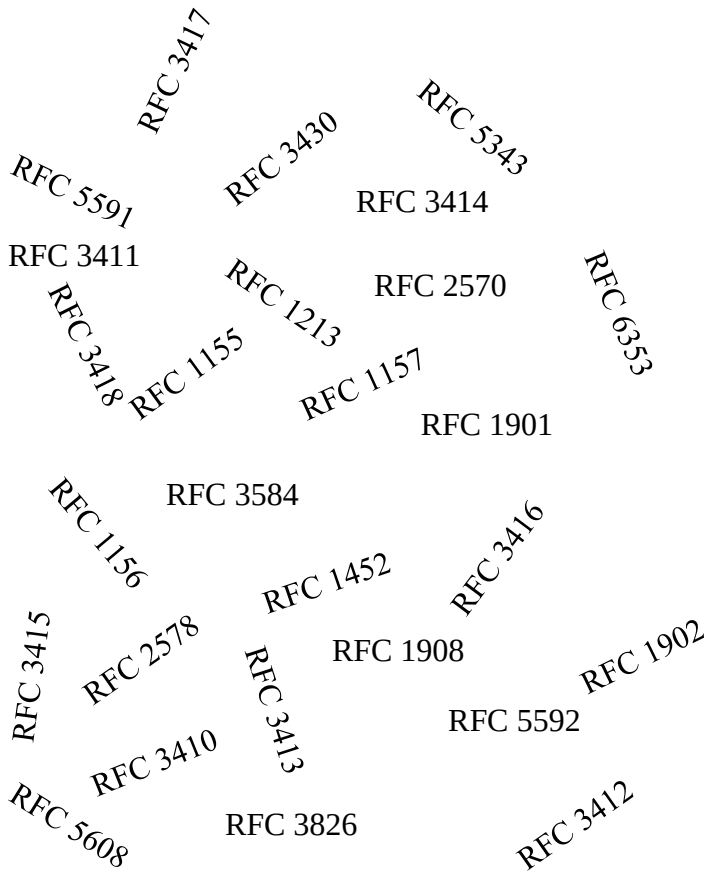
Linnéuniversitetet
Institutionen för datavetenskap, fysik och matematik

Projekt

SNMP



Författare: Andreas Pettersson
Handledare: Marcus Wilhelmsson
Termin: HT12-VT13
Kurskod: 1DV427

Innehåll

1 Inledning

SNMP (Simple Network Management Protocol), är en samling protokoll som används för att managera komplexa nätverk. Enheter i nätverket som har stöd för SNMP använder agenter för att utlämna OID:er (Object identifiers) som innehåller variabler som beskriver enheten och lagrar dem i MIBs (Management Information Bases) för att sedan skicka iväg dem med hjälp av PDUs (Protocol Data units) till enheter som gör SNMP-förfrågningar om att få denna information. [100, 200] Dessa variabler kan vara temperaturen för hårdvara, portstatus, belastning med mera. [200]

Enheter som typiskt har stöd för SNMP innefattar routrar, switchar, servrar, arbetsstationer, skrivare och liknande. Med SNMP kan man även aktivt managera enheter genom att modifiera värderna i de utlämnade variablerna. [200]

Första versionen, ICMPv1, utvecklades under 1980-talet [100] av IETF (Internet Engineering Task Force) och är beskrivet i en rad dokument kallade RFCs (Request for Comments). I dagsläget är det SNMPv3 som är den senaste versionen. [200]

2 Historia

2.1 SNMPv1

De första tre RFC:erna om SNMP, känt som SNMPv1, släpptes 1988. [100] De tog upp strukturen och identifikationen på paketen som hade hand om informationen, hur MIBs skulle se ut samt hur SNMP var tänkt att fungera. Dessa dokument ersattes senare av andra RFCer med samma mål. [200]

SNMPv1, beskriven i RFC 1157, är kritiserad för att sakna starkt skydd. En brist var att en attackerare skulle kunna maskera sig så det ser ut som om attackeraren ser ut att vara en annan legitim användare och på så vis få ut information som ej var ämnat till någon annan. Spoofing kan användas för att få attacken att lyckas. En annan brist var att tredjepart kunde modifiera innehållet i BDU:erna när de skickades i nätverket men ändå få det att se ut som om det är orginalavsändaren som skickat paketet. Andra svagheter var att SNMP var svagt för sniffing, DoS och att helt enkelt en attackerare kunde modifiera BDU:erna så de bad nätverksutrustningen att stänga av sig. [400]

2.2 SNMPv2c

SNMPv2, beskriven i RFC 1441, släpptes 1993. [300] Standardiseringsprocessen resulterade i tre olika standarder som var okampatibla med varandra: SNMPv2 party-based, SNMPv2u och SNMPv2* där de två sistnämna tävlade om att bli den slutgiltiga standarden som resulterade i en kompromiss vid namn SNMPv2c. Säkerheten i SNMPv2c var

visserligen bättre än SNMPv1 men förlitade sig mycket på andra. [400] SNMPv2 har en annan paketuppbyggnad än SNMPv1 och är inte bakåtkompatibelt. Dessutom finns det två nya pakettyper som inte var definierade i första versionen. [200]

3 SNMPv3

SNMPv3, beskriven i RFC 2271 - 2275, släpptes 2002. [500] Det är den senaste versionen och i och med att IETF gjort den till full standard är numera SNMPv1 och SNMPv2c klassificerade som historiska. [400]

3.1 Säkerhet

Med SMNPv3 behöver man inte vara rädd för att PDU:erna har blivit fifflade med. De PDUer som används för att ställa in andra enheter kan krypteras så ingen kan läsa dessa. Symmetriska nycklar används för autentisering och dessa lagras inte i MIBen. Det är möjligt att med hjälp av att sätta rättigheter begränsa så valda användare endast får tillgång till att läsa vissa delar av MIB:en. [400]

Detta har påverkat paketens uppbyggnad från föregående versioner och har i praktiken inneburit att fler fält introducerats, bl.a. kan flaggor, tidsparametrar, identifikationer av olika slag och säkerhetsparametrar. [600]

3.2 PDU-typer

Det finns olika typer av PDU:er som används i SNMP.

- GetRequest - Används för att begära ut OID:er.
- GetNextRequest - Används för att begära ut nästa OID som finns direkt efter förra begärda i listan över OID:s.
- SetRequest - Används för att ändra värden i OID:erna.
- Response - Dessa används för att svara på förfrågningarna.
- Trap - Skickas av SNMP-agenterna när ett visst kriterie är uppfyllt på enheten.
- GetBulkRequest PDU - Klarar att göra förfrågningar om flera OID:s samtidigt. Detta paket introducerades först i SNMPv2.
- InformRequest PDU - Paket som skickas mellan olika managers (maskiner som hämtar information om enheter i nätverket). Även detta paket introducerades i SNMPv2. [200]
- report - Används för intern SNMP kommunikation. [1500]
- notification - Liknande som traps. [1400]

3.3 Portar

SNMP jobbar i lager 7, applikationslagret, i OSI-modellen. Fyra olika portar är associerade med SNMP. Normalt används UPD som transportprotokoll [200] men även motsvarande TCP-portar kan användas [800].

- Port 161: Här tar SNMP-agenter emot förfrågningar.
- Port 162: Här tar Managers emot Trap och InformRequest PDU:er.
- Port 10161: Används för de krypterade förfrågningarna.
- Port 10162: Här tar Managers emot Trap och InformRequest PDU:er som skickas i krypterad form. [200]

4 MIB och OID

Varje OID har en variabel associerad till den och dessa är sedan organiserade enligt en trädstruktur (hierarkisk struktur). Den fulla sökvägen till ett specifikt OID skulle kunna vara: 1.3.6.1.4.1.2681.1.2.102. Det sista talet, i det här fallet 102, hittas om man först går till 1, vidare till 3, vidare till 6, vidare till 1 och så vidare. Alla dessa siffror representerar kategorier. De första står för: iso (1), org (3), dod (6), internet (1). Varje OID är unikt och de första i ordningen är standardiserade på vad de representerar. [900] De finns 318 bland de första 5000 RFC:er som innehåller MIBs. Organisationer kan sedan reservera top-level MIBs och använda dessa till deras maskiner. [1100]

Maskinerna skickar endast siffrorna till varandra och vi människor behöver få dessa siffror översatta av MIBs för att få dem i textformat. En förutsättning är förståss att de OIDs man vill ha översatta finns i MIB:en. [900] Det finns programvaror som är speciellt avsedda för att läsa MIBs. [1100] Eftersom företagen själva får definiera OIDs så finns det därför en uppsjö av MIBs att använda och man behöver hitta rätt MIB. Cisco har ensamt en mängd MIBs som deras kunder får hämta ner. [1000]

5 Agenter och communities

En agent är en mjukvara som körs på den enheten i nätverket som övervakas. Det körs antingen som ett program (kallad daemon i linux) eller är inbyggt i operativsystemet (som i Cisco Routrars IOS). Idag medföljer SNMP-stöd för de flesta enheter som köps. Agenterna är det som svarar på requests och delar med sig av OIDs. [1200]

Windows och linux har inbyggt stöd för SNMP. Programvaran skiljer sig beroende på vilket operativsystem som används. Det är dock en simpel installation oavsett vilket som används. I Windows är det helt enkelt en Service som aktiveras och i Linux är det ett paket som hämtas hem och installeras. [1300]

Communities används skapa tillit mellan övervakningsmaskinerna och agenterna. En agent kommer konfigurerad med tre community: read-only, read-write och trap. De har olika funktion, Read-only kan man endast hämta information ifrån, read-write kan man även modifiera och trap tillåter att traps får tas emot från agenten.Standardnamnet är public för read-only och private för read-write. Namnen i sig är även lösenorden. I de gamla

versionerna av SNMP skickades community-namnet i klartext, något som man med SNMPv3 har åtgärdat. [1200]

6 Diskussion

Ett problem med att använda transportprotokollet UDP för traps är att UDP inte har någon funktion som bekräftar om meddelandet kommit fram. Det kan i praktiken innebära att ett trap-paket går förlorad och att övervakningsservern därför inte får meddelandet. Hur stort problemet är däremot beror på hur viktig information som meddelandet innehåller.

För att minimera risken för att obehöriga ska kunna avlyssna och sabortera SNMP-trafiken så kan man ställa in brandväggen att endast tillåta övervakningsmaskinerna och enheterna med agenter att skicka via port UDP 161, 162, 10161 och 10162. På så vis kan inte de obehöriga skicka bl.a. SetRequst PDU till enheterna och på så vis är enheterna skyddade från att vem som helst kan ändra på dem.

En hel del enheter idag som används idag har endast stöd för de äldre versionerna av SNMP. Man kan alltid leta efter uppdateringar av mjukvaran som ger stöd för SNMPv3 men det kommer inte finnas för alla enheter. Om dessa enheterna skickar känslig information får man lösa detta genom att sätta brandväggsregler som ovan sagt eller ha en övervakningserver kopplad i nära anslutning till enheten, kanske rent av på ett helt seperat nätverk.

Eftersom communitynamnen används som lösenord borde de behandlas som desamma. Namnen borde därför bytas från public och private till komplexa slumpgenererade lösenord innehållande både stora och små bokstäver mixade med specialtecken och siffror. Detta spelar visserligen mindre roll om inte SNMPv1 eller SNMPv2c används eftersom namnet ändå skickas i klartext och därför kan snappas upp, men används SNMPv3 så kommer det krävas mycket innan någon gissar rätt på communitynamnet.

Tack vare hur strukturen på OIDs är, att organisationer äger vissa grenar, gör att övervakningen genom SNMP är väldigt enkelt att skräddarsy. Organisationerna skapar egna grenar under det OID som representerar företaget och låter dessa representera vad som än önskas. Det som däremot kan vara krongligt är att hitta rätt MIB till rätt enhet. Det är mindre problematiskt för populäraste enheterna men använder man utrustning som inte är vida använd kan det till och med vara som så att man inte hittar rätt MIB och därför inte vet vad de olika varabelvärderna i alla dessa OID betyder. Det innebär då att det inte är någon mening att övervaka enheten eftersom man inte vet vad värderna innebär.

7 Referenser

[100] Webopedia, "SNMP", Dec. 2012;
http://www.webopedia.com/TERM/S/SNMP.html

[200] Wikipedia, "Simple Network Management Protocol", Dec. 2012;
http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

[300] J. Case et al., Introduction to version 2 of the Internet-standard Network Management Framework, IETF RFC 1441, April 1993;
http://tools.ietf.org/html/rfc1441

[400] ubizen, "Security in SNMPv3 versus SNMPv1 or v2c", 2002;
http://www.aethis.com/solutions/snmp_research/snmpv3_vs_wp.pdf

[500] D. Harrington et al., "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", Dec. 1012;
http://tools.ietf.org/html/rfc3411

[600] Vertical Horizons, "SNMP MEssage Format - SNMP PDU Format", Dec. 2012; http://verticalhorizons.in/snmp-message-format-snmp-pdu-format/

[800] IANA, "Service Name and Transport Protocol Port Number Registry", Dec. 2012; http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml

[900] DPS Telecom, "SNMP OID", Dec. 2012;
http://www.dpstele.com/dpsnews/techinfo/snmp/snmp_oid.php

[1000] Cisco, "MIBs Supported by product", Dec. 2012;
http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

[1100] Wikipedia, "Management information base", Dec. 2012;
http://en.wikipedia.org/wiki/Management_information_base

[1200] D. R. Mauro, K. J. Schmidt, Essential SNMP Second Edition, USA, 2005.

[1300] Manage Engine, "SNMP Agent Installation", Dec. 2012;
http://www.manageengine.com/products/applications_manager/help/appendix/snmp-agent-discovery.html

[1400] Vertical Horizons, "Difference Between SNMP Trap and SNMP Notification", Dec. 2012; http://verticalhorizons.in/difference-between-snmp-trap-and-snmp-notification/

[1500] The TCP/IP Guide, "SNMP Protocol General Operation, Communication Methods and Message Classes", Dec. 2012;
http://www.tcpipguide.com/free/t_SNMPProtocolGeneralOperationCommunicationMethodsan-2.htm