Wojciech Horzelski, Dariusz Doliwa, Mariusz Frydrych
Wydział Matematyki i Informatyki Uniwersytetu Łódzkiego
ul. Banacha 22, 90-238 Łódź
email: horzel,doliwa,frydrych@math.uni.lodz.pl

SYSTEM MONITOROWANIA SIECI

Streszczenie – Niniejszy artykuł przedstawia koncepcję systemu monitorowania sieci komputerowej dużego przedsiębiorstwa z hybrydową infrastrukturą. System oparty jest o oprogramowanie Nagios, oprogramowaniu Multi Router Traffic Grapher, NdoUtils, systemie zarządzania relacyjną bazą danych MySQL, systemach wizualizacyjnych dla Nagios (NagVis, NagMap) oraz dedykowanej aplikacji stworzonej na potrzeby systemu pozwalającej na prezentację monitorowanych zasobów.

Słowa kluczowe: Nagios, monitorowanie sieci, SNMP

1 Wprowadzenie

Sieci komputerowe przedsiębiorstw są aktualnie coraz częściej sieciami o charakterze heterogenicznym łącząc ze sobą różne technologie zarówno lokalne jak i rozległe, używając urządzeń pracujących pod kontrolą różnych systemów operacyjnych. Ponadto monitorowanie i zarządzanie siecią nie ogranicza się do jednego miejsca, ale wymaga dostępu często do zdalnych lokalizacji. W takich przypadkach pojedyncze dedykowane narzędzia nie spełniają swojej roli lub istnieje potrzeba użycia kilku różnych narzędzi jednocześnie, co znacznie komplikuje administrację siecią oraz zwiększa jej koszty (zakup wielu narzędzi, szkolenie pracowników do ich stosowania). Dodatkowo często narzędzia te mają ograniczenia związane ze skalowalnością czy dostosowaniem się do zmian zachodzących w wykorzystywanych technologiach sieciowych. W pracach [1] i [2] autorzy uwzględniając te czynniki przedstawili rozważania na temat funkcjonalności, którą powinien gwarantować system do zarządzania i monitorowania siecią. Te cechy to: automatyzacja procesu monitorowania, zdolność do dostosowywania się do zmieniających się rozwiązań stosowanych w sieciach, możliwość działania w wielu różnych środowiskach, moduło-wość pozwalająca wybrać tylko konieczne komponenty w zależności od charakteru monitorowanej sieci, inteligentne składowanie, analiza i wizualizacja uzyskanych danych, zdolność do wpływania na projekt sieci

np. poprzez zdalne i automatyczne zarządzanie konfiguracją urządzeń sieciowych. W niniejszym artykule przedstawiono koncepcję budowy systemu, który posiadałby postulowane cechy.

System oparty będzie na platformie Nagios[3], będącej oprogramowaniem otwartym, rozwijanym i dokładnie przetestowanym w ostatnich latach. W 2007 roku pojawiły się pierwsze propozycje [4] związane z wdrożeniem tej platformy w firmie o zasięgu globalnym wskazując na takie cechy jak skalowalność, zabezpieczenia danych, możliwość integracji standardowych protokołów (jak np. SNMP, CMIP) z monitorowaniem aplikacji i urządzeń o architekturze zamkniętej. Od tego czasu platforma znacznie się rozwinęła [5] poszerzając swoje możliwości o monitorowanie zużycia pasma przenoszenia, jakości usługi (QoS), czy system powiadomień, który może być zintegrowany z pocztą elektroniczną czy alertami w postaci komunikatów SMS. Pozytywne wyniki testów przeprowadzonych dla elementów platformy Nagios[6] zdecydowały o wyborze tego systemu jako podstawy budowania przedstawionej tutaj aplikacji.

2 Opis koncepcji aplikacji

Prezentowany będzie wykorzystywał również system Multi Router Traffic Grapher (MRTG)[7], oprogramowanie NdoUtils, system zarządzania relacyjną bazą danych MySQL, systemy wizualizacyjne dla Nagios (NagVis, NagMap) oraz dedykowaną aplikację stworzoną na potrzeby systemu (prezentacja monitorowanych własności) .

System będzie posiadał interface pozwalający na:

- dostęp do informacji o wybranym urządzeniu (automatycznie zbieranych w zdefiniowanych odstępach czasowych – domyślnie co 5 minut),
- przeprowadzenie kontroli na żądanie wybranych parametrów urządzenia,
- dostęp do konfiguracji urządzenia,
- powiadamianie w przypadku wystąpienia zdefiniowanej sytuacji nadzwyczajnej na urządzeniu.
- dostęp do danych historycznych

Przedmiotem monitorowania będą urządzenia sieciowe tj. routery i przełączniki.

3 Przechowywanie danych

Aplikacja będzie składała się z 3 baz danych zrealizowanych przy pomocy systemu zarządzania relacyjną bazą danych MySQL:

- pierwsza baza (baza konfiguracyjna) będzie zawierała informacje konfiguracyjne dla systemu

- drugą bazą (baza NdoUtlis, baza aktualnych stanów) będzie baza generowana przez plugin NdoUtils z aktualnymi wartościami monitorowanych parametrów;
- trzecia baza (baza pojemnościowa) będzie bazą gromadząca informacje archiwalne dla monitorowanych parametrów pozwalającą na ich analizę w wybranych przedziałach czasu oraz przechowująca pliki konfiguracyjne monitorowanych urządzeń (aktualne i historyczne).

Baza konfiguracyjna będzie przechowywała:

- konfigurację systemu:
  - katalogi, z których korzysta system (miejsce instalacji systemu, położenie plików konfiguracyjnych systemu i plików z danymi, katalog dla danych tymczasowych);
  - parametry związane z zabezpieczeniami dostępu do systemu;
  - parametry komunikacyjne (adresy i porty usług);
- konta użytkowników systemu:
  - system będzie miał zdefiniowane konta użytkowników oraz możliwość grupowania użytkowników; w bazie będą przechowywane informacje o istniejących kontach zawierające takie dane jak id użytkownika, jego nazwa, dane osobowe i adresowe, adres email i telefon (w celu umożliwienia informowania użytkownika o zdefiniowanych zdarzeniach). Konta i grupy będą wykorzystywane w celu nadawania uprawnień do poszczególnych komponentów systemu. Uprawnienia będą dotyczyły takich zadań jak dostęp do modułu konfiguracyjnego, monitorującego, przeglądanie, dodawanie, usuwanie i edycja użytkowników i ich grup, operacje na hostach i serwisach
- informacje o monitorowanych lokalizacjach (id lokalizacji, nazwa, alias, dane adresowe, współrzędne GPS);
- informacje o monitorowanych urządzeniach (hostach):nazwa , alias, typ urządzenia, model, adres IP, użytkownicy i hasła dla protokołu SNMP, interwały monitorowania urządzenia, parametry powiadomień o zmianie statusu urządzenia (czas przez który generowane są powiadomienia, okres powtarzania powiadomień), zdefiniowane na urządzeniu „trapy” (w postaci opisu); o wystąpieniu zdefiniowanego zdarzenia będą powiadamiani członkowie grupy powiadomień itp.
- monitorowane serwisy (wirtualne obiekty, o których mają być gromadzone informacje); zakłada się dla dowolnego hosta będzie istniała możliwość zdefiniowania serwisów monitorowanych na urządzeniu; dla większości urządzeń będą one reprezentowały interfejsy urządzenia oraz wykorzystanie pasma przenoszenia dla danego interfejsu; dla każdego z serwisów będzie określona nazwa

urządzenia, na którym jest monitorowany jest serwis oraz parametry monitorowania (interwał monitorowania, parametry powiadomień o zmianie statusu serwisu)
- informacje o połączeniach sieciowych: id operatora, nazwa operatora, alias, dane adresowe, opis łącza, pasmo przenoszenia

Największą część bazy konfiguracyjnej będą zajmowały opisy urządzeń i monitorowanych na nich serwisów.

Baza aktualnych stanów będzie okresowo zapisywała wybrane informacje wygenerowane przez Nagios (przy pomocy pluginu NdoUtils) i Multi Router Traffic Grapher, oraz gromadziła pliki konfiguracyjne urządzeń po wykryciu ich zmiany na monitorowanych urządzeniach („trapy" SNMP, protokół TFTP).

Baza pojemnościowa będzie bazą gromadząca informacje archiwalne dla monitorowanych parametrów oraz przechowująca archiwalne pliki konfiguracyjne monitorowanych urządzeń.

Do obsługi baz zostaną dostarczone aplikacje pozwalające na zarządzanie nimi przy pomocy przyjaznego i łatwego w obsłudze interfejsu graficznego.

Aplikacja do bazy konfiguracyjnej będzie pozwalać na:

- definiowanie kont i grup użytkowników systemu,
- dodawanie/usuwanie/modyfikowanie urządzeń do monitorowania,
- dodawanie usuwanie/modyfikowanie monitorowanych serwisów,
- dodawanie/usuwanie/modyfikowanie opisu połączeń

Dodawanie urządzeń będzie wspomagane przez zdefiniowane dla urządzenia każdego typu szablony, które pozwolą w prosty sposób zdefiniować cechy urządzenia oraz wybrać charakterystyczne dla niego serwisy i zdefiniować domyślne ustawienia dotyczące monitorowania.

Modyfikacja bazy monitorowanych hostów i serwisów będzie powodowała automatyczne wygenerowanie plików konfiguracyjnych dla systemu Nagios oraz jego przeładowanie pozwalając na zaktualizowanie obiektów i ich parametrów podlegających monitorowaniu.

Aplikacja pozwalająca wyświetlać aktualne wartości parametrów dla wybranych przez użytkownika urządzeń, serwisów na podstawie danych zebranych przez plugin NdoUtils lub zapytań przy pomocy protokołów SNMP, ICMP, CDP.

Aplikacja w zależności od użytkownika i jego przynależności do grup wyświetli wartości monitorowanych parametrów, których do ma on uprawnienia. Aplikacja pozwoli filtrować i sortować dane po takich kryteriach jak lokalizacja, typ urządzenia, wartości monitorowanych parametrów.

Aplikacja do analizy danych historycznych zgromadzonych w bazie pojemnościowej, wyświetlania i porównywania aktualnych i archiwalnych konfiguracji urządzeń.

4 Moduł monitorowania

Moduł monitorujący odpowiedzialny będzie za okresowe zbieranie informacji o urządzeniach i umieszczanie ich w odpowiednich tabelach bazy. Do jego realizacji wykorzystane będą NagiosCore oraz plugin NdoUtils oraz monitor MRTG. Konfiguracje parametrów niezbędnych do właściwego funkcjonowania systemu Nagios przechowywane będą w odpowiednich plikach konfiguracyjnych generowanych automatycznie na podstawie zmian w opisanych wcześniej bazach danych.

Definicja każdego serwisu będzie poprzedzona definicją hosta, którego on dotyczy.

Dla każdego serwisu określona zostanie częstotliwość monitorowania. Możliwe będzie wykonanie testu na żądanie operatora.

Dla uproszczenia konfiguracji urządzeń przewidywane jest tworzenie wzorców hostów oraz wzorców serwisów. W celu ułatwienia administrowania hostami i serwisami możliwe będzie ich grupowanie (szczegółowy opis składni plików konfiguracyjnych oraz ich pól znajduje się w dokumentacji systemu: http://nagios.sourceforge.net/docs/3_0/objectdefinitions.html).

System Nagios Core posiada kilkadziesiąt komend opartych o wbudowane plugin'y służących do monitorowania zdefiniowanych serwisów. Planowane jest wykorzystanie następujących komend:

- check_host_alive – komenda pozwalająca kontrolować dostępność hosta w sieci;
- check_interface_alive – komenda pozwalająca monitorować dostępność portu;
- check_snmp - komenda pozwalająca na odczyt dowolnej wartości dla urządzenia z wykorzystaniem protokołu SNMP;
- check_snmp_getinterfacedata – komenda pozwaljąca na połączenie ze wskazanym hostem i pobranie stanu wszystkich liczników oraz stanu dla wszystkich interfejsów;
- check_displaydata – komenda parsująca plik tymczasowy filtrując dane dotyczące wskazanego interfejsu;
- check_snmp_device_status – komenda pobierająca ze wskazanego hosta dane o utylizacji CPU i pamięci RAM oraz informacje o temperaturze;
- check_snmp_backup_config – komenda pozwalająca na wykonanie kopii zapasowej konfiguracji urządzenia sieciowego.

5 Moduł obsługi zdarzeń

W bazie konfiguracyjnej urządzeń opisane są zdefiniowane na tych urządzeniach „trapy" oraz wartości krytyczne, które powodować będą wygenerowanie komunikatu przez urządzenie. Opisywany moduł za zadanie będzie miał odbiór trapów SNMP wysyłanych z urządzeń sieciowych oraz ich interpretację i aktywowanie powiadomień odpowiednich użytkowników.

Zakłada się, że na serwerze gdzie zainstalowany jest NagMon zostanie zainstalowany serwis snmptrapd oraz serwis snmptt. W momencie, gdy urządzenie wygeneruje sygnał trap (w konfiguracji urządzenia będą ustawione parametry gdzie trapy mają być wysyłane) zostanie on przesłany do serwera snmptrapd. Serwer snmptrapd przesyła otrzymane trapy do parsera snmptt, który analizuje otrzymane informacje i podejmuje odpowiednie działania.

Moduł ma również interpretować trap SNMP object „ciscoConfigManEvent" z MIB „CISCO-CONFIG-MAN-MIB" o statusie zmiany konfiguracji przez operatora i zapisie jej z running-config do startup-config. Następnie zdarzenie zostanie odnotowane w sys-temie Nagios Core oraz uruchomiony skrypt przeprowadzający procedurę wykonania kopii zapasowej.

6 Moduł wykrywania urządzeń

Zadaniem tego modułu jest wykrywanie zmian w topologii sieci polegającej na dodaniu nowego urządzenia. Po wykryciu nowego urządzenia system będzie pozwalał na jego dodanie do bazy urządzeń i dalszej konfiguracji lub połączenie z wcześniej utworzonym urządzeniem (w sytuacji czasowej niedostępności hosta).

Wykrywanie urządzeń sąsiadujących będzie opierać się będzie o protokoły:

- Cisco Discovery Protocol (CDP)
- Link Layer Discovery Protocol (LLDP)

W przypadku dowolnych urządzeń (niesąsiadujących) wykorzystany zostanie skaner Network Mapper (Nmap).

Wykrywanie hostów będzie mogło odbywać się okresowo bądź na żądanie. Parametrem wyszukiwana będą zakresy adresów IP do weryfikacji, ze wskazaniem wyłączonych adresów (urządzeń już znanych).

Po przeprowadzeniu skanowania system przygotuje listę aktywnych urządzeń, a nas-tępnie (używając systemowo ustawionego community string) spróbuje uzyskać informacje o odpowiednim obiekcie „CISCO-CDP-MIB" lub „CISCO-LLDP-EXT-MED-CAPABILITY" .

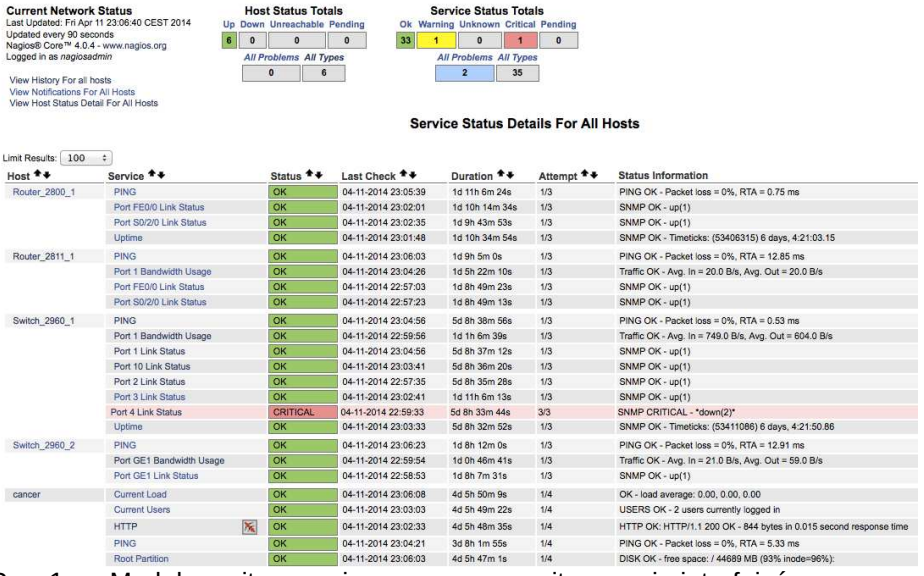
System pozwoli na sprawdzenie, czy znalezione urządzenia znajdują się już w bazie danych oraz ewentualne, na ich wprowadzenie do systemu oraz dalszą konfigurację parametrów.

System pozwoli również na automatyczne wprowadzenie serwisów monitorujących połączenia pomiędzy urządzeniem skanowanym i znalezionym jego sąsiadem.

7 Podsumowanie

Zaprezentowana koncepcja systemu monitorującego pozwala na zbudowanie wydajnej aplikacji monitorującej sieci LAN i WAN opartej o narzędzia klasy Open Source. Zaproponowane rozwiązania pozwalają na skalowalność takiego systemu, przez co może on być wykorzystywany zarówno w małych, średnich, jak i dużych przedsiębiorstwach.

Poszczególne jego elementy zostały zainstalowane, skonfigurowane i przetestowane w środowisku laboratoryjnym (rys. 1).



Current Network Status
Last Updated: Fri Apr 11 23:06:40 CEST 2014
Updated every 90 seconds
Nagios® Core™ 4.0.4 - www.nagios.org
Logged in as *nagiosadmin*

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
6	0	0	0

All Problems	All Types
0	6

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
33	1	0	1	0

All Problems	All Types
2	35

Service Status Details For All Hosts

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Router_2800_1	PING	OK	04-11-2014 23:05:39	1d 11h 6m 24s	1/3	PING OK - Packet loss = 0%, RTA = 0.75 ms
	Port FE0/0 Link Status	OK	04-11-2014 23:02:01	1d 10h 14m 34s	1/3	SNMP OK - up(1)
	Port S0/2/0 Link Status	OK	04-11-2014 23:02:35	1d 9h 43m 53s	1/3	SNMP OK - up(1)
	Uptime	OK	04-11-2014 23:01:48	1d 10h 34m 54s	1/3	SNMP OK - Timeticks: (53406315) 6 days, 4:21:03.15
Router_2811_1	PING	OK	04-11-2014 23:06:03	1d 9h 5m 0s	1/3	PING OK - Packet loss = 0%, RTA = 12.85 ms
	Port 1 Bandwidth Usage	OK	04-11-2014 23:04:26	1d 5h 22m 10s	1/3	Traffic OK - Avg. In = 20.0 B/s, Avg. Out = 20.0 B/s
	Port FE0/0 Link Status	OK	04-11-2014 22:57:03	1d 8h 49m 23s	1/3	SNMP OK - up(1)
	Port S0/2/0 Link Status	OK	04-11-2014 22:57:23	1d 8h 49m 13s	1/3	SNMP OK - up(1)
Switch_2960_1	PING	OK	04-11-2014 23:04:56	5d 8h 38m 56s	1/3	PING OK - Packet loss = 0%, RTA = 0.53 ms
	Port 1 Bandwidth Usage	OK	04-11-2014 22:59:56	1d 1h 6m 39s	1/3	Traffic OK - Avg. In = 749.0 B/s, Avg. Out = 604.0 B/s
	Port 1 Link Status	OK	04-11-2014 23:04:56	5d 8h 37m 12s	1/3	SNMP OK - up(1)
	Port 10 Link Status	OK	04-11-2014 23:03:41	5d 8h 36m 20s	1/3	SNMP OK - up(1)
	Port 2 Link Status	OK	04-11-2014 22:57:35	5d 8h 35m 28s	1/3	SNMP OK - up(1)
	Port 3 Link Status	OK	04-11-2014 23:02:41	1d 11h 6m 13s	1/3	SNMP OK - up(1)
	Port 4 Link Status	CRITICAL	04-11-2014 22:59:33	5d 8h 33m 44s	3/3	SNMP CRITICAL - *down(2)*
	Uptime	OK	04-11-2014 23:03:33	5d 8h 32m 52s	1/3	SNMP OK - Timeticks: (53411086) 6 days, 4:21:50.86
Switch_2960_2	PING	OK	04-11-2014 23:06:23	1d 8h 12m 0s	1/3	PING OK - Packet loss = 0%, RTA = 12.91 ms
	Port GE1 Bandwidth Usage	OK	04-11-2014 22:59:54	1d 0h 46m 41s	1/3	Traffic OK - Avg. In = 21.0 B/s, Avg. Out = 59.0 B/s
	Port GE1 Link Status	OK	04-11-2014 22:58:53	1d 8h 7m 31s	1/3	SNMP OK - up(1)
cancer	Current Load	OK	04-11-2014 23:06:08	4d 5h 50m 9s	1/4	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	04-11-2014 23:03:03	4d 5h 49m 22s	1/4	USERS OK - 2 users currently logged in
	HTTP	OK	04-11-2014 23:02:33	4d 5h 48m 35s	1/4	HTTP OK: HTTP/1.1 200 OK - 844 bytes in 0.015 second response time
	PING	OK	04-11-2014 23:04:21	3d 8h 1m 55s	1/4	PING OK - Packet loss = 0%, RTA = 5.33 ms
	Root Partition	OK	04-11-2014 23:06:03	4d 5h 47m 1s	1/4	DISK OK - free space: / 44689 MB (93% inode=96%):

Rys. 1. Moduł monitorowania - pasywne monitorowanie interfejsów w środowisku testowym za pomocą narzędzia Nagios

Ze względu na wykorzystywane rozwiązania i protokoły sieciowe system taki nie będzie w istotny sposób obciążał zasobów sieci produkcyjnej oraz nie będzie wymagał dużych nakładów sprzętowych. Pozwala to na zachowanie niskich kosztów zarówno jego stworzenia, jak i wdrożenia w przedsiębiorstwie. W zaproponowanej obecnie formie system będzie wymagał dużej wiedzy administratorów sieci – zakłada

się, iż będą oni współtwórcami tego rozwiązania oraz będą aktywnie uczestniczyć w procesie jego wdrażania.

W przyszłości autorzy planują dodanie rozbudowanego interfejsu graficznego (w szczególności modułu wizualizacji danych), pozwalającego na łatwiejsze wykorzystanie systemu przez mniej zaawansowanych użytkowników.

8 Literatura

[1] S. Lee, K. Levanti, Hyong S. Kim, *Network monitoring: Present and future,* Computer Networks,Volume 65, 2014, pp: 84–98

[2] D. Padi, *Telecommunications & Information Technology Network Management, challenges in acquisition, design and systems development*, NGNS'2009: 2nd International Conference on Adaptive Science & Technology pp 52-53,

[3] Nagios manual: http://library.nagios.com/library/products/ nagioscore/ manuals/

[4] C. Gaspar, *Deploying Nagios in a Large Enterprise Environment, at USENIX LISA '07*

[5] S. Mohd, I. Roslan, A. Zainal, S. Anawar, *The new services in Nagios: Network bandwidth utility, email notification and sms alert in improving the network performance*, Information Assurance and Security (IAS), 2011 7th International Conference

[6] A. Dooguy Kora, M. Moindze Soidridine, *Nagios Based Enhanced IT Management System*, International Journal of Engineering Science and Technology (IJEST), Vol. 4 No.3, 2012, pp:1199-1207

[7] MRTG configuration reference: http://oss.oetiker.ch/mrtg/doc/mrtg-reference.en.html

NETWORK MONITORING SYSTEM

Summary – This paper presents the concept of network monitoring system for a large company with a hybrid infrastructure. The system is based on Nagios software, Multi Router Traffic Grapher utility, NdoUtils, relational database management system MySQL, visualization systems for Nagios (NagVis, NagMap) and a dedicated application created for the system allowing presentation of the monitored resources.

Keywords: Nagios, network management, SNMP