UNIVERZITA PARDUBICE
ÚSTAV ELEKTROTECHNIKY A INFORMATIKY

DOHLEDOVÉ SYSTÉMY POČÍTAČOVÝCH SÍTÍ

BAKALÁŘSKÁ PRÁCE

AUTOR PRÁCE: Tomáš Krupička
VEDOUCÍ PRÁCE: Ing. Lukáš Slánský

2007

UNIVERSITY OF PARDUBICE
INSTITUTE OF ELECTRICAL ENGINEERING AND INFORMATICS

NETWORK MONITORING TOOLS

BACHELOR WORK

AUTHOR: Tomáš Krupička
SUPERVISOR: Ing. Lukáš Slánský

2007

Vysokoškolský ústav: Ústav elektrotechniky a informatiky
Katedra/Ústav: Ústav elektrotechniky a informatiky
Akademický rok: 2006/2007

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Pro: Krupička Tomáš

Studijní program: Informační technologie

Studijní obor: Informační technologie

Název tématu: Dohledové systémy počítačových sítí

Zásady pro zpracování:
Teoretická část:

- Popis technologií používaných pro dohled funkčnosti počítačových systémů.
- Výběr vhodných kandidátů pro implementaci dohledového systému na ÚEI, jejich zhodnocení.

Praktická část:

- Implementace vybraného dohledového systému pro potřeby ÚEI.

Seznam odborné literatury:

- http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html
- Různé internetové zdroje

Rozsah: Přibližně 40 stran

Vedoucí práce: Ing. Slánský Lukáš

Vedoucí katedry (ústavu): prof. Ing. Pavel Bezoušek, CSc.

Datum zadání práce: 30.11.2006

Termín odevzdání práce: 12.05.2007

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně Univerzity Pardubice.

V Pardubicích dne

Tomáš Krupička
(vlastnoruční podpis)

Poděkování:

Rád bych touto formou poděkoval vedoucímu mé bakalářské práce panu Ing. Lukáši Slánskému za odborné vedení a cenné rady, které mi poskytl v průběhu práce.

ABSTRAKT

Tato práce si klade za cíl seznámit čtenáře s dohledovými systémy počítačových sítí, které jsou určené pro monitorování síťových prvků a pracovních stanic. Informuje čtenáře o vlastnostech těchto dohledových systémů.

Obsah

Seznam obrázků

Úvod a cíl práce

1.1. Úvod

Problematika efektivní správy počítačové sítě je hlavní otázkou každého administrátora sítě. Dobře fungující počítačová síť je základem úspěchu v každé organizaci. Správa sítě není jen o kontrole aktivních prvků sítě, ale i o službách, které jsou na síti využívány, např.: webové služby, služby využívající databázi atd. Dohledový systém počítačových sítí má za úkol sledovat změny aktivních prvků a služeb na celé síti. Tento systém umožní značné zjednodušení a hledání možných závad na počítačové síti. Odhalení problému a jeho následné rychlé řešení zajistí správnou a bezchybnou funkčnost počítačové sítě.

V současné době existuje velmi mnoho zajímavých produktů jak komerčních, tak open source. Dohledové systémy se uplatňují nejen ve spojení s velkými počítačovými sítěmi, které obsahují velké množství počítačů a serverů, ale i v podstatně menších počítačových sítích.

1.2. Cíl práce

Cílem bakalářské práce je získání obecného přehledu o všech dostupných dohledových (monitorovacích) systémech pro použití v počítačových sítích, získání základních informací o těchto systémech a přehledu jejich základních funkcí a vlastností. Dohledový systém musí splňovat požadavky, které na něj klade správce počítačové sítě ÚEI. Porovnání vlastností a následné vybrání vhodného systému pro uplatnění dohledového systému na ÚEI a jeho nasazení do provozu v síti ÚEI.

2 Základní informace

2.1. Co si představit pod pojmem dohledový systém

Dohledový systém může být též nazýván jako monitorovací systém, jehož úkolem je monitorování stavu sítě, aplikací, zátěže počítače atd. Termín monitorování stavu sítě popisuje systém, který dovolí správcům sítí kontrolovat síť, služby nebo umožní síťovému správci analyzovat a řídit síťovou strukturu vzdáleně z jednoho místa bez toho, aby řešil problémy osobním zásahem. Systémy mohou kontrolovat vybrané podsítě a zobrazovat síťové statistiky a hardwarový seznam, seznam software a seznam služeb běžících na sledovaném počítači. Systém může kontrolovat všechny aspekty LAN serverů a WAN sítí, pracovních stanic a IP zařízení, ale samozřejmě i monitorovat všechny spuštěné služby a aplikace jak na stolních počítačích, tak na serverových zařízeních.

Posláním všech monitorovacích systémů je maximalizovat spolehlivost všech zařízení zapojených v síti a aplikací pomocí automatického odhalení a opravy problémů. Monitorovací systémy reagují na chyby a na všechny problémy, které se vyskytly v síti v reálném čase. To znamená, že reagují v nejkratším možném čase. Mohou posílat správci sítě oznámení o vyskytnuvším se problému emailem, SMS zprávou nebo zasláním upozornění na pager. Tyto systémy mohou také zajistit opravu nebo nápravu daného problému samy a poté pouze vytvořit chybový soubor a do něho uložit informace o vyskytnuvším se problému. Monitorovací systémy mohou běžet na všech známých operačních systémech, např.: na Linuxu, Unixových systémech, Netware, MacOS-X, Windows atd. (14)

2.2. Složení monitorovacího systému

Monitorovací systém je založen na modelu klient/server. Server je nazýván jako manager a klient je nazýván agent. Agent běží na sledovaném síťovém zařízení a monitoruje stav daného zařízení a

posílá o jeho stavu informace manažeru. Manager sbírá informace od jednotlivých agentů. Agent navíc dokáže komunikovat s jednotlivými agenty navzájem. Manager lze obsluhovat pomocí internetového prohlížeče a ve většině případů pomocí velmi příjemného uživatelského prostředí.

2.3. Druhy monitorování

2.3.1. Ping

Příkaz Ping je jedním z prvních, a řekl bych, možná i jeden z nejpoužívanějších a nejjednodušších ověření dostupnosti připojení aktivního zařízení v síti. Ping pracuje posláním ICMP[1] paketu "echo žádosti" směrem k cílovému hostiteli a opětovnému naslouchání ICMP paketu "echo odpověď", kterou pokud dostane, je zařízení aktivní. Odpověď je někdy též přezdívána "Pong!" jako obdoba z Ping-Pongu (stolního tenisu). Použitím intervalu měřeného času a rychlosti odezvy Ping odhaduje obousměrný čas (obecně v milisekundách, ačkoli jednotka je často vynechána) a paketovou ztrátu (pokud je) mezi hostitelskými počítači. (16)

2.3.2. SNMP[2]

Vznik protokolu SNMP je datován na konec 80. let minulého století. V roce 1990 byl protokol SNMP potvrzen jako standard pro správu sítí. Na protokolu SNMP je dnes založena většina nástrojů a prostředků, které se věnují správě sítě. Protokol SNMP je založen na modelu klient/server. Server je nazýván jako manager a klient je nazýván agent. Agent běží na sledovaném síťovém zařízení a monitoruje stav sledovaného zařízení a posílá o jeho stavu informace manageru. Manager sbírá informace a dovede komunikovat s jednotlivými agenty.

V současná době jsou existují 3 verze protokolu SNMP: SNMPv1, SNMPv2 (ten je nejrozšířenější) a SNMPv3. První specifikace protokolu

[1] Internet Control Message Protocol
[2] Simple Network Management Protokol – standard síťového protokolu

SNMPv1 (RFC1157) vznikla v roce 1989, tato verze specifikovala pouze ochranu heslem v řetězci *community string*, který je součástí paketu. Bylo to nešifrované heslo, které se dalo pomocí filtrování paketů zjistit a velice snadno odhalit. SNMPv2 bohužel tuto obrovskou slabinu nedokázala odstranit, ale používá autentizaci, neboli ověření identity uživatele a služeb. Poslední specifikace SNMPv3 pochází z roku 1998 a umožňuje šifrování dat pomocí algoritmu DES[3]. V protokolu TCP/IP využívá transportní vrstvy bez spojení – protokol UDP. Pro komunikaci se typicky používá port 161 a pro TRAP naslouchá na portu 162. (17)

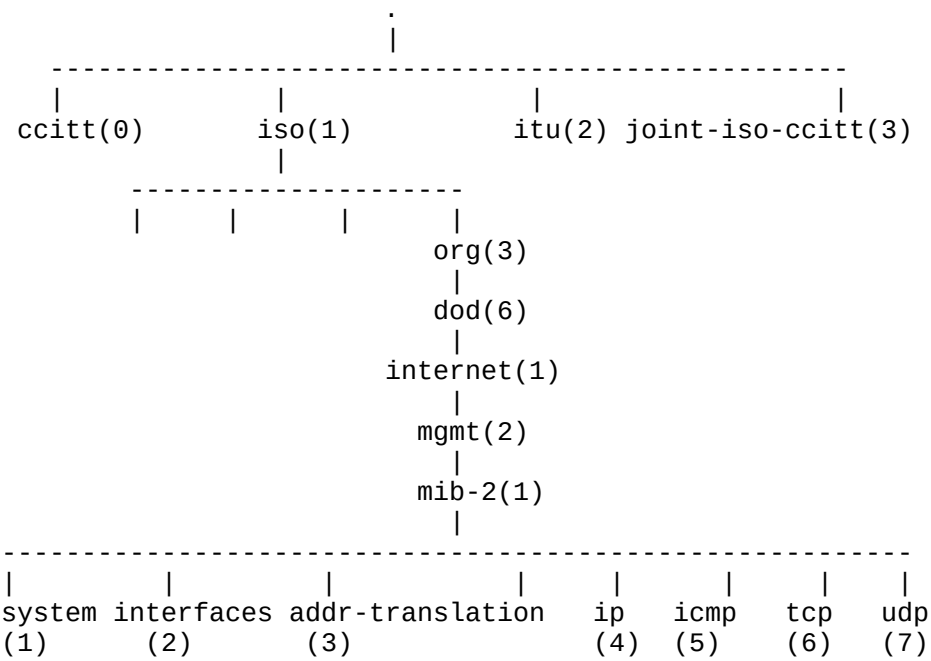
SNMP využívá následující příkazy:

- get-request a set-request – přečtení a nastavení hodnot MIB pro daného agenta,
- get-response – odpověď agenta na událost get-request,
- trap – agent jej vysílá manažerovi, jako reakci na událost, kterou považuje za důležitou, není zaručena jistota doručení.

MIB[4]

MIB je databáze, která svojí strukturou odpovídá danému zařízení a je využívána především agenty. Proto, aby mohl agent získat a předávat informace, musí znát dokonale strukturu MIB. MIB je stromová struktura, kde jsou určitá data uložena v každém listu stromu. Každý z uzlů ve stromu má své označení, jak číselné, tak i slovní. Lze teda přistupovat pomocí cesty od kořene stromu až k danému uzlu a tato cesta je vždy jednoznačně určena (číselně nebo slovně). (Obr. 1).

[3] Data Encryption Standard – šifrovací algoritmus
[4] Management Information Base – informační databáze



Obr. 1 - Ukázka MIB stromu

MIB specifikuje jaký typ dat může položka obsahovat. Nejčastěji obsahují hodnoty typu integer, string nebo je možné použít složitější datové struktury. Objekty jsou listy MIB stromu. Na následujícím příkladu si ukážeme, jak se můžeme odkazovat na uzly MIB stromu. Každý uzel je jednoznačně identifikovaný číslem nebo slovně. Například objekt ifNumber z kategorie "interfaces" obsahuje číselnou hodnotu vyjadřující počet síťových rozhraní. Na objekt ifNumber se lze odkázat řetězcem: (2) (3)

```
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifnumber
```

nebo přesnou číselnou hodnotu (OID[5])

```
.1.3.6.1.2.1.2.1
```

Na instanci objektu se můžeme odkázat řetězcem

```
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifnumber.0
```

nebo číselnou hodnotou

```
.1.3.6.1.2.1.2.1.0
```

[5] Object ID – jednoznačný identifikátor

2.3.3. Sledování portů

Nejprve na úvod něco o síťovém portu obecně. Síťové porty jsou očíslovány od 0 až do 65535. Protokoly (TCP a UDP) používají porty ke svému chodu. (Tabulka 1). V rámci protokolů TCP a UDP se úplné síťové spojení udává typem protokolu, IP adresou odesílatele a příjemce, číslem portu odesílatele a příjemce.

Porty můžeme rozdělit do 3 skupin:

- 0 – 1023 běžně známé porty,
- 1024 – 49151 používají se pro méně známé služby a je možno si je zaregistrovat pro své aplikace,
- 49152 – 65535 privátní porty, užívané pro odchozí spojení .

Tabulka 1 - Přehled portů a služeb, které na nich běží

Port	Protokol	Popis
21	FTP	Užívaný pro přenos souborů
22	SSH	Secure shell – obdoba protokolu telnet, ale v šifrované podobě
23	Telnet	Vzdálený terminálový klient
25	SMTP	Přenos elektronické pošty (Simple Mail Transfer Protocol)
80	HTTP	Protokol pro přenos www stránek
110	POP3	Stahování elektronické pošty ze serveru
443	HTTPS	Šifrovaný protokol pro přenos www stránek

Nyní trochu více o jejich samotném sledování. Port může být otevřený, což znamená, že na něm běží nějaká služba, nebo zavřený, pokud na něm nic neběží. Je možno rozpoznat ještě jeden stav, a to je filtrovaný, kdy je port chráněn firewalem. Při pokusu o připojení na port TCP je zpět odeslán paket s příznaky RST a ACK. V případě, že se jedná o UDP porty, je zpět poslán ICMP paket typu a kódu 3, z čehož vyplývá, že port je nedosažitelný. Existuje řada způsobů, jak porty sledovat (scanovat). Některé jsou více nápadné, jiné jsou postaveny takovým způsobem, aby si administrátor vzdáleného systému pokud

možno ničeho nevšimnul. Podívejme se proto nyní krátce na některé běžné metody užívané při scanování portů: (1) (11) (12)

- **TCP connect scan** – snaží se o normální navázání spojení pomocí TCP na určitý port voláním connect(), zpravidla nepřehlédnutelné v systémovém logu vzdáleného počítače, který reaguje na takovéto pokusy zapsáním chybové hlášky.

- **TCP SYN scan** – neotvírá plnohodnotné spojení, ale realizuje pouze část navazování spojení: tj. pošle pouze SYN paket neboli žádost o navázání spojení a poté čeká na odpověď. Odpoví – li vzdálený počítač paketem RST, je scanovaný port zavřený nebo odpoví – li pakety SYN + ACK, je scanovaný port otevřený.

- **FIN scan** – odesílá v paketu příznak FIN, což je příznak pro ukončení veškerého spojení mezi počítači. Jednou z jeho variant je Xmas scan, který má mimo FIN nastaveny příznaky URG a PUSH. Pokud dostane počítač od sledovaného odpověď s paketem RST, je port zavřený. Oproti tomu pokud je otevřený, nebude na něj vůbec reagovat.

- **ACK scan** – slouží ke zjištění, zda je port počítače filtrován, to je zda je chráněn firewalem. Odešle paket s příznakem ACK a náhodně vygenerovanými sekvencemi čísel. Port není filtrován, pokud se vrácen paket RST, v ostatních případech je port filtrován.

2.4. Vlastnosti monitorovacích systémů

2.4.1. Inventář celé sítě:

- nalezne všechny počítače, servery a jiná zařízení s adresou IP v síti,
- získá MAC[6] adresy z počítačů a aktivních prvků v síti pro snadné setřídění a vytvoření seznamu,
- zobrazí mapu sítě se všemi prvky sítě a popisem prvků sítě,
- nalezne uzly používající vícenásobné IP adresy,
- zjistí softwarové balíky, služby, hotfixy nainstalované na počítačích ve vaší síti,
- automaticky obnoví seznam prvků bez nutnosti manuálního zásahu administrátora.

2.4.2. Monitorování sítě:

- zachytí a dekóduje přenosy mezi pracovními stanicemi,
- aplikační monitorování zahrnuje stav TCP/UDP portů (HTTP, SMTP, FTP, Telnet a dalších),
- varuje při výpadku serverů (webový server, databázový server, atd.),
- monitoruje databáze (MySQL, Oracle, PostgreSQL, atd.),
- monitoruje funkčnost webových stránek,
- monitoruje místo na disku, paměť, stav CPU[7], procesy, latenci a síťové prvky.

2.4.3. Odstranění závad na síti:

- prohlíží síť po MAC adresách, a to pro rychlé identifikování zařízení, která nejsou součástí sítě a oznámí neautorizovaná zařízení na síti,

[6] Media Access Control – jednoznačná identifikace síťového zařízení
[7] Central Processing Unit – centrální procesorová jednotka

- v evidenci softwaru je seznam aplikací, služeb a hotfixů nainstalovaných v celé počítačové síti za poslední den, týden nebo měsíc,
- porovnává dva počítače a dovoluje nám identifikovat rozdíly mezi stanicemi, hardware, softwaru, záplaty, atd.,
- kontrolujte, jestli uživatelé mají vyřazený antivirový software a zabezpečuje aktualizaci antivirových balíků,
- zobrazí seznam disků a jejich obsazení, zda jsou plné nebo jsou prázdné, tím se vyhne výkonovým nebo aplikačním problémům.

2.4.4. Informace o síti:

- export oznámení o problémech do PDF, Excelu nebo databáze a jejich skladování pro pozdější tisk,
- vytvoří statistiky celého systému pro den, týden, měsíc nebo dokonce pro celý rok,
- poskytne rozsáhlé zpracování dat a vytvoří ilustrativní grafy,
- zobrazení informace pomocí internetového prohlížeče,
- odešle výstražné zprávy přes ICQ a ostatní komunikátory,
- umožní vytvoření výstražných zpráv pomocí RSS/RDF kanálů.

2.5. Rozdělení monitorovacích systémů do kategorií

2.5.1. Alerting

Tyto systémy využívají různé způsoby upozornění na chyby nebo problémy vzniklé na síti a informují administrátora sítě nebo osobu odpovědnou za stav celé počítačové sítě. Mohou být integrovány přímo v monitorovacím systému nebo mohou existovat jako specializované systémy, např.: na odesílání SMS zpráv, na odesílání emailových zpráv nebo odeslání pouhého upozornění přes nástroje monitorující stav počítačové sítě a obsažených prvků. (10) (13)

Možné způsoby oznamování pomocí:

- webového rozhraní,
- příkazovou řádkou,
- zprávou na pager,
- textovými SMS zprávami,
- MMS multimediálními oznamovacími zprávami,
- hlasovou poštou/emailem/faxovými údaji,
- pomocí WAP,
- vytvořením log souborů,
- umožní vytvoření výstražných zpráv pomocí RSS/RDF kanálů,
- zpráv přes ICQ a ostatní komunikátory.

2.5.2. Application monitoring

Application monitoring může sledovat a kontrolovat servery pracující na různých operačních systémech. Můžeme sledovat systémové prostředky z operačních systémů Linux, Solaris, HP/UX, AIX, *BSD, MacOS-X, Netware, Windows atd. Může zkoumat využití CPU, použití paměti, užívání disku, síťové rozhraní, průměrný přenos na síti, velikost souborů a log soubory. Pravidelně kontroluje webové servery (HTTP, HTTPS), mail servery (POP3, SMTP), databáze (MySQL, Oracle, atd.). Nástroj administrátora pro kontrolu a možné předcházení problémů se správou aplikací a sítě. (10) (13)

2.5.3. Database monitoring

Databázové monitorovací systémy nebo software dokáží nejen monitorovat stav databáze, ale mohou též obnovit poškozenou databázi do původní verze. Lze provádět různé typy testů zaměřených na kontrolu kvality databázového a aplikačního prostředí. Aktivní monitorování pomůže předejít době nečinnosti a rychlému odstranění problému poté, co nastal a poznat stav jednotlivých součástí a identifikovat potenciální problémy se snížením výkonu databáze ještě předtím, než se projeví u koncového uživatele. (13) (15)

Vlastnosti:

- rychlé zjištění serverových problémů a minimalizace doby nečinnosti databázového systému,
- určení přesného bodu poruchy a ujištění, že server běží a je připraven pro běžné používání,
- zjistí a opraví potenciální snížení výkonu předtím, než se projeví u koncového uživatele,
- monitoruje databázi nepřetržitě nebo pomocí vhodně zvoleného časového intervalu,
- zjištění reálných výkonnostních ukazatelů chování SQL příkazů,
- grafický přehled celkových výkonnostních parametrů SQL zátěže (čekání na CPU, disky, síť),
- umožňuje sledovat výkonnostní parametry SQL zátěže za sledovaný interval pro jednotlivé,
  - SQL příkazy,
  - uživatele databáze,
  - pracovní stanice,
  - programy,
- umožňuje zálohování databáze, SQL příkazů.

2.5.4. Enterprise monitoring

Enterprise monitoring je kompletní řešení pro podniky pracující s rozsáhlou sítí nabízející kontrolu kritických obchodních procesů v základní počítačové síťové struktuře a kritických technických prostředků. Zahrnuje v sobě sloučení více funkcí monitorovacího systému (např.: application monitoring, event log monitoring, atd.).

Jsou to multifunkční systémy pracující s velkým množstvím informací a dat. Většina systémů nabízí nejen rozsáhlé monitorování stavu sítě, ale i kompletní přehled log souborů a jejich následnou analýzu, samozřejmě v reálném čase. (10) (13)

Vlastnosti:

- kontroluje všechny standardní internetové a autorizační služby,
- kontroluje kompletní široké síťové podnikové prostředí,
- monitoruje uživatelská výstražná hlášení,
- dlouhodobé monitorování datových log souborů,
- monitorovaná data exportuje do Excelu, Wordu, XML nebo do databáze,
- velmi přátelské/rychlé uživatelské rozhraní pro správu historie log souborů.

2.5.5. Enviroment monitoring

Enviroment monitoring je monitorování stavu prostředí určeného pro vzdálené monitorování teploty, vlhkostních podmínek, kouře a pro odhalování bezpečnostních poruch a ztráty výkonu v datových centrech s IT technologií. Teplota a vlhkost mohou nepříjemně ovlivnit a dokonce narušit výkon a stabilitu počítačových sítí a serverů. Ve velké míře to bývá především hardwarové řešení, neboť obsahuje senzory pro měření teploty a vlhkosti, senzory pro měření napětí a kouřové senzory. Enviroment monitoring je využitelný ve většině serverových center s velkým množstvím serverů. (10) (13)

Vlastnosti:

- monitorování teploty/vlhkosti, kouře, napětí v elektrické síti, atd.,
- uživatelem definované varování při kritické teplotě a vlhkosti,
- monitoring pomocí webového rozhraní,
- oznámení emailem,
- kompletní statistika.

2.5.6. Event Log monitoring

Užívá se pro kontrolu událostí vygenerovaných na počítači. Event Log monitoring monitoruje každý log soubor na lokálním počítači nebo pouze výběr jednotlivých log souborů podle potřeb administrátora. Poskytuje snadnou metodu sběru a analýzy log souborů v centrální

podobě. Administrátor sítě může zhodnotit události v něm uvedené a podle toho podniknout patřičné kroky k nápravě vyskytnuté situace. Pokud nastane nějaká nebezpečná událost, pošle se administrátorovi sítě email s popisem dané události. (10) (13)

Možné monitorované soubory:

- Microsoft Server log soubory,
- IIS log soubory,
- SQL Server log soubory,
- log soubory zálohovacího software,
- log soubory antivirových programů,
- statické HTML soubory,
- uživatelsky vytvořené log soubory.

2.5.7. Network and System monitoring

Monitorování sítě a systému v sobě zahrnuje monitorování a kontrolu zařízení obsažených v síti. Monitorování může být konfigurované přímo pro daná síťová rozhraní na počítači, Windows a Unixových serverech, routeru, switchi a další zařízení pracujících s protokolem SNMP. Dále podporují monitorování routerů firem Cisco, Juniper, 3Com, Nortel, Foundryand a stejně tak jako firewally od firem Netscreen, Fortinet, Ciscoor Checkpoint atd. Nabízí možnosti informačních zpráv o stavu sítě, které dovolí administrátorům sledovat síťovou dostupnost a výkonové parametry, např.: frekvence vyskytnuvších se chyb, souvislosti v selhání přenosu, dobu latence a jiné technické položky. (10) (13)

Vlastnosti:

- informace o přenosu na sítí a jeho analýza,
- zobrazení statistiky na všech síťových zařízeních,
- umožňuje vytvoření síťových map, které jsou čitelné; je zde podrobné zobrazení sledované síťové infrastruktury,
- síťový přenos je zobrazen graficky,
- podpora rámců např.: IP, IPv6, IPX, ICMP, TCP, UDP, IDP atd.,

- paketových typů : TCP a UDP jako TELNET, FTP, HTTP, POP3, NETBIOS, IRC, SNMP atd.

2.5.8. Network traffic monitoring

Je monitorovací software, který zaznamenává všechny datové pakety, které si vyměňují uzly na síti, a nabízí všechny diagnostické, dekódovací a filtrovací funkce pro jejich důkladnou analýzu. Mohou poskytnout detailní informace o využití sítě, komunikaci jednotlivých uzlů, komunikaci mezi vybranými uzly a v neposlední řadě informace o obsahu paketů. Jsou schopny vytvořit mnoho diagnostických testů a dokáží zobrazit záznam zakázaných, ale i povolených síťových aktivit v celém síťovém prostředí. Mohou zasahovat do nastavení síťového hardware a software. (10) (13)

Vlastnosti:

- filtrování komunikace,
- monitoring výkonu sítě v reálném čase a zobrazení záznamů,
- izolace podle protokolů, typu chyb nebo obsahu paketů,
- podrobné statistiky portů, protokolů, množství přenosů, výkonnosti a počtu uživatelů.

2.5.9. PC monitoring

Je monitorování programů nebo aplikací běžících na počítači, který je právě sledován a monitorován. Tímto monitorováním lze snadno zjistit veškeré aktivity na počítači, jako např.: přihlašovací jméno osoby, která užívá jakýkoli program nebo kdy byl program spuštěn a jak dlouho už běží. Samozřejmě i jak dlouhou dobu byl aktivně používaný k práci nebo byl jen puštěný v pozadí. Mohou sledovat i stisknutí jednotlivých kláves a samozřejmě i pohyby myší na počítači a v jednotlivých programech. Je schopen rychle reagovat na ovlivnění výkonu sledovaného počítače a okamžitě o tom informuje administrátora nebo uživatele sledovaného počítače. Většina monitorovacích programů umožňuje vzdálenou kontrolu počítače a ovládání vzdálené plochy počítače. Počítačové

monitorování není jen užitečné pro sledování počítače, ale může také chránit počítač proti různým druhům škodlivých programů jako je spyware a ostatních programů, které zpomalují rychlost počítače. (10) (13)

Vlastnosti:

- umožňují kontrolu nad sledovaným počítačem,
- informace o programech a aplikacích běžících na sledovaném počítači,
- ochrání počítač před napadením viry a spyware,
- umožňují zjistit informace o uživateli,
- umožní restartovat počítač nebo ukončit, spustit nebo odhlásit uživatele ze sledovaného počítače,
- umožní monitorovat komunikační nástroje jako jsou ICQ, MSN, Yahoo atd.

2.5.10. Performance monitoring

Termín Performance monitoring by se dal přeložit jako monitorování výkonu, a to jak celého počítače, tak serveru nebo jen jeho komponent. Slouží k monitorování a zároveň následné optimalizaci komponent sledovaného počítače. Někdy též bývá součástí některých druhů monitorovacích systémů. (10) (13)

Vlastnosti:

- monitorování užívání CPU, pamětí, diskového prostoru,
- optimalizace jednotlivých komponent.

2.5.11. Protocol Analyzing and Packet Capturing

Jsou programy, které slouží k zachycení veškeré komunikace na síti. Dokáží spolupracovat se všemi prvky sítě jako jsou switche a routery. Sledují aktivitu na všech portech v pracovní stanicích a spolupracují s velkým množstvím síťových protokolů. Mohou též snímat a analyzovat pakety procházející uvnitř sítě mezi jednotlivými pracovními stanicemi.

Administrátor sítě si může nakonfigurovat vlastní filtr, kterým odfiltruje a zachytí pouze pakety určitého typu nebo pakety obsahující pouze určitá data. (10) (13)

Vlastnosti:

- zachycuje pakety poslané v rámci sítě,
- umožňuje sledovat a analyzovat pakety,
- analyzuje a dekóduje různorodé síťové protokoly,
- získává detailních informací o paketech,
- umožní sledování (až 100 000) uživatelů,
- zobrazuje statistiky pro každý port a pro každého uživatele sítě.

2.5.12. Security monitoring

Monitorování bezpečnosti nejen počítačů zapojených do sítě je nezbytnou součástí každého administrátora. Na zajištění bezpečnosti dat na síti jsou kladeny opravdu vysoké nároky. Pokud jsou narušena bezpečnostní opatření, je podezření, že by mohla být narušena stabilita celé sítě a důsledky mohou být katastrofální. K zajištění bezpečnosti je možné použít jednoduché firewally nebo lze použít složitější zabezpečovací systémy. Nezbytnou součástí bezpečnostního monitoringu je pravidelná aktualizace antivirového programu a zjišťování jeho funkčnosti v rámci celého systému z centrálního bodu. (10) (13)

Vlastnosti:

- zabezpečení vnitřní sítě před útoky hackerů,
- odstranění virů z internetových prohlížečů a stažených souborů,
- informace o stavu antivirových programů,
- kontrolování navštěvovaných internetových stránek a kontrola odeslaných a přijatých emailů,
- zobrazení zpráv o spojeních a otevřených portech,
- TCP, UDP a ICMP statistiky,
- kontroluje všechny pakety na síti.

2.5.13. Monitoring protokolu HTTP(S)

Je založeno na sledování protokolu HTTP(S), což je standardní protokol v síťové architektuře TCP/IP. Monitorování může kontrolovat HTML stránky. Poskytuje celkový pohled na strukturu webového rozhraní a zabezpečuje optimální výkon základních webových aplikací a snaží se dodržet co nejvyšší kvalitu služeb poskytovaných koncovému uživateli. Je to způsob jak řídit webové aplikace a infrastrukturu kombinující měření zákaznických zkušeností s určitými metrikami výkonu a dostupnosti podporovaných aplikací. (10) (13)

Vlastnosti:

- kontrola protokolů HTTP(S),
- zajištění dostupnosti stránek z každého místa na zemi,
- monitorování všech standardů Internetu a autorizačních služeb,
- dovolí sledovat heslem chráněné stránky,
- kontroluje platnost SSL certifikátů.

3 Výběr vhodného kandidáta pro implementaci

3.1. Kritéria pro výběr vhodného kandidáta

Požadavky, co by měl a mohl monitorovací systém umět od pana Ing. Lukáše Slánského, jsou hlavní kritéria pro výběr vhodného kandidáta.

3.1.1. Serverová platforma

Serverová část bude umístěná na serveru s OS Linux na platformě AMD64 nebo UltraSPARC T1. Je možné použít standardních skriptovacích jazyků používaných na Linuxové platformě, příp. Javy a kompilovaných programů v jazyce C/C++ z důvěryhodných zdrojů. Ukládání dat je možné buď v databázi přímo na serveru (MySQL, PostgreSQL) či na aplikačním serveru ÚEI (MySQL, PostgreSQL, Oracle).

3.1.2. Sledovaná platforma

Je potřebné provádět sledování zařízení na různých platformách. Jedná se o servery, pro které bude možné použít aktivní sledování s použitím agentů instalovaných přímo na serveru. Dále je potřebné sledovat aktivní síťové prvky zajišťující provoz učeben ÚEI. Zde bude možné provádět buď vzdálené sledování či sledování s využitím SNMP.

Jedná se zejména o prostředí:

- Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 SP2 a Windows Server 2003 R2 SP2 na platformě x86,
- Linux (distribuce Ubuntu, Debian, CentOS) na platformách x86, AMD64 a UltraSPARC T1,
- Solaris 10 na platformě AMD64 a případně také UltraSPARC T1,
- HP ProCurve 2524 a HP ProCurve 2650.

3.1.3. Požadavky na sledování

U sledovaných systémů je potřebné hlídat zejména dostupnost a funkčnost klíčových služeb na systémech. U systémů sledovaných pomocí agentů je vhodné sledovat klíčové parametry interiéru operačního systému (např. dostupná paměť, zátěž procesoru, dostupné místo na pevných discích). Všechny dané sledované parametry je potřeba zaznamenávat v čase po nastavitelnou dobu s možností statistického vyhodnocování a tvorby grafů.

V případě výpadku některé služby či výskytu problémového stavu v operačním systému je nutné mít možnost zaslat zprávu (email, příp. RSS, ICQ) administrátorovi, který může zajistit nápravu. Případně je možné použít jednoduchý automatizovaný zásah přímo na serveru (např.: restart serveru) pomocí skriptu či spuštění příkazu.

Systém může (není nutnou podmínkou) být použit i pro zachytávání některých informací, které lze zařadit do kategorie auditování – zjištění kdo, kdy a jaké akce na počítači prováděl (přihlášení, odhlášení, spuštění programu). Další z možných doplňkových vlastností je možnost sledování výkonnostních parametrů databázových a webových serverů.

3.2. Porovnání vlastností vybraných systémů

Tabulka 2 - Zhodnocení vlastností monitorovacích systémů

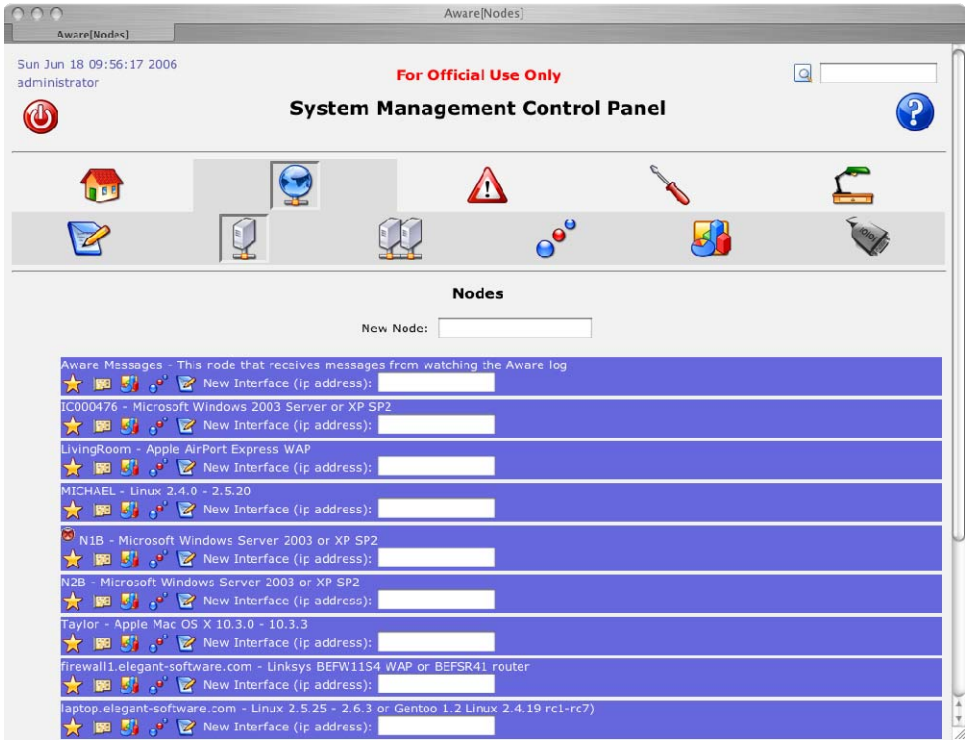
Název	Aware	Pandora	Nagios	Zabbix
Distribuce				
• komerční				
• open source	✔	✔	✔	✔
Sledovatelné platformy				
• Linux	✔	✔	✔	✔
• Unix	✔	✔	✔	✔
• Windows 2003/XP	✔	✔	✔	✔
• Solaris	✔	✔	✔	✔
Zjišťování dostupnosti serverů				
• webový	✔	✔	✔	✔
• databázový	✔	✔	✔	✔
• DNS	✔	✔		✔
• mail server	✔	✔	✔	✔
Monitorování protokolů				
• FTP	✔	✔	✔	✔
• SSH	✔	✔	✔	✔
• Telnet				
• SMTP	✔	✔	✔	✔
• DNS		✔		✔
• HTTP/HTTPS	✔	✔	✔	✔
• POP3	✔	✔	✔	✔
Sledování dostupnosti				
• ping	✔	✔	✔	✔
Monitorování portů				
• TCP/UDP	✔	✔	✔	✔
Sledování stavu PC				
• dostupná paměť	✔	✔	✔	✔
• kapacity disků		✔	✔	✔
• obsazení CPU	✔	✔	✔	✔
Informování o problémech				
• email	✔	✔	✔	✔
• ICQ				
• SMS		✔		✔
Statistiky				
• v databázi		✔	✔	✔
• log souborech	✔			

3.3. Zhodnocení kandidátů

Mezi vybrané systémy patří Aware, Pandora, Nagios a Zabbix. Z Tabulka 2 je patrné, že všechny systémy vyhovují nejen v požadavcích na sledovatelný operační systém, ale i s menšími rozdíly v ostatních kritériích. Všechny tyto produkty patří mezi open source produkty a mají licenci GNU/GPL. Postupně se podařilo nainstalovat a otestovat všechny monitorovací systémy. Některé svou instalací a následnou konfigurací nejen samotného systému, ale hlavně konfigurací samotných platforem, na kterých běží, nejsou zcela jednoduché.

3.3.1. Aware

Je to velmi zajímavý produkt, který byl vyvinut v roce 2007 a tedy je poměrně mladý, nicméně to mu z jeho vlastností neubírá. Lze ho nainstalovat na systémy Linux, Unix a platformy pracující s 64bitovou technologií. Dokáže monitorovat stav serverů a aktivních prvků, a to hned po své instalaci. Pár slov k instalaci: instalace je poměrně jednoduchá i pro nezkušeného uživatele, pro instalování jak manažera tak agenta se používá jeden a tentýž balíček. Výhodou je, že po nainstalování agenta na sledovaný počítač si sám stáhne od managera všechny informace potřebné k jeho chodu. Horší už je to s konfigurací samotného produktu, a to v nastavení informování o problémech na síti. To je asi nejslabší stránka Aware. Grafické prostředí je na dobré úrovni, ale v některých případech ne příliš přehledné. (Obr. 2). Aware je opravdu dobrý produkt, ale pro uplatnění na sledování sítě ÚEI bych ho nedoporučil.



Obr. 2 - Ukázka webové administrace produktu Aware (18)

Výhody:

- GNU/GPL licence,
- jednoduchá instalace i pro nezkušeného uživatele,
- agent automaticky stahuje konfiguraci od managera,
- dobrá úroveň grafického prostředí.

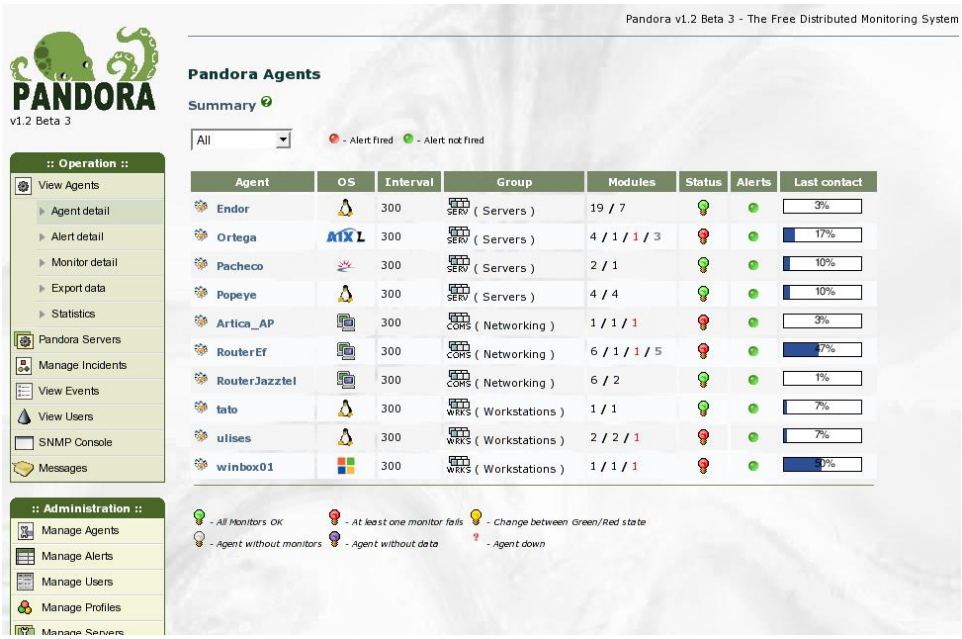
Nevýhody:

- poměrně složitá konfigurace.

3.3.2. Pandora

Pandora nabízí možnosti sledování statistik serverů, spuštěných služeb, statistiky a bližší informace o stavu hardware. Lze tento produkt nainstalovat na všechny systémy uvedené v předcházející tabulce. Robustní produkt na stejné úrovni jako produkt Aware, ale s trochu více propracovanou technikou konfigurace, a to na úkor kvality instalování jak na sledovaný server, tak na pracovní stanici. Instalace není právě jednoduchá a potrápí i zkušenější uživatele. K instalaci je potřeba nejen nainstalovat Pandora server, ale k němu zvlášť podporu pro administraci přes webové rozhraní pro vizualizaci výsledků monitorování. Grafická

úprava administrátorského prostředí je na velmi dobré úrovni a je v něm snadná orientace i pro méně zkušeného administrátora a uživatele. (Obr. 3). Největší slabinou je ale nutné spojení pomocí SSH mezi agentem a managerem. Vzhledem k poslední poznámce bych tento produkt nedoporučil jako monitorovací systém sítě ÚEI.



Obr. 3 - Ukázka webové administrace produktu Pandora (4)

Výhody:

- GNU/GPL licence,
- přehledná a snadná orientace v samotném programu,
- mnoho uživatelských nastavení.

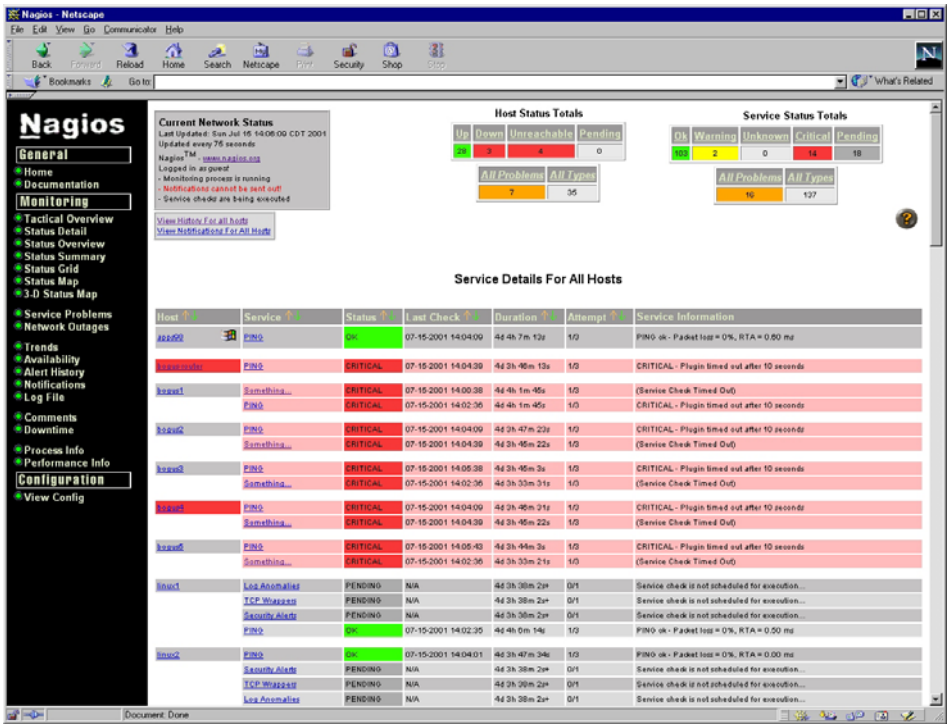
Nevýhody:

- komunikace přes SSH,
- složitá instalace, nutnost konfigurace každého prvku zvlášť.

3.3.3. Nagios

Další z mnoha produktů z dílny open source. Určený speciálně pro instalaci na platformu Linux a Unix, kde běží opravdu dokonale, ale lze s ním i monitorovat systém Windows a jeho služby. Instalace není jednoduchá, ale s pomocí opravdu dobré nápovědy ji lze zvládnout poměrně za slušnou dobu. Velice inteligentní a propracovaná je

konfigurace pomocí šablon. Úprava každé šablony je na potřebách administrátora a podle potřeb síťových prvků. Grafické řešení je dobré a vcelku přehledné. (Obr. 4). Ač je Nagios opravdu kvalitní produkt, moje doporučení je neimplementovat na sledování sítě ÚEI.



Obr. 4 - Ukázka webové administrace produktu Nagios (5)

Výhody:

- konfigurace pomocí šablon,
- GNU/GPL licence,
- rozšíření pomocí pluginů.

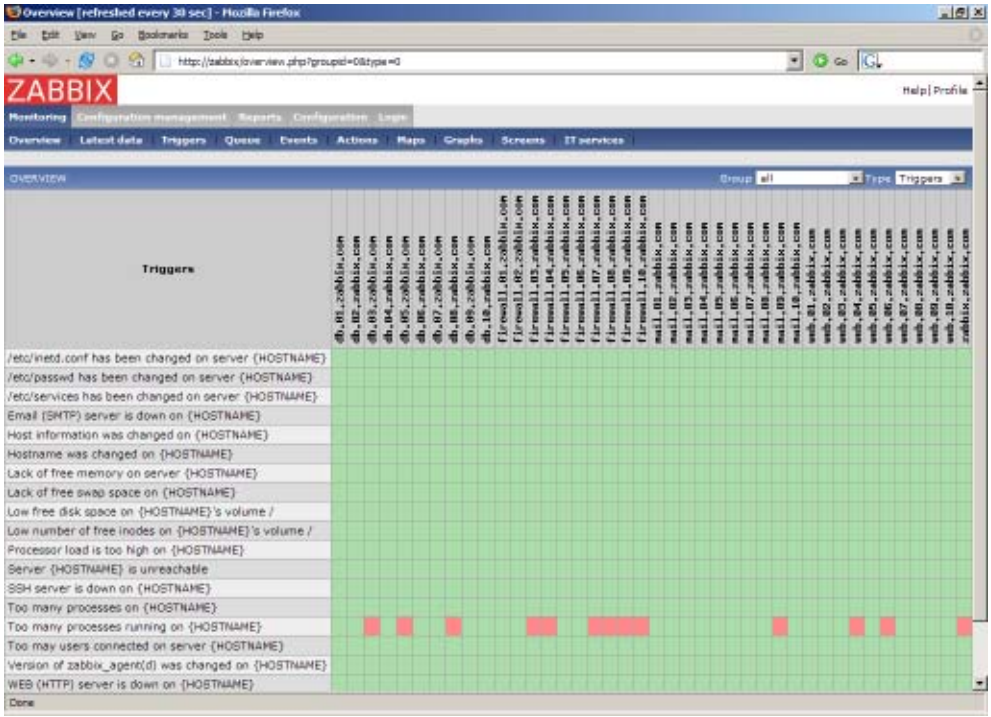
Nevýhody:

- poměrně neznámý produkt.

3.3.4. Zabbix

Zabbix je poměrně známý a kvalitní produkt. Je to nástroj pro aplikační a síťové monitorovaní. Zabbix podporuje všechny operační systémy a je to tedy komplexní produkt. Instalace není z jednodušších, ale je úměrná složitosti produktu. Výhodou je obsáhlá a řekl bych

vyčerpávající nápověda nejen na Internetu, ale i v různých diskusích. Na systém Windows se použije stejná konfigurace agenta jako na systému Linux, což je opravdu výborné řešení. Prostředí webového klienta je přehledné a dá se v něm lehce orientovat. (Obr. 5). Systém je možné konfigurovat přesně podle přání správce sítě a sledovat lze velké množství statistik. Jelikož systém pracuje s MySQL, je uložení všech dat v databázi naprostou součástí. Výhodou je spolupráce s databázemi MySQL, Oracle a PostgreSQL. Díky výhodám produktu a vyhovujícím podmínkám jsem vybral a doporučil produkt Zabbix pro nainstalovaní na monitorování sítě ÚEI.



Obr. 5 - Ukázka webové administrace produktu Zabbix (6)

Výhody:

- snadná konfigurace agenta,
- GNU/GPL licence,
- komplexní a efektivní produkt,
- spolupráce s databázemi MySQL, PostgreSQL, Oracle,
- je součástí některých distribucí Linuxu (např.: Fedora, Gentoo, Debian, Ubuntu atd.).

3.4. Instalace a konfigurace Zabbixu

V následujících krocích si popíšeme instalaci a konfiguraci vybraného systému, a to je Zabbix. Instalace je rozdělena na více části z důvodu postupné instalace. V některých distribucích bývá součástí základní instalace operačního systému Linux.

3.5. Instalace Zabbix serveru

1) První kroky instalace budou směřovat k vytvoření uživatele zabbix, který je nutný k přístupu do databáze: (8)

```
adduser zabbix
passwd zabbix
```

2) Stáhneme a rozbalíme instalační zdroje do námi vytvořeného adresáře.

3) Třetí krok je vytvoření a naplnění databáze s názvem zabbix:

```
mysql -u root –p heslo
create database zabbix
grant all privilegies on zabbix to zabbix
```

naplnění databáze se provede pomocí příkazů:

```
cat schema.sql | mysql –u zabbix –p zabbix
cat data.sql | mysql –u zabbix –p zabbix
cat images.sql | mysql –u zabbix –p zabbix
```

4) Nyní už se dostáváme k samotné instalaci, v tomto případě spíše kompilaci.

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

make install
```

5) Je třeba povolit v nastavení firewallu síťové porty, na kterých komunikuje server se svými agenty, a to jsou TCP i UDP porty 10050 a 10051.

6) Poslední fáze konfigurace je změna souboru zabbix_server.conf. Ten zkopírujeme ze zdrojů do adresáře /etc/, kde si vytvoříme adresář zabbix. Následující změna údajů v konfiguračním souboru by měla stačit jako základ pro fungování:

```
DBHost = „localhost“          - server MySQL
DBName = „zabbix“             - jméno databáze
DBUser = „zabbix“             - uživatelské jméno
DBPasword = „heslo“           - uživatelské heslo
```

7) Nyní zbývá pouze spuštění serveru:

```
./zabbix_server
```

3.6. Instalace agenta Zabbixu na systém Unix

Agent na systému Unix instalujeme z úplně stejných zdrojů jako instalujeme server. Pouze použijeme příkaz:

```
./configure --enable-agent
```

Samozřejmě musíme povolit síťové porty, aby mohl agent komunikovat se serverem. Spuštění agenta se provede zadáním příkazu: (7) (9)

```
./zabbix_agentd
```

3.7. Instalace a konfigurace agenta Zabbixu na systém Windows

Instalace agenta pro systém Windows je vcelku jednoduchá, je to otázka několika příkazů. První krok je stažení kompletního zdroje a zkopírováním spustitelného souboru ZabbixW32.exe z adresáře /bin/ nebo zkopírováním souboru ZabbixW64.exe, který je určen pro 64bitové

platformy. Tento soubor zkopírujeme například do rootu diskového oddílu, kde je nainstalován operační systém Windows. Poté zkopírujeme soubor zabbix_agentd.conf také do root oddílu stejně jako v prvním kroku postupu. Výhodou je použití stejného konfiguračního souboru pro agenta jak pro systém Unix, tak pro systém Windows. Stačí odkomentovat a změnit pouze tyto údaje: (7) (9)

```
Server=192.168.0.1
ServerPort=10050
Hostname=192.168.0.94
ListenPort=10050
```

Samotná instalace se provede spuštěním příkazu:

```
ZabbixW32 --config  c:\zabbix_agentd.conf install
ZabbixW32 start
```

3.8. Zprovoznění webového rozhraní

Příprava webového administrátorského rozhraní je opět otázkou několika málo minut. Jelikož je řešeno pomocí jazyka HTML a PHP s podporou databáze MySQL, tak stačí pouze zkopírovat obsah z adresáře frontends/php do námi vytvořeného adresáře, kde jsou umístěny „DocumentRoot“ stránky našeho webového serveru. Otevřeme si konfigurační soubor a opravíme pouze několik základních údajů:

```
$DB_TYPE= “MySQL“
$DB_SERVER=“localhost“
$DB_DATABASE=“zabbix“
$DB_USER=“zabbix“
$DB_PASSWORD=“heslo“
```

nutnou samozřejmostí je funkční webový server (např.: Apache). (7) (9)

3.9. Přidání hosta

Přidání hosta je možné přes webovou administraci. Přihlásíme se do administrátorského prostředí a v záložce Configuration vybereme položku Hosts. Po kliknutí se nám zobrazí již nakonfigurovaní hosté. Pokud chceme přidat hosta, klikneme na Create Host.
Zde jsou možné položky na vyplnění:

`Name` - jméno zařízení

`Groups` - zde můžeme nastavit skupiny zařízení

`IP adress` - nemusí se vyplňovat

`Status` - má 2 možnosti (monitored, notmonitored)

`Link with template`
- nastavení jaké zařízení bude monitorováno
na výběr je z MySQL_t, SNMP_t, Standalone_t, Unix_t a Windows_t

Pokud je správně nakonfigurován agent, měla by se okamžitě zobrazit informace, že je monitorovací agent dostupný a sbírá informace.

4 Závěr

Zavedení dohledového systému Zabbix bude pro ÚEI jistě nesporným přínosem. Vzhledem k open source produktu je investice do tohoto produktu nulová. Jediná nutná investice, je investice do času instalace a konfigurace, ale ta se vrátí ve formě dobře fungujícího a kvalitního systému pro monitorování sítě z centrálního bodu.

Produkt Zabbix je nesmírně mocný a efektivní nástroj. Nebudu zde popisovat kompletní konfiguraci všech jeho vlastností a nastavení, to není úkolem této práce. Kompletní popis všech vlastností a nastavení agentů najdete v manuálu produktu Zabbix, kde jsou popsány opravdu dokonale. (7)

5 Použité zdroje

(1) Sojka, Lukáš. *Síťový port* [online]. [cit. 2007-05-10].
URL: <http://cs.wikipedia.org/wiki/Síťový_port_%28software%29>.

(2) *Network Management & Monitoring with Linux* [online]. [cit. 2007-05-10].
URL: <http://david-guerrero.com/papers/snmp/>.

(3) Klaška, Luboš. *SNMP objekty a MIB* [online]. [cit. 2007-04-04].
URL: < http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=23&clanekID=3>.

(4) *Pandora* [online]. [cit. 2007-05-01].
URL: <http://pandora.sourceforge.net/screenshots/pandora_3.jpg>.

(5) Nagios, *Nagios: Screenshots* [online]. [cit. 2007-05-01].
URL: <http://www.nagios.org/about/screenshots.php>.

(6) *Homepage of Zabbix* [online]. [cit. 2007-05-01].
URL: <http://www.zabbix.com/screenshots_11_overview.php>.

(7) *Homepage of Zabbix* [online]. [cit. 2007-05-02].
URL: <http://www.zabbix.com/manual/v1.1/>.

(8) Karliak, Josef. *Dohledový systém Zabbix* [online]. [cit. 2007-05-02].
URL: <http://www.root.cz/clanky/dohledovy-system-zabbix/>.

(9) Karliak, Josef. *Sběr dat se systémem Zabbix* [online]. [cit. 2007-05-02].
URL: <http://www.root.cz/clanky/sber-dat-se-systemem-zabbix/>.

(10) *Network monitoring tools* [online]. [cit. 2007-05-02].
URL: <http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html>.

(11) Haller, Martin. *Scanování portů: techniky* [online]. [cit. 2007-04-20].
URL: <http://www.lupa.cz/clanky/skenovani-portu-techniky/>.

(12) Häring, David. *Ochrana před scanováním portů* [online]. [cit. 2007-04-20].
URL: <http://www.linux.cz/noviny/2000-11/clanek10.html>.

(13) *Network Monitor Software and Windows Development Tools* [online]. [cit. 2007-04-20]. URL: <http://www.monitortools.com/>.

(14) Smith, Roy. *Network monitoring* [online]. [cit. 2007-03-15]. URL: <http://en.wikipedia.org/wiki/Network_monitoring>.

(15) *Database Health Check for Oracle* [online]. [cit. 2007-04-10]. URL: <http://www.per4mance.cz/reseni/per4_db_dhc.php>.

(16) Switzer, John. *Ping* [online]. [cit. 2007-05-08]. URL: < http://en.wikipedia.org/wiki/Ping>.

(17) Kadlčík, Jiří. *Simple Network Management Protocol* [online]. [cit. 2007-05-09]. URL: <http://cs.wikipedia.org/wiki/Simple_Network_Management_Protocol>.

(18) Aware, *See all nodes* [online]. [cit. 2007-05-13].
URL: <http://www.elegant-software.com/software/aware/doc/html/uiNodePage1.html>.

ÚDAJE PRO KNIHOVNICKOU DATABÁZI

Název práce	Dohledové systémy počítačových sítí
Autor práce	Tomáš Krupička
Obor	Informační technologie
Rok obhajoby	2007
Vedoucí práce	Ing. Lukáš Slánský
Anotace	Tato bakalářská práce si klade za cíl seznámit čtenáře s dohledovými systémy počítačových sítí, které jsou určené pro monitorování síťových prvků a pracovních stanic. Informuje čtenáře o vlastnostech těchto dohledových systémů.
Klíčová slova	Dohledový systém, monitorování sítě, počítačové sítě