Počítačová sieť pod palcom

Martin Miškus
Slezská univerzita
martin18@centrum.sk

ABSTRAKT

Dnes si už svet nevieme predstaviť bez informačných a komunikačných technológií. Prichádzame s nimi do styku na každom kroku. Ani si pritom neuvedomujeme ako veľmi sme na nich závislí. Platí to aj pre počítačové siete, ktoré sú navzájom poprepájané. Mojou úlohou je Vám predstaviť princíp počítačových sietí a na základe akých vzťahoch fungujú. Hlavným bodom je správa a monitorovanie sietí s dôrazom na predchádzanie problémov skôr ako nastanú. Avšak bez softvérových riešení by sme to nemohli zvládnuť.
Z tohto dôvodu sa budem venovať produktom s otvoreným kódom, ktoré fungujú na základe vybraných protokolov SNMP, ICMP a ďalších. Z najpoužívanejších ako sú ako Pandora FMS, OpenNMS a Nagios, som vybral a detailnejšie rozoberiem aplikáciu Zabbix, s ktorou mám praktické skúsenosti.

Kľúčové slová

počítačová sieť, správa, monitoring, SNMP, Zabbix

1. ÚVOD

Každý kto sa zaujíma o počítačové siete, či už je to administrátor alebo technik Vám môže povedať, že správa siete je obtiažná a časovo náročná činnosť. Dochádza k sledovaniu veľkého počtu sieťových prvkov. Pre podnik a najmä managment firmy je vnímané informačné oddelenie ako náklady, ktoré existujú a nemali by ďalej narastať. Preto spoločnosti hľadajú produkty na monitorovanie a správu siete, ktoré by uľahčili správcom a technikom zavedenie určitej úrovne kontroly nad zariadeniami sieti čím dochádza k úprave nákladov. V dnešnej dobe je na trhu množstvo kvalitných produktov, ktoré sa vyskytujú nie len ako platené produkty ale tiež freeware alebo open source programy.

2. PRINCÍP SPRÁVY

Správa a údržba siete môže klásť obrovské požiadavky na prostredie IT. Aby sme docenili dôležitosť správy siete mali by ste porozumieť niektorým základným úlohám, ktoré správca musí v rôznych situáciách prevádzať - spraviť:

- nové pracovné stanice a servery je nutné nainštalovať a konfigurovať
- stávajúce pracovné stanice a servery je nutné aktualizovať
- operačné systémy a ovládače je nutné aktualizovať
- aplikácie ako antivírové nástroje je nutné nainštalovať, aktualizovať a vybavovať oprávnenými programami
- zariadenie ako sú rozbočovače, prepínače a smerovače je nutné inštalovať a konfigurovať
- je nutné inštalovať nové káble a vymeniť poškodené
- nutné vytvárať a overovať zálohy
- je nutné udržovať záznamy o zariadeniach napríklad konfigurácia každého počítača či servera
- dokumentácie je nutné doplňať o najnovšie údaje, aby odrážali výsledné zmeny a aktualizácie
- výstrahy a upozornenia je nutné ohlasovať, protokolovať a riešiť
- výkon siete je nutné pravidelne vyhodnocovať a sledovať

Toto je samozrejme len stručný zoznam úloh. Každá úloha musí byť obvykle nastavená správcom alebo technikom. Typický príklad predstavuje stredne veľká firemná sieť s 50 užívateľmi, niekoľkými servermi prepojenými pomocou smerovačov a prepínačov. V minulosti už len samotná aktualizácia operačného systému, či inštalácia antivírusového programu znamenala dlhé noci strávené ručnou inštaláciou v jednotlivých počítačoch. Ako sa siete rozrastajú a začínali byť zložitejšie, čas potrebný k nastaveniu týchto typov úloh sa stal problémom. Avšak za pomoci nástrojov pre správu siete si môže správca urobiť automatický súpis a vygenerovať podrobný výpis o obsahu všetkých pracovných staníc.

2.1 Oblasť správy

Správa siete je často definovaná ako proces ovládania siete za účelom dosiahnutia maximálneho výkonu a produktivity siete a zodpovednosti pracovníkov. Jedná sa samozrejme o veľmi širokú definíciu, ktorá je obmedzená len na používanú platformu pre správu a danú úroveň implementácie.

Správa siete sa typicky rozdeľuje do piatich oblastí:

- Problémy v sieti
- Nastavenie a konfigurácie siete
- Zabezpečenie siete
- Činnosť siete
- Analýza nákladov na sieť

3. MONITORING SIETÍ

Monitoring predstavuje sledovanie veľkého množstva hardwarových a softwarových oblastí. Ani tu neexistuje presné rozdelenie, pretože každá počítačová sieť je určitým spôsobom jedinečná. A preto aj prístup k nej musí byť individuálny. Niekedy potrebujeme kontrolovať vyťaženie CPU[1], na iných zas využitie kapacít sieťových rozhraní alebo diskových plôch. Nájdu sa aj systémy, na ktorých je nutné monitorovať napríklad počet prístupov používateľov za určité časové obdobie.

3.1 Monitorovanie hardvérových súčastí siete

Pri monitorovaní hardvérových súčastí systému sa často využíva aplikačný protokol SNMP, ktorý je primárne určený na monitorovanie stavu zariadení pripojených k počítačovej sieti.

[1] CPU – Central Processing unit, centrálna procesorová jednotka. Interprtuje, vykonáva alebo spracúva inštrukcie v počítači. Je to riadiaca jednotka.

Zaraďujeme tu napríklad monitorovanie vyťaženia CPU, pamäte RAM, kapacity pevných diskov či sieťových rozhraní. Podstata komunikácie prostredníctvom tohto protokolu je veľmi jednoduchá. Klient (agent) si vyžiada od servera (subagenta) informácie o nejakom konkrétnom objekte, ktorý server pozná a vie o ňom poskytnúť informácie. Server zašle klientovi v odpovedi aktuálnu hodnotu prislúchajúcu danému objektu. Všetko sa ukladá v špeciálnej databáze MIB, ktorá je v ňom implementovaná. Ak chce výrobca hardvéru pre svoj produkt zaviesť podporu do rôznych agentov alebo subagentov, stačí ak vydá rozšírenie MIB.

Výhodou oproti webovým a telnetovým správcovským rozhraniam je možnosť vytvárať skripty a všetko kompletne automatizovať.

3.2 Monitorovanie softvérových súčastí siete

Softvérové monitorovanie prvkov má za úlohu dohľad nad integritou súborového systému, systémových procesov, spustených procesov, kontrole voči útoku a pokusu o prienik alebo sledovaniu využitia sieťových aktivít.
Procesu monitorovania sieťových aktivít systému môžeme rozdeliť na monitorovanie využitia sieťových kapacít a na monitorovanie aktuálnych spojení a otvorených sieťových portov.

Na monitorovanie využitia sieťových kapacít alebo inak povedané vyťaženia dostupnej linky sa používajú dva druhy nástrojov, ktoré majú mierne odlišný princíp činnosti. Nástroje z prvej skupiny využívajú na získanie aktuálnych hodnôt protokol SNMP. Zozbierané dáta následne do grafickej podoby spracováva vizualizačný softvér.

Nástroje z druhej skupiny sú väčšinou založené na knižnici libpcap, ktorá je hojne využívaná napríklad analyzátormi sieťových protokolov kde sa analyzujú všetky prichádzajúce pakety. Ich výhodou oproti riešeniam založeným na protokole SNMP je, že sa s nimi dajú monitorovať napríklad iba určité rozsahy adries alebo vybrané protokoly.

Monitorovanie aktívnych spojení a otvorených sieťových portov plní v procese zabezpečenia a monitorovania operačného systému veľmi dôležitú úlohu. Pokiaľ by sa útočník pripájal pomocou tunelovaných spojení alebo cez „zadné dvierka“ (backdoor) tak monitorovanie aktívnych spojení a otvorených sieťových portov je prakticky jediná možnosť ako ho odhaliť.

4. Open source monitorovacie systémy

Monitorovací systém v praxi tvorí skupina programov, ktorej účelom je poskytovať prehľadnou formou informácie o sledovanej sieti. Cieľom moderných systémov je ale možnosť sledovať čím väčšie množstvo rôznych služieb. Všetky majú veľmi podobnú vnútornú štruktúru s rôznym množstvom drobných obmien, ktoré nájdeme vo väčšine z nich.

Monitorovací systém sa dá rozdeliť na tri časti, ktoré spolu navzájom komunikujú cez jasne určené rozhrania:

- komunikačné rozhranie – stará sa o zber informácií zo siete
- jadro – zabezpečuje plánovanie kontrol služieb a spracovanie nazbieraných informácií
- prezentačné rozhranie – zobrazuje spracované údaje v zrozumiteľnej forme

Následne sa jednotlivo delia na aktívne a pasívne komunikačné rozhranie. Jadro obsahuje tri hlavné časti - modul na správu konfigurácie, riadiacu logiku a plánovač. Prezentačná vrstva má v tomto modeli tiež dve základné časti - modul pre zapisovanie logov a prezentačné rozhranie.

4.1 Výber monitorovacieho sysému

Dnes má správca siete k dispozícií veľké portfólio dostupných dohľadových produktov, ktoré môže využiť pre monitoring danej siete. Je tiež nutné dodať, že vo veľa prípadoch nie je možné dokonale a objektívne porovnať systémy, ktoré sa v mnohých ohľadoch a prístupoch výrazne líšia. Pri výbere programu by mal zvážiť nasledovné kritéria:

- Cena
- Typ licence
- Podporované metódy monitoringu (nativný agent, SNMP,WBEM, externé skripty)
- Distribuovaný monitoring
- Webové rozhranie
- Definícia medzných hodnôt a zasielanie upozornení
- Inventár
- Vizualizačné výstupy (mapy, grafy, trendy, predikcie trendov)
- Automatická detekcia zariadení v sieti

5. ZABBIX

Predstavuje voľne dostupný systém na monitorovanie aplikácií, sietí a serverov. Podporuje aktívne aj pasívne techniky na získavanie dát z monitorovaných zariadení. Ľahko prispôsobitelný notifikačný mechanizmus umožňuje rýchle a pohodlné nastavenie rôznych typov notifikácií na preddefinované udalosti.

5.1 Podpora a požiadavky

Aplikácia Zabbix podporuje veľký počet operačných systémov (Mac OS, Windows, Solaris atď). Čo sa týka ďalších programov, ktoré potrebuje pre svoj beh, tak tu patria Apache, PHP a databázový server pre ukladanie všetkých svojich dát. Nevyhnutnou súčasťou je databáza MySQL, ale využívané sú aj Oracle, postgre SQL a SQLite. V prípade použitia týchto databáz je nutné doinštalovať PHP modul (napríklad PHP, MySQL), ktorý tomu zodpovedá. Keďže v databázach sú uschované všetky konfigurácie a dáta systému je nutné premýšľať aj nad nutnosťou hardwarových požiadaviek.

5.2 Inštalácia Zabbix agenta

Keď sa pozrieme na samotnú inštaláciu môžeme si vybrať voliteľné komponenty ako napríklad podpora pre SNMP protokol. Ďalej podpora pre web a monitorovací modul alebo externú utilitu ICMP. Pri inštalácií si vyberáme medzi serverom a agentom. Ak siahneme po agentovi, ponúka sa nám základná možnosť a to vytvoriť práva. Následne máme možnosť výberu medzi štandardnou a voliteľnou inštaláciou. Všetky konfigurácie si musíme dopredu nastaviť skôr ako začneme s programom pracovať. S tým súvisí aj inštaláciu webového rozhrania.

Zabbix agent je služba bežiaca na monitorovanom hostiteľovi a aktívne zbierajúca dáta o systémových zdrojoch a bežiacich aplikáciách. Následne sú všetky informácie posúvané od agenta k serveru, kde dôjde k ich spracovaniu. Zabbix agent je naprogramovaný v jazyku C a využíva priamo systémové volania preto je pre získavanie dát veľmi efektívny.

5.3 Nastavenie a používanie

Ako základné prostredie sa využíva webové rozhranie systému Zabbix, ktoré je prehľadné a intuitívne ako u väčšiny softvérov a aj tu si musí administrátor zvyknúť a získať skúsenosti s jeho

používaním a nastavením. Základom je dobrá orientácia v užívateľskom rozhraní. Menu je prehľadné a rozdelené do dvoch respektíve troch úrovní.

Správa užívateľských účtov prebieha pomocou definície užívateľov systému. Na základe typu, členstva v skupinách a oprávnenia k prístupu k dohľadovým prostriedkom sú rozdelení. Je to dôležité vzhľadom k prístupe rôznych užívateľov k zdrojom. Užívateľské účty sa tiež dotýkajú definovaných kanálov pre zasielanie upozornení v prípade výpadku monitorovaného zdroja. U webového rozhrania systému Zabbix existujú len dva typy užívateľských účtov. Prvým z nich je účet „Admin“ s plným prístupom k systému a druhým je účet „Guest“, ktorý definuje práva neprihlaseného užívateľa.

Jednotlivé nastavenia a vlastné udeľovanie práv k monitorovacím objektom je veľmi flexibilné a efektívne. Na jednej strane môžeme mať užívateľov, ktorí sú zoskupený do skupín užívateľov, na druhej strane sú hostitelia, ktorý môžu patriť do jednej alebo viac skupín hostiteľov. Využívajú sa práva ako čítať-zapisovať (read-write), iba na čítanie (read only) a posledným je zamietnutý prístup (deny). Na základe nich sú tieto skupiny prepojené s presne určitými právami.

Každý užívateľ má samostatne nastavený užívateľský typ - Zabbix user, Zabbix admin, Zabbix super admin

Už spomínané účty ovplyvňujú proces výpočtu jednotlivých práv užívateľom a určuje prístup funkciám vo webovom rozhraní. Pri nastavovaní práv je treba pamätať na niekoľko pravidiel. Napríklad ak má užívateľ (napr. Zabbix admin) nastavené read only na skupinu hostiteľov neobjavujú sa mu títo hostitelia v menu, ale stále ich môže monitorovať. Pokiaľ má ľubovoľný užívateľ nastavené - zamietnutý prístup na skupinu hostiteľov neobjavia sa mu následne ani v prehľadoch, ktoré monitoruje. Ďalej ak nastavíme skupine hostiteľov - zamietnuté na skupinu hostiteľov nebudú títo užívatelia schopný priradiť žiadnu šablónu k hostiteľom.

Keď máme účty vytvorené a prihlásime sa ako užívateľ admin môžeme v menu Administration vytvárať a spravovať jednotlivé užívateľské účty. K dispozícii sú napríklad tieto parametre, ktoré môžu byť nastavené – alias, name, surname, groups, refresh atď.

Program Zabbix nám ponúka vytváranie skupín, ktoré vedú k zjednodušenému procesu priraďovania práv. Pritom každý užívateľ musí byť aspoň v jednej skupine užívateľov, samozrejme skupiny je možné ľubovoľne vytvárať a meniť. Nastavenie sa nachádza v menu Administration/users/user group. V skupinách máme tiež k dispozícii určité parametre, ktoré sa môžu meniť. Patria tu napríklad group name, users alebo rights.

Na upozornenia slúži v Zabbixe ako informačný kanál časť „Media“ pomocou, ktorého sú prenášané upozornenia generované Zabbixom. Administrátor si najskôr zvolí a nadefinuje všeobecné média, ktoré sú potom využívané užívateľmi. Ide o spôsob zasielania správ formou emailu cez Jabber, prostredníctvom GSM brány – SMS správy.

Sila monitorovacieho systému závisí na jednoduchosti správy monitorovaných zariadení a ich parametrov. Sú definovaé tieto objekty – skupiny pracovných staníc, hostitelia a samotné monitorovacie položky.

Zabbix využíva aj prvok, ktorému hovoríme trigger[2]. Ide o logický výraz, ktorý reprezentuje stav monitorovanej položky. Vďaka nim môžeme čiastočne nastavovať hodnoty, ktoré keď sa prekročia považované za chybné.

Hodnota triggeru je prepočítavaná za každým keď server obdrží novú hodnotu, ktorá sa využije k výpočtu. Sú definované tri výrazy: false, true a unknown. Tiež je možné definovať rôznym udalostiam rôzny stupeň dôležitosti. Ich závažnosť má vplyv na vizuálnu prezentáciu daného stavu, zvukové upozornenie vo webovom rozhraní a použité médium pre odoslanie upozornení.

5.4 Vizualizačné nástroje

Zabbix ponúka vizualizáciu štatistických a reálne–časových informácií v rozsahu jednoduchých grafov až po komplexné pohľady obsahujúce grafy, mapy a textové informácie. Historické grafy informujú správcu o slabinách a výkonnosti IT infraštruktúry. Všetky grafické informácie sú prístupné cez webové rozhranie.

V mapách môžeme umiestňovať rôzne jednotlivé monitorovacie objekty navzájom ich prepájať a vytvárať schému sietí. Každý prvok môže byť zobrazený rôznymi ikonami podľa toho v akom stave sa nachádza.

Medzi nástroje, ktoré pomáhajú lepšie vykresliť situáciu ohľadne monitorovania siete patria aj obrazovky (screens).

Daná funkcia screens nám slúži pre zoskupenie niekoľko logicky súvisiacich výstupov na jednu obrazovku do tabuľky s nastaviteľným počtom riadkou a stĺpcou je možné umiestniť veľa rôznych výstupov, od jednoduchých textových informácií až po grafy a mapy.

Jednou z posledným ale zato veľmi dôležitých možností je Export/Import údajov. V aplikácii Zabbix je povolený export a import všetkých nastavení do formátu XML, čo veľmi uľahčuje tvorbu a výmenu šablón medzi užívateľmi. Je tiež možné v rámci hostiteľov exportovať alebo importovať ich monitorované položky, triggery a grafy. Vzhľadom k jednoduchému použitiu formátu XML je veľmi jednoduché vytvoriť vlastné skripty a regenerovanie týchto súborov.

6. ZHODNOTENIE PRODUKTU

Zabbix je aplikácia je v základe podobná ako mnohým iným aplikácii – Nagios, OpenNMS. Je určený pre monitorovanie stavu siete, avšak ponúka jednoduchšiu konfiguráciu nastavení. Obsahuje prepracované možnosti na získavanie informácií o sieti. Tieto informácie sa vzťahujú iba na dostupnosť vopred definovaných prvkov a služieb siete. Dosahuje sa to pravidelným overovaním dostupnosti zariadení. Všetky nastavenia sú uložené v databáze a sú editovateľné priamo pomocou webového rozhrania. Ďalšou výhodou je existencia automatizovaného pridávania zariadení do schémy čo v súčasnej dobe aplikácia Nagios neponúka.

7. POUŽITÁ LITERATÚRA

[1] Zabbix Manual. Riga: Zabbix SIA, 2009. Url: http://www.zabbix.com/downloads/ZABBIX%20Manual%20v1.4.pdf

[2] Miškus, M., Správa a monitoring počítačových sietí pomocou open source nástrojov a utilít, 2009

[3] BIGELOW, S. J. Mistrovství v počítačových sítích : správa, konfigurace, diagnostika a řešení problémů. 1. vyd. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9

[2] Trigger - spúšť, v databázi definuje činnosti, ktoré sa majú previesť v prípade definovaném udalosti nad databázovou tabuľkou.