

PA159 – Správa sítě

6. 11. 2009

Správa sítě (Network Management)

- **Obecné principy**
 - Sledování (monitoring) jednotlivých prvků a případně jejich kombinací
 - Analýza získaných výsledků (průběžná, periodická, na vyžádání)
 - Reaktivní řízení (správa)
 - Proaktivní řízení (správa)

Počátky

- 27. 10. 1980: První skutečné zhroucení sítě
 - Popsáno v RFC 789
 - Včetně popisu kroků pro nápravu
- Další zkušenosti získávány na podobných případech
 - Např. „červ“ z roku 1988
- Závěr: jsou nezbytné procesy a nástroje sledování a správy sítě (anglicky *Monitoring a Management*)

Co sledovat

- Základní prvky infrastruktury
 - síťová rozhraní
 - aktivní i pasivní prvky (servery, směrovače, ...)
 - fyzické spoje (linky)
- Provoz: detekce slabých (přetížených) míst
- Směrovací informace
- Dodržení SLA (Service Level Agreement)
- Podezřelé chování (vzory, detekce útoku)

ISO model správy sítě

- Správa výkonu (performance management)
- Správa chyb
- Správa konfigurací
- Správa účetnictví (bookkeeping)
- Správa bezpečnosti

Správa výkonu

- Výkon sítě v nejširším slova smyslu
- Sleduje jak jednotlivé komponenty, tak i komplexní objekty (např. end to end cesta)
- Základ v SNMP (Simple Network Monitoring Protocol, RFC 2570)

Správa chyb

- Záznam, detekce a náprava chybových stavů
- Oproti správě výkonu spíše zaměřen na okamžité problémy
- Rovněž postaven na SNMP

Správa konfigurací

- Co je na síti, resp. z čeho se síť skládá (co mám sledovat)
- Údržba konkrétních konfigurací
- Snadná distribuce změn konfigurací (konfigurace z minulého pátku)

Správa účetnictví (Accounting management)

- Detekce, záznam a správa uživatelů (uživatelů monitoringu, nikoliv obecně sítě)
- Přístup k zařízením
- Správa jednotlivých uživatelských účtů (zřízení, modifikace, . . .)
- Přirozenou součástí jsou i procesy spojené se skutečným *účtováním za služby*

Bezpečnostní správa

- Zajištění nebo odmítnutí přístupu dle definovaných vlastností
- Autorizace
- Ochrana prvků
 - Distribuce klíčů
 - Firewally

Ne-stručná definice

Správa sítě zahrnuje zavádění, integraci a koordinaci technických, programových a lidských zdrojů, zajišťujících sledování, testy, dotazování, konfiguraci, analýzu, vyhodnocování a řízení sítě a jejích prvků s cílem zajistit požadavky real-time, provozního výkonu a kvality služeb za uspokojivou cenu.

Základní architektura

- Správce (řídící entita)
 - Typicky aplikace + člověk
 - Centralizovaná (interface pro správce/člověka)
- Spravované (řízené) zařízení
- Protokol správy sítě

Spravované zařízení

- Příklad: směrovač, hub, přepínač, modem, tiskárna
- Může být tvořeno více *objekty*
 - Směrovač: Síťové karty
Konkrétní konfigurace směrovacího protokolu
- MIB (Management Information Base)
 - Identifikace zařízení
 - Informace o stavu zařízení
- Agent správy sítě (network management agent)
 - Lokální proces s lokální působností (čte data, modifikuje konfiguraci, ...)

Protokol správy sítě

- Zajišťuje komunikaci mezi správcem a spravovanými zařízeními/objekty
- Zajišťuje oboustrannou komunikaci
 - Příkazy agentům
 - Předávání monitorovacích dat
 - Předávání událostí
 - ...

Standardy

- OSI CMISE/CMIP (the Common Management Service Element/Common Management Information Protocol)
- SNMP (Simple Network Management Protocol)
- Oba navrženy jako nezávislé na zařízení/výrobci
- SNMP dnes nejrozšířenější protokol správy sítě

SNMP

- Původně: Simple Gateway Monitoring Protocol, SGMP (RFC 1028)
- SNMPv1 v roce 1993
- aktuální SNMPv3 (1999)

SNMP – základy

- Definice objektů (MIB objektu)
 - Příklady
 - * Čítač počtu datagramů
 - * Verze použitého směrovacího protokolu
 - * Stavová informace
 - Společné informace sdruženy do MIB modulů

SNMP – Jazyk

- Jazyk pro definici dat: Structure of Management Information, SMI
 - Datové typy
 - Objektový model
 - Pravidla pro práci s informacemi (nezbytnými pro správu sítě)
- Specifikace MIB používá tento jazyk

SNMP – protokol a bezpečnost

- Vlastní monitorovací protokol (the SNMP)
 - Doprava informací
- Administrace a zajištění (bezpečnost)
 - Hlavní rozdíl mezi verzí 2 a 3

SMI

- Structure of management information
- Definice v RFC 2578, 2579, 2580
- Vychází z ASN.1 (ISO 1987, ISO X.680, 1998)
- 11 základních datových typů
 - Možno konstruovat „tabulky“ užitím konstruktoru SEQUENCE OF

SMI – základní typy

Integer

Counter32

Integer32

Counter64

Unsigned32

Gauge32

OCTET STRING

TimeTicks (1/100s)

OBJECT IDENTIFIER
Opaque

IPAddress

- Octet string je max 65KB dlouhý, ASN.1 řetězec
- Opaque je neinterpretovaný objekt, pro zpětnou kompatibilitu

SMI – identifikace objektu

- U spravovaného objektu definuje
 - Typ
 - Status
 - Sémantiku
- Cca 10 000 objektů popsáno v různých RFC

Příklad objektu

ipInDelivers OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

„The total number of input datagrams successfully delivered to IP user-protocols (including ICMP)“

::= { ip 9 }

MODULE-IDENTITY

- Speciální objekt
- Sdružuje konkrétní spravované objekty
- Základní pole
 - DESCRIPTION
 - REVISION
 - NOTIFICATION-TYPE
 - MODULE-COMPLIANCE
 - AGENT-CAPABILITIES

MIB

- Management Information Base
- Aktivita ISO (International Standards Organization)
- Syntax: A.B.C.D....
- Hierarchická struktura popisu
 - 1. Nejvyšší úroveň, odpovídá ISO
 - 1.2.840 USE
 - 1.2.840.113556.4.2 Microsoft
 - 1.3 Sítě

MIB – struktura

- Hierarchie sítí:
 - 1.3.1.6.1 Internet
 - 1.3.1.6.1.4 private: jména registrovaných organizací (přiděluje IANA)
 - 1.3.1.6.1.2 management
 - 1.3.1.6.1.2.1 MIB ve verzi 2 (MIB-2)
 - * Prefix standardních modulů

MIB – standardní moduly

- RFC 2400
- Prefix vždy 1.3.1.6.1.2.1
- Příklady:
 - (1.3.1.6.1.2.1.)1 system
 - 2 interface
 - 4 ip
 - 7 udp
 - 11 snmp

MIB – příklady objektů

- 1.3.1.6.1.2.1.1 sysDescr jména a verze OS, ...
- 1.3.1.6.1.2.1.2 sysObjetID ID objektu (určí výrobce)
- 1.3.1.6.1.2.1.3 sysUpTime doba (v 1/100 s)
- 1.3.1.6.1.2.1.5 sysName administrativní jméno
- 1.3.1.6.1.2.1.6 sysLocation Fyzické umístění
- 1.3.1.6.1.2.1.7 sysServices definuje služby (int32)

MIB – UDP objekty

- 1.3.1.6.1.2.1.7.1 udpInDatagrams
- 1.3.1.6.1.2.1.7.2 udpNoPorts počet datagramů, kterým chyběla aplikace (nebyl aktivní port)
- 1.3.1.6.1.2.1.7.3 udpInErrors
- 1.3.1.6.1.2.1.7.4 udpOutDatagrams

Role protokolu SNMPv2

- Přenos MIB informací mezi řídicími agenty a řízenými objekty
- Módy
 - Požadavek – odpověď
 - Událost (trap)

Požadavek a odpověď

- Řídící entita vydá požadavek
- ten je přenesen k agentovi dotazované (řízené) entity
- Řízená entita požadavek splní a pošle odpověď
 - Pošli hodnotu konkrétního objektu: odpovědí hodnota
 - Nastav hodnotu: odpovědí úspěch a/nebo cílový stav

Směrování dat

- Zpravidla komunikuje řízená a řídicí entita přímo
 - agent2manager nebo manager2agent
- SNMP podporuje i postupné předávání informací
 - Např. přes několik administrativních domén
 - V případě přímé nedostupnosti
 - Mezistupeň přes druhého managera (možné řetězení): manager2manager

Typy událostí

GetRequest	manager2agent
GetNextRequest	manager2agent
GetBulkRequest	manager2agent
InformRequest	manager2manager
SetRequest	manager2agent
Response	manager2manager agent2manager
SNMPv2-Trap	

Formát PDU

- PDU = Protocol Data Unit
 - Protokolem přenášená „skutečná“ data (payload)

- Typ 0–3:

Type	Request	Error	Error	Name	Value	Name	Value	...
	ID	status	index					

- Typ 4 (trap)

Type	Enterprise	Aent	Trap	Spec.	Time	Name	Value	...
		Add	Type	Code	stamp			

SNMP architektura

- SNMP aplikace (řídící entita)
 - Generátor příkazu (command generator)
 - Příjemce upozornění (notification receiver)
 - „Směrovač“ (proxy forwarder)
- Agent
 - Systém odpovídání na dotazy (command responder)
 - Generátor upozornění (notification responder)

SNMPv3 a bezpečnost

- Starší verze v podstatě bezpečnost ignorovaly
 - Heslo se volně šířilo sítí, nebylo jak tento fakt ovlivnit
- SNMPv3 – user based security (RFC 2574)
 - Uživatelské jméno
 - s ním spojené heslo, hodnota klíče, přístupová práva

Použitelné v „běžné“ síti, s rizikem odposlechu

SNMPv3 – základní rysy

- Šifrování zpráv
 - DES CBC
- Autentizace
 - HMAC (Hashed Message Authentication Codes)
 - RFC 2104
 - * Spočte Message Integrity Code $MIC(m,k)$, kde m je zpráva a k je sdílený klíč
 - * Pošle zprávu a $MIC(m,k)$
 - * Používá MD5 pro MIC

ASN.1

- Abstract Syntax Notation One
- Data Description Language
- Transfer dat mezi různými architekturami
- Basic Encoding Rules (BER), v poslední době jako Packet Encoding Rules (PER)
 - Zasílání dat přes síť (jak přenášené informace kódovat)
 - TLV (Type, Length, Value)
- Široce rozšířené (dostupné pro většinu OS a jazyků)
- Další informace: <http://asn1.elibel.tm.fr/>,
<http://www.obj-sys.com/asn1tutorial>

ASN.1 – přiřazení typu

```
InventoryList 1 2 0 0 6 1 DEFINITIONS ::=
  BEGIN {
    ItemId ::= SEQUENCE {
      partnumber IAString,
      quantity INTEGER,
      wholesaleprice REAL,
      saleprice REAL    }
    StoreLocation ::= ENUMERATED {
      Baltimore (0),
      Philadelphia (1),
      Washington (2)    }
  } END
```

ASN.1 – přiřazení hodnot

```
gadget  ItemId ::=
{
  partnumber      ,,7685B2'',
  quantity        73,
  wholesaleprice  13.50,
  saleprice       24.95
}
```