SNMP

je protokol, který umožňuje průběžný sběr nejrůznějších dat pro potřeby správy sítě a jejich následné vyhodnocován. Na tomto protokolu je dnes založena většina prostředků a nástrojů pro správu sítě.

Typickými úlohami pro SNMP protokol jsou:

- zjišťoavání stavových informací o zařízeních (množství volné paměti, počet spojení, počet přihlášených uživatelů, ...)
- nastavování parametrů (atributů) na síťových prvcích
- Monitorování uptimu
- Monitorování verzí běžících systémů
- Sběr dat o existujících síťových rozhraních(ifName, ifDescr, ifSpeed, ifType, ifPhysAddr)
- Measuring network interface throughput (ifInOctets, ifOutOctets)
- Dotazování ARP (ipNetToMedia)

Protokol je nyní ve verzi 3.0. Současní klienti nejčastěji podporují všechny tři verze. Od verze 2.0 je do protokolu začleněna podpora autentizace, od 3.0 navíc i šifrování (DES).

Protokol rozlišuje mezi monitorovanou stranou (dohledávaný systém) a monitorovací stranou (sběrna dat). Tyto strany mohou běžet buď odděleně na různých fyzických strojích, nebo v rámci jednoho stroje.

Na monitorované straně je spuštěn agent a na straně monitorovací manager. Monitorovací strana pak shromažďuje informace o stavu systému. Manager vznáší požadavky agentovi, který pak zajišťuje realizaci vhodných reakcí. Získaný obsah správ se pak může různě zpracovávat (grafy, tabulky).
Je možné také agenta nakonfigurovat tak, aby automaticky zasílá informace při výskytu výjimečné události (trap), jako je výpadek větráku, překročení mezních údajů, objevení nového zařízení a další, managerovi, který je odchytává a dále zpracovává.

SNMP typicky běží na portu 161 pro agenty a 162 pro management.

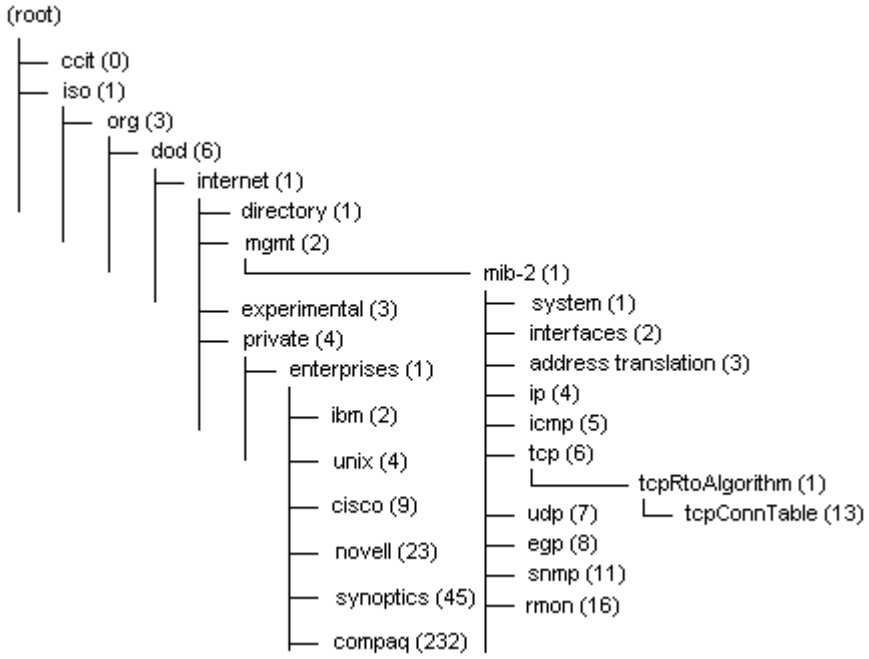
SNMP ve verzích 1 a 2 používá následující příkazy:

- **get-request** -získání informace z MIB (management information base)
- **get-next-request** - umožňuje managerovi získat informace o objektech v MIB bez znalosti jejich přesných jmen, umožňuje postupné procházení celým hierarchickým stromem;
- **set-request** - změna hodnoty proměnné agenta;
- **trap** - jediný typ příkazu vysílaný bez předchozího vyžádání, agent jej zasílá managerovi jako reakci na specifikovanou událost, zpráva zůstává nepotvrzená, proto agent nemá jistotu, zda byla doručena;
- **get-response** - agent vykoná tuto operaci jako reakci na předchozí příkazy - je to vlastně odpověď agenta managerovi. Odpověď obsahuje i dotaz, protože protokol nezajišťuje souvislost mezi dotazem a odpovědí.
- **get-bulk** - operace, která je součástí SNMP v.2. Umožňuje vyžádat si k přečtení celou skupinu informací z MIB, čímž se mnohdy urychluje komunikace.
- **inform** - umožňuje komunikaci dvou managerů mezi sebou.

MIB databáze

MIB (Management Information Base) je databáze, která dovoluje jednoznačně identifikovat informace využívané systémem správy. Aby mohl SNMP manager i agent tyto informace získat a předávat, tak je nutná znalost struktury MIB.

Báze dat je objektově orientovaná. Data jsou uložena jako objekty a sdružují se do tříd. Jednotlivé objekty mají hodnoty. Každý řízený objekt v MIB obsahuje veškeré informace potřebné pro popis. Způsob pojmenování objektů je založen na jejich vztahu. Jeden objekt může obsahovat jiné objekty nebo jiné třídy. MIB je tedy tvořena jedním stromem.



Každý agent by měl udržovat objekty standardní MIB (např. síťové adresy, typy rozhraní, čítače). Jsou definovány tři mechanismy pro přidání:

- přidání nových objektů prostřednictvím definice nové verze MIB-II;
- přidání nestandardních objektů přidáním experimentální větve;
- přidání vlastních objektů v rámci podstromu soukromé větve.

Do MIB byly zařazeny jen nejnutnější objekty. Předem byly vyloučeny objekty svým způsobem nadbytečné, např. ty, které mají konkrétní (např. aritmetické) vztahy s jinými objekty v MIB. Jednoduchost definice a omezená velikost báze umožňuje zaručit minimální dopad na činnost a složitost agentů. To se pak samozřejmě projeví v nárocích na zpracovatelský systém.

Dnes lze nalézt spoustu existujících a v praxi používaných systémů, které pracují 24 hodin denně, 7 dní v týdnu, 365 dnů v roce monitorují stav systémů a služeb v počítačové síti. V případě výpadku informují definovanými kanály (nejčastěji email, SMS, vizuální výstraha) příslušnou obsluhu, popř. spustí definovanou akci.

Díky podpoře SNMP není problém realizovat systém pro sběr informací z agentů, kteří SNMP podporují, a sestavit tak konkrétní aplikaci, která se bude chovat podle našich požadavků. Následně pak lze realizovat skutečně velmi jednoduše systém, který bude příslušná data zpřístupňovat na WWW stránkách. Navíc získáme možnost testování a monitorování řízeného systému třetí stranou.

SNMP packet

verze community string PDU typ ID dotazu error status error ID OID hodnota

SNMP prakticky

Standardním balíkem pro práci s protokolem SNMP je v linuxových systémech Net-SNMP, který obsahuje nástroje pro práci se SNMP i příslušné démony.

Nejzákladnější konfigurace bezpečnosti se provádí pomocí rouser/rwuser resp. rocommunity/rwcommunity. Můžete jednoduše specifikovat, které community řetězce a kteří uživatelé mohou přistupovat do jakých částí stromu. Typicky se může použít například nastavení, které povolí přístup pouze pro čtení pro celou MIB databázi ze sítě 10.10.10.0 s community řetězcem "tajnyklic":

rocommunity tajnyklic 10.10.10.0/24

Je nutné si uvědomit, že toto není zrovna nejbezpečnější nastavení pro zápisy (vzdálenou konfiguraci), tudíž lze tento přístup doporučit jen pro read-only přístup, tedy jednoduchý monitoring. Pokud si ani nechcete pamatovat tajný klíč, použijte "public", což je implicitní klíč, který klienty obvykle předpokládají.

Protokol SNMPv3 přidal pokročilejší podporu pro autentifikaci i autorizaci. Ke konfiguraci se pak použijí spíše nové příkazy com2sec, group, view a access.

Nástroje:

- snmptranslate: překládá MIB adresy
- snmpget: vyžadá konkrétní data od agenta
- snmpgetnext: Vrací totéž, jako snmpget, ale o OID dál (tj. následující údaj
- snmpwalk:zřetězuje volání snmpgetnext - vrací výpis stromu. Pozor, může vrátit hodně dat.
- snmptable: formátuje data do tabulky -což je jejich přirozenější podoba
- snmpset:zapíše konkrétní data
- snmpbulkget: komunikuje pomocí SNMP GETBULK se síťovým zařízením
- snmpbulkwalk: získá podstrom MIB informací pomocí SNMP GETBULK
- snmptrap:Umí odesílat TRAP signál. Tento příkaz je příkaz agenta, nikoli správce. Tento signál musíme ještě zachytit

Démoni:

snmpd

Démon snmpd je praktickou ukázkou agenta, který běží v operačním systému. Typicky poskytuje odpovědi na dotazy týkající se stroje, na kterém běží, může ale také fungovat jako proxy agent, tj agent, který zapouzdřuje informace od jiných zařízení či agetnů. Umí zaslat TRAP zprávu.

snmptrapd

Příjem TRAP signálů zachycuje snmptrapd démon.

MRTG

Multi Router Traffic Grapher - http://oss.oetiker.ch/mrtg/ se používá v případech, kdy nás zajímá kolik na daném zařízení proteče dat. Tento program dělá to, že po nastaveném intervalu kontaktuje router a zapisuje si stav protčených dat. MRTG zjišťuje počet přetečených dat a generuje výstup. K tomu využívá protokolu SNMP (Simple Network Management Protocol) jehož pomocí jsou tyto data poskytována. K instalaci je nutné tedy zprovoznit SNMP démona port 161.

Konfigurace SNMP neni tak složitá, provádí se v `/etc/snmp/snmp.conf`, je jen třeba si uvědomit, zda budou informace poskytovány **public** nebo jen **privat** přesně se tomu říka komunita.

```
 ####
# First, map the community name "public" into a "security name"

#       sec.name  source          community
com2sec domena    default         public

####
# Second, map the security name into a group name:

#       groupName      securityModel securityName
group   domenaGroup v1          domena
group   domenaGroup v2c         domena

####
# Third, create a view for us to let the group have rights to:

#       name           incl/excl     subtree         mask(optional)
#view    systemview     included      system
view all    included  .1                              80

# Finally, grant the group read-only access to the systemview view.

#       group          context sec.model sec.level prefix read   write notif
#access  notConfigGroup ""      any       noauth    exact  systemview none none
access domenaGroup ""      any       noauth    exact      all           all
none
access domenaGroup ""      any       noauth    exact      system        none
none
...
```

Instalace je možná buď z distribučních balíků, nebo přímo ze zdrojových kódů výrobce. Po nainstalování programem cfgmaker vytvoříme konfigurační soubor, který obsahuje jednotliva zařízení i se stručným popisem např. eth0, eth1. Dále je nutno nastavit proměnnou workdir, to je adresář do kterého se budou ukládat jak logy, tak png grafy a i samotný vygenerovaný ns.domena.cz_2.html soubor.

```
# WorkDir: /home/http/mrtg
```

Na závěr necháme v cronu spouštět program mrtg, který nám bude generovat grafy.

```
*/5 * * * * exec /usr/local/mrtg-2/bin/mrtg domena.cfg 2>&1 /dev/null
```

Graf je rozdělen na čtyři části. A to na denní, týdenní, měsíční a roční.

Podobným programem je IPAC. Tento program plní obdobnou funkci, ale neumí získávat informace o routeru na vzdálených zařízeních. Zato jeho grafy informují o přenosu jednotlivých služeb např. www, ftp, dns atd. O tomto programu si můžeme popovídat zase příště.

NAGIOS

je framework pro sledování a správu služeb a sítě. Autorem je Ethan Galstad. Nagios je trochu náročnější na konfiguraci, ale zato umožňuje velice přesně definovat požadované chování kontroly, závislostí, způsobu reakce na různé stavy. Nagios neumí sám o sobě kontrolovat žádné služby ani oznamovat změny stavů. Kontrola stavu služby se dělá pomocí pluginů, což je v podstatě libovolný spustitelný soubor, kterému se přes argumenty příkazové řádky předávají parametry kontroly a podle návratové hodnoty se vyhodnocuje, jestli je služba funkční, v kritickém stavu, nebo nefunkční. Oznámení o nevhodném stavu služby se děje pomocí volání externího programu, kterému se opět přes argumenty příkazové řádky předávají informace o způsobu oznámení.

Program je možné ovládat prostřednictvím webového rozhraní sadou CGI skriptů. Přes toto rozhraní jsou také přístupné grafy dostupnosti služeb a trend jejích chování, historii stavů služeb a další. Nagios je také možné přes toto rozhraní částečně konfigurovat, což je alternativa k ručnímu editování konfiguráků.

Zdroje:

SNMP

- The NET-SNMP Project Home Page
- Network Management & Monitoring with Linux
- SNMP protokol a jeho využití

MRTG

- MRTG Home Page
- Kolik dat tudy teče?
- MRTG - grafické prehľady

Nagios

- Nagios Home Page

http://www.fi.muni.cz/~kas/p090/referaty/