SLOVENSKÁ TECHNICKÁ UNIVERZITA

Fakulta Elektrotechniky a Informatiky

Katedra telekomunikácií

Riadenie telekomunikačných systémov

Zadanie 2

Jozef Matický

Ak. rok 2012/13

Zadanie

Navrhnite manažment pre dohľad nad sieťou na ÚT FEI STU v Bratislave. Vypracujte referát v ktorom svoj návrh popíšete. Pripravte si krátku prezentáciu (cca 7 min), počas ktorej svoj návrh odprezentujete.

Úvod

Manažment sietí a dohľad nad nimi je dôležitou súčasťou väčších sieťových a počítačových inštalácií. Ide o aktivity, metódy, procedúry a nástroje, ktoré sa týkajú prevádzky, administrácie, údržby a správy sieťových systémov. Funckie, ktoré sú robené za účelom správy sietí zahŕňajú kontrolu, plánovanie, vyhradzovanie zdrojov, nasadzovanie hardwaru a softwaru, koordináciu a monitorovanie prostriedkov na sieti, sieťové návrhy a podobne. Účelom je priebežne zisťovať výkonnosť celej siete, identifikovať a vyriešiť problémy ešte pred tým, ako ovplyvnia fungovanie dotknutej organizácie a ľudí.

Zaužívaným spôsobom, ako charakterizovať správu sietí a zariadení je FCAPS – Fault, Configuration, Accounting, Performance and Security.

- Fault – porucha. Ide o udalosť, ktorá má negatívny význam. Cieľom správy porúch je rozoznať, izolovať a opraviť poruchu, ktorá sa na sieti vyskytne. Správa porúch monitoruje viaceré parametre zariadenia a hľadá neobvyklé správanie a parametre.
  Pokiaľ už porucha nastane, monitorované zariadenie väčšinou vyšle upozornenie do NMS buď štandardizovaným protokolom ako je SNMP ale proprietárnym. Toto upozornenie má za úlohu spustiť buď automaticky, alebo manuálne vybrané aktivity. Jednou z takých aktivít môže byť zistenie podrobnejších informácií o zariadení, alebo zariadenie zálohovať.
  Okrem toho správa porúch môže zaznamenávať poruhové udalosti a na základe nich poskytovať štatistiky fungovania siete, alebo jej častí.
- Configuration – konfigurácia zariadení. Jej cieľom je zbierať a ukladať konfigurácie sieťových zariadení, zjednodušiť ich konfiguráciu a sledovať zmeny v konfigurácii zariadení.
- Accounting – správa účtov. Úlohou je zbierať štatistiky užívateľov. Ide napríklad o obsadené miesto na pevnom disku, vyťaženie procesora, alebo siete. Okrem štatistík taktiež poskytuje užívateľské kontá a to pomocou protokolov ako RADIUS alebo TACACS.
- Performance – zisťovanie výkonnosti. Údaje o výkonnosti umožňujú pripraviť sa na budúcnosť, ako aj zistiť efektivitu siete. Výkonnosť a efektivita siete zahŕňajú monitorovanie priepustnosti jednotlivých sieťových prvkov, ich vyťaženie, chybovosť a podobne. Zbieraním

a analýzou uvedených dát je možné riešiť kapacitné problémy a problémy so spoľahlivosťou ešte predtým, ako nastanú a ovplyvnia poskytované služby.

- Security – bezpečnosť. Správa bezpečnosti je proces kontrolovania a prideľovania prostriedkov v sieti. Bezpečnosť je dosiahnuteľná použitím autentifikácie a šifrovania.

Dáta pre uvedený sieťový manažment môžu byť na sieti zbierané viacerými mechanizmami – programovým vybavením, ktoré dobrovoľne poskytuje informácie o zariadení, na ktorom beží – tzv. Agent, protokolmi, ktoré poskytujú rôzne informácie o systéme alebo sieti, odpočúvaním siete a podobne. V minulosti sa zvykol zisťovať iba jeden parameter monitorovaného zariadenia – to, či je zariadenie v prevádzke, alebo nie. V dnešnej dobe je monitorovanie sieťových zariadení dôležitou súčasťou náplne práce IT oddelení.

Najbežnejším protokolom správy siete je SNMP. Pomocou SNMP je možné spravovať a monitorovať zariadenia na IP sieti. Zariadenia typicky podporujúce SNMP sú smerovače, prepínače, bežný HW s vyspelejším operačným systémom, tlačiarne, telefóny a podobne.

V SNMP má za úlohu jedno, alebo viac zariadení manažovať manažované zariadenia, na ktorých je Agent. Agent pomocou SNMP posiela manažérovi informácie o zariadení, na ktorom beží.

Protokol taktiež umožňuje správu zariadenia, ako napríklad nastavenie rôznych parametrov operačného systému. To, ktoré parametre je možné na zariadení sledovať a ktoré upravovať určuje tabuľka MIB.

Sieť, ktorá je spravovaná pomocou SNMP pozostáva z troch hlavných komponentov:

1. Zariadenie, na ktoré chceme dohliadať a ktoré chceme spravovať
2. Agent – software, ktorý beží na manažovaných zariadeniach
3. Systém na správu sietí – NMS. Ide o programové vybavenie, ktoré beží na manažérovi

Okrem SNMP je možné na sieť dohliadať aj pomocou iných nástrojov a protokolov. Ďalším pomerne bežným je zisťovanie informácií o zariadení cez CLI – príkazové rozhranie. Cez toto rozhranie je možné monitorovať zariadenia, ktoré nedisponujú SNMP agentom. Toto rozhranie je väčšinou dostupné cez protokol SSH alebo Telnet a je možné preň vytvoriť tzv. skripty - série po sebe nasledujúcich príkazov, ktoré vedú k nejakému výsledku, ktorý manažér následne spracuje, alebo na ňom iba pasívne počúvať.

Iným spôsobom monitorovania sietí je tiež kontrola dostupnosti otvorených portov na zariadeniach, ICMP protokol, WMI, CMIP, RMON a mnoho ďalších.

Aby bolo možné získavať informácie z rôznych zariadení pomocou rôznych metód a protokolov, je potrebné vlastniť NMS. NSM je kombináciou hardwaru a softwaru použitého na monitorovanie a správu počítačových sietí.

Úlohou NMS je manažment sieťových prvkov – manažovaných zariadení. Pomocou NMS je možné sieťové zariadenia vyhľadávať, monitorovať a konfigurovať.

Existuje nepreberné množstvo rôznych nástrojov na monitorovanie sietí. Delia sa na dve skupiny a to:

1. Komerčné riešenia – platený software, ku ktorému je dostupná aj podpora výrobcu
2. Open Source – bezplatné riešenia, no väčšinou iba s komunitnou podporou a otáznou podporou do budúcnosti

Pre potreby menších sietí, ako je aj sieť ÚT, je dostačujúce aj bezplatné riešenie. Medzi bezplatné patria riešenia ako Nagios, OpenNMS, Cacti, SpiceWorks, OpenQRM, Hyperic HQ a mnoho mnoho ďalších. Ja som pre potreby ÚT vybral software Icinga.

Icinga

Icinga ako plno iných NMS riešení umožňuje správcom siete sledovať stav neobmedzeného[1] počtu zariadení na sieti a služieb, ktoré poskytujú. Icinga vznikla ako fork Nagiosu, no neskôr sa úplne odčlenila a dnes je to samostatný, plnohodnotný systém na monitorovanie sieťových prvkov. Oproti Nagiosu poskytuje množstvo výhod. Má moderné užívateľské rozhranie s podporou Ajaxu a Drag-and-drop rozhrania. Taktiež je kompatibilná s rozšíreniami určenými pre Nagios a má užívateľsky prívetivé API. Nakoľko sa jedná o systém používajúci ako frontend webové rozhranie, nie je potrebné na termináli, na ktorom sieťový administrátor sleduje stav siete, nič dodatočné inštalovať.

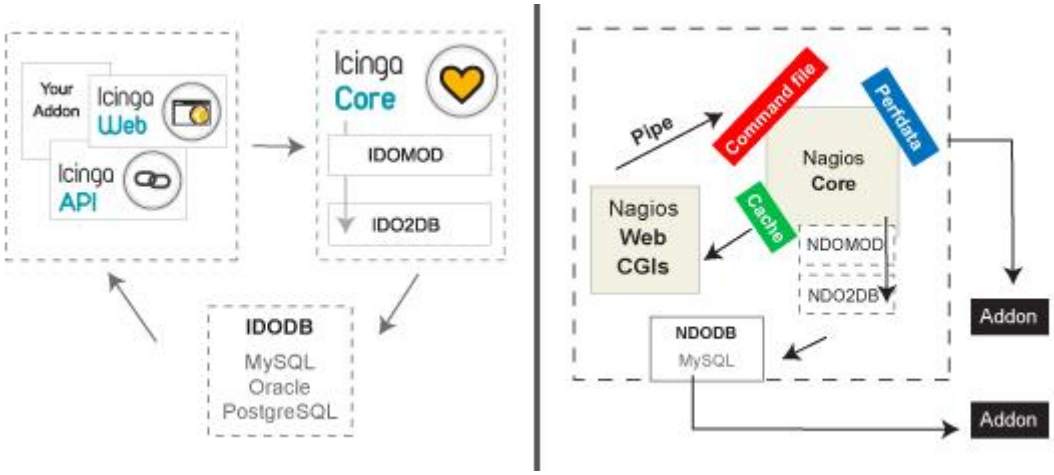
Icinga pozostáva z viacerých komponentov. Samotný monitoring siete zabezpečuje Icinga, ktorá pomocou rozhrania IDOMOD a služby IDO2DB komunikuje s MySQL/PostgreSQL/Oracle databázou, do ktorej ukladá informácie o monitorovaných zariadeniach, prevádzkové denníky a ďalšie parametre. Samotná Icinga poskytuje aj API iným aplikáciám. Frontend je dostupný po inštalácií Icinga-web view. Iginga-web komunikuje s databázou, z ktorej vyberá dáta, ktoré tam uložila Icinga. K dispozícii je taktiež rozhranie pre mobilné telefóny Icinga-mobile, ktoré je napísané aj pomocou Java Scriptu a je užívateľsky veľmi prívetivé. Monitorovací systém je možné riešiť aj distribuovane, čo napríklad Nagios nepodporuje. Podporuje tiež plánované odstávky sieťových prvkov a plno nových a unikátnych vlastností v svete NMS.

[1] Neobmedzené v závislosti na použitom HW, distribúcii záťaže a podobne

Icinga taktiež umožňuje zasielať upozornenia o problémoch na sieti a to pomocou rôznych služieb, ako e-mail, sms ale taktiež pomocou množstva služieb poskytujúcich okamžité správy ako ICQ, XMPP, MSN, IRC a ďalšie.

Icinga môže komunikovať s množstvom zariadení a to buď cez SNMP, RMON alebo pomocou skriptov a externých programov, ktoré je možné jednoducho do NMS integrovať. Taktiež podporuje SNMP trap, ale až po inštalácií niektorého z rozšírení.

Konfigurácia zariadení prebieha úpravou konfiguračných textových súborov. Toto je možno drobná nevýhoda konfigurácie, nakoľko môže byť zdĺhavejšia ako pridávanie cez webové rozhranie, alebo priamo pridávaním záznamov do niektorej z podporovaných databáz. Po počiatočnej konfigurácii zariadení je pridanie ďalšieho už iba otázkou skopírovania a vloženia pár ďalších riadkov. Samozrejme aj toto má svoje výhody - Icinga nie je závislá na ďalšej službe, ktorá nemusí byť 100% dostupná.



Obr. 1.: Porovnanie štruktúry - naľavo Icinga, napravo Nagios

Ako je možné vidieť z obrázku vyššie, Nagios používa pre komunikáciu s rozšíreniami množstvo rôznych metód, ako príkazový súbor, vyrovnávaciu pamäť, MySQL databázu, Pipeline a ďalšie. Toto vytvára nesúrodú štruktúru rozšírení, z ktorých každé závisí na inej metóde prístupu k dátam. Vďaka tomu vznikajú problémy s kompatibilitou rozšírení medzi verziami a podobne.

Icinga má na rozdiel od Nagiosu vytvorené API, cez ktoré komunikuje s rozšíreniami a ďalším softwarom. V prípade aktualizácií vďaka tomu neprichádza k toľkým problémom.

Realizácia

Icinga je open source software, s pravidelnými aktualizáciami. Inštalácia prebieha postupne inštalovaním jednotlivých prvkov systému a to:

1. Icinga – samotný monitorovací software
2. IDO2DB – rozhranie medzi Icingou a MySQL
3. MySQL – databáza, ktorá slúži na uchovávanie informácií o zariadeniach (ich momentálneho stavu a stavu služieb na nich bežiacich)
4. Apache – web server poskytujúci webové rozhranie[2]
5. PHP – PHP interpreter pre webové rozhranie
6. *Python – Niektoré zo skriptov, ktoré Icinga používa sú napísané v Pythone*[3]
7. *Perl – Niektoré z zo skriptov, ktoré Icinga používa sú napísané v Perle*
8. Icinga-web – Moderné webové rozhranie
9. *Icinga-mobile – Rozhranie pre chytré telefóny s OS Android, Windows, alebo Apple IOS*

Po nainštalovaní jednotlivých komponentov je potrebné pristúpiť ku konfigurácii softwaru. Prvotne je potrebné vytvoriť databázu pre Icingu a webové rozhranie. Následne nainštalovať databázovú štruktúru, vytvoriť používateľské kontá pre NMS a pre prístup k databázam. Potom je potrebné nakonfigurovať Icingu tak, aby používala ako backend IDO2DB a Mysql. Po spustení softwaru a webového servra je rozhranie softwaru prístupné cez webový prehliadač.

Po overení, že software beží a je dostupný pristúpime ku konfigurácii zoznamu monitorovaných zariadení. Zariadenia je potrebné pridať ručne, Icinga nepodporuje scanovanie siete. Zariadenia môže monitorovať pomocou rôznych nástrojov, cez SNMP, ICMP, TCP, UDP a mnoho ďalších. Po pridaní zariadenia je možné k nemu priradiť služby, ktoré majú byť spolu so zariadením monitorované.

Po konfigurácii zariadení je možné nakonfigurovať užívateľov, skupiny služieb, ktoré spolu súvisia, skupiny zariadení, závislosti a tak ďalej. Možnosti konfigurácie sú nespočetné a je dobré si pred ňou aspoň prebehnúť manuál.

Následne je software potrebné reštartovať, resp. reloadnuť, aby si načítal nové nastavenia a je možné ho používať.

Nižšie je ukážka konfiguračného súboru, v ktorom sú definované zariadenia a služby.

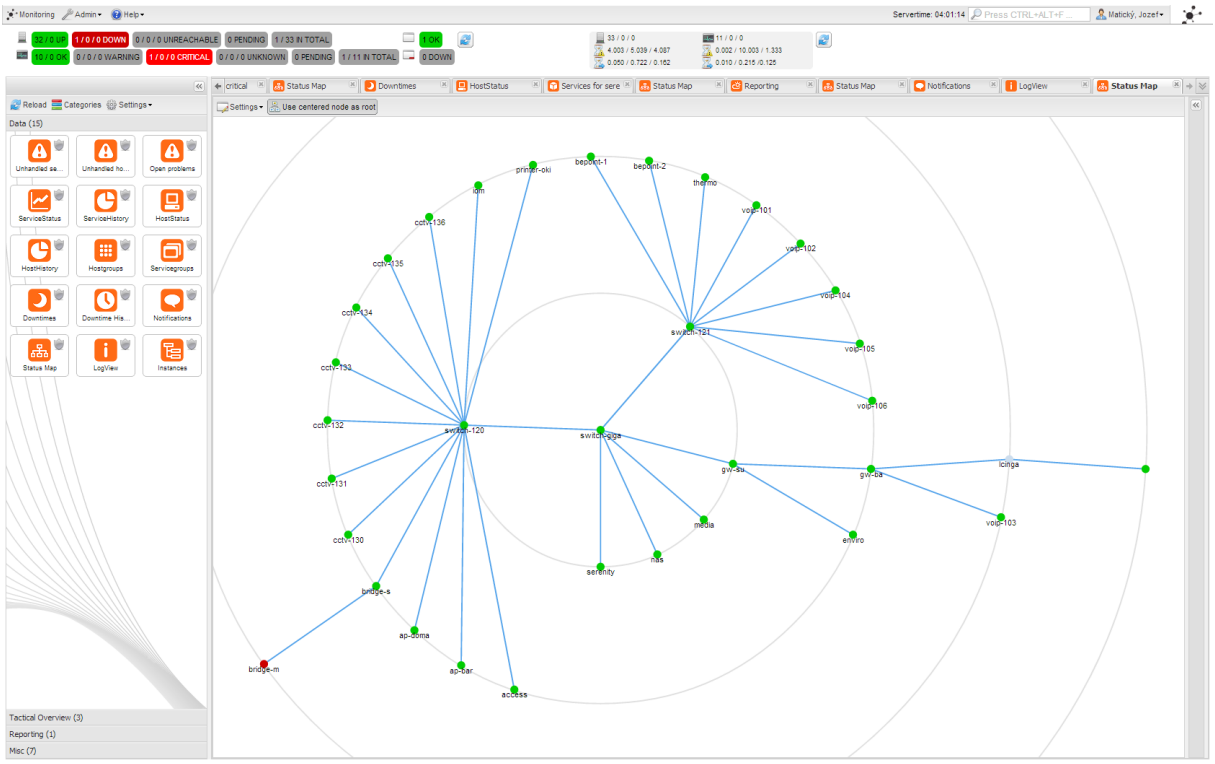
[2] Konfiguráciu Apache a PHP rozoberať nebudem
[3] Prvky vyznačené kurzívou nie sú pre potreby základného monitorovania potrebné

```
define host {
        use                     linux-server
        host_name               serenity
        address                 192.168.0.80
        check_command           check-host-alive
        contact groups          admins
        parents                 switch-giga
}

define service {
        host_name                       serenity
        service description             Apache
        check command                   check http
        max_check_attempts              5
        check_interval                  5
        retry_interval                  3
        check_period                    24x7
        notification interval           30
        notification_period             24x7
        notification_options            w,c,r
        contact_groups                  admins
}
```

Obr. 2.: Ukážka konfigurácie zariadení

Pri používaní softwaru je k dispozícii niekoľko rôznych pohľadov na monitorovanú sieť, ako pohľad na zariadenia, na služby, na skupiny služieb a skupiny zariadení a taktický náhľad na sieť. Pre pohodlné monitorovanie siete je k dispozícii aj sieťová mapa s vyznačením závislostí. Vďaka závislostiam vie Icinga rozšíriť, že v prípade výpadku prepínača ide o poruchu prepínača a nie o poruchu prepínača aj všetkých zariadení za ním.



Obr. 3.: Sieťová mapa v NMS Icinga

Pohľad na skupiny služieb umožňuje monitorovať poskytované služby ako jeden celok. V prípade IP telefónie je možné na jednom mieste monitorovať ako dostupnosť IP telefónov, tak aj dostupnosť telefónnej ústredne a služieb, ktoré poskytuje – SIP, RTSP a podobne. V prípade poruchy ktoréhokoľvek zariadenia, alebo služby je vytvorené upozornenie, že IP telefónia nefunguje správne.

Podobne je možné monitorovať prístup do siete cez WLAN – monitorujeme spolu Radius server, ktorý riadi prístupy za prístupové body a aj samotné prístupové body. V prípade poruchy ktoréhokoľvek komponentu je zjavné, že prístup do siete cez WLAN nefunguje tak, ako má.

Sieťový administrátor má vďaka tomu prehľad, ktoré služby nie sú plne funkčné a dostupné bez zisťovania, ktoré služby sú ovplyvnené výpadkom toho ktorého zariadenia.

Všetky uvedené vlastnosti umožňujú flexibilnejšie reagovať na výpadky na sieti a aj výpadkom predchádzať. To jednak šetrí čas, ale aj prispieva k spokojnosti užívateľov používajúcich počítačovú sieť.

Záver

Icinga, tak ako je tu prezentovaná, je primárne dohľadový software. Pre manažment samotných zariadení by bolo potrebné využiť aj ďalšie programy ako VNC pre prístup k vzdialenej pracovnej ploche počítačov, Putty ako Telnet a SSH terminál a podobne. Osobne si však myslím, že jednoznačnou výhodou spomenutého systému sú takmer žiadne náklady na jeho nasadenie, jeho moderné užívateľské rozhranie, výkonný backend, možnosti rozširovania a pravidelné aktualizácie. Taktiež ďalší spomenutý software je bezplatný a každý administrátor už s ním prišiel do kontaktu a vie ho obsluhovať.

Použitá literatúra

http://en.wikipedia.org/wiki/FCAPS
http://docs.icinga.org/latest/en/
https://www.icinga.org/nagios/architecture/