Mittuniversitetet
MID SWEDEN UNIVERSITY

Laboration:
Simple Network Monitoring Protocol

Lennart Franked*

lab1.tex 950 2013-04-18 19:15:40Z lenfra

Innehåll

1 Introduktion **1**

2 Syfte **1**

3 Läsanvisningar **2**

4 Genomförande **2**
4.1 Installation av SNMP 2
4.2 Användning av SNMP 2

5 Examination **3**

1 Introduktion

I denna laboration ska vi gå in på några olika metoder kring hur man kan samla in data. Det vi främst kommer att undersöka i denna laboration är datainsamling med Simple Network Monitoring Protocol (SNMP).

2 Syfte

Syftet med denna laboration är att:

- Att ge dig en översiktlig bild över Simple Network Monitoring Protocol (SNMP), Structure of Management Information (SMI) och Management Information Base (MIB).
- Att känna till olika tekniker som används för att samla in data i ett switchat nätverk.
- Att installera och konfigurera en SNMP-agent.

3 Läsanvisningar

Du ska först läsa kapitel 3 till och med kapitel 6 i [12] därefter läser ni följande [2], [4].

Slutligen läser ni översiktligt följande RFC:er: [11], [3], [9], [8], [13], [6], [7], [10].

4 Genomförande

Observera att anvisningarna nedan är skrivna för Ubuntu/Linux, väljer ni att använda något annat system får ni anpassa instruktionerna därefter.

4.1 Installation av SNMP

Börja med att installera en SNMP-server, exempelvis Net-SNMP [1]. Ni kan med fördel använd den officiella dokumentationen till hjälp vid installationen. För denna laboration går det utmärkt att använda version 2c av SNMP och vi kommer att kolla på version 3 senare. Kom ihåg att kolla vilka beroenden (eng. *dependencies*) som krävs (Python, Perl) vid installationen.

Nästa steg blir nu att konfigurera er SNMP-server, vilket enklast kan göras med hjälp utav `snmpconf(1)` om ni använder er utav Net-SNMP. De konfigurationsfiler ni måste skapa är `snmpd.conf` vilket är agentens konfiguration, samt `snmp.conf` vilket är SNMP-klientens konfiguration. Ni kan senare under projektet experimentera med exempelvis traps och andra funktioner som SNMP har.

I `snmpd.conf` måste följande konfigureras:

- Community sträng för SNMPv2c, en för read-only och en för read-write.
- System information.

I `snmp.conf` kan ni sätta *default community* till det ni satte för er SNMP-agent, på så sätt behöver ni inte fylla i community-strängen varje gång ni ska göra en SNMP-förfrågan mot er nyligt installerade agent. Ange även att den som standard ska använda version 2c av SNMP.

Avsluta `snmpconf(1)` och kopiera `snmp.conf` samt `snmpd.conf` enligt anvisningarna och starta därefter `snmpd(8)` med root-rättigheter.

4.2 Användning av SNMP

Du har nu installerat både en SNMP-agent samt en SNMP-klient och kan nu börja samla in information från agenten med hjälp utav

- `snmpget(1)`,
- `snmpgetnext(1)` samt
- `snmpwalk(1)`.

Testa att din agent är igång genom att exempelvis göra en `snmpwalk(1)` på grenen

`iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1)`

i MIB-trädet. Se Net-SNMP:s officiella dokumentation [1] alternativt manualsidorna för `snmpget(1)` och `snmpwalk(1)` för information om hur ni använder SNMP-klienten.

Om ni vet vilken information ni vill hämta ut från MIB-trädet kan ni använda [5] för att söka efter objekt. Sök exempelvis efter vilket objekt som visar vilken IP-adress er dator har och bekräfta sedan detta genom att göra en `snmpget(1)` på detta OID.

5 Examination

För att examineras på denna laboration ska du lämna in följande:

1. Med hjälp utav SNMP, hämta ut så mycket information du kan om nätverksanvändningen på din dator.
   - Hur många UDP-datagram och TCP-segment har skickats och tagits emot?
   - Hur många korrupta paket har tagits emot samt vilka typer av korrupta paket kan man se?
   - Din dators lager 3-adresser samt lager 2-adresser.
   - Datorns routing- och ARP-tabeller.
   - Vad mer kan du hitta av intresse?
2. Med hjälp utav SNMP, hämta ut så mycket information du kan om ditt system:
   - primärminne,
   - swapminne,
   - CPU-användning,
   - vad mer du kan hitta som du anser vara intressant att veta.
3. Redogör för de olika datatyper som används för att spara informationen i MIB-trädet, samt ge ett exempel på objekt som använder datatypen för respektive datatyp.
4. Med 300-500 ord, beskriv de olika beståndsdelarna i SNMP-protokollet.

I de fall du hämtat information från MIB trädet, ange både objektnamn samt OID till detta objekt. Detta ska lämnas in sammanställt i ett PDF-dokument.

Referenser

[1] Net-SNMP. URL `http://www.net-snmp.org/`. 2013.

[2] Network tap. URL `http://en.wikipedia.org/wiki/Network_tap`. Wiki, 2013.

[3] Case, J.D., Fedor, M., Schoffstall, M.L., och Davin, J. Simple Network Management Protocol (SNMP). RFC 1157 (Historic), maj 1990. URL http://www.ietf.org/rfc/rfc1157.txt.

[4] Cisco. Configuring SPAN and RSPAN. URL http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_55_se/configuration/guide/swspan.html. 2010.

[5] Cisco. SNMP object navigator. URL http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en. 2013.

[6] Claise, B. Cisco Systems NetFlow Services Export Version 9. RFC 3954 (Informational), oktober 2004. URL http://www.ietf.org/rfc/rfc3954.txt.

[7] Claise, B. Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information. RFC 5101 (Proposed Standard), januari 2008. URL http://www.ietf.org/rfc/rfc5101.txt. Obsoleted by RFC 7011.

[8] McCloghrie, K., Perkins, D., och Schoenwaelder, J. Structure of Management Information Version 2 (SMIv2). RFC 2578 (INTERNET STANDARD), april 1999. URL http://www.ietf.org/rfc/rfc2578.txt.

[9] McCloghrie, K. och Rose, M. Management Information Base for Network Management of TCP/IP-based internets:MIB-II. RFC 1213 (INTERNET STANDARD), mars 1991. URL http://www.ietf.org/rfc/rfc1213.txt. Updated by RFCs 2011, 2012, 2013.

[10] Quittek, J., Bryant, S., Claise, B., Aitken, P., och Meyer, J. Information Model for IP Flow Information Export. RFC 5102 (Proposed Standard), januari 2008. URL http://www.ietf.org/rfc/rfc5102.txt. Obsoleted by RFC 7012, updated by RFC 6313.

[11] Rose, M.T. och McCloghrie, K. Structure and identification of management information for TCP/IP-based internets. RFC 1155 (INTERNET STANDARD), maj 1990. URL http://www.ietf.org/rfc/rfc1155.txt.

[12] Subramanian, Mani., Gonsalves, Timothy A., och Usha Rani, N. *Network management : principles and practice*. Dorling Kindersley, Noida, India, 2011. ISBN 978-81-317-3404-9.

[13] Waldbusser, S., Cole, R., Kalbfleisch, C., och Romascanu, D. Introduction to the Remote Monitoring (RMON) Family of MIB Modules. RFC 3577 (Informational), augusti 2003. URL http://www.ietf.org/rfc/rfc3577.txt.