

ZenOSS nadzorni softver

Andrej Brkić i Dinko
Korunić: ZenOSS i SNMP radionica

SNMP uvod

- SNMP - Simple Network Management Protocol
 - ne samo protokol, već kompletno okruženje
 - set tehnologija za nadzor i upravljanje TCP/IP uređajima
 - jednostavan za implementaciju u uređajima
 - protokol - vrlo jednostavan, TCP/IP aplikacijski
- dizajn orijentiran prema samim informacijama
 - zbog raznoraznih tipova i namjene uređaja
 - čitaju/pišu se varijable (objekti), a ne šalju se naredbe
- niz inačica: v1, v2, v3
- SNMPv1 - RFC1157
 - tipično se danas koristi
 - definira SMI, MIB i protokol
 - sigurnost?! - autentikacija kroz community string!

SNMP uvod (2)

- SNMPsec
 - ekstenzija na v1 koja nije nikad javno prihvaćena
- SNMPv2 - RFC1441-1452
 - definira SMIv2
 - gužva i zbrka od različitih verzija protokola...
 - SNMPv2p - originalni protokol
 - SNMPv1.5 - v2p sa community string autentikacijom
 - SNMPv2c - bazično SNMPv1.5
 - SNMPv2u - korisnička imena umjesto communityja
 - SNMPv2* - kombinacija v2p i v2u
- SNMPv3
 - integritet poruka, autentikacija, enkripcija
 - nadogradnja na SNMPv2 protokol, puni standard

SNMP MIB i SMI

- skup objekata = MIB (Management Information Base)
 - SNMPv1 - definirao MIB za cijeli SNMP
 - danas proizvođači izdaju MIB module za pojedine uređaje ili klase uređaja - veća fleksibilnost
 - Ethernet MIB, Token Ring MIB, Cisco MIB, HP MIB, itd.
 - definira što su same varijable/objekti
- problem prezentacije informacija na različit način
 - nužna konzistencija i univerzalnost prezentacije
- SMI (Structure of Management Information) standard
 - precizno definira pravila konstruiranja MIB objekata i modula, njihovo opisivanje i međusobnu hijerarhiju
 - MIB objekti su definirani kroz DDL ISO ASN.1 standard
- instance objekata = OID (Object Identifier)
 - jedinstveno određen objekt

SNMP tipična situacija

- scenarij:
 - nadzorni sustav (jedno ili više računala) redovno obavlja poll odnosno očitava vrijednosti (GET)
 - nadzirani uređaji po nekom događaju šalju informacije (TRAP)
- komponente:
 - slave - upravljani uređaj (usmjernik, preklopnik, IP kamera, itd.)
 - agent - SNMP softver na upravljanom uređaju
 - master - sustav za upravljanje (NMS)
 - proxy - prosljeđuje SNMP upite i odgovore
- komunikacija:
 - unidirekcionalna: read-only
 - bidirekcionalna: read-write

SNMP Unix servis

- Net-SNMP servis + alati:

- SNMP v1, v2c, v3

- snmpwalk - alat za testiranje/dohvat:

```
snmpwalk -v1 -c public 192.168.1.1 system
```

- SNMP v1 r/o zenoss123 community:

```
com2sec readonly default zenoss123
```

- brzina ifova ne odgovara stvarnim

```
interface eth0 6 1000000000
```

```
interface eth1 6 1000000000
```

- instalacija - promijeniti /etc/default/snmpd da sluša i javna sučelja:

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p
```

```
/var/run/snmpd.pid'
```

SNMP Windows servis

- Windows komponenta
- Net-Informant
- WMI

SNMPv1 na Cisco usmjernicima

- uobičajeni početak konfiguracije:

```
zen-2811#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

- *za SNMP pristup*

```
zen-2811(config)#snmp-server community zenoss123 RO
```

- *za SNMP TRAPove*

```
zen-2811(config)#snmp-server host 172.16.1.1 public
```

- kraj

```
zen-2811(config)#end
```

```
zen-2811#
```

ZenOSS općenito

- OSS NMS, napisan u Pythonu
- čemu služi:
 - nadzor poslužitelja, aktivne opreme i ostalih SNMP-enabled uređaja
 - podržava nadzor kroz WMI i SSH
- omogućava:
 - nadzor mrežnih uređaja
 - nadzor mrežnih servisa (HTTP, FTP, POP3, itd.)
 - vremensko praćenje resursa i performansi uređaja
 - Windows Management Instrumentation praćenje
 - autodiscovery uređaja
 - praćenje promjena na uređajima

ZenOSS općenito (2)

- ZenOSS SNMP podržanost:
 - v1, v2c, v3
- ZenOSS arhitektura/komponente:
 - korisnički sloj: Web App / Reports
 - podatkovni: ZenModel, ZenEvents, ZenRRD
 - procesni: ZenHub, ZenActions, ZenJobs
 - skupljački: Discovery, Performance, Availability, Events
- modularna izvedba:
 - ZenPacks, Nagios pluginovi, ...
- tehnologije u pozadini:
 - Zope, Python, Twisted
 - Net-SNMP, RRDtool
 - MySQL

ZenOSS najvažnije komponente

- ZenRRD
 - podaci o performansama
 - RRD datoteke kao baza
- ZenModel
 - konfiguracijski model
 - sadrži sve uređaje, komponente, grupe, lokacije
 - ZEO kao baza
- ZenEvents
 - povijest bolesti
 - MySQL kao baza

ZenOSS sučelje

The screenshot displays the ZenOSS Core web interface. At the top left, the logo 'ZenOSS Core' is visible. On the top right, there is a search bar for 'Device/IP Search' and navigation links for 'admin', 'Preferences', 'Logout', and 'Help'. The server time is shown as 'Zenoss server time: 16:04:29'.

The interface is divided into several sections:

- Main Views:** Dashboard, Event Console, Device List, Network Map.
- Classes:** Events, Devices, Services, Processes, Products.
- Browse By:** Systems, Groups, Locations, Networks, Reports.
- Management:** Add Device, MIBs, Collectors, Settings, Event Manager.

The main content area contains three panels:

- Zenoss Issues:** A table with columns 'Device', 'Daemon', and 'Seconds'. It displays 'No records found.'
- Device Issues:** A table with columns 'Device' and 'Events'. It lists three devices with their respective event counts:

| Device | Events |
|-------------|--------|
| sw402south2 | 1 |
| sw402crtb2 | 1 |
| cisco01 | 1 |
- Object Watch List:** A table with columns 'Object' and 'Events'. It lists various object paths and their event counts:

| Object | Events |
|--------------------------|--------|
| /Devices/Network/Switch | 3 |
| /Devices/Server/Linux | 3 |
| /Devices/Network/Router | 0 |
| /Devices/Network/Printer | 0 |
| /Devices/Network/WiFi | 0 |
| /Devices/Server/Windows | 0 |
| /Devices/Ping | 0 |

ZenOSS demonstracija

- instalacija ZenOSS
- inicijalna konfiguracija
- dodavanje aktivnih uređaja u ZenOSS
- snmpd.conf na Linux poslužiteljima i fino podešavanje (brzine, itd.)
- dodavanje Linux poslužitelja u ZenOSS
- remote syslog kroz ZenOSS
- prihvati SNMP TRAP-ova
- dodavanje MIB-ova
- napredno:
 - izvršavanje eksternih skripti kroz SNMP
 - WMI na Windows poslužiteljima
 - transform skripte

ZenOSS savjeti, praksa

- zahtjevi:
 - potrošnja memorije, cpu, disk
- optimiranje, čišćenje:
 - Zope baza i zeopack
 - zec datoteke
- dodatna sigurnost:
 - SSL redirekcija kroz Apache
- napredno:
 - filteri (bad OID)
 - transformovi