určitý časový úsek a poskytnout přehledy v určitém časovém horizontu. To může pomoci k vyzorování určité frekvence výpadku či zvýšení využití procesoru a do budoucna tento jev eliminovat.

7 Typy notifikace

Notifikace je oznámení o nějaké události. V našem případě je to oznámení o chybovém stavu některého z monitorovaných objektů. Obecně existuje několik možných notifikací.

- První notifikací je obyčejné oznámení v takzvané souhrnné stránce monitorovacího systému, kde se ve vizuální podobě objeví chybové hlášení.
- Druhou možností notifikace je možnost odesílání takzvaných chybových emailů v podobě popisu chyby odesílané předem nakonfigurovaným příjemcům, administrátorům.
- Třetí, pravděpodobně nejméně používanou možností je notifikace za pomoci SMS zprávy. Tento typ notifikace je vhodný pro administrátory pracující s 24 hodinovou pohotovostí s největší pravděpodobností okamžité reakce informované strany.

- V dalších případech se používá navíc notifikace za pomoci instant-message klientů, to znamená za pomoci chatovacích programů, ke kterým je člověk obvykle připojen většinu dne. Tím je zajištěna rychlá reakce na vzniklý problém.

8 Monitorované technologie

V informačních technologiích existuje velké množství objektů, které je možné dohledovými systémy monitorovat. Obecně si je můžeme shrnout do těchto následujících bodů:

- Servery (hardware i jednotlivé aplikace)
- Konektivita (internet, propojení poboček)
- Firewally
- Aktivních síťové prvky
- Platnost SSL certifikátů
- Periferie (stav tiskáren – docházející tonery a podobně)
- Teplotní a vlhkostní čidla
- Webové prezentace

9 Přehled monitorovacích systémů

Jak již bylo řečeno v úvodu, IT sféra prožívá obrovský a rychlý rozmach co se týče HW a ruku v ruce s ním i SW. S tím je spojen fakt, že neexistuje pouze jeden monitorovací systém. Proto, než se dostanu k mému vybranému monitorovacímu systému a jeho specifikaci, rád bych uvedl i několik jeho konkurentů.

Je třeba říci, že se v této práci zabírám pouze open-source systémy, systémy, které nejsou vyvíjeny pod vlastnickými právy a každý, kdo se na vývoji podílí, přispívá svým dílem.

Open-source software lze detailněji prostudovat v propracovaném článku na webových stránkách v následujícím zdroji.

“ Otevřený software (anglicky open-source software nebo open software, zkratka OSS) je počítačový software s otevřeným zdrojovým kódem. Otevřenost zde znamená jak technickou dostupnost kódu, tak legální dostupnost - licenci software, která umožňuje, při dodržení jistých podmínek, uživatelům zdrojový kód využívat, například prohlížet a upravovat (na rozdíl od proprietárního software).”

(Zdroj: http://cs.wikipedia.org/wiki/Open_source)

Asi nejstarším monitorovacím systémem je systém Zabbix, který jsem si vybral pro svoji praktickou část diplomové práce. Níže je uvedený přehled začátků několika porovnávaných monitorovacích systémů.

- Zabbix – 1998 od 2001 licence GPL
- Nagios – 2002 licence GPL
- Cacti -2004
- Zenoss - 2002

Licence GPL (General Public Licence) je licence, která označuje svobodný software.

9.1 Zabbix

- + jeho přehlednost a konfigurace se může zdát jednodušší než u Nagios
- + velmi dobrá dokumentace (360 stránek PDF + webová dokumentace)
- + graficky hezky zpracovaný (PHP)
- + dostatečná podpora platformy Windows
- + živý projekt (stále nové inovace, velká komunita)
- editor pro tvorbu serverových map je z pohledu konfigurace náročný
- jedna Item(položka) vrací pouze jednu hodnotu
- při tvorbě nové Item, obtížné vyřešit, proč daná Item nevrací hodnotu

9.2 Nagios

- + open source
- + mnoho pluginu
- + ladění pluginu je jednoduché
- + živý projekt (stále nové inovace, velká komunita)
- důraz kladen na kontrolu dostupnosti monitorovaných objektů
- některé detaily ve webovém rozhraní nejsou dostatečně zřejmé
- textová konfigurace, mnoho různých nastavení a často je nutno se vracet k parametrům nastavení

9.3 Cacti

- + velmi pěkné webové rozhraní
- + velmi pěkné grafické výstupy – lze například za pomoci javascriptů přibližovat grafy
- + široké nastavení uživatelských práv systému
- + jednoduchá úprava grafů pro specifické view(pohledy) na grafy
- grafy občas samy od sebe přestanou vykreslovat
- občas se vyskytují mezery v nasbíraných datech (při snížení defaultní frekvence sbírání dat pod 5 minut)
- problémy se zpracováním SNMP
- neumí skládat výsledky monitorování clustrovaných zařízení

9.4 Zenoss

- + velmi pěkné webové rozhraní
- + integrace webových map od společnosti Google pro zobrazení jednotlivých monitorovaných serverů
- + parametry systému jsou částečně zjišťovány automaticky
- + funguje na původním SNMP protokolu bez specifického agenta
- + velká základna uživatelů, z čehož plyne hodně informací a zkušenosti online
- webové rozhraní je pomalé
- pouze jedna základní obecná obrazovka pro vypisování výsledků monitorování
- limitované open-source verze, plná verze je zpoplatněna

Z výše uvedených kladů a záporu jednotlivých porovnávaných open-source sw pro sledování sítě můžeme vypozařovat, že se vytvořily dvě skupiny, které mají sobě podobnější vlastnosti. První je Zabbix a Nagios a druhá je Cacti a Zenoss. Zabbix a Nagios můžeme zařadit do softwaru pro pokročilé a rozsáhlejší monitorování větších sítí s jistotou monitorování. Cacti a Zenoss můžeme zařadit do skupiny monitorovacích systémů pro menší sítě, pro méně sledovaných prvků, jsou méně konfiguračně náročné, za to s velmi pěkně zpracovanými výstupy.

Více informací lze dohledat v níže uvedeném článku, který posloužil jako zdroj uvedeného srovnání.

(Zdroj: <http://www.serverfocus.org/nagios-vs-cacti-vs-zabbix-vs-zenoss>)

10 Platformy monitorovacího systému

Jak je zřejmé, není možné, aby se dnes software vyvíjel na specifický operační systém, jednoduše řečeno se snažil držet pouze jednoho směru. Je potřeba zajistit funkčnost na všech možných platformách, aby se pokryl co největší počet zájemců o daný systém a firma vyvíjející určitý SW tak získala větší základnu potencionálních zákazníků, v našem případě open-source uživatelů.

Je možné debatovat několik hodin na téma jaká serverová platforma je dnes ve světě nejvíce využívána, ale z mého pohledu, nejvíce serverů obecně funguje na platformě Unix, z kterého vychází většina vyvinutých OS.

Jako další nejvíce využívaná platforma je z mého pohledu operační systém Linux, který částečně vychází z platformy Unix.

V poslední řadě je to od společnosti Microsoft platforma Windows Server.

Dále můžeme zmínit platformy FreeBSD, OpenBSD, MAC či Aix.

Ve společnosti, kde se také používá mnou probíraný Zabbix monitorovací systém, existuje přibližně 200 serverů, a to pouze ve spolupráci s jednou firmou.

Pro takové množství serverů a rozmanitost využívaných serverových platforem je jasné, že monitorovací systém musí podporovat sledování různých operačních systémů.

11 Seznámení se Zabbix

Nyní se již dostáváme k praktické části diplomové práce. Pro začátek si detailněji přiblížíme monitorovací systém Zabbix, jeho začátky, kdo stojí za jeho vznikem, kam až šahají jeho kořeny a v neposlední řadě jeho dnešní podobu.

11.1 Zabbix – Historie

Historie tohoto monitorovacího systému sahá až do roku 1998. V tu dobu přišla na svět myšlenka pana Alexeie Vladisheva, pocházejícího z Litvy, vytvořit monitorovací systém pro servery a sítě na open-source bázi.

První převratný zlom pro Zabbix byl v roce 2001, kdy vyšla první verze systému Zabbix 1.0.

V roce 2005 byla založena společnost Zabbix SIA pro poskytování služeb podpory Zabbix monitorovacích systémů ze strany expertů na tuto problematiku.

V roce 2007 vyšla nová verze systému Zabbix 1.7.

V roce 2008 vyšla další verze systému Zabbix 1.8.

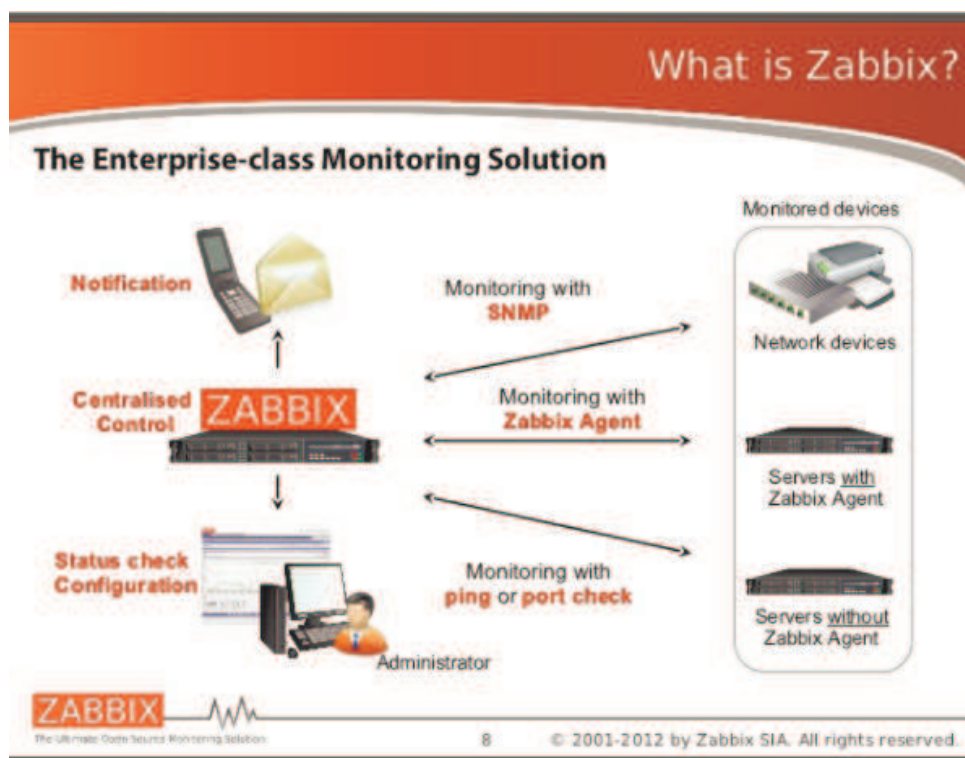
V roce 2009 vyšla verze systému Zabbix 1.9.

A jako poslední v roce 2012 vyšla verze 2.0, která je nyní stále zlepšována a vyvíjena ve spolupráci s širokou komunitou uživatelů tohoto systému.

V současnosti má společnost Zabbix SIA celosvětově více jak 45 partnerů, s kterými spolupracuje na vývoji.

11.2 Zabbix – Co je to Zabbix

V této kapitole si graficky přiblížíme, co je to Zabbix a jak funguje.



Obrázek 1. – Co je to Zabbix, zdroj: <http://www.zabbix.com/presentation.php>

Zabbix monitorovací systém je centralizovaný sledovací systém nainstalovaný na určitý server. Na tomto serveru se konfiguruje jednotlivé prvky sítě, které se následně budou monitorovat a také jakým způsobem bude monitoring realizován.

Zabbix, jak již bylo řečeno obecně v kapitole o notifikacích monitorovacích systémů, informuje o problémech několika cestami. Jsou jimi například SMS nebo e-mail. Dále umí notifikovat za pomoci Jabberu neboli zprávy do chatu nebo spuštěním určitého, námi definovaného příkazu či skriptu.

11.3 Zabbix – Myšlenka

Hlavní myšlenkou monitorovacího systému Zabbix je ušetření nákladů na downtime sítě či jejich prvků. Pojmem downtime rozumíme čas, kdy prvek sítě či celá síť je nefunkční. Za pomoci sledovacího systému se snažíme předejít výpadku prvků.

Dále také pracuje s myšlenkou zpracovávání a uchovávání dat monitorovaných prvků a jejich následné reportování či grafické zpracování.

11.4 Zabbix – Funkce

Jednotlivé funkce Zabbix monitorovacího systému lze rozdělit do 4 kategorií.

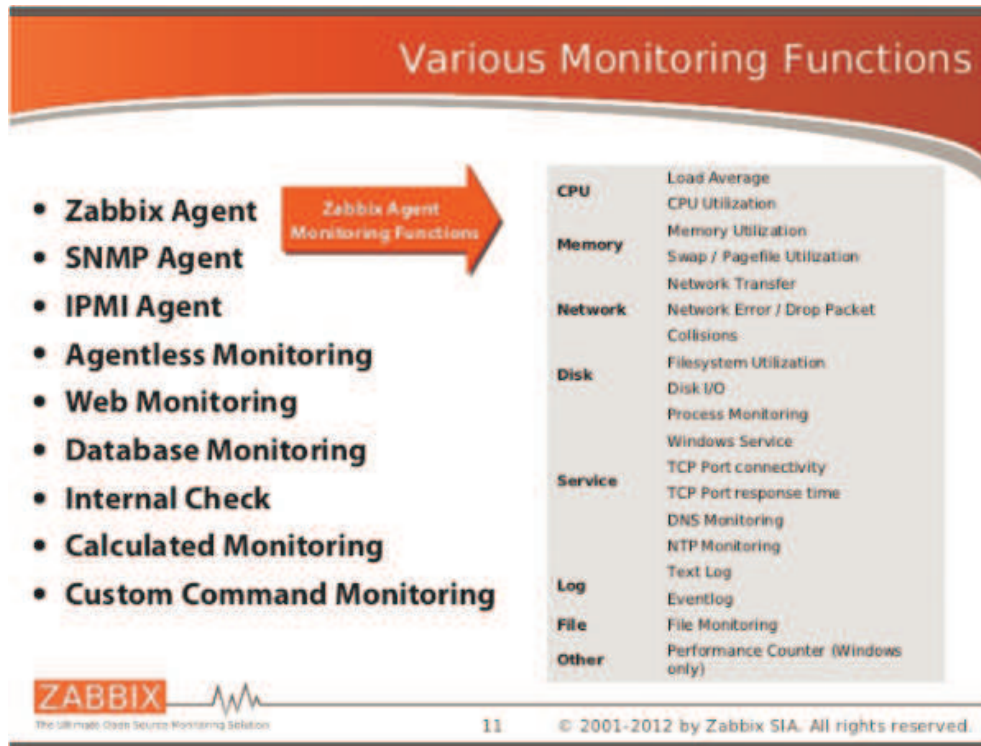
Jsou jimi:

- Sběr dat
- Tvorba datových základů
- Zasílání upozornění
- Grafická vizualizace

Základní funkce nejen tohoto monitorovacího systému je sbírání dat z jednotlivých sledovaných prvků. Na jejich základě si za podpory databáze systém vytváří velké množství nasbíraných dat, z kterých lze vyvodit jisté důsledky chování daných síťových prvků či celé sítě. Naskytne-li se nějaký problém, Zabbix systém zašle upozornění v podobě SMS či e-mailu.

11.5 Zabbix – Monitorovací funkce

Uvedeme si zde obrázek, který nám definuje různé možnosti monitorování tohoto systému.



Obrázek 2. – Monitorovací funkce, zdroj: <http://www.zabbix.com/presentation.php>

Na tomto obrázku v levé části jsou k vidění možnosti monitorování, které podporuje Zabbix monitorovací systém.

Samozřejmě je vlastní Zabbix agent. Dále ovšem Zabbix umí podporovat samotné monitorování za pomoci SNMP Agentu, IPMI Agentu, ale také monitorování bez agenta.

V neposlední řadě Zabbix umí monitorovat například databáze a weby, kde sleduje například čas odezvy, rychlost download nebo odesílaný webový kód, zda se webová stránka zobrazuje korektně.

V pravé části obrázku jsou vidět jednotlivé položky, které mohou být monitorovány. Nutno podotknout, že se jedná se o základní rozdělení.

11.6 Zabbix – Podporované platformy

Jak již bylo řečeno obecně, je potřeba kvůli dnešnímu množství operačních systémů zajistit chod softwaru na více platformách.

Díky open-source licenci Zabbix a jeho četné skupině uživatelů je možné vyvíjet software na tolika platformách, s kolika pracují jeho fanoušci a proto jich není zrovna málo.

Níže je uvedený seznam platform, na kterých byl Zabbix testován a existují naň oficiální instalační balíčky.

- Linux
- IBM AIX
- FreeBSD
- NetBSD
- OpenBSD
- HP-UX
- Mac OS X
- Solaris
- Windows: 2000, Server 2003, XP, Vista, Server 2008, 7, Server 2012 (Zabbix agent only)

Seznam platform vychází z níže uvedeného zdroje pro verzi Zabbix 2.0

(Zdroj: <https://www.zabbix.com/documentation/2.0/manual/installation>)

11.7 Zabbix – Slovníček

Aby se lépe orientovalo v této práci, uvedu zde několik slovíček, která budou v práci dále hojně používány. Mezi základní názvosloví patří následující.

host

- host je síťové zařízení, které chceme monitorovat za pomoci IP nebo DNS

item

- položka definuje konkrétní typ dat, které chceme sbírat od hosta

trigger

- trigger, čti trigr, je pomyslná hodnota nasbíraných dat sledované položky od hosta, která definuje takové hodnoty, které jsou v pořádku a hodnoty které jsou rizikové, nepřijatelné.

Funkci triggerů si můžeme demonstrovat na následujícím příkladu. Když dostáváme hodnoty položky od hosta v rozmezí 1 až 10 a my nastavíme trigger na hodnotu 7, která je pro nás již kritická, objeví se u položky status OK v případě, že hodnoty budou od 1 do 6. Status PROBLEM, se objeví, bude-li hodnota položky od 7 do 10.

event

- událost je informace o tom, že se někde něco stalo. Většinou je událost spojena s triggerem a jeho změnou stavu například z OK na PROBLEM. Dále se může evidovat za pomoci „objevení“ nebo „auto-registrací“ aktivních agentů. Objevením je myšleno například automatické zjištění nové položky k monitorování na serveru.

action

- akce je předdefinovaná reakce na událost.

Akce je většinou složena z notifikace a podmínky notifikování. Pod notifikací si můžeme představit například zasílání SMS, e-mailu atp.

frontend

„Frontend“ neboli nadstavba je program, který usnadňuje práci s konzolovými nástroji tím, že pro zadávání parametrů a obsluhu funkcí poskytuje grafické (GUI) nebo textové (TUI) uživatelské rozhraní.“

(Zdroj: <http://www.abclinuxu.cz/slovník/frontend>)

- za frontend neboli nadstavbu je považováno webové rozhraní sloužící k obsluze Zabbix monitorovacího systému.

backend

„Stojí za zmínku, že skoro všechny poloprofesionální až profesionální weby s dynamickým obsahem skončí u koncepcie "frontend-backend". To jednoduše znamená, že existují stránky pro uživatele portálu (tedy frontend), na nichž je zobrazeno to, co potřebuje návštěvník webu vidět, a stránky pro administrátora, kde je zase naopak to, co potřebuje ke vkládání dat (backend). Někde "mezi" tím vším jsou data k zobrazení, převážně uložená v databázi“

(Zdroj: http://www.linuxsoft.cz/article.php?id_article=551)

- za backend neboli administraci je považováno to, co je potřeba k správě a provozu naší databáze či webového rozhraní, čili administrátorský software. U Zabbix monitorovacího prostředí za backend považujeme samotnou instalaci Zabbixu, Apache webový server či databázový systém.

Zabbix server

- Zabbix server je takzvaný centrální mozek monitorování. Jedná se o proces, který provádí monitorování, sběr dat, komunikaci s agenty, hlídání triggerů, posílá notifikace, ukládá data.

Zabbix agent

- Jedná se o proces instalovaný na cílených hostech, které chceme monitorovat a slouží k aktivnímu monitorování serveru, aplikací atp.

11.8 Zabbix – Potřebný software

Tato kapitola pojednává o dodatečném software, který je potřebný k provozu Zabbix monitorovacího systému.

Jsou jim Apache webový server s podporou PHP a databázový systém.

Níže jsou uvedené možnosti software pro konstrukci databáze pro ukládání namonitorovaných dat. Kvůli kompatibilitě je nutné zachovat podporovanou verzi.

<i>Software</i>	<i>Version</i>	<i>Comments</i>
MySQL	5.0 or later	Required if MySQL is used as Zabbix back end database. InnoDB engine is required.
Oracle	10g or later	Required if Oracle is used as Zabbix back-end database.
PostgreSQL	8.1 or later	Required if PostgreSQL is used as Zabbix back-end database.
SQLite	3.3.5 or later	Required if SQLite is used as Zabbix back-end database.
IBM DB2	9.7 or later	Required if IBM DB2 is used as Zabbix back end database.

Tabulka 1. - Podporované databázové systémy, zdroj:
<https://www.zabbix.com/documentation/2.0/manual/installation>

U možnosti MySQL je zapotřebí, dle výše uvedené tabulky, InnoDB engine. InnoDB engine je jeden z formátů úložiště dat kompatibilní se Zabbix.

Níže jsou uvedené možnosti software pro konstrukci frontend prezentace Zabbix serveru, jinými slovy software, který je potřeba, aby se nám korektně zobrazoval Zabbix ve webovém prohlížeči.

<i>Software</i>	<i>Version</i>	<i>Comments</i>
Apache	1.3.12 or later	
PHP	5.1.6 or later	
<i>PHP extensions:</i>		<i>Comments</i>
gd	2.0 or later	PHP GD extension must support PNG images (--with-png-dir), JPEG (--with-jpeg-dir) images and FreeType 2 (--with-freetype-dir).
bcmath		php-bcmath (--enable-bcmath)
ctype		php-ctype (--enable-ctype)
libXML	2.6.15 or later	php-xml or php5-dom, if provided as a separate package by the distributor.
xmlreader		php-xmlreader, if provided as a separate package by the distributor.
xmlwriter		php-xmlwriter, if provided as a separate package by the distributor.
session		php-session, if provided as a separate package by the distributor.
sockets		php-net-socket (--enable-sockets). Required for user script support.
mbstring		php-mbstring (--enable-mbstring)
gettext		php-gettext (--with-gettext)
ibm_db2		Required if IBM DB2 is used as Zabbix back end database.
mysql		Required if MySQL is used as Zabbix back end database.
oci8		Required if Oracle is used as Zabbix back-end database.
pgsql		Required if PostgreSQL is used as Zabbix back-end database.
sqlite3		Required if SQLite is used as Zabbix back-end database.

Tabulka 2. - Dodatečný software, zdroj:
<https://www.zabbix.com/documentation/2.0/manual/installation>

Opět kvůli kompatibilitě je nutné zachovat podporovanou verzi.

11.9 Zabbix – Velikost databáze

Dalším krokem před instalací je zjistit, jak velkou databázi budeme potřebovat a za tímto účelem zajistit dostatečné místo na disku serveru.

Jednoduchým příkladem si spočítáme případnou velikost naší databáze, která je závislá na počtu sledovaných položek, času obnovovací frekvence a intervalu uchovávání historie naměřených dat.

Mějme 3000 položek, které chceme monitorovat a jejich frekvence znovuoobnovení bude 60 vteřin. To znamená, že každým 60 vteřin se do Zabbix databáze přepíše nová hodnota dané položky.

Příklad: $3000/60=50$ Hodnota 50 je počet nových hodnot připsaných každou vteřinu do databáze.

Nyní si musíme uvědomit, jak dlouho chceme naměřená data uchovávat v databázi. Čím déle budeme data uchovávat, tím budeme potřebovat větší databázi a současně ale budeme mít i větší možnost vrátit se v čase zpět.

Řekněme, že budeme chtít uchovávat informace po dobu jednoho měsíce, tedy 30 dní, aby se nám lépe počítalo.

Příklad: $50*(30*24*3600)=129\ 600\ 000$ Hodnota 129 600 000 je počet nových hodnot připsaných do databáze za 30 dní.

Velikost jedné zapsané hodnoty do databáze se může lišit díky několika aspektům. Jeden je například použitý databázový SW, druhý pak typ ukládané hodnoty jako jsou například Integer, Var, String, Varchar, Numeric atd.

„Depending on the database engine used, type of received values (floats, integers, strings, log files, etc), the disk space for keeping a single value may vary from 40 bytes to hundreds of bytes. Normally it is around 50 bytes per value.“

(Zdroj: <https://www.zabbix.com/documentation/2.0/manual/installation>)

Z výše uvedené citace lze však říci, že průměrná hodnota uložené jedné položky je 50 Bytes.

- Historii spočítáme následovně.

Příklad: $129\,600\,000 \cdot 50 \text{ Bytes} = 6\,480\,000\,000 \text{ Bytes}$ Hodnota 6,48 GB reprezentuje velikost databáze pro uchování hodnot pro jeden měsíc pro zobrazení naměřených hodnot.

<i>Parameter</i>	<i>Formula for required disk space (in bytes)</i>	
Zabbix configuration	Fixed size. Normally 10MB or less.	
History	items : number of items	days*(items/refresh rate)*24*3600*bytes
	days : number of days to keep history	
	refresh rate : average refresh rate of items	
	bytes : number of bytes required to keep single value, depends on database engine, normally 50 bytes.	
Trends	items : number of items	days*(items/3600)*24*3600*bytes
	days : number of days to keep history	
	bytes : number of bytes required to keep single trend, depends on database engine, normally 128 bytes.	
Events	events : number of event per second. One (1) event per second in worst case scenario.	days*events*24*3600*bytes
	days : number of days to keep history	
	bytes : number of bytes required to keep single trend, depends on database engine, normally 130 bytes.	

Tabulka 3. - Vzor pro výpočet velikosti databáze, zdroj: <https://www.zabbix.com/documentation/2.0/manual/installation>

Toto je jeden ze způsobů, jak vypočítat velikost databáze pro archivaci naměřených hodnot. Níže je uvedena tabulka, kde jsou uvedeny i další výpočty pro trendy a události potřebné k specifikaci velikosti Zabbix databáze.

(Zdroj: <https://www.zabbix.com/documentation/2.0/manual/installation>)

- Trendy spočítáme následovně.

Příklad: $30 \cdot (3000/3600) \cdot 24 \cdot 3600 \cdot 128$ Bytes = **276 480 000** Hodnota 0,27648 GB reprezentuje velikost databáze pro uchování hodnot pro jeden měsíc pro zobrazení trendů.

Hodnota 128 je velikost 128Bytes jedné uložené hodnoty pro zobrazení dlouhodobých trendů, grafů.

„Zabbix database, depending on database type, requires about 128 bytes per each total“

(Zdroj: <https://www.zabbix.com/documentation/2.0/manual/installation>)

- Události spočítáme následovně.

Z počátku je třeba říci, že je těžké odhadnout, kolik událostí bude vyvoláno za jeden den. Nelze to jednoznačně definovat, a tak budeme uvažovat poměrně nereálnou možnou situaci, že se vyvolá 1 událost za jeden den provozu.

Příklad: $30 \cdot 24 \cdot 3600 \cdot 130$ Bytes = **336 960 000** Hodnota 0,336960 GB reprezentuje velikost databáze pro uchování hodnot pro jeden měsíc pro zpětné zobrazení vyskytnutých událostí.

„Each Zabbix event requires approximately 130 bytes of disk space.“

(Zdroj: <https://www.zabbix.com/documentation/2.0/manual/installation>)

Hodnota 130 je velikost 130Bytes jedné uložené hodnoty pro zobrazení vyskytnutých událostí.

Ke konečné velikosti naší databáze je potřeba sečíst výsledné hodnoty pro Historii, Trendy a Události.

11.10 Zabbix – HW a SW nároky

Hned ze začátku bych rád uvedl, že pro naše účely byla nainstalována verze Zabbix monitorovacího systému Zabbix 2.0.

Ještě před instalací tohoto sledovacího systému je třeba si uvědomit, jak velkou síť chceme monitorovat.

Níže je uvedená tabulka, která nám ukazuje doporučené „vybavení“ SW a HW pro různé velikosti sítí.

<i>Name</i>	<i>Platform</i>	<i>CPU/Memory</i>	<i>Database</i>	<i>Monitored hosts</i>
Small	Ubuntu Linux	PII 350MHz 256MB	SQLite	20
Medium	Ubuntu Linux 64	AMD Athlon 3200+ 2GB	MySQL InnoDB	500
Large	Ubuntu Linux 64	Intel Dual Core 6400 4GB	RAID10 MySQL InnoDB or PostgreSQL	>1000
Very large	RedHat Enterprise	Intel Xeon 2xCPU 8GB	Fast RAID10 MySQL InnoDB or PostgreSQL	>10000

Tabulka 4. - HW a SW nároky, zdroj:
<https://www.zabbix.com/documentation/2.0/manual/installation>

11.11 Zabbix – Jak jej získat

Je několik možností, jak získat instalační soubory Zabbix.

První možností je Instalovat Zabbix z balíčku zkompilevaného pro Vámi používanou platformu.

Druhou možností je stáhnout z Internetu binární soubory a za pomoci C kompiléru, je zkompilevat na náš specifický hardware.

Třetí a poslední možností je stáhnout virtuální instalaci Zabbix, která za pomoci internetového prohlížeče nainstaluje Zabbix server.

V našem případě jsem zvolil první možnost, stažení již hotového balíčku na danou platformu.

Navíc od klasické instalace byl upraven konfigurační soubor tak, aby vyhovoval specifickým požadavkům na instalaci v našem korporátním prostředí a byl zajištěn bezproblémový chod pro monitoring skoro 160 serverů.

12 Zabbix – Instalace serveru

V této kapitole se již podíváme na samotnou instalaci a jednotlivé příkazy, které jsou potřebné pro provedení instalace.

Instalaci provádíme na platformu **GNU/Linux 64-bit** ve verzi **2.6.32**.

12.1 Zabbix – Instalace serveru - Zdroj

Nejprve si stažený balíček z webových stránek Zabbix musíme rozbalit.

To provedeme následujícím příkazem:

```
tar -zxvf zabbix-2.0.0.tar.gz
```

Parametr „x“ ukazuje, že chceme extrahovat daný soubor a parametr „z“ ukazuje, že se jedná o archivátor gzip. „v“ pak ukazuje možnost „verbous“, ve volném překladu řečeno mluvený. V tomto případě nám to vypíše jednotlivé kroky extrahace. „f“ parametr poté naznačuje, že v syntaxi příkazu jako další bude uvedena cesta k souboru, s kterým budeme pracovat.

12.2 Zabbix – Instalace serveru - Uživatel

Dále je potřeba vytvořit neprivilegovaného uživatele, pod kterým bude Zabbix server spuštěn. Privilegovaným uživatelem se rozumí uživatel, který má práva administrátora nebo uživatel uživatelů, root.

Proto si vytvoříme uživatele, v našem případě, „**zabbix**“. Vytvoříme jej následující posloupností příkazů:

```
groupadd zabbix  
useradd -g zabbix zabbix
```

Nejprve byla vytvořena skupina **zabbix** a následně do ní přidán nově vytvořený uživatel **zabbix**.

12.3 Zabbix – Instalace serveru – MySQL databáze

Nyní si vytvoříme Zabbix databázi. V jedné z předchozích kapitol, kde jsme rozebírali potřebný software, jsme uvedli podporované databázové systémy. Pro praktickou část diplomové práce jsem zvolil systém MySQL. Je to free software, s kterým umí komunikovat velké množství dalšího software.

Instalaci samotného SQL serveru přeskočíme, jelikož se tímto tématem tato práce nezabývá. Uvedu zde však alespoň jeden zdroj, kde konkrétní informace o instalaci SQL serveru jsou k dispozici.

Na níže uvedeném zdroji lze detailně nastudovat instalaci SQL serveru.

(Zdroj: <http://interval.cz/clanky/instalujeme-mysql-na-linux>)

Po Instalaci SQL serveru je potřeba vytvořit databázi pro Zabbix server. Databázi vytvoříme následující posloupností příkazů.

```
shell> mysql -u<username> -p<password>

mysql> create database zabbix character set utf8 collate utf8_bin;

mysql> grant all privileges on zabbix.* to zabbix@localhost identified by 'zabbix';

mysql> quit;

shell> mysql -u<username> -p<password> zabbix < database/mysql/schema.sql

# stop here if you are creating database for Zabbix proxy

shell> mysql -u<username> -p<password> zabbix < database/mysql/images.sql
```

V poznámce mezi příkazy můžeme vidět „*Stop here if you are creating database for Zabbix proxy.*“

Zabbix proxy slouží ke sběru dat od druhého Zabbix serveru. Slouží k propojení dvou oddělených sítí. Namísto konfigurování jednotlivých agentů v druhé síti a možného zpomalení komunikace kvůli vzdálenosti nebo nedostačující techniky, se v druhé síti nainstaluje druhý Zabbix server – proxy, který v této síti shromažďuje data ze sledovaných prvků sítě a posílá je zpět Zabbix serveru nainstalovaném v první síti.

Vysvětlení příkazů je následující.

- Nejprve se přihlásíme k SQL serveru za pomoci uživatele a hesla, který jsme si vytvořili při instalaci SQL serveru.

- Poté vytvoříme databázi „zabbix“. Z požadavků na databázi je potřeba, aby databáze byla vytvořena na základě znakové sady UTF-8.

Detailní informace k znakové sadě UTF-8 jsou k nalezení na níže uvedeném zdroji.

(Zdroj: <http://cs.wikipedia.org/wiki/UTF-8>)

- Pro práci s databází zabbix přiřadíme všechny práva v MySQL uživateli zabbix.

- Tímto jsme vytvořili databázi se jménem „zabbix“ a nyní je potřeba vytvořit její strukturu. Tu vytvoříme za pomoci importování schémat. Tvorbu struktury zabbix databáze zajišťují poslední 3 příkazy. Schémata databáze jsou přiložena v instalačním balíčku Zabbix monitorovacího systému.

V tuto chvíli jsme v bodě, kdy máme splněny tyto úlohy.

- Stažen „Zabbix server“ balíček a rozbalen na serveru
- Stažen „MySQL server“ balíček, rozbalen a nainstalován
- Vytvořena SQL databáze pro Zabbix server (před instalací) jménem zabbix

12.4 Zabbix – Instalace serveru – Konfigurace zdrojů

V této kapitole si nastavíme zdroje před instalací tak, aby instalace byla provedena s konkrétními prvky, které jsou vyžadovány pro správný chod Zabbix serveru.

Tuto konfiguraci uděláme následujícími příkazy. Musíme být ve složce s rozbaleným zdrojem Zabbix serveru.

```
./configure --enable-server --enable-agent --with-mysql --  
enable-ipv6 --with-net-snmp --with-libcurl
```

12.5 Zabbix – Instalace serveru – Instalace

Nyní jsme se dostali k bodu, který se dá považovat již za samotnou instalaci Zabbix serveru.

Instalaci provedeme následujícím příkazem.

```
./make install
```

Instalaci provedeme pod uživatelem, který má dostatečná oprávnění. V obecné podobě by to měl být administrátor nebo root.

Samotná instalace serveru je instalována do defaultní cesty, a to **/usr/local/sbin**.

12.6 Zabbix – Instalace serveru – Konfigurace po instalaci

Po instalaci je potřeba nakonfigurovat soubor samotného Zabbix serveru, kde je potřeba specifikovat konkrétně cestu k databázi, jméno databáze, uživatele a jeho heslo k připojení se do této databáze.

Tento konfigurační soubor pro server najdete v defaultním uložení **/usr/local/etc/zabbix_server.conf**

Úpravu konfiguračního souboru provedeme níže uvedeným příkazem.

```
# vi /etc/zabbix/zabbix_server.conf
```

Níže je uvedená specifikace konfiguračního souboru, kterou je třeba do souboru zanést.

```
DBHost=localhost  
DBName=zabbix  
DBUser=zabbix  
DBPassword=zabbix
```

Textový editor „Vi“ typický pro Linux je pro začátečníky jistá zkouška ohněm. Je těžké si zapamatovat klávesové zkratky nejen z důvodů jejich velkého množství, ale také složitého logického systému umístění kombinací klávesových zkratek na klávesnici.

Proto bych zde rád uvedl zdroj pro informace týkající se „Vi“ textového editoru.

(Zdroj: [http://cs.wikipedia.org/wiki/Vi_\(editor\)](http://cs.wikipedia.org/wiki/Vi_(editor)))

12.7 Zabbix – Instalace serveru – Spuštění

Po instalaci a nakonfigurování všech potřebných souborů můžeme spustit Zabbix server.

Spouštěcí soubor se nachází v defaultním umístění **/usr/local/sbin** stejně jako celá instalace.

Před samotným spuštěním je potřeba se ujistit, že nám OS dovolí alokovat minimálně 36MB paměti počítače. Nebude-li tato velikost paměti k dispozici, Zabbix při spuštění nahlásí chybu.

Pokud by bylo potřeba naalokovat dostatečné množství paměti, pomocníkem se může stát níže uvedený zdroj.

(Zdroj: https://www.zabbix.org/wiki/How_to/configure_shared_memory)

V defaultním umístění instalace si najdeme spouštěcí soubor **zabbix_server**, který spustíme následujícím příkazem.

```
./zabbix_server start
```

Za pomoci níže uvedeného příkazu lze zkontrolovat, jestli zabbix server opravdu běží. Je to prostý výpis běžících procesů.

```
ps -A | grep zabbix_server
```

Příklad výpisu běžících procesů zabbix_serveru po instalaci je uvedený na obrázku níže.

```
[zabbix@server]$ ps -A | grep zab
1923 ?        00:00:00 zabbix_server
1925 ?        00:50:19 zabbix_server
1926 ?        00:00:50 zabbix_server
```

Obrazek 3. - Běžící proces Zabbix Server, zdroj: vlastní tvorba

13 Zabbix – Instalace webového rozhraní

V tomto bodě praktické části diplomové práce jsme již nainstalovali a spustili software potřebný k běhu Zabbix serveru a zároveň nainstalovali a spustili samotný Zabbix server.

Nyní je však možné pracovat se Zabbix monitorovacím systémem pouze na úrovni příkazového řádku.

Již jsme se zmínili o webovém serveru s podporou PHP a jeho jistých rozšířeních.

Samotnou instalaci webového serveru přeskočíme, neboť se opět nejedná o předmět této diplomové práce.

Je na místě ovšem zmínit alespoň zdroj informací k instalaci Apache webového serveru.

(Zdroj: <http://httpd.apache.org/docs/2.2/install.html>)

Ukážeme si zde jednoduchou konfiguraci podpory PHP, jelikož frontend Zabbix monitorovacího systému je napsán v tomto programovacím jazyce.

V kapitole o potřebném software jsme psali o webovém serveru Apache. Pro správný chod frontendu Zabbix systému, je potřeba zkopírovat všechny složky pro jeho podporu do adresáře s názvem „HTDOCS“, který bude umístěn v kořenovém adresáři instalace webového serveru.

Obsah pro podporu Zabbix frontendu je obsažen v jeho rozbalené složce **/frontend/php**

Tvorbu adresáře pro zkopírování frontend PHP podpory uděláme následujícími příkazy.

```
mkdir <htdocs>/zabbix  
cd frontends/php  
cp -a . <htdocs>/zabbix
```

Mkdir příkaz vytvoří soubor, pak se přepneme do uložení PHP podpory frontendu za pomoci příkazu **cd**, a posledním příkazem **cp -a** zkopírujeme obsah aktuálního

adresáře do již vytvořeného htdocs. Po této části počáteční konfigurace se již pomalu dostáváme k oku líbivému webovému rozhraní.

13.1 Zabbix - Instalace GUI

Nyní již nainstalujeme uživatelské rozhraní za pomoci webového prohlížeče a připojení se na server.

V této kapitole si popíšeme 6 kroků ke spuštění webového rozhraní Zabbix monitorovacího systému.

Pro prvotní nastavení konfiguraci frontend webového rozhraní nám poslouží jednoduchý instalační wizard, jinými slovy instalační pomocník, průvodce.

13.1.1 Zabbix – instalace GUI - welcome

Na server se připojíme otevřením této URL `http:// <Server IP or name>:10051` ve webovém prohlížeči. Za „server IP or name“ vložíme naší adekvátní náhradu. To znamená, kam jsme nainstalovali Zabbix monitorovací systém.



Obrázek. 4. - Welcome to Zabbix Server, zdroj: <https://www.zabbix.com/documentation/2.0/manual/installation/install>

13.1.2 Zabbix – instalace GUI – Check of pre-requisites

Tato část počáteční konfigurace GUI slouží k překontrolování předchozích nastavení PHP rozšiřujících modulu. Je potřeba být v takovém statusu, kdy pro každý řádek vidíme stav „OK“



Obrázek. 5. - Check of pre-requisites, zdroj: <https://www.zabbix.com/documentation/2.0/manual/installation/install>

13.1.3 Zabbix – instalace GUI – Configuration DB connection

V této kapitole je popsána konfigurace nastavení připojení do databáze pro webové rozhraní.

Je potřeba nastavit v obrázku zobrazené parametry připojení, které jsme nastavovali již v předchozích kapitolách.



Obrázek. 6. - Configure of DB connection, zdroj: <https://www.zabbix.com/documentation/2.0/manual/installation/install>

Jméno databáze, jejího uživatele a jeho heslo jsme nastavovali v kapitole pro instalaci MySQL databáze.

13.1.4 Zabbix – instalace GUI – Zabbix server details

Zde si nastavíme detaily pro nainstalovaný Zabbix server.

Jak je z obrázku níže patrné, jedná se o defaultní nastavení Zabbix serveru. Konkrétně kde je nainstalován a port, na kterém běží aplikace Zabbix server. Ten je defaultně nastaven na 10051.



Obrázek. 7. - Zabbix server details, zdroj: <https://www.zabbix.com/documentation/2.0/manual/installation/install>

13.1.5 Zabbix – instalace GUI – Install

Při samotné instalaci je potřeba ještě dodat konfigurační soubor pro PHP. Buď jej můžeme vytvořit manuálně nebo za pomoci tlačítka pro jeho stažení jako předdefinovaného souboru.

Po jeho uložení do složky webového serveru pro konfigurační soubory zabbix `/srv/www/htdocs/zabbix/conf` spustíme instalaci znova. Objeví se stav „OK“



Obrázek. 8. - Install: <https://www.zabbix.com/documentation/2.0/manual/installation/install>

13.1.6 Zabbix – instalace GUI – Frontend is ready

V tuto chvíli jsme již ukončili instalaci webového rozhraní Zabbix monitorovacího systému a můžeme se s ním seznámit detailněji.

V první řadě je třeba mít na mysli, že Zabbix monitorovací systém má určitou úroveň ochrany. To znamená, že bez přihlášení pod platným uživatelským jménem a heslem se do monitorovacího systému nedostaneme.

Jako defaultní uživatel byl zvolen „**admin**“ s heslem „**zabbix**“.

Po úspěšném zalogování pod admin uživatelem je doporučováno si dané heslo změnit dle platných bezpečnostních kritérií s ohledem na snížení rizika zneužití.

Níže je uvedený obrázek, jak vypadá absolutně první obrazovka, s kterou se po instalaci setkáme.



Obrázek. 9. - Log-in obrazovka, zdroj: <https://www.zabbix.com/documentation/2.0/manual/installation/install>

Kvůli možným nejasnostem je nutné poznamenat, že design výše uvedeného screenu Log-In obrazovky byl použit již ve verzi 1.9.7 a dále převzat i do verze 2.0. To pouze pro upřesnění nesrovnalosti s verzí uvedenou v části instalace Zabbix serveru a uvedeným obrázkem.

13.2 Zabbix – Instalace Zabbix Agenta

Instalace a konfigurace Zabbix agenta je podstatně jednodušší než Zabbix serveru.

Pro agenta nemusíme instalovat žádný webový server či vytvářet databázi.

Zprvu rovnou upozorním, že největším problémem, proč spolu nekomunikuje nainstalovaný Zabbix agent a Zabbix server je, že nejsou porty povoleny ve firewallu serveru a tudíž neexistuje tunel pro komunikaci. Proto, pokud se po instalaci agenta nepodaří navázat komunikaci se serverem, právě firewall by mohl být jednou z hlavních příčin.

Na níže uvedeném odkazu lze najít problematiku firewall ochrany serverů.

(Zdroj: <http://cs.wikipedia.org/wiki/Firewall>)

V praxi instalování agentů na hosty byla zvolena jiná cesta než defaultní instalace.

Základní binární soubory jednotlivých typů agentů zůstaly stejné, liší se pouze typem platformy, pro kterou je daný agent určen, stejně jako Zabbix server. Navíc ovšem byl

přidán vlastní konfigurační soubor instalace, který do samotného procesu instalace zanáší určité nové parametry, dle kterých instalace probíhá. Například zanesení informace o Zabbix agentu do tabulky Crontab v Unix systémech. Ten zajistí to, že pokud server byl vypnut, nebo spadl, tak po jeho opětovném nastartování bude Zabbix agent automaticky spuštěn. Je to v podstatě stejný prvek Linuxu jako u Windows „scheduler“.

Postup instalace je takový, že se na server pod určitým uživatelem, stejně jako u instalace Zabbix serveru, jiným než privilegovaným, nakopíruje balíček instalačního souboru Zabbix agenta poskytnutého od společnosti Zabbix spolu s konfiguračním souborem.

Opět je nejlepší cestou pro budoucí přehlednost vytvořit takového uživatele, který bude specifický pouze pro instalaci a běh Zabbix agenta.

Konfigurační soubor instalace byl pojmenován jako „install“

Bohužel kvůli ochraně citlivých informací z korporátního prostředí nelze uvést přesný obsah tohoto souboru, proto přejdeme rovnou k instalaci.

Za pomoci individuálně vytvořeného konfiguračního souboru instalace spustíme danou instalaci tímto příkazem.

```
bash install.sh
```

Po jeho instalaci se agent automaticky spustí, a to dle konfigurace instalačního souboru.

Je však nutné uvést v nově nainstalovaném konfiguračním souboru Zabbix agenta, IP adresu či název Zabbix serveru, se kterým bude agent komunikovat.

Ten je k nalezení v **/usr/local/etc/zabbix_agentd.conf**

V našem případě je toto opět specifikovaná v konfiguračním souboru instalace.

Jak vypadá konfigurační soubor Zabbix agenta a místo, kde vyplnit místo pro IP adresu či název, lze shlédnout na níže uvedeném obrázku. Dále je z něj čitelný řádek pro vyplnění portu Zabbix serveru. Ten je však defaultně přednastavený na 10050.

```
# Default:
# Server=
Server=

### Option: ListenPort
#   Agent will listen on this port for connections from the server.
#
# Mandatory: no
# Range: 1024-32767
# Default:
ListenPort=10050
```

Obrázek. 10. - Zabbix_agentd.conf, zdroj: vlastní tvorba

Po úspěšné instalaci agenta ověříme, zda byl Zabbix agent doopravdy spuštěn.

Podobně jako u kontroly spuštění Zabbix serveru, kontrolu provedeme následujícím příkazem.

```
ps -A | grep zabbix_agent
```

Na níže uvedeném obrázku je vidět, že Zabbix agent je spuštěný.

```
bash-3.2$ ps -A | grep zabb
4546 ?          2:42 zabbix_a
4547 ?          2:12 zabbix_a
4548 ?          0:36 zabbix_a
4543 ?          0:00 zabbix_a
4545 ?          2:04 zabbix_a
4544 ?          19:31 zabbix_a
```

Obrázek. 11. - Běžící procesy zabbix_agentd, zdroj: vlastní tvorba

14 Zabbix – Komunikace Server – Agent

Po úspěšné instalaci agenta a nastavení jeho konfiguračního souboru již agent a server sami navážou komunikaci.

Pro jasné prokázání navázání komunikace mezi serverem a agentem je potřebné nejdříve přidat v uživatelském rozhraní Zabbix serveru hosta, na kterém je agent nainstalovaný. Tato činnost je popsána v následujících kapitolách. Předtím si však přiblížíme pracovní prostředí Zabbix monitorovacího prostředí, abychom se naučili se systémem pracovat.

Pro ukázkou navázání komunikace mezi serverem a agentem slouží níže uvedený obrázek.



Obrázek. 12. - Korektně navázaná komunikace, zdroj: vlastní tvorba

Korektně navázanou komunikaci lze poznat z informace o „Availability“, a to tak, že se zobrazí **zelený** znak „Z“.

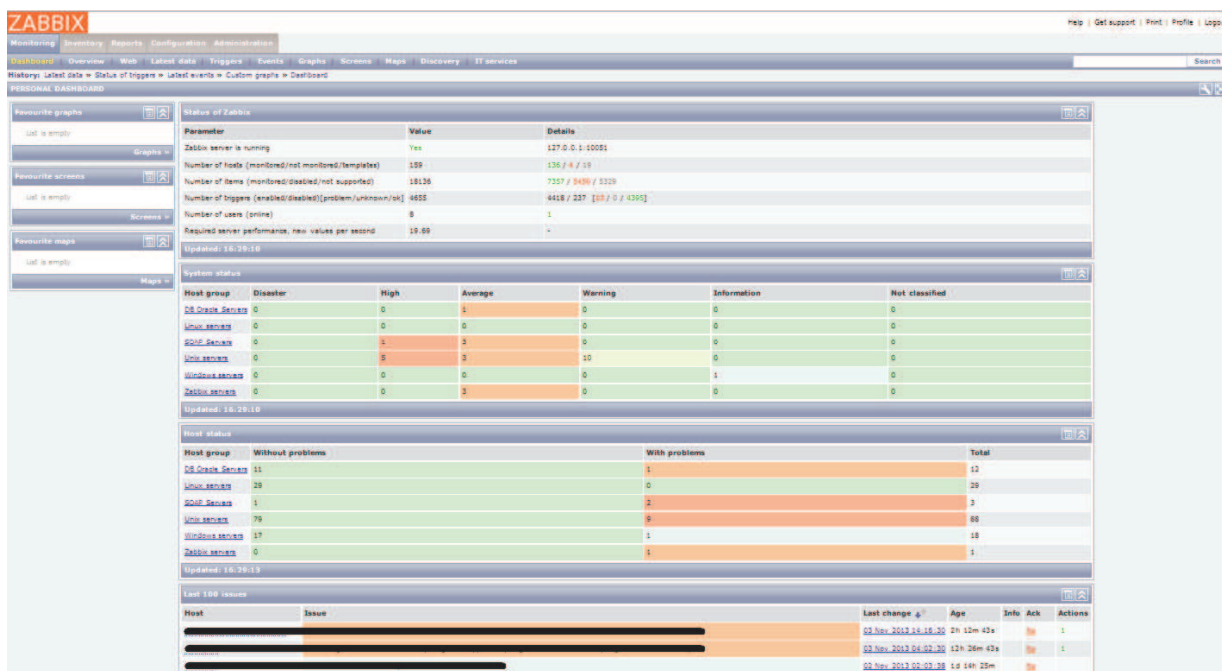
Znak „Z“ proto, jelikož jsme použili k monitoringu Zabbix agenta. V případě, že by spojení nebylo navázáno, „Z“ by bylo **červené** barvy a po přjetí kurzorem myši nad touto ikonou se nám zobrazí chybový kód a hlášení, z jakých příčin spojení pravděpodobně nebylo navázáno.

15 Zabbix – GUI

V této kapitole si již ukážeme, jak vypadá webové rozhraní pro Zabbix server, seznámíme se s jeho ovládacími prvky a ukážeme si, kde se nacházejí jednotlivé důležité funkce.

15.1 Zabbix – GUI - Dashboard

Dashboard, ve volném překladu pracovní deska, je obecné okno nesoucí informace o aktuálním dění na zabbix serveru, o stavu monitorování, o četnosti monitorování, o posledních vyhodnocených položkách atp. Tuto obrazovku si lze opět customizovat do vlastní podoby za pomoci levé části okna, kde si můžeme zařadit oblíbené grafy, obrazovky či mapy. Na níže uvedeném obrázku je vidět, jak Zabbix Dashboard vypadá.



Obrázek. 13. - Dashboard, zdroj: vlastní tvorba

Hlavní menu šedé barvy je v levé horní části obrazovky.

Pod Hlavním menu se nachází **Navigační menu**, je zbarveno do modré barvy.

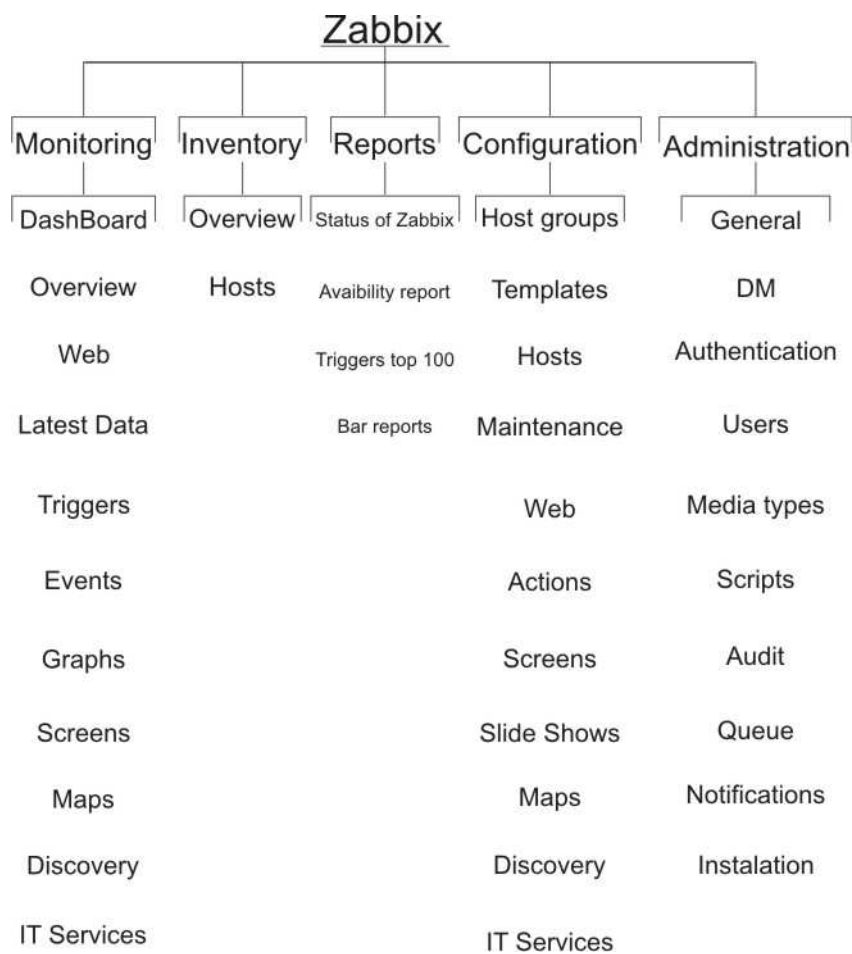
Pod Navigačním menu můžeme vidět **historii** našeho procházení, což velmi ulehčí přepnutí se na předchozí obrazovku.

Pod touto historií již najdeme **Hlavní zobrazovací okno**, ve kterém se zobrazují námi vybrané volby z horních menu.

V pravém horním rohu můžeme vidět možnosti pro práci s přihlášeným **uživatel**em a **všeobecné informace**. Zde je umístěna například nápověda, logování uživatele nebo možnost úpravy jeho profilu.

15.2 Zabbix – GUI - Struktura

V této kapitole si přiblížíme jednotlivé položky obou menu a jejich záložky. Konkrétní stromovou strukturu GUI Zabbix je k nahlédnutí na následujícím obrázku.



Obrázek. 14. – Struktura Zabbix, zdroj: Vlastní tvorba

15.3 Zabbix – GUI – Popis prvků menu

Již jsme si ukázali jednotlivé ovládací prvky v menu a nyní si je popíšeme z pohledu jejich obsahu.

Monitoring

Dash Board - Kompletní přehledka informací o Zabbixu, vyhodnocených triggerů respektive objevení problémů.

Overview - Zobrazení kompletního seznamu hostů napříč kompletním výpisem sledovaných položek.

Web – Stav webového monitorování.

Latest Data – Zobrazuje poslední naměřená data pro daný server, jejich hodnoty a možnost zobrazení grafů. Vyčten kompletní seznam aplikací a pro ně jejich položky.

Triggers – Výpis všech triggerů pro daný server.

Events – Výpis všech událostí pro daný server.

Graphs – Možnost zobrazení grafů pro daný server.

Screens – Zobrazení customizovaných obrazovek. Tím je myšlena možnost nadefinovat si, co chceme zobrazit na obrazovce, například graf, mapu, výpis určitých triggerů atp. a po nadefinování se nám vše zobrazí na jedné obrazovce.

Maps – Mapy monitorované sítě. Aktivní mapy zobrazující cesty, IP adresy, servery, síťové prvky atp.

Discovery – Zde se definují pravidla, dle kterých se bude nově objevovat síť. Například automatické rozpoznání nově nainstalovaného agenta.

IT Services – Detailní přehled úrovně poskytovaných služeb neboli SLA.

Inventory

Overview – Zobrazení kompletního seznamu hostů vymezených dle definovaných pravidel jako jsou typ OS, počet běžících procesů, vytížení CPU, umístění, kdo jej instaloval atd.

Hosts – kompletní přehled hostů a informací o nich.

Reports

Status of Zabbix – Přehled parametrů Zabbix serveru, například počet sledovaných serverů, hostů. Součást Dashboard.

Availability report – Přehled reportů dostupnosti. Je potřeba pro tuto možnost nahlédnutí mít definované události.

Triggers top 100 – Přehled seřazených triggerů podle parametru nejčastěji měnících se stavů.

Bar reports – Klasické barové grafy, vizuálně zpracovány v podobě sloupců, možnost si zvolit vlastní proměnné (položky) a graficky je porovnávat.

Configuration

Host Group – Přehled skupin pro hosty a možnost jejich konfigurace.

Templates – Přehled šablon a možnost jejich konfigurace.

Hosts – Přehled hostů, jejich položek, triggerů, událostí, akcí, aplikací, stavů a dostupnosti.

Maintenance – Přehled údržby, například oznámení o plánovaném výpadku serveru, nastavení jeho trvání a tím pádem jeho nezapočítávání například do SLA.

Web – Přehled web monitoringu a možnost jeho konfigurace.

Actions – Přehled akcí a možnost jejich nastavení. Součást notifikací.

Screens – Přehled obrazovek a jejich konfigurace.

Slide show – Možnost automatického posouvání předdefinovaných obrazovek v časovém sledu.

Maps – Přehled map monitorovaných sítí a možnost jejich konfigurace.

Discovery – Konfigurace pravidel objevování nových prvků sítě.

IT Services – Přehled SLA a možnost jeho konfigurace.

Administration

General – Hlavní administrace Zabbix GUI.

DM – Administrace Zabbix proxy.

Authentication – Nastavení autentizace.

Users – Administrace uživatelů.

Media types – Nastavení typů medií používaných k upozornění na vyskytnutý problém. Jinými slovy nastavení e - mailu, Jabberu či SMS.

Scripts – Interní skripty pro zefektivnění a zrychlení práci se Zabbixem. Například skript „PING“ při otevření hosta v Dashboard, na kterém je hlášen problém, umí z GUI Zabbix příkaz „ping“. Nemusí se volat z příkazové řádky.

Audit – Celkový přehled o změnách konaných na serveru či agentech.

Queue – Přehled položek, které čekají na svoje informace.

Notifications – Přehled komu byly zasílány notifikace napříč jednotlivými dny.

Installation – Možnost instalace webové GUI.

16 Zabbix – GUI - Nejpoužívanější ovládací prvky

V této kapitole si mírně zredukujeme vypsané prvky Zabbix monitorovacího systému, neboť se může na první pohled zdát, že jich je příliš.

Vycházím-li z mé praxe, z počátku jsou kvůli konfiguraci nejvíce používány tyto prvky.

- *Administration – Users a Media Types*
- *Configuration – Host Groups, Templates, Hosts, Actions a využívá-li uživatel SLA, tak IT Services.*

Po nakonfigurování všech monitorovaných prvků sítě v Zabbixu, administrátor využívá spíše přehledových funkcí Zabbix, kterými jsou následující.

- *Monitoring – Dashboard, Latest Data a Graphs*

Tento výčet nejpoužívanějších prvků je v tuto chvíli pouze informativní, je přizpůsoben mým možnostem administrace tohoto monitorovacího systému a nakonec mě samotnému tak, jak mě vyhovuje.

17 Zabbix – Započítání monitorování

V této kapitole se dozvíme více konkrétních informací. Jsou jimi například jak přidat do Zabbix systému hosta, monitorovanou položku a k ní vytvořený trigger. Toto jsou základní prvky potřebné k provádění monitoringu. Jako výstupy dále budou sloužit informace o SLA a grafické zpracování sledovaných položek.

17.1 Zabbix – Přidání Hosta

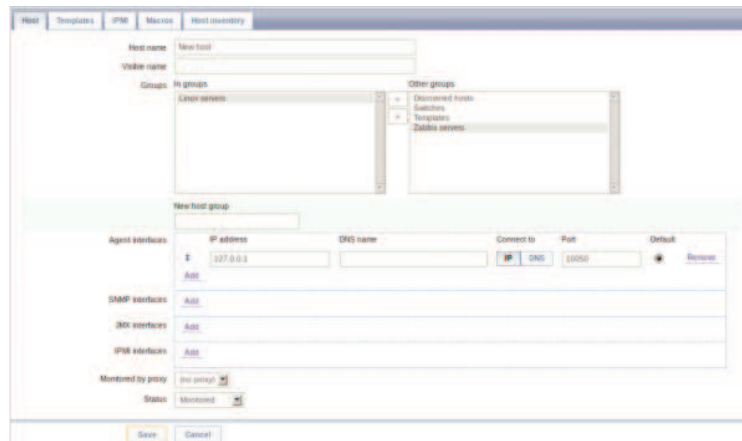
Host, jak již bylo řečeno, je síťový prvek, který chceme monitorovat a dohlížet naň.

„The definition of what can be a “host” in Zabbix is quite flexible. It can be a physical server, a network switch, a virtual machine or some application.“

(Zdroj: <https://www.zabbix.com/documentation/2.0/manual/quickstart>)

Z výše uvedené citace je vidět, že Host nemusí vždy být pouze fyzický server. Může to být například i virtuální server, síťový prvek switch nebo například aplikace.

Níže je uvedený příkladný obrázek, na kterém je vidět konfigurační tabulka pro přidání hosta do Zabbix serveru.



Obrázek. 15. - Host, zdroj: <https://www.zabbix.com/documentation/2.0/manual/config/hosts/host>

V první řadě si nového hosta příkladně pojmenujeme (Host name). Je dobré si vymyslet nějaké logické značení, které do budoucna počítá s určitým nárůstem monitorovaných hostů. V pozdější době, kdy již budeme přidávat například dvoustého hosta v řadě, je potřeba se rychle a jednoduše orientovat. Poté jej přiřadíme do určité skupiny serverů (Groups) a zadáme základní parametry, za pomoci kterých spolu bude Zabbix server a daný sledovaný server, respektive agent komunikovat. Tím jsou IP a DNS. Doporučuji vyplnit oba parametry, jelikož občas se může stát, že v případě doménových serverů nebude schopné se za pomoci DNS dostat na požadovaný server a jednoduchým řešením tak je monitorovat za pomoci IP adresy serveru. To, kterým parametrem se budeme připojovat na server, si zvolíme ve volbě „Connect to“. Nakonec je potřeba definovat port, na kterém běží Zabbix agent a tím je při defaultní instalaci 10050. Pokud je tento port z jakýchkoliv důvodů jiný, je potřeba jej vyplnit korektně, jinak se komunikace nenaváže.

Po klepnutí na tlačítko „Save“ daný server uložíme a vytvořili jsme tak prvního hosta, kterého chceme monitorovat.

17.2 Zabbix – Přidání položky

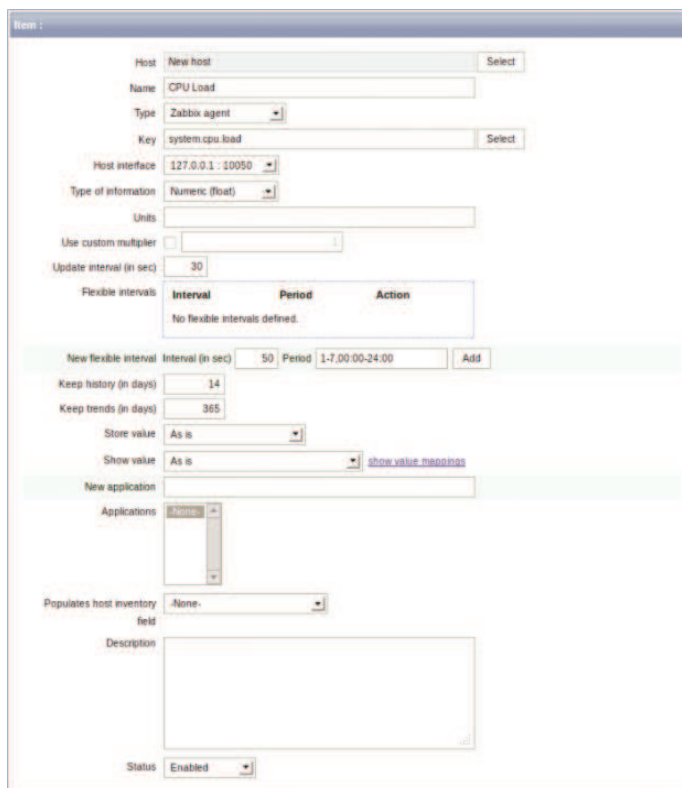
Jak již bylo řečeno, položka je základní stavební kámen systém Zabbix. Položka neboli „Item“ definuje, jaký druh dat chceme sbírat, jinými slovy co chceme monitorovat.

Položky jsou definovaný pro jednotlivé hosty. Proto je potřeba najít námi již vytvořeného hosta.

Nalezneme jej v menu „Konfigurace“ a dále v záložce „Hosts“. V této záložce se vyskytují všichni námi definovaní hosté.

Vybereme si daného hosta, na kterém chceme konfigurovat položku a poté v menu „Items“.

Po tomto výběru v pravém horním rohu vybereme možnost „Create Item“ a objeví se nám níže uvedená tabulka.



Interval	Period	Action
No flexible intervals defined.		

Interval (in sec)	Period	Action
50	1-7,00:00-24:00	Add

Obrázek. 16. - Item, zdroj: <https://www.zabbix.com/documentation/2.0/manual/config/items/item>

Jako v případě hosta, je potřeba danou položku výstižně pojmenovat. Dále zvolit typ sbírání dat (Zabbix agent) a definovat klíč, dle kterého určíme, o jakou sledovanou hodnotu se jedná. V příkladné ukázce se jedná o vytížení procesoru.

Klíč může nabývat velké množství hodnot, respektive typů monitorovaných dat. Na níže uvedeném zdroji lze dohledat všechny možné typy sledovaných veličin za pomoci Zabbix agenta.

(Zdroj: https://www.zabbix.com/documentation/2.0/manual/config/items/itemtypes/zabbix_agent)

Ne méně důležitou informací je, jaký bude typ zasílaných informací například text, numeric či logfile.

Další důležitou částí konfigurace je „Update Interval“, který udává frekvenci zasílání informací na Zabbix server. S touto informací jsme se již setkali při tvorbě Zabbix databáze a vypočítávání její velikosti.

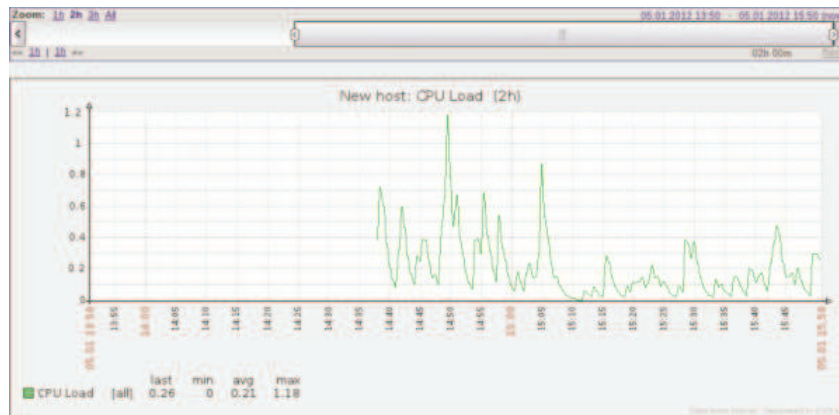
Po uložení konfigurace položky si ověříme, zda se pro ní ukládají data.

Půjdeme proto do sekce „Monitoring“ a poté do podsekce „Latest data“.

Zde můžeme vidět přehled aplikací a pod nimi dané položky. Zvolíme si námi definovanou položku „CPU Load“.

Po rozkliknutí možnosti „Graph“ v pravé části informací posledních naměřených dat položky se objeví níže uvedený obrázek. Je jím graf, ve kterém jsou znázorněny naměřené hodnoty.

Tento graf je zobrazen v intervalu 2 hodin. Sledovaná položka CPU Load nemá na sobě navázaný žádný trigger.



Obrázek. 17. - Zatížení procesoru, zdroj: <https://www.zabbix.com/documentation/2.0/manual/config/items/item>

17.3 Zabbix – Přidání triggeru

Již jsme si na hostu definovali položku, čili data, které chceme monitorovat. Nyní si definujeme určitou hranici, kdy nám Zabbix nahlásí abnormální chování určité položky.

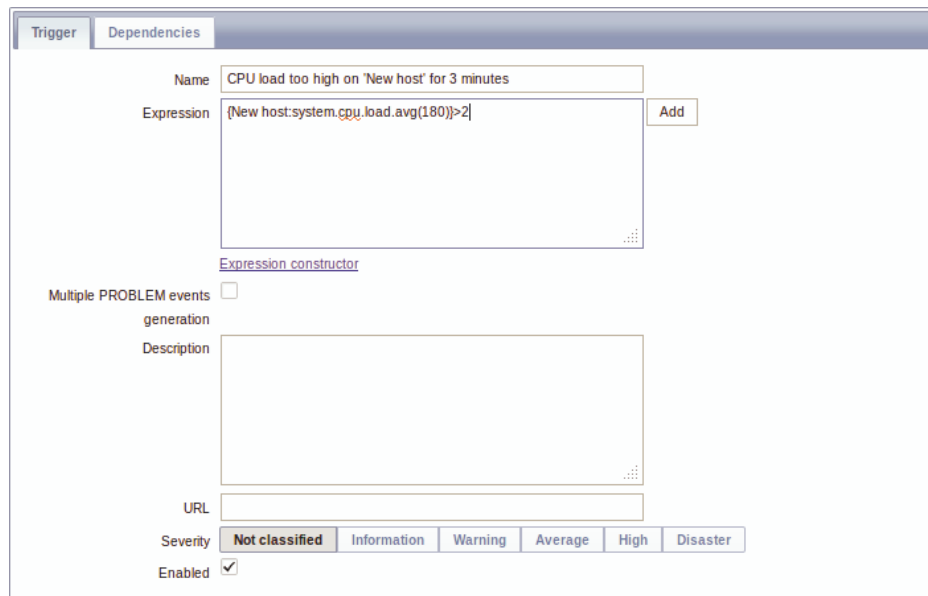
Trigger je tedy takový pomyslný hlídač pro položku.

Slouží k upozornění administrátora o specifickém dění na serveru, na které by se měl zaměřit.

Pro nakonfigurování triggeru je nutné opět zajít do sekce „Configuration“ poté Hosts a pro daný host otevřít v menu „Triggers“.

Podobně jako u Items, v pravém horním rohu zvolíme volbu „Create Trigger“.

Po této volbě se nám otevře níže uvedená tabulka.



Obrázek. 18. - Trigger, zdroj: <https://www.zabbix.com/documentation/2.0/manual/config/triggers/trigger>

Zvolíme si název pro daný Trigger. Je dobré si jej zvolit jako nějakou smysluplnou větu, jelikož se nám při problémových stavech bude zobrazovat právě ona a my tak rovnou uvidíme, o jaký problém se jedná.

V konfiguraci Trigger je nejdůležitější sekcí tzv. Expression neboli výraz. Ten má jasně definovanou syntax, ze které Zabbix server pochopí, jak má daný trigger fungovat.

Pro podrobné informace k problematice syntaxe skládání triggeru lze využít níže uvedený zdroj.

(Zdroj: <https://www.zabbix.com/documentation/2.0/manual/config/triggers/expression>)

Jako poslední nastavení je určení Severity neboli závažnosti vyskytnutého problému.

Jako hlavní přehled vyskytnutých problému, které trigger nahlásí, slouží takzvaný „Dashboard“ v sekci „Monitoring“, o kterém jsme se zmínili již dříve v jedné z předchozích kapitol.

17.4 Zabbix – Konfigurace notifikace

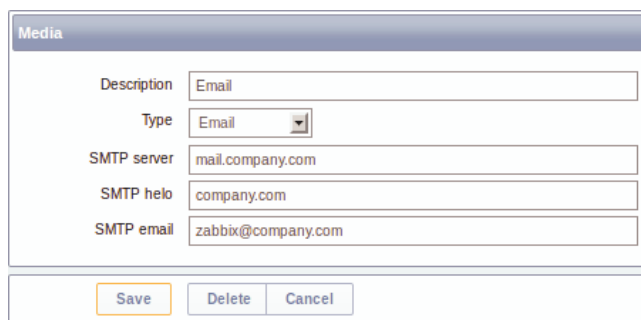
V této kapitole se podíváme na konfiguraci notifikace, jinými slovy upozornění na nějaký problém vyhodnocený za pomoci triggeru.

17.4.1 Zabbix – Konfigurace notifikace – e-mail

Nastavíme si zde jednu z notifikací, a to zasílání informačních e-mailů. Jedná se o nejběžnější notifikaci a to byl důvod k její volbě.

Jako první nastavíme e-mail pro zasílání notifikací.

Konfigurační tabulku nalezneme v sekci „Administration“ dále potom v podsektí „Media Types“ a nakonec zvolíme e-mail. Otevře se následující konfigurační okno.



The screenshot shows a web-based configuration window titled "Media". It contains several input fields and a dropdown menu:

- Description: Email
- Type: Email (dropdown menu)
- SMTP server: mail.company.com
- SMTP helo: company.com
- SMTP email: zabbix@company.com

At the bottom of the window, there are three buttons: "Save", "Delete", and "Cancel".

Obrázek. 19. - Notifikace - email, zdroj:

<https://www.zabbix.com/documentation/2.0/manual/config/notifications/media/email>

Po nastavení detailu jako SMTP server, SMTP helo a SMTP e-mail jsme nakonfigurovali tzv. „Media Type“. Tento „Media Type“ musí být přiřazen specifickému uživateli, který je vytvořen na samotném Zabbix serveru.

„SMTP email“ zde slouží pro vyplnění pole „Od:“ v přijatém e-mailu notifikace.

„SMTP server“ je e-mailový server sloužící k samotnému odeslání informačního e-mailů.

Zaslání informačního e-mailu Zabbixem funguje tak, že Zabbix server na definovaný SMTP server odešle definovanou podobu zprávy neboli e-mailu a ten pokračuje v dalším zpracování odesílání k cíli.

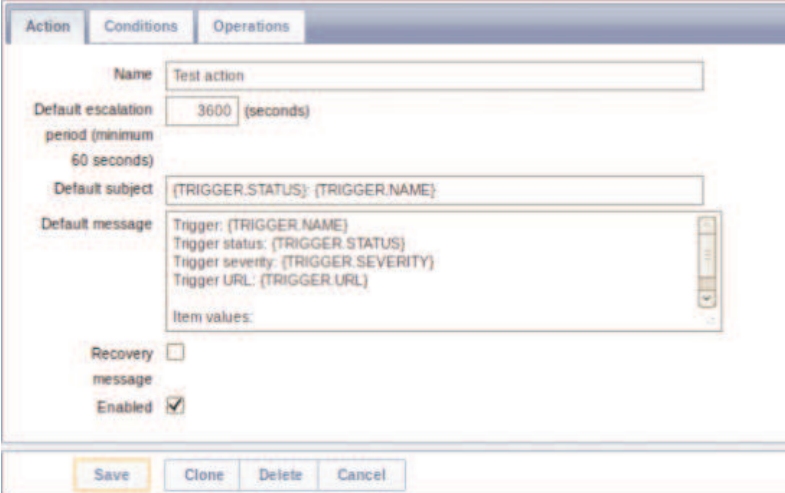
Jak se definuje vzhled informačního e-mailu si ukážeme v následující kapitole.

17.4.2 Zabbix – Konfigurace notifikace – Akce

Akce, je reakce na vyhodnocení triggeru.

Nejdříve jsme si nadefinovali e-mail jako jednu z možností notifikace a nyní se dostaneme k samotnému odeslání upozornění.

Je potřeba opět otevřít konfigurační okno Akce za pomoci „Configuration“ a následně „Actions“.



Obrázek. 20. - Notifikace - akce, zdroj:

<https://www.zabbix.com/documentation/2.0/manual/config/notifications/action>

Opět si zvolíme název akce.

{TRIGGER.STATUS} a {TRIGGER.NAME} a {TRIGGER.SEVERITY} a {TRIGGER.URL} jsou proměnné Zabbix serveru, které zde slouží ke kompletaci zprávy

Tyto proměnné budou v e-mailu nahrazeny aktuálními daty.

„Default subjekt“ jak překlad napovídá, je předmět zasílaného e-mailu a „Default message“ je samotná náplň e-mailové zprávy.

Jako poslední konfiguraci, kterou je nutné provést, je nastavení samotného odesílání e-mailu v záložce „Operations“. Konfigurační tabulka vypadá takto.

The screenshot shows the Zabbix configuration interface for an action operation. The 'Operations' tab is selected. The 'Action operations' section is empty, showing 'No operations defined'. The 'Operation details' section is expanded, showing the following configuration:

- Step: 1
- From: 1
- To: 1 (0 - infinitely)
- Escalation period: 0 (minimum 60 seconds, 0 - use action default)
- Operation type: Send message
- Send to User groups: Add
- Send to Users: user, Remove, Add
- Send only to: Email
- Default message:
- Conditions: No conditions defined, New

Buttons for Save, Clone, Delete, and Cancel are located at the bottom of the form.

Obrázek. 21. - Notifikace - operace, zdroj:

<https://www.zabbix.com/documentation/2.0/manual/config/notifications/action/operation>

V části formuláře „Send to Users“ klikneme na „Add“ a vybereme uživatele, kterého jsme na začátku instalace Zabbix serveru definovali.

Dále zvolíme e-mail, na který chceme odesílat upozornění. Tento e mail nastavíme v části „Send only to“.

17.5 Zabbix – Vytvoření template

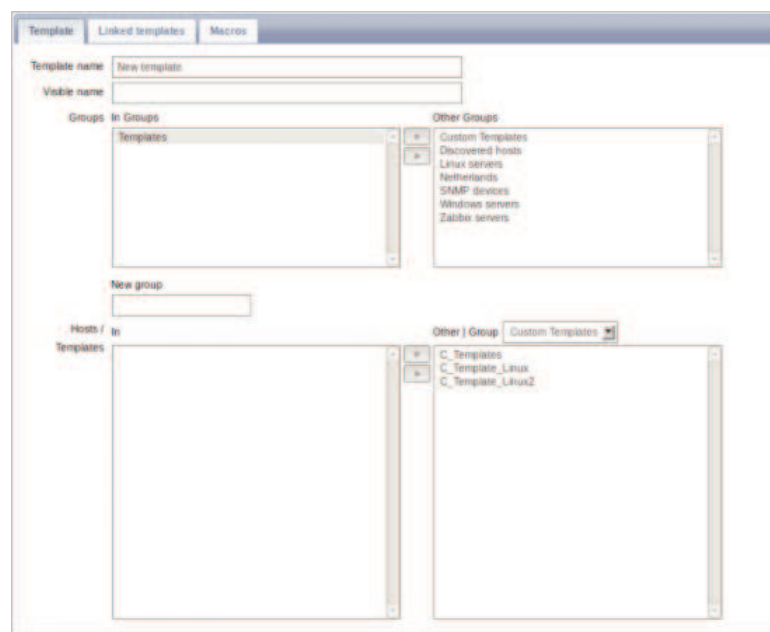
Pod pojmem template, se ve volném překladu nachází šablona.

Tato šablona se využívá pro práci se Zabbixem, který obsahuje stovky či tisíce sledovaných zařízení, hostů.

Konkrétní využití spočívá v tom, že namísto toho, abychom při každém přidání hosta museli definovat jemu sledované položky, jej přidáme do této šablony z již definovaného hosta a automaticky se pro něj začnou sledovat nadefinované položky šablony.

Urychlíme tak celý proces rozrůstání sledovaných prvků sítě.

Níže je uvedený obrázek, který ukazuje formulář pro vytvoření šablony.



Obrázek. 22. - Template, zdroj: <https://www.zabbix.com/documentation/2.0/manual/config/templates/template>

K tomuto formuláři se dostaneme za pomoci navigačního menu, kde zvolíme „Configuration“, dále „Templates“ a jako u předchozí tvorby, zvolíme „Create template“ neboli vytvoření šablony.

Nově tvořenou šablonu si pojmenujeme a přiřadíme do určité skupiny, nejlépe do skupiny šablon neboli „Templates“.

V tuto chvíli máme vytvořenou šablonu, ale neobsahuje žádné položky k monitorování.

Proto nějaké přidáme za pomoci již vytvořeného hosta a pro něj definovanými položkami.

Přes navigační menu a „Configuratuon“ a dále „Hosts“ vybereme již nadefinovaného hosta. Pro něj vybereme možnost „Items“, kde najdeme všechny doposud vytvořené položky.

„Items“, které se nám logicky hodí do nově vytvořené šablony, zaškrtneme za pomoci Check-boxu v levé části seznamu a po vybrání všech adekvátním položek, v levé dolní části vybereme možnost „Copy selected to...“ a klikneme na „Go“.

Po tomto výběru se nám otevře tabulka, kam chceme vybrané položky kopírovat. Vybereme námi vytvořenou novou šablonu a tímto jsme dokončili tvorbu šablony.

Když máme danou šablonu vytvořenou, při tvorbě nového hosta ji přidáme v záložce „Templates“ kliknutím na tlačítko „Add“ a poté vybráním adekvátní šablony.

18 Zabbix – IT Services

Po ukázce základního nastavení položek triggerů a notifikace si řekneme pár informací k vyšší úrovni monitoringu.

Jedná se o takzvané SLA.

„Termín SLA označuje smlouvu sjednanou mezi poskytovatelem služby a jejím konzumentem.“

(Zdroj: http://cs.wikipedia.org/wiki/Service-level_agreement)

SLA znamená „Service Level Agreement“ a z výše uvedené citace vyplývá, že se jedná o úroveň poskytování služeb. Jinak řečeno se jedná o dobu, po kterou je poskytovaná služba dostupná. Nemusí se jednat jen o odvětví informačních technologií.

Takovéto SLA umí zpracovávat i Zabbix server. Je ovšem potřeba jej adekvátně nastavit a pak se již jen sbírají data a vypočítává se úroveň SLA.

Na níže uvedeném obrázku je ukázána hierarchická struktura, na které SLA v Zabbixu funguje.

Service	Status calculation	Trigger
Root		
SLA by service	Problem, if all children have problems	None
Server 1	Problem, if at least one child has a problem	None
Server 2	Problem, if at least one child has a problem	None
Server 3	Problem, if at least one child has a problem	None
Server 4	Problem, if at least one child has a problem	None
Add Service	Problem, if at least one child has a problem	None
Edit Service		
Delete Service		

Obrázek. 23. - SLA, zdroj: https://www.zabbix.com/documentation/2.0/manual/it_services

V případě systému Zabbix struktura funguje na bázi dvou názvosloví. Jsou jimi „Rodič“ a „Dítě“.

Rodičem může být například jeden fyzický server a dítě pro daný fyzický server může být webový server na něm běžící.

Jako hlavní rodič neboli rodič rodičů, je tzv. „Root“, v překladu kořen.

Danou hierarchickou strukturu si každý může vymyslet tak, jak uzná za vhodné. Měla by splňovat určitá pravidla logického provázání. Například, že webový server, který běží na virtuálním serveru, bude dítě pro virtuální server a ne pro fyzický server.

Jakmile založíme sledování jedné služby pro SLA, automaticky je přednastavena na hodnotě 100%, to znamená, že běží po celou dobu provozu od doby jeho sledování pro SLA.

Jakmile nastane výpadek této služby, začne se dle nastavených podmínek přepočítávat úroveň SLA, respektive úroveň se snižuje.

Byla řeč o určitých podmínkách, s kterými pracuje výpočet SLA.

Podmínky jsou:

- „*Nezapočítávat*“ – Nezapočítávat do SLA úrovně.
- „*Problém, jestli alespoň jedno dítě má problém*“ – Alespoň jedna služba nesmí fungovat, aby se snížila úroveň SLA.
- „*Problém, jestli všechny děti mají problém*“ – Všechny služby nesmí fungovat, aby se snížila úroveň SLA.

Pro více informací ohledně Zabbix a jeho možnosti sledování úrovně poskytovaných služeb lze navštívit níže uvedený zdroj informací.

(Zdroj: https://www.zabbix.com/documentation/2.0/manual/it_services)

Pro více obecných informací o SLA lze navštívit níže uvedený zdroj.

(Zdroj: <http://www.systemonline.cz/outsourcing-ict/tajemstvi-zkratky-sla-1.html>)

19 Zabbix – Výstupní informace

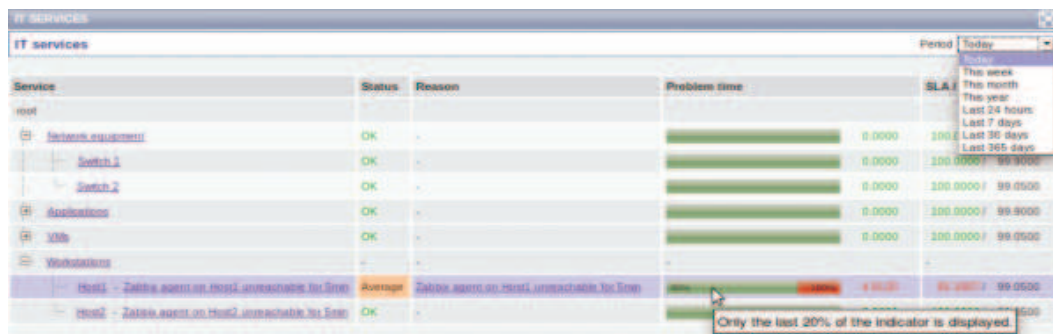
Jako výstupní informace Zabbix monitorovacího systému můžeme považovat v podstatě cokoliv. Otevřeme si GUI Zabbix monitorovacího systému, vidíme, že určitá položka se vyskytuje v problémovém stavu a již toto můžeme považovat za výstupní informaci.

Pro výstupní informace vyšší úrovně jsem zvolil dva typy. Jedním je výstupní informace Zabbix monitorovacího systému v podobě SLA a druhá je výstupní informace v grafické podobě monitorování určité položky.

19.1 Zabbix – Výstupní informace - SLA

Jako první typ výstupní informace Zabbix monitorovacího systému jsem zvolil sledování úrovně SLA.

Níže můžeme vidět obrázek ze sledování úrovně poskytování služeb.



Obrázek. 24. - SLA 2., zdroj:

https://www.zabbix.com/documentation/2.0/manual/web_interface/frontend_sections/monitoring/it_services

Informace z uvedeného obrázku lze komentovat následovně.

Úroveň poskytovaných služeb pro „Sítové vybavení“ dosahuje 100%. To znamená, že dané síťové prvky neměly žádný výpadek.

Úroveň poskytovaných služeb pro „Aplikace“ dosahuje 100%. To znamená, že dané aplikace neměly žádný výpadek.

Úroveň poskytovaných služeb pro „Virtuální servery“ dosahuje 100%. To znamená, že dané virtuální servery neměly žádný výpadek.

Úroveň poskytovaných služeb pro „Host1“ dosahuje 80%. To znamená, že pro daný host byl zaznamenán výpadek po dobu 20% z celkové sledované doby provozu.

V tomto případě jsme zaznamenali nepříznivý stav naší smluvené úrovně poskytovaných služeb a je na nás, jaké důsledky z toho vyvodíme. Například snížení poplatků za poskytovanou službu připojení k serveru pro daného Host1.

19.2 Zabbix – Výstupní informace - SLA

Jako druhý typ výstupní informace Zabbix monitorovacího systému jsem zvolil grafický výstup sledování určité položky.

Jako sledovanou položku jsem zvolil zatížení procesoru na serveru.

Grafický výstup je v příloze č. 2.

Z grafu je patrné, že se jedná o monitoring položky po dobu 1 měsíce.

Ode dne 17.10. do 25.10. můžeme vidět normální, běžné vytížení procesoru.

Ode dne 26.10. do 29.10. můžeme vidět snížené zatížení procesoru, například kvůli údržbě nebo instalaci se vypnuly některé aplikace a instalovali se nové verze.

Ode dne 30.10.2013 do 16.11.2013 můžeme vidět postupné mírně zvyšování zátěže procesoru s několika extrémními pozorováními. Jedná se například o dny 2.11., 4.11. 12:00, 9.11. a 15.11.2013.

Tyto pozorování překročili námi definovaný trigger, sledující hranici zdravého zatížení procesoru 8. V průběhu měsíce tyto hodnoty byly vypořizovány a bylo možné na ně reagovat například způsobem, že se instalované aplikace musí nově vyvinout tak, aby snížili zatížení procesoru.

Do budoucna můžeme reagovat například tak, že konkrétní vývojové pracovníky upozorníme na nevhodné metody vývoje nebo nevhodnost použitého prvku při vývoji a do budoucna se těmto typům dodávaných aplikací, více než normálně zatěžujících procesor, snažit vyhnout.

Výstupními informacemi o sledovaných položkách hosta jsme se dostali k závěru této práce.

20 Závěr

„Cílem této práce je praktická ukázka instalace monitorovacího systému Zabbix, jeho sledovacího serveru a agenta, náhled do komunikace mezi Zabbix serverem a agentem, popis monitorovacího systému Zabbix. Účelem je také názorně přiblížit monitorovací prostředí s popisem jednotlivých prvků a funkcí tohoto systému.

Dále v této práci rozebereme, jak se vytváří jednotlivé prvky sledování, ukážeme si grafický vývoj sledovaných prvků a definujeme si závěry z těchto grafů vyplývajících.“

(Zdroj: Cíl práce a metodika, DP - Nasazení Zabbix v korporátním prostředí)

Z výše uvedených cílů a metodiky jsme se dostali do korektního závěrečného stavu.

Prakticky jsme nainstalovali komponenty sledovacího systému Zabbix, byla prokázána správně navázaná komunikace agenta a serveru a detailně jsem přiblížil pracovní prostředí tohoto software.

Jako další bod praktické části byl popis tvorby základních prvků potřebných k monitorování. Těmi jsou tvorba Hosta, Item, Triggeru a ne méně důležitá šablona.

Posledním cílem této práce bylo definovat závěry z naměřených hodnot sledovaných veličin, které jsem prokázal na SLA a výstupních grafech.

V závěru práce bych také rád uvedl některé fakty doprovázející mojí práci.

Jak je již běžné v dnešní době velké konkurence, společnosti se snaží držet své vnitřní informace v určité míře utajení. Proto se tato práce skládá z pohledu praktických ukázek i z takových, které nejsou přímo autentické k praktické části a nepopisují přesnou podobu průběhu praktické části této práce.

Snažil jsem se ovšem nahradit citlivé ukázky takovými, díky kterým lze jednoduše pochopit danou problematiku a v případě, že by bylo možné ukázku prezentovat s možností malé korekce zobrazovaných informací, jsem tak učinil.

Jako další fakt, který bych rád uvedl je ten, že se jedná o diplomovou práci, a proto jsem počítal s určitou hladinou znalostí anglického jazyka potenciálních čtenářů.

Některé části práce jsem cíleně nepřekládal, například některé popisy či citace, kde jsem čerpal zdroj v cizím jazyce.

Tato práce byla koncipovaná tak, aby dle ní a její praktické části bylo možné Zabbix monitorovací systém bez problémů nainstalovat. Je ovšem samozřejmostí, že rozsah práce by nedokázal obsáhnout kompletní postup instalace s dalšími instalacemi doprovodných programů či samotného operačního systému Linux, ale za určitých podmínek by mohla tato práce fungovat jako jistý návod.

Z mého pohledu jsem se v práci snažil popsat postupy či popisy do detailů tak, aby i méně znalý uživatel informačních technologií pochopil problematiku monitorování sítí s využitím systému Zabbix. Je zde ovšem nutné podotknout, že při tvorbě této práce jsem přistupoval k ní s myšlenkou, že potenciální čtenáři budou mít alespoň základní znalosti o informačních technologiích.

21 Zdroje

Publikace:

1. HONTAÑÓN, Ramón J. *Linux: praktická bezpečnost*. 1. vyd. Praha: Grada, 2003, 438 s. ISBN 80-247-0652-0.
2. Bruckner, T. - Voříšek, J.: *Outsourcing informačních systémů*. Praha, EKOPRESS, 1998, ISBN 80-86119-07-6
3. Shah, Steve; Soyinka, Wale. *Administrace systému Linux*. Grada, 2007, ISBN 978-80-247-1694-7
4. BRUST, Andrew J. FORT, Stephen, *Mistrovství v programování SQL Serveru*, Brno, Computer Press, ISBN 978-80-251-1607-4
5. Carla Schroder, *Linux: Kuchařka programátora/administrátora*, COMPUTER PRESS 2009, ISBN: 978-80-251-2407-9
6. Bednář Vojtěch: *Linux na firemním PC - možnosti, rizika cena, BEN - technická literatura*, 2007, ISBN 978-80-7300-225-1
7. Matt Welsh a kolektiv autorů, *Používáme Linux*, Computer Press 2003 ISBN: 80-7226-698-5

Odborné články a elektronické zdroje:

1. http://cs.wikipedia.org/wiki/Open_source
2. <http://www.serverfocus.org/nagios-vs-cacti-vs-zabbix-vs-zenoss>
3. <http://www.zabbix.com/presentation.php>
4. <https://www.zabbix.com/documentation/2.0/manual/installation>
5. <http://www.abclinuxu.cz/slovník/frontend>
6. http://www.linuxsoft.cz/article.php?id_article=551
7. <http://interval.cz/clanky/instalujeme-mysql-na-linux>
8. [http://cs.wikipedia.org/wiki/Vi_\(editor\)](http://cs.wikipedia.org/wiki/Vi_(editor))
9. https://www.zabbix.org/wiki/How_to/configure_shared_memory

10. <http://httpd.apache.org/docs/2.2/install.html>
11. <https://www.zabbix.com/documentation/2.0/manual/quickstart>
12. <http://cs.wikipedia.org/wiki/Firewall>
13. https://www.zabbix.com/documentation/2.0/manual/config/items/itemtypes/zabbix_agent
14. <https://www.zabbix.com/documentation/2.0/manual/config/triggers/expression>
15. http://cs.wikipedia.org/wiki/Service-level_agreement
16. https://www.zabbix.com/documentation/2.0/manual/it_services
17. <http://www.systemonline.cz/outsourcing-ict/tajemstvi-zkratky-sla-1.html>

22 Seznam Obrázků

Obrázek. 1. - Co je to Zabbix.....	13
Obrázek. 2. - Monitorovací funkce	15
Obrázek. 3. - Běžící proces Zabbix Server	30
Obrázek. 4. - Welcome to Zabbix Server	32
Obrázek. 5. - Check of pre-requisites	33
Obrázek. 6. - Configure of DB connection.....	33
Obrázek. 7. - Zabbix server details	34
Obrázek. 8. - Install.....	35
Obrázek. 9. - Log-in obrazovka	36
Obrázek. 10. - Zabbix_agentd.conf, zdroj.....	38
Obrázek. 11. - Běžící procesy zabbix_agentd.....	38
Obrázek. 12. - Korektně navázaná komunikace	39
Obrázek. 13. - Dashboard	40
Obrázek. 14. - Struktura Zabbix.....	41
Obrázek. 15. - Host	46
Obrázek. 16. - Item.....	47
Obrázek. 17. - Zatížení procesoru.....	49
Obrázek. 18. - Trigger	50
Obrázek. 19. - Notifikace – e-mail.....	51
Obrázek. 20. - Notifikace – akce.....	52
Obrázek. 21. - Notifikace – operace.....	53
Obrázek. 22. - Template	54
Obrázek. 23. - SLA	56
Obrázek. 24. - SLA 2.....	58

23 Seznam tabulek

Tabulka 1. - Podporované databázové systémy	19
Tabulka 2. - Dodatečný software	20
Tabulka 3. - Vzor pro výpočet velikosti databáze.....	22
Tabulka 4. - HW a SW nároky.....	24

24 Přílohy

Příloha 1. – DashBoard

[Home](#) | [Dashboard](#) | [Reports](#) | [Configuration](#) | [Administration](#) | [Help](#) | [Get Support](#) | [Print](#) | [Profile](#) | [Logout](#)

[Dashboard](#) | [Overview](#) | [Maps](#) | [Latest data](#) | [Triggers](#) | [Events](#) | [Graphs](#) | [Screens](#) | [Maps](#) | [Discovery](#) | [IT services](#)

[History](#) | [Latest data](#) | [Status of Triggers](#) | [Latest events](#) | [Custom graphs](#) | [Dashboard](#)

PERSONAL DASHBOARD

Status of Zabbix

Parameter	Value	Details
Zabbix server is running	Yes	137.0.0.110054
Number of hosts (monitored/not monitored/templated)	159	136 / 0 / 23
Number of items (monitored/duplicated/not supported)	46136	7357 / 4090 / 5359
Number of triggers (enabled/disabled/problems/unknown/ok)	4418 / 237	[137 / 0 / 4399]
Number of users (online)	8	1
Required server performance: min values per second	16.46	-

Updated: 16.09.2010

System status

Host group	Disaster	High	Average	Warning	Information	Not classified
OS-CENTR-SERVICES	0	0	1	0	0	0
Linux-MISC	0	0	0	0	0	0
SQL-SERVICES	0	1	3	0	0	0
MAIL-SERVICES	0	5	3	10	0	0
APPLICATIONS	0	0	0	0	1	0
Zabbix-SERVICES	0	0	3	0	0	0

Updated: 16.09.2010

Host status

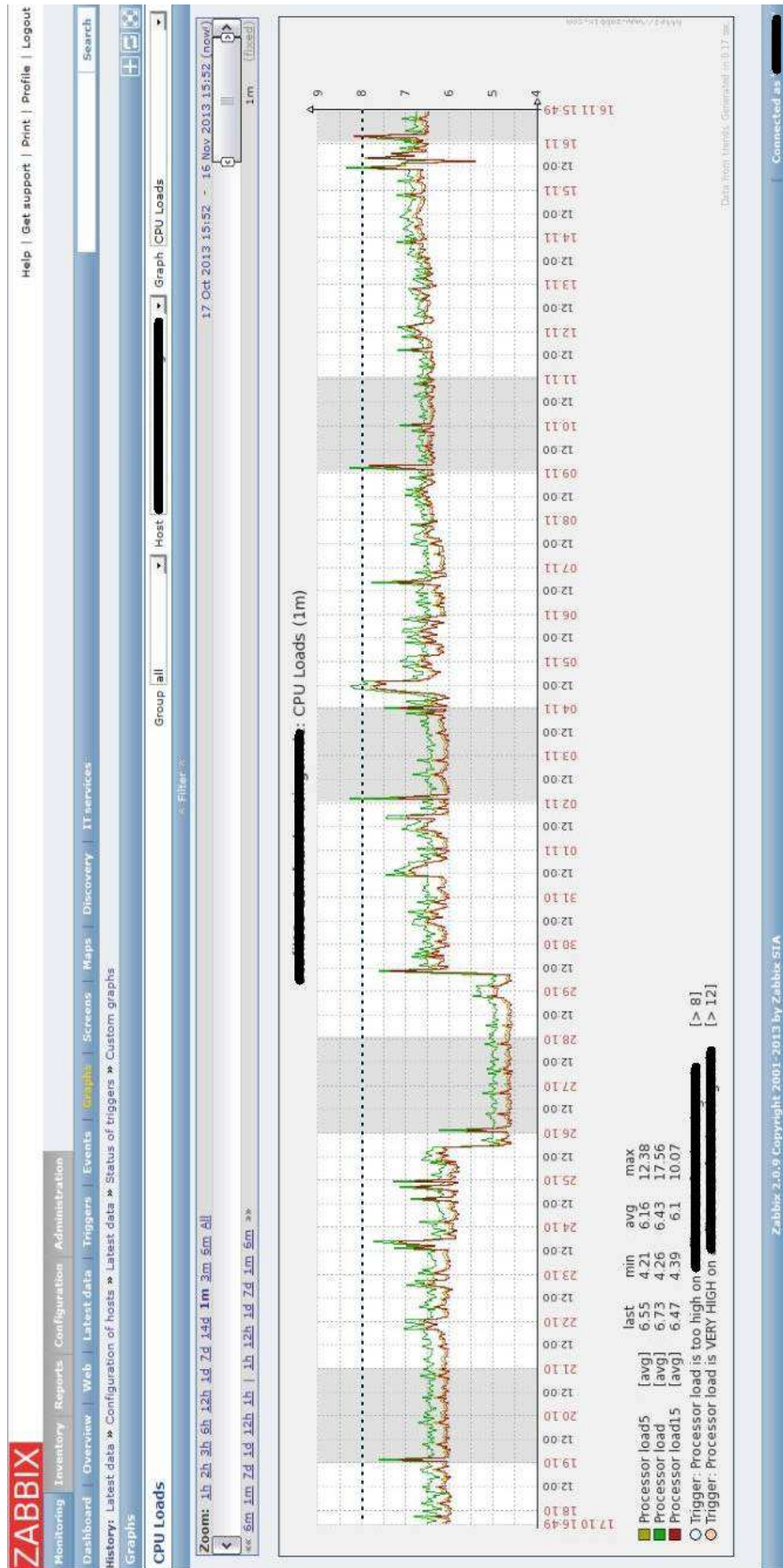
Host group	Without problems	With problems	Total
OS-CENTR-SERVICES	11	1	12
Linux-MISC	29	0	29
SQL-SERVICES	1	2	3
MAIL-SERVICES	79	9	88
APPLICATIONS	17	1	18
Zabbix-SERVICES	0	1	1

Updated: 16.09.2010

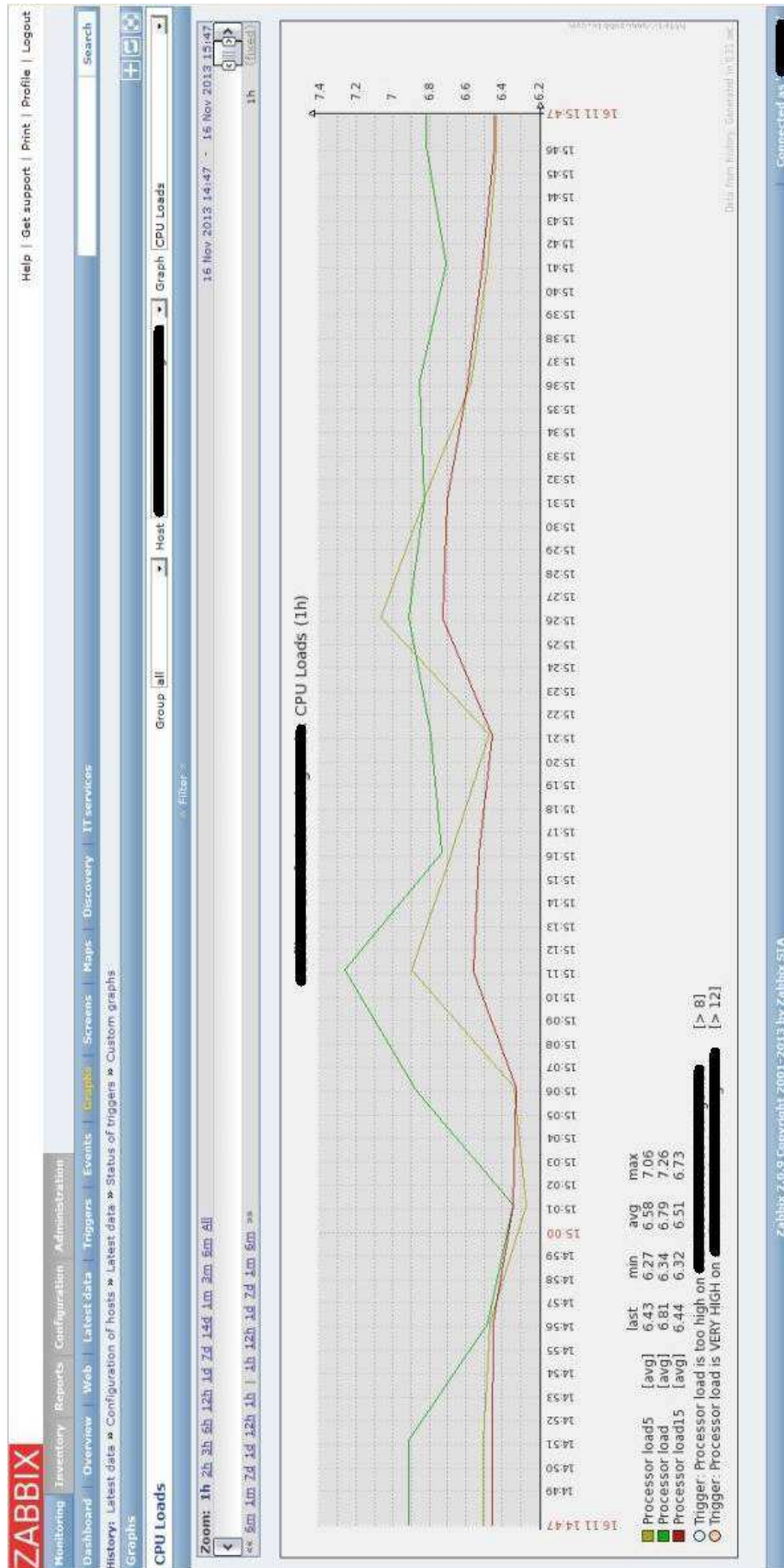
Last 100 issues

Host	Issue	Last change	Age	Info	Ack	Actions
.....	02.09.2010 14:14:39	2h 12m 42s	1
.....	02.09.2010 04:03:20	12h 26m 43s	1
.....	02.09.2010 04:03:28	12h 26m 35m	1

Příloha 2. - Ukázka grafu – délka sběru dat 1 měsíc



Příloha 3. - Ukázka grafu – délka sběru dat 1 hodina



Příloha 4. - Latest Data

The screenshot shows the Zabbix web interface. At the top, there is a navigation menu with links for Monitoring, Inventory, Reports, Configuration, and Administration. Below this is a breadcrumb trail: Dashboard > Overview > Web > Latest data > Triggers > Events > Graphs > Screens > Maps > Discovery > IT services. The main content area is titled 'LATEST DATA' and shows a list of items for a specific host. The list has four columns: Name, Last check, Last value, and History. The items listed include: apps (2 items), Availability (25 items), CPU (7 items), Database (10 items), Filesystem (22 items), General (7 items), Integrity (4 items), Memory (2 items), OS (8 items), Performance (7 items), Ping (1 item), Processes (25 items), Services (122 items), and Custom Scripts (20 items). The 'Last check' column shows the time of the last data update for each item, and the 'Last value' column shows the current value of each item. The 'History' column shows the number of historical data points for each item.