NMS.SH - Network Monitoring System

Moris Bangoura

Installfest 2011
Silicon Hill

5.3. 2011

Obsah

Proč NMS na SH?

NMS - Network Monitoring System.
Hlavním cílem je monitorování dostupnosti a výkonů veškerých (důležitých) síťových prvků na Strahově.
NMS zajišťuje:

- performance monitoring
- failure, abuse monitoring
- alert msgs delivery

Důležité prvky

Routery/Switche:

- Core: 1x Cisco Catalyst 6509
- Distribution: 10x Cisco 3750
- Access: cca 200x Cisco 2950/2960, Air Ap 1242AG-E-K9

Servery (cca 50x) - CS bl8:

- Linux/BSD servers
- Windows servers
- UPS, KVM, ...

O serveru

- Operační systém: Debian Linux 6.0
- HW: Dell Power Edge, 2x Intel Xeon E5420 (4C), 8 GB RAM
- Řešitelé nms.sh.cvut.cz: Alexander Leonov, Jakub Římek
- Aktuální správce: me :)
- URL: https://nms.sh.cvut.cz/

Outline

Aktuální datový tok

Informace o aktuáním vytížení distribuční částí síťě + WAN

- URL: https://nms.sh.cvut.cz/
- průměrná rychlost z rcv/snd dat za 10s na daném iface GW
- snmpwalk -v2c -c **** gw.sh.cvut.cz IF-MIB::ifOutOctets.port_n
- webové rozhraní: apache2, php5, xml, javascript

Outline

Cacti

PHP frontend pro RRDTool (RoundRobin Db, grafy).

- URL: https://nms.sh.cvut.cz/cacti/graph_view.php
- historie vytížení ifaces síťových prvků Cisco (via SNMP)
- široké množství dalších templates

Outline

Struktura Zabbixu

The Ultimate Open Source Monitoring Solution :-)

- URL: https://nms.sh.cvut.cz/zabbix/
- monitoring via ICMP, SNMP(cisco), zabbix-agenta (servers), IPMI (nepoužíváme)
- zabbix-agent pro všechna OS
- IPv4, IPv6
- flexibilní příst.práva (dle u.sk., R/RW)
- rychlá konf. via templates (items, triggers)

Jak to funguje - templates

Definice hostovských templates:

- items - via SNMP, zabbix-agenta (do Mysql)
- triggers (různé severity, generují msgs): FAN, PSU failure; passwd checksum chng; OS restart; UPC on batt; ...
- graphs (z items uložených hodnot)

Definice hostovských skupin, hostů (discovery), Map (není nagios-like parent-child vstah), Screens.

Jak to funguje - uživatelé

Přístupová práva, uživatelé, notifikace:

- bloková admins (distr., acces daného bloku)
- správci serverů (jen svůj server)
- network admins (core, distribution, wan, main srv.)

DUSPS -> uživatelské účty správců, LDAP -> hesla.

Outline

Syslog

Také ukládáme centrálně na NMS via syslog-ng.

- Zatím jen síťové prvky.
- Zatím neanalyzujeme (abuse monitoring)

Outline

NATdet

Pro zlobivé uživatele SH sítě. . . :)

Future

Vše integrovat do 1 aplikace (grafy, dostupnost, analýza logů)... Zenoss Core (testujeme)?

- Grafy ukládá do RRD.
- Umí analyzovat syslogy a reagovat: port-security violation on portX, count >20 -> send msg...
- only IPv4 :-/

Logy serverů ukládat také centrálně.

Rekapitulace

1. Popis prostředí
2. Přehled řešení
3. NMS...

Q/A

?

Zdroje

- jsou kolem vás. . .

Diskuze

- Postradate nejakou tucnackou technologii, ktera nam na SH chybi?

Diskuze

- KVM?
- docmgr
- SHare