Jan Rojek
Wydział Informatyki i Zarządzania
Wyższej Szkoły Informatyki w Łodzi

Promotor: dr Mariusz Zarzycki

MONITORING INFRASTRUKTURY SIECIOWEJ Z WYKORZYSTANIEM PAKIETU „OPENNMS”

Streszczenie – Głównym tematem artykułu jest stworzenie kompleksowego systemu monitorującego infrastrukturę sieciową (ang. Network Monitoring System) z wykorzystaniem darmowych narzędzi, w tym pakietu OpenNMS. Opisane są: instalacja, konfiguracja i użytkowanie pakietu, jak również konfiguracja urządzeń sieciowych do współpracy z systemem monitoringu. Jako środowisko uruchomieniowe pakietu użyty został darmowy system operacyjny Linux.

1 Wstęp

Jednym z aspektów administrowania infrastrukturą sieciową jest monitorowanie działania poszczególnych urządzeń i usług. Wraz z wzrostem znaczenia informatyki w kluczowych obszarach biznesu, rośnie potrzeba zapewnienia nieprzerwanego dostępu do zasobów sieciowych, takich jak systemy finansowe, bazy danych, systemy ERP etc. Niedopuszczalne stają się sytuacje, w których systemy te nie byłyby dostępne przez dłuższy czas. Wymusza to na administratorach sieci opracowywanie rozwiązań gwarantujących jak największą niezawodność, ograniczając przestoje do minimum. Niezbędne są tutaj narzędzia zbierające dane o działaniu infrastruktury sieciowej, bowiem oprócz dostarczania informacji o awariach, są w stanie pokazać wszelkie anomalie w funkcjonowaniu sieci, począwszy od wzmożonego ruchu na łączach, kończąc na braku wolnego miejsca na dyskach twardych serwerów. Daje to możliwość szybkiego reagowania w przypadku wystąpienia awarii, oraz pozwala wykryć potencjalne problemy, nim przerodzą się w awarie uniemożliwiające pracę.

W rozbudowanych środowiskach istnieje potrzeba monitorowania nie tylko dostępności poszczególnych urządzeń, ale również świadczonych przez nie usług, obciążenia aktywnych elementów sieci, takich jak routery, przełączniki, serwery czy wreszcie wykorzystania dostępnego

pasma na łączach WAN. Do systemu monitorowania można dodatkowo włączyć takie urządzenia jak zasilacze awaryjne UPS, czy klimatyzatory. Można wtedy na bieżąco kontrolować środowisko, w jakim działają maszyny, znając stan naładowania akumulatorów UPS oraz temperaturę w serwerowni. Tak kompleksowe monitorowanie jest niezbędne w celu szybkiego wykrywania problemów i awarii, co za tym idzie wpływa pozytywnie na dostępność świadczonych usług.

2 Monitoring infrastruktury sieciowej

Monitoring polega na sprawdzaniu stanu elementów infrastruktury sieciowej pod względem ich prawidłowego funkcjonowania. W razie wykrycia nieprawidłowości automatycznie mogą zostać podjęte działania takie jak wysłanie powiadomienia o awarii, restart urządzenia, etc.
Celem monitorowania jest:

- Wykrywanie awarii

Idealnie działający system monitorujący powinien informować o zbliżających się awariach zanim one wystąpią. Jednak przewidzenie awarii z odpowiednim wyprzedzeniem jest często niemożliwe, dlatego celem takiego systemu jest jak najszybsze wykrycie zaistniałych nieprawidłowości w funkcjonowaniu systemu i poinformowanie osób nim zarządzających, aby czas reakcji był jak najkrótszy.

- Prowadzenie dziennika zdarzeń

Dane rejestrowane w dzienniku zdarzeń można podzielić na dwie grupy:

a) Parametry systemowe, takie jak użycie pamięci, procesora, obciążenie kart sieciowych, ilość dostępnego miejsca na dyskach. W oparciu o te parametry można przeanalizować stan systemu na przestrzeni czasu i na tej podstawie podjąć ewentualne kroki mające na celu przeciwdziałanie awariom.
b) Komunikaty systemowe, informujące o stanie urządzeń i działających na nich aplikacji. Dzięki nim można przeanalizować poprawność działania systemu pod kątem występowania błędów aplikacyjnych, sprzętowych i środowiskowych. Do ich przeglądania przydatne są dedykowane narzędzia do analizy dzienników systemowych.

Dobry system monitorujący jest w stanie zbierać informacje ze wszystkich aktywnych elementów infrastruktury sieciowej, począwszy od warunków środowiskowych panujących w serwerowni (napięcie zasilania, wilgotność i temperatura powietrza), poprzez stan fizyczny sprzętu (sprawność zasilaczy, wentylatorów), stan macierzy dyskowych, dostępność w sieci, kończąc na sprawdzeniu stanu usług świadczonych przez urządzenia.

Skuteczny monitoring sieci pozwala:

- Zmniejszyć czas niedostępności usług spowodowanych awarią
- Zmniejszyć przestoje w pracy użytkowników spowodowane niedostępnością usług
- Zmniejszyć nakład pracy administratorów systemów
- Wykrywać potencjalne źródła problemów zanim wystąpią
- Obniżyć koszta działania działów IT

Dobrą praktyką jest monitorowanie wszystkich warstw systemu, w których istnieje taka możliwość i w których ma to sens. Dla przykładu monitorowanie jedynie dostępności w sieci danego adresu IP nie ma większego sensu, jeśli stan działających na nim usług i aplikacji jest nieznany. Z drugiej strony monitorowanie samej aplikacji często nie wykaże problemów z warstwą sieciową, np. awarią łącza głównego i przekierowaniem ruchu przez łącze zapasowe.
Monitorowanie dostępności strony WWW we wszystkich warstwach TCP/IP wyglądałoby następująco:

Warstwa Dostępu do sieci	*Detekcja IP przy pomocy ARP*
Warstwa Internetu	*Detekcja dostępności przy pomocy ICMP*
Warstwa Transportowa	*Nawiązanie połączenia TCP*
Warstwa Aplikacji	*Pobranie pliku z serwera http*

3 Architektura systemu monitorującego

W zależności od rozmiarów monitorowanej sieci, można wyróżnić systemy proste i złożone.

Systemy proste zazwyczaj składają się z jednego serwera monitorującego umieszczonego w centrali, który z jednego miejsca monitoruje wszystkie urządzenia. Tego typu systemy dobrze sprawdzają się w scentralizowanych środowiskach o niewielkiej liczbie podsieci, lub kiedy między oddziałami istnieją stabilne łącza o przepustowości pozwalającej na utrzymanie dodatkowego ruchu związanego z monitorowaniem urządzeń.

Systemy złożone składają się z więcej niż jednego serwera monitorującego, a ich liczba uwarunkowana jest często ilością oddziałów i podsieci. Jeśli sieć obejmuje swoim zasięgiem wiele lokalizacji, często instaluje się podrzędną stację monitorującą w każdym oddziale, a nawet w każdej podsieci, o ile w oddziale znajduje się więcej niż jedna podsieć. Podrzędne stacje monitorujące zbierają informacje o ściśle określonym fragmencie sieci i raportują okresowo (lub w przypadku wystąpienia awarii) do serwera monitorującego w centrali. Również sama centrala

może składać się z więcej niż jednego serwera, aby zapewnić maksymalną niezawodność. W takich systemach łącza między oddziałami nie są stale obciążane ruchem związanym z monitoringiem. Zadaniem systemu monitorującego jest :

- zbieranie danych
- zarządzanie komunikatami
- wykonywanie poleceń na zarządzanych węzłach
- wysyłanie powiadomień o zdarzeniach
- przekazywanie danych do narzędzi analizujących logi i innych systemów monitorujących

Większość z dostępnych na rynku systemów monitorowania wykorzystują tzw. agentów w celu zbierania bardziej szczegółowych danych. Agent jest to program instalowany na monitorowanym systemie, który ma za zadanie zbierać i udostępniać stacji monitorującej informacje o stanie systemu, na którym jest zainstalowany. Bez instalacji agenta system monitorujący jest w stanie jedynie sprawdzać, czy określone adresy IP i działające na nich usługi są dostępne, bez odczytywania konkretnych stanów, tj. obciążenia, dostępnego miejsca na dyskach, komunikatów o błędach, ostrzeżeniach etc.

Zadaniem agenta zainstalowanego na maszynie jest:

- przechwytywanie komunikatów sprzętowych i systemowych
- monitorowanie wydajności systemu
- buforowanie informacji, aby nie zostały utracone w przypadku braku połączenia ze stacją monitorującą
- wykonywanie na lokalnym systemie poleceń ze stacji monitorującej

W systemie monitorującym gromadzone są newralgiczne informacje dotyczące całego środowiska sieciowego, z tego powodu powinien być on należycie zabezpieczony przed niepowołanym dostępem. System operacyjny serwera powinien być na bieżąco aktualizowany, ze szczególnym uwzględnieniem poprawek bezpieczeństwa. Dobrą praktyką jest umieszczenie stacji monitorującej w osobnej podsieci odizolowanej od środowiska produkcyjnego, co ogranicza możliwość podsłuchania transmisji. W tym celu można użyć dedykowanych przełączników lub VLAN'ów. Jeśli nie jest to możliwe, warto przynajmniej zabezpieczyć transmisję przy pomocy dodatkowej warstwy szyfrującej, np. TLS dostępnego w SNMPv3.

4 Monitoring aktywny i pasywny

Najpopularniejszą metodą monitorowania stanu urządzeń w sieci jest

tak zwany monitoring aktywny. Polega on na odpytywaniu urządzeń przez system monitorujący. Najprostsze metody aktywnego monitoringu to wysyłanie zapytań ICMP echo-request bądź nawiązywanie połączenia TCP z konkretną usługą.

W przypadku, kiedy system monitorujący nie ma bezpośredniego dostępu do monitorowanego hosta, istnieje możliwość zastosowania tak zwanego monitoringu pasywnego. Zazwyczaj polega to na instalacji specjalnego agenta na monitorowanym hoście, który zbiera informacje o jego działaniu i wysyła je cyklicznie do stacji monitorującej. Ten typ monitoringu ma zastosowanie wówczas, kiedy monitorowany host znajduje się w innej sieci, jest chroniony zaporą sieciową, lub jest zainstalowany u zewnętrznego klienta, którego polityka bezpieczeństwa nie pozwala na dostęp do urządzenia z zewnątrz sieci. Wtedy monitorowany host nawiązuje bezpieczne połączenie ze stacją monitorującą i przesyła informacje o swoim stanie. Za niedostępność urządzenia monitorowanego tą metodą uznaje się sytuację, kiedy stacja monitorująca nie otrzymała w zdefiniowanym czasie kolejnej informacji określającej poprawną pracę hosta (tak zwany heartbeat, ang. uderzenie serca). Taka sytuacja powinna wywołać alarm i wysłanie powiadomienia.

5 Integracja z innymi systemami

Przy doborze systemu monitorującego warto zwrócić uwagę, czy umożliwi on integrację z używanymi systemami używanymi w przedsiębiorstwie. Na uwagę zasługuje tu przede wszystkim możliwość integracji z systemem LDAP/Kerberos (np. Active Directory Microsoftu), aby nie tworzyć kolejnej bazy użytkowników i haseł.

Kolejną przydatną funkcją jest możliwość integracji z systemami raportowania błędów i obsługi zgłoszeń, takimi jak Bugzilla, IBM Rational ClearQuest, Mantis etc. Pozwoli to automatycznie rejestrować konkretne zdarzenia i przydzielać je do odpowiednich osób i grup.

Przydatną funkcją jest również możliwość eksportu zebranych logów, aby można je było przetworzyć w wyspecjalizowanych programach. Często bowiem ilość zarejestrowanych zdarzeń jest tak duża, że ręczne przeglądanie ich jest nieefektywne.

6 Usługa

Zasadniczo każde urządzenie (węzeł) w sieci świadczy określone usługi (ang. service). Każda usługa komunikuje się ze środowiskiem sieciowym przy wykorzystaniu określonych protokołów, najczęściej TCP lub UDP. Zadaniem systemu monitorującego jest okresowe sprawdzanie dostępności usług świadczonych i poprawności ich funkcjonowania. Procedura testowa polega na nawiązaniu połączenia z określonym

portem, na którym działa usługa, wysłaniu zapytania, odebraniu odpowiedzi i weryfikacji jej poprawności. Jeśli na którymkolwiek etapie sprawdzania wystąpi błąd, np. nie można nawiązać sesji TCP, nie ma odpowiedzi na zapytanie lub jest ona błędna, usługa zostaje uznana za niefunkcjonującą poprawnie.

7 Awaria sieciowa

Każdy system monitorujący powinien poprawnie wykrywać awarie sieciowe. Awaria sieciowa występuje w przypadku uszkodzenia routera, przełącznika, koncentratora lub fizycznego połączenia między tymi elementami (kable, światłowody etc.). Awaria sieciowa ma wpływ na dostępność wszystkich hostów, do których system monitorujący nie będzie miał dostępu w przypadku jej wystąpienia. System monitorujący powinien wykryć, że źródłem problemów z niedostępnością hostów jest awaria urządzenia sieciowego, znajdującego się po drodze do nich. Przykładowo, jeśli awarii ulegnie przełącznik, do którego podłączonych jest dziesięć hostów, system monitorujący powinien to wykryć i wysłać jedynie jedno powiadomienie – o niedziałającym przełączniku, oraz oznaczyć hosty za nim jako tymczasowo niedostępne, a nie niedziałające. W wypadku niewykrycia awarii sieciowej, administrator dostałby dziesięć alarmów o niedziałających hostach, co odwróciłoby jego uwagę od rzeczywistego źródła problemu.

8 Powiadomienie

W przypadku wykrycia jakichkolwiek nieprawidłowości w funkcjonowaniu systemu informatycznego, system monitorujący powinien wysłać powiadomienie. Powiadomienia mogą być wysyłane wieloma drogami. Najbardziej popularne to E-mail i SMS. E-mail jest wygodny i przede wszystkim darmowy, ale gwarantuje odczytanie powiadomienia jedynie w godzinach pracy administratora, a właściwie w godzinach, kiedy znajduje się on przy komputerze. SMS sprawdza się najlepiej kiedy administrator znajduje się poza biurem. Technicznie istnieje wiele możliwości wysyłania wiadomości SMS. Mogą one być wysyłane przy pomocy bramek E-mail-SMS dostarczanych przez operatorów sieci komórkowych, jednak wiadomości wysyłane przy ich pomocy niejednokrotnie przychodzą z opóźnieniem, co w tym przypadku jest niedopuszczalne. Inną metodą jest fizyczne podłączenie telefonu komórkowego lub modemu GSM/UMTS i użycie odpowiedniego programu do jego obsługi. Jest to zdecydowanie pewniejsza metoda, jednak wysłanie każdej wiadomości kosztuje i należy wykupić u operatora odpowiedni abonament.

Istnieje jeszcze możliwość wysyłania wiadomości na komunikatory internetowe, jednak z uwagi na poufność informacji oraz uzależnienie dostarczenia wiadomości od działania zewnętrznych serwerów, ten sposób dostarczania powiadomień jest mocno kontrowersyjny. Wyjątkiem jest używanie do tego celu wewnętrznych, odpowiednio zabezpieczonych serwerów Jabber/XMPP.

9 Eskalacja

Eskalacja polega na informowaniu kolejnych linii wsparcia, jeśli awaria nie jest usunięta w założonym czasie. Dla przykładu – aplikacja działająca na serwerze jest niedostępna. Powiadomienie odbiera helpdesk, lecz jego pracownicy nie poradzili sobie z usunięciem awarii w ustalonym czasie. System wysyła więc powiadomienie do administratora, który również nie usunął awarii w ustalonym czasie. Powiadomienie jest więc wysyłane do programistów tworzących tę aplikację. Dopiero na tym szczeblu udaje się usunąć awarię i oznaczyć ją w systemie jako usuniętą.

10 Centralne zarządzanie siecią

Im bardziej rozbudowana sieć, im więcej jest w nich urządzeń, tym więcej czasu zajmuje zarządzanie nią. System monitorujący może wspomagać zarządzanie siecią, poprzez udostępnienie jednego interfejsu do konfiguracji najpopularniejszych routerów, przełączników etc, eliminując konieczność logowania się do każdego z nich z osobna. Dodatkowym atutem jest automatyczne tworzenie map połączeń sieciowych, tworzenie raportów czy śledzenie anomalii w funkcjonowaniu sieci. Dzięki zebraniu tych wszystkich funkcji w jednym miejscu, czynności administracyjne można wykonywać szybciej i efektywniej.

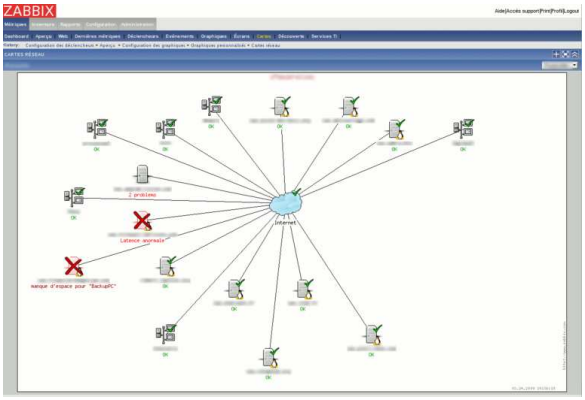
11 Topologia sieci

Większość systemów monitoringu posiada możliwość graficznego odwzorowania środowiska sieciowego w postaci map i diagramów połączeń (rys. 1).

12 Wykresy

Na podstawie zebranych danych, system monitorujący może wygenerować wykresy, które w przejrzysty sposób pokazują stan urządzeń sieciowych w przedziale czasu. Jest to bardzo przydatne

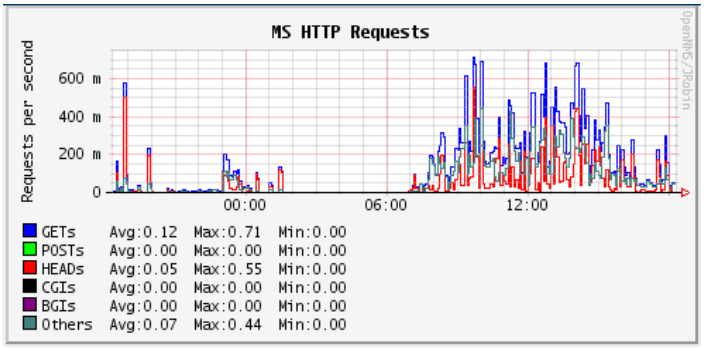
narzędzie, obrazujące np. dobowe obciążenie łącz, wykorzystanie pamięci i procesorów, a nawet zmiany temperatury w serwerowni. Pozwala to ocenić, czy urządzenia dysponują stosownym zapasem mocy obliczeniowej, czy łącza mają wystarczającą przepustowość, lub czy klimatyzator ma odpowiednią moc, by schłodzić serwery w czasie ich najintensywniejszego wykorzystania. Na podstawie tej wiedzy można przewidzieć wystąpienie problemów, i zawczasu podjąć działania, mające na celu dostosowanie infrastruktury sieciowej do bieżących wymagań.



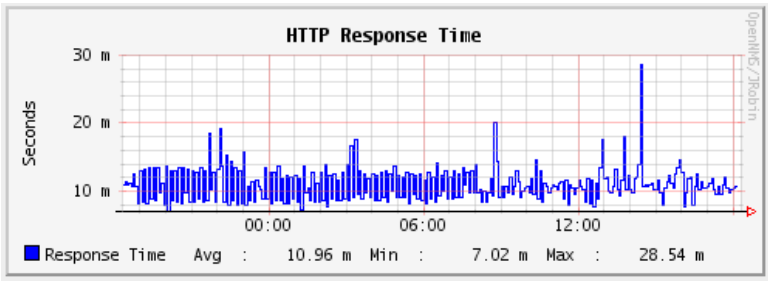
Rys. 1. Mapa topologii sieci

13 Wykresy usług

Wykresy usług obrazują stan poszczególnych usług, działających na danym hoście. Mogą obrazować np. ilość połączeń, typy zapytań (rys. 2) lub czasy odpowiedzi (rys. 3). Na ich podstawie można określić, czy usługi (a pośrednio aplikacje) działają prawidłowo.



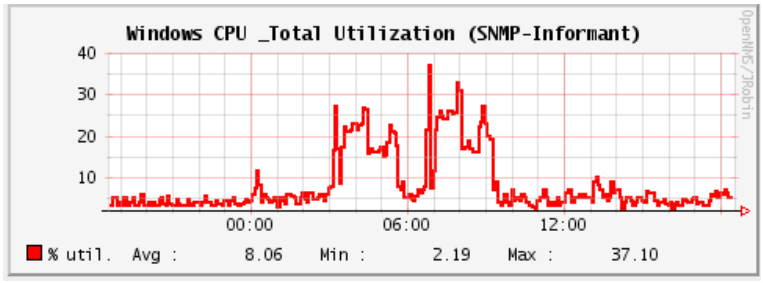
Rys. 2. Wykres zapytań do serwera HTTP



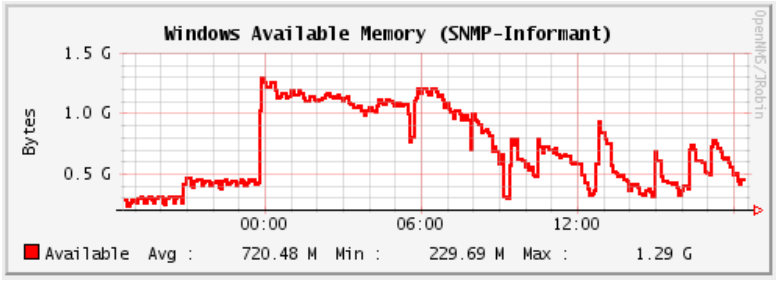
Rys. 3. Czas odpowiedzi usługi HTTP

14 Wykresy części składowych systemów

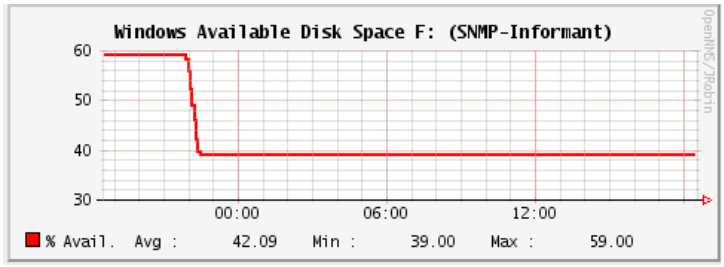
Wykresami części składowych systemu nazywa się wykresy użycia pamięci operacyjnej (rys. 5), procesora (rys. 4), dostępnej wolnej przestrzeni na dyskach (rys. 6) etc. Na ich podstawie można określić, czy warstwa sprzętowa jest w stanie w sposób płynny obsługiwać uruchomione na niej aplikacje.



Rys. 4. Dobowy wykres obciążenia procesora



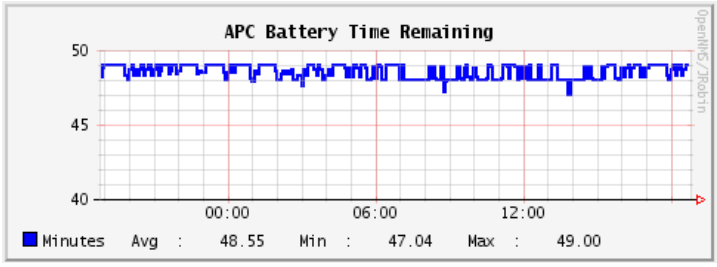
Rys. 5. Dobowy wykres użycia pamięci



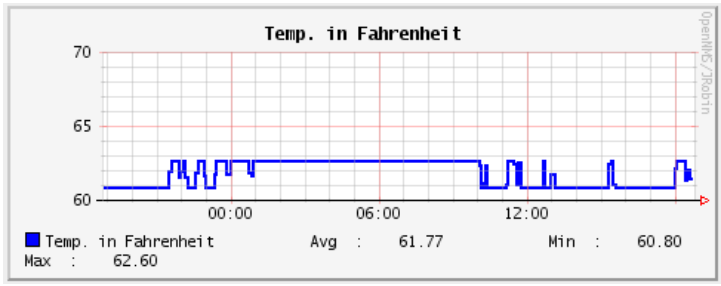
Rys. 6. Dobowy wykres dostępnego miejsca na dysku

15 Wykresy parametrów środowiska

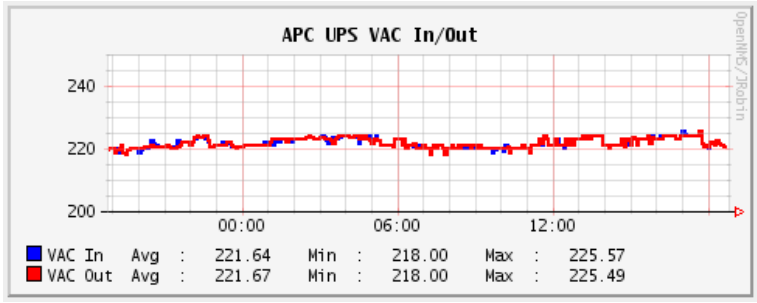
Wykresy parametrów środowiska obrazują takie parametry jak temperatura (rys. 8), wilgotność czy napięcie zasilania (rys. 9) i pozostały czas pracy na bateriach (rys. 7). Dzięki temu można ocenić, czy zastosowane urządzenia chłodnicze, agregaty prądotwórcze, zasilacze UPS etc. są dobrze dobrane i czy warunki środowiskowe nie zagrażają urządzeniom zainstalowanym w serwerowni. Wykresy tego typu przydają się do oceny ryzyka wystąpienia awarii lub do śledzenia przyczyn awarii.



Rys. 7. Dobowy wykres pozostałego czasu pracy zasilacza UPS



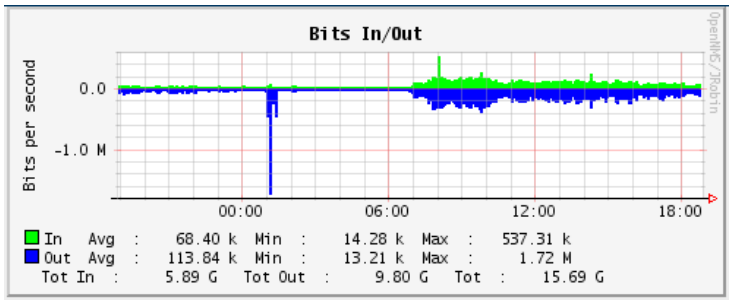
Rys. 8. Dobowy wykres temperatury w serwerowni



Rys. 9. Dobowy wykres napięcia zasilania w serwerowi

16 Wykresy użycia interfejsów sieciowych

Wykresy użycia interfejsów sieciowych pokazują, jaka ilość danych jest przesyłana do i z maszyny w jednostce czasu (rys. 10). Dodatkowo mogą pokazywać ilość błędów transmisji, ilość pakietów broadcast i multicast. Pozwala to ocenić, czy posiadane łącza internetowe są wystarczająco szybkie, aby przenieść realny ruch, oraz czy nie występują np. wycieki danych lub ataki DoS, na co mógłby wskazywać wzmożony ruch na interfejsie, w godzinach, w których teoretycznie serwer nie powinien mieć znaczącego obciążenia.

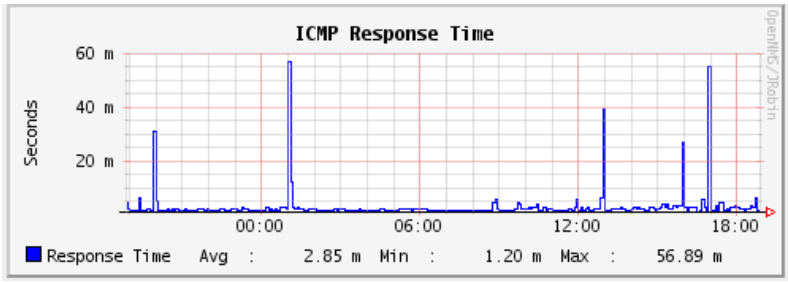


Rys. 10. Dobowy wykres użycia interfejsu sieciowego

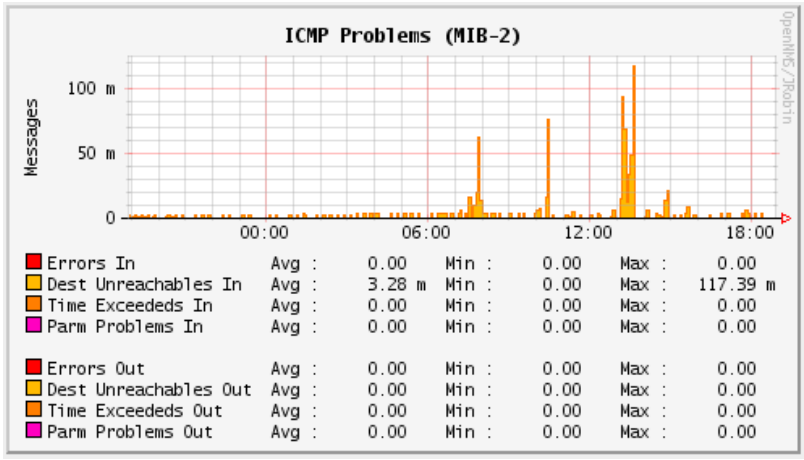
17 Wykresy stanu łącza

Wykresy stanu łącza pokazują poprawność działania połączeń sieciowych, np. łącz internetowych. Typową metodą badania stanu łącza jest wysyłanie pakietów ICMP (rys. 11). Należy badać nie tylko czasy

odpowiedzi, ale również rejestrować utraty pakietów (rys. 12), co może wskazywać na niepoprawne funkcjonowanie łącza, lub jego awarię.



Rys. 11. Dobowy wykres czasu odpowiedzi ICMP



Rys. 12. Dobowy wykres problemów ICMP

18 Zarządzanie komunikatami

Komunikaty generowane przez węzły sieci zawierają ostrzeżenia i informacje, są więc przydatnym narzędziem do oceny stanu nie tylko poszczególnych węzłów, ale również całej sieci. Niejednokrotnie zawierają kluczowe informacje, których wyciek mógłby zagrozić bezpieczeństwu całej sieci, a ich utrata uniemożliwiłaby skuteczną ocenę np. przyczyny awarii. Z tego względu komunikaty powinny być przechowywane w innym miejscu, niż są generowane – na przykład przekazywane do systemu monitorującego. Dzięki przekazywaniu komunikatów do systemu monitorującego istnieje pewność, że w przypadku awarii hosta,

który te komunikaty wygenerował, nie zostaną one bezpowrotnie utracone. Dodatkowo przechowywanie komunikatów ze wszystkich węzłów sieci w jednym miejscu sprawia, że ich przeglądane jest szybsze i efektywniejsze, ponieważ administrator nie musi logować się na każdej maszynie z osobna, aby zweryfikować stan usług i urządzeń. Dodatkowo należy zadbać o bezpieczeństwo serwera monitorującego, aby niepowołane osoby nie miały do niego dostępu, a komunikaty były przesyłane szyfrowanymi lub izolowanymi kanałami, uniemożliwiającymi podsłuchanie. W tym celu zaleca się stosowanie sieci VLAN lub dedykowanych przełączników oraz używanie szyfrowanych połączeń między monitorowanym węzłem a stacją monitorującą.

19 Monitorowanie przynależności adresów IP

Monitorowanie przynależności adresów IP polega na śledzeniu powiązań adresów IP z adresami fizycznymi MAC. Ma ono na celu wykrywanie błędów w konfiguracji interfejsów sieciowych, jak również błędów działania serwerów DHCP, czy wreszcie ataków sieciowych, polegających na celowym podszywaniu się pod inny adres IP lub duplikowanie adresu IP celem wywołania konfliktu i uniemożliwienia komunikacji np. z serwerem. System monitorujący może sprawdzać, jakie adresy MAC kryją się za zdefiniowanymi adresami IP i generować powiadomienie, jeśli doszło do ich zmiany. Aby ograniczyć możliwość występowania konfliktów IP pomiędzy przypadkowymi hostami a ważnymi serwerami, nie zaleca się umieszczania ich w tej samej domenie rozgłoszeniowej [5].

20 Technologie monitorowania sieci

Na potrzeby monitorowania sieci komputerowych powstało wiele narzędzi i protokołów, mających za zadanie testowanie poprawności ich działania, jak również automatyzowanie procesów zbierania danych o stanach poszczególnych węzłów.

21 ICMP

ICMP (ang. *Internet Control Message Protocol*, internetowy protokół komunikatów kontrolnych) – opisany w RFC 792 protokół warstwy sieciowej OSI/TCP/IP używany w diagnostyce sieci oraz trasowaniu. Komunikaty ICMP są narzędziami diagnostycznymi „wbudowanymi" w warstwę internetową. Jeśli dwa węzły sieci nie są w stanie komunikować się ze sobą, ICMP może pomóc w zdiagnozowaniu problemu. ICMP pełni również funkcję kontroli transmisji [9].

Pakiety typu ICMP są wykorzystywane przez popularne programy Ping i Traceroute, które są często używane przez systemy monitorujące sieci.

22 Ping

Ping jest nazwą programu używanego w sieciach komputerowych TCP/IP, służącego do testowania połączeń sieciowych. Jego zadaniem jest sprawdzenie, czy istnieje połączenie pomiędzy hostami. Umożliwia również pomiar liczby zgubionych pakietów oraz opóźnień w ich transmisji, zwanych lagami. Ping używa protokołu ICMP, wysyłając pakiety *ICMP Echo Request* i odbierając *ICMP Echo Reply*. Tego samego mechanizmu używają systemy monitorujące sieci do określenia dostępności węzłów.

23 Traceroute

Traceroute jest programem służącym do śledzenia trasy pakietów w sieciach TCP/IP. Do działania wykorzystuje protokoły komunikacyjne ICMP oraz UDP.

W pierwszej fazie Traceroute wysyła pakiet ICMP do docelowego hosta, z wartością TTL (Time To Live) ustawioną na 1. Wartość TTL jest zmniejszana o 1 przy przejściu przez każdy router, znajdujący się po drodze między hostem badanym i badającym. Po osiągnięciu wartości TTL równej 0, router odrzuca pakiet wysyłając zwrotny komunikat ICMP typu Time Exceeded. Na tej podstawie Traceroute określa adres IP pierwszego routera po drodze. W kolejnych fazach wartość TTL jest każdorazowo zwiększana o 1, aby uzyskiwać informacje o kolejnych routerach. Po dotarciu do docelowego wysyłany jest pakiet UDP na port o numerze wyższym od 30000, na którym zazwyczaj nie działają żadne usługi. W odpowiedzi host przesyła wiadomość ICMP Port Unreachable, co kończy śledzenie trasy.

Systemu monitorujące mogą używać Traceroute do sprawdzania, czy droga pakietów wewnątrz sieci jest zgodna z założoną. Rozbieżności mogą wskazywać np. problemy z łączami operatorskimi czy protokołami routingu.

24 SNMP

SNMP (Simple Network Management Protocol) jest rodziną protokołów sieciowych, używanych do zarządzania urządzeniami pracującymi w sieci komputerowej, takimi jak przełączniki, routery, komputery, serwery etc. Domyślnie protokół SNMP wykorzystuje dwa

porty UDP do komunikacji, port 161 do przesyłania żądań i odbierania odpowiedzi, oraz port 162 do odbierania sygnałów Trap, jednak możliwe jest wykorzystanie innych portów, oraz protokołu TCP.

Zaistnieją cztery wersje protokołu SNMP [10]:

- SNMPv1 – Opublikowana w 1988 roku, pierwsza wersja protokołu, opisana w RFC 1157. v1 nie zapewnia rozsądnego poziomu bezpieczeństwa, ponieważ opiera się na hasłach communities, które są przesyłane przez sieć w nieszyfrowanej postaci.
- SNMPv2 – Opisana w RFC 1441 wersja posiada znaczące ulepszenia w dziedzinie wydajności oraz bezpieczeństwa, jednak zastosowany w niej nowy model bezpieczeństwa nie przyjął się.
- SNMPv2c – Opisana w RFC 1901. Jest to wersja v2, jednak pozbawiona nowego modelu bezpieczeństwa. Zamiast niego zastosowano model oparty na hasłach communities znany z v1.

SNMPv3 – Opisana w RFC 3411 wersja v3 zwiększa bezpieczeństwo poprzez wprowadzenie rozwiązań kryptograficznych i zaawansowanego uwierzytelniania.

Protokół SNMP zakłada istnienie w zarządzanej sieci urządzeń zarządzanych i zarządzających. Urządzeniem zarządzającym jest urządzenie, na którym uruchomiony jest zarządca SNMP (SNMP manager), zbierający dane ze stacji zarządzanych. Urządzeniem zarządzanym jest każde urządzenie, na którym uruchomiony jest agent SNMP, odpowiedzialny za zbieranie danych i przesyłanie ich do urządzenia zarządzającego.

SNMP wykorzystuje bazy informacji zarządzania MIB (Management Information Base), czyli zbiory zmiennych, jakie zarządca SNMP, w zależności od uprawnień, może odczytać lub ustawić. W tym celu zarządca SNMP komunikuje się z agentem SNMP, działającym na zarządzanym urządzeniu, podając jedno ze zdefiniowanych wcześniej haseł community, odpowiednio:

- public_community – hasło do odczytu
- private_community – hasło do zapisu

Każdy odczytywany lub zapisywany komunikat dotyczy określonego identyfikatora obiektu OID (Object IDentifier). Na przykład identyfikator zmiennej sysUpTime ma postać 1.3.6.1.2.1.1.3.0, co odpowiada jego adresowi w drzewie MIB.

Odczytanie określonej zmiennej daje zarządcy informacje na temat stanu danego elementu sieci, natomiast zapis do określonej zmiennej umożliwia sterowanie zachowaniem urządzenia lub zmienia jego konfigurację [18].

Oprócz odczytywania i zapisywania zmiennych OID, SNMP oferuje również opcje automatycznego przesyłania do managera komunikatów o zmianach stanów OID w postaci komunikatów Trap (v1) lub Inform (v2 i v3).
W pierwszej wersji protokołu SNMP dostępne były następujące komunikaty:

- Get – żądanie informacji na temat jednej pozycji z bazy MIB
- GetNext – żądanie przesłania następnej pozycji
- Set – zapis wartości pozycji MIB do agenta
- Response – zwrócenie żądanych informacji do zarządcy
- Trap – samoistnie przesłana informacja do zarządcy

W wersji drugiej dodano komunikaty:

- GetBulk – żądanie jak największej ilości informacji w jednej ramce
- Inform – informacja Trap, wymagająca potwierdzenia

Wersja trzecia nie dodała nowych komunikatów.

25 RMON

Remote Network MONitoring (RMON) jest standardem monitorowania sieci komputerowych. Jest dobrym uzupełnieniem dla SNMP, ponieważ w odróżnieniu od SNMP, który służy do badania stanu urządzeń, RMON potrafi analizować ruch sieciowy. Przy jego pomocy można uzyskać informacje odnośnie używanych protokołów i aplikacji [14]. Aplikacje RMON działają w oparciu o architekturę klient/serwer. Klient jest uruchamiany na stacji monitorującej i służy do prezentacji danych RMON. Serwerami są elementy instalowane w różnych miejscach sieci – zbierają one informacje RMON i analizują pakiety przesyłane przez dany segment sieci. Urządzenia monitorujące noszą nazwę sond. Sonda współpracuje z oprogramowaniem instalowanym w pamięci węzła sieci, będące niczym innym jak agentem systemu RMON. Agenci są instalowani w hubach, routerach, przełącznikach itd. Agent komunikuje się ze stacją zarządzania korzystając z usług protokołu SNMP [8]. Sondy RMON definiują szereg dodatkowych grup baz danych MIB. Dane gromadzone w tych bazach służą do dokładnego analizowania pracy danego urządzenia lub całego segmentu sieci LAN. Nowe bazy danych MIB zakładane przez sondy RMON, instalowane w sieciach Ethernet to:

- Statistics – statystyki, np. wykorzystanie, kolizje, błędy CRC
- History – historia statystyk

- Alarm – definicja progów, po przekroczeniu których wysyłane są komunikaty RMON SNMP Trap
- Host – dane specyficzne dla konkretnych hostów, np. ilość ramek in/out
- HostTopN – przedstawia N najaktywniejszych hostów w sieci
- Matrix – przedstawia siatkę połączeń pomiędzy hostami w sieci
- Filter – definicja typu danych, jakie mają być zbierane przez RMON
- Capture - możliwość przechwytywania i przekazywania określonych pakietów zdefiniowanych w Filter
- Event – wysyłanie SNMP Trap po przekroczeniu progów Alert

26 Pakiet OpenNMS

OpenNMS jest wysoce skalowalnym systemem do monitorowania i zarządzania zarówno niewielkimi, jak i rozległymi, bardzo rozbudowanymi sieciami komputerowymi. Jest rozwijany w oparciu o wolna licencję GNU General Public License, co za tym idzie ma doskonałe wsparcie społeczności oraz zespołu OpenNMS Group, który oferuje również komercyjne wsparcie.

System monitorujący jest napisany w Javie, więc może działać na dowolnej platformie sprzętowej i programowej, która wspiera Java SDK. Do pobrania są gotowe kompilacje na systemy Windows, Linux, Solaris i OS X. Poza Javą, OpenNMS wykorzystuje bazę danych PostgreSQL i na chwilę obecną nie ma możliwości wykorzystania innej bazy.

27 Zalety i wady OpenNMS

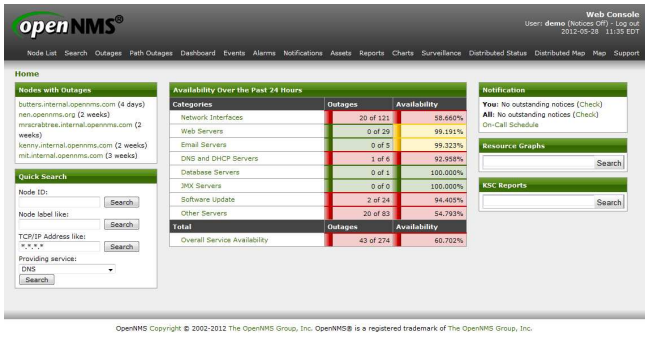
W przeciwieństwie do innych platform monitorujących, OpenNMS nie wymaga instalacji agentów na monitorowanych urządzeniach. Wiele konkurencyjnych produktów do monitorowania sieci wymaga instalacji agentów (np. Nagios), bez których nie działają wcale, lub oferują jedynie podstawową funkcjonalność. OpenNMS jest w stanie sprawdzać dostępność urządzeń i status usług używając standardowych protokołów, takich jak ICMP, SSH, http FTP etc. I na ich podstawie buduje wykresy dostępności i czasu odpowiedzi. Do monitorowania bardziej zaawansowanych funkcji urządzeń i ich stanów używany jest protokół SNMP, przy pomocy którego odczytywane są takie parametry jak obciążenie, dostępne miejsce itp. Dodatkowo urządzenia można skonfigurować tak, aby przesyłały komunikaty SNMP Trap do serwera.

Drugą rzeczą przemawiającą na korzyść OpenNMS jest brak podziału na wersję płatną, oferująca wszystkie funkcje i darmową, oferująca jedynie podstawowe możliwości. W wypadku OpenNMS niezależnie od tego, czy zostało wykupione komercyjne wsparcie i usługa wdrożenia, czy pakiet został pobrany za darmo z Internetu, jest to ten sam, w pełni funkcjonalny produkt.

Na obecną chwilę wsparcie dna IPv6 jest prowizoryczne, tylko niektóre wtyczki potrafią go obsłużyć. Kolejnym minusem jest brak współpracy z innymi bazami danych niż PostgreSQL.

28 Konfiguracja i zarządzanie

Do zarządzania programem służy napisany w Javie interfejs webowy, który domyślnie działa pod kontrolą wbudowanego w aplikację serwera Jetty (rys. 13). Przy jego pomocy można zarówno konfigurować podstawowe funkcje monitorowania, jak również zarządzać bazą monitorowanych urządzeń i usług oraz przeglądać zdarzenia, wykresy i alarmy. Bardziej zaawansowane funkcje konfiguruje się edytując bezpośrednio odpowiednie pliki XML.



Rys. 13. Interfejs OpenNMS

29 Wyszukiwanie i dodawanie urządzeń

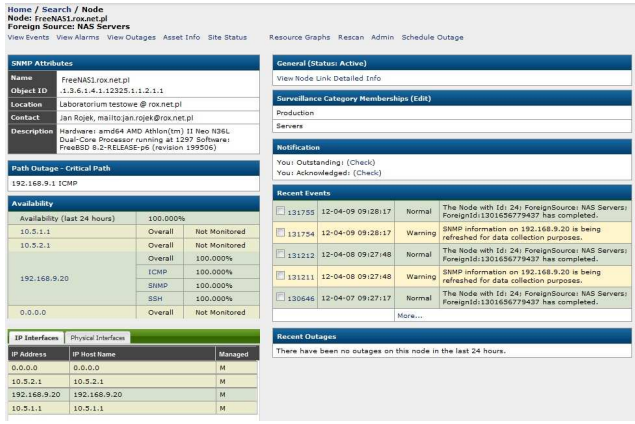
OpenNMS udostępnia dwa sposoby dodawania urządzeń do monitorowanych grup. Pierwszy z nich jest w pełni zautomatyzowany i polega na wykrywaniu urządzeń i usług działajacych w zdeklarowanych podsieciach. Oprócz automatycznego wykrywania, urządzenia można dodawać manualnie, podając pojedyncze adresy IP i działające na nich usługi. Konfiguracja wyszukiwania zapisana jest w plikach XML, więc ustawień można dokonać zarówno przez interfejs webowy jak i poprzez manualną ich edycję.

30 Zbieranie danych

OpenNMS jest w stanie zbierać dane z różnych protokołów, między innymi SNMP, WMI, JMX i NSClient. Zebrane dane mogą być przedstawiane w postaci list i wykresów, oraz sprawdzane pod względem osiągania wartości krytycznych, generujących alarmy.

31 Monitorowanie

Do monitorowania urządzeń pracujących w sieci, OpenNMS używa ogólnie dostępnych metod, takich jak sprawdzanie dostępności z użyciem ICMP i SNMP, czy nawiązywanie sesji TCP z usługami HTTP, FTP, SSH etc. Możliwe jest również sprawdzanie stron internetowych pod kątem występowania określonych treści, oraz korzystanie z wtyczek pakietu Nagios i dostęp do usługi WMI (Windows Management Instrumentation). Oprócz stanu usług i ich dostępności, badane są również czasy odpowiedzi usług i opóźnienia sieciowe.



Rys. 14. Widok monitorowanego węzła

Domyślnie OpenNMS sprawdza dostępność urządzeń, korzystając z cyklu pięciominutowego (tj. co pięć minut sprawdza węzły, usługi itd.). Po wykryciu awarii rozpoczyna się sprawdzanie usługi co trzydzieści sekund przez pięć minut. Po zakończeniu procesu awaria zostaje uznana za poważną, a system powraca do monitorowania w cyklu pięciominutowym przez dwanaście godzin. Jeżeli po upływie dwunastu godzin okaże się, że usługa w dalszym ciągu nie działa, częstotliwość monitorowania zostaje zredukowana do przedziałów dziesięciu minutowych na pięć dni. Po tym czasie usługa zostaje oznaczona jako „niezarządzana” i przestaje być monitorowana. Ustawienia te można zmienić edytując plik poler-configuration.xml.

Zasadniczo OpenNMS nie wymaga instalacji agentów na monitorowanych węzłach, jednak można ich używać w celu pasywnego monitorowania urzadzeń i usług, znajdujących się za zaporami ogniowymi. Należy zauważyć, że OpenNMS nie posiada własnego agenta, może jednak używać np. Net-SNMP lub NSClient++.

Rysunek 14 przedstawia widok monitorowanego węzła.

32 Zarządzanie zdarzeniami

Stan dostępności badanych urządzeń, oraz komunikaty otrzymywane przy użyciu protokołów monitoringu, są zapisywane w systemie jako zdarzenia. Na ich podstawie mogą być podejmowane określone akcje, lub generowane inne zdarzenia. Akcją może być na przykład wysłanie powiadomienia. Standardowo OpenNMS ma zaprogramowane akcje dla najbardziej popularnych i uniwersalnych zdarzeń, takich jak utrata dostępności węzła lub usługi, istnieje jednak możliwość przypisania akcji do każdego zdarzenia, jakie może zostać odnotowane przez system monitorujący.

Zdarzenia są automatycznie klasyfikowane pod względem powagi. OpenNMS wyróżnia zdarzenia:

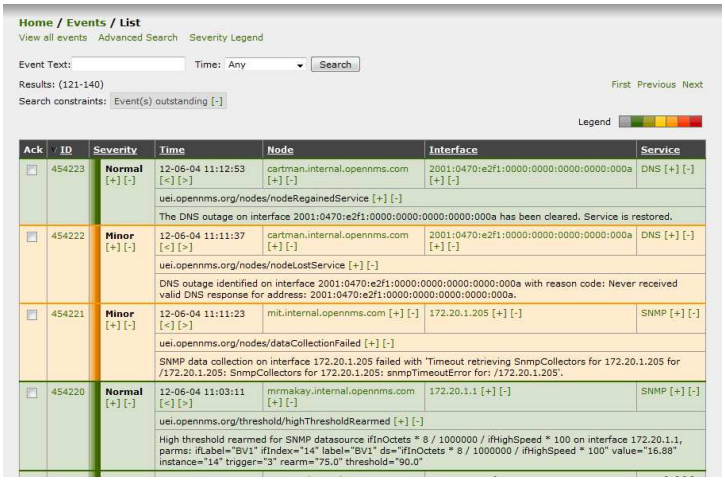
- Krytyczne (Critical) – wiele urządzeń w sieci jest niedostępnych, wymagana jest natychmiastowa akcja
- Poważne (Major) – urządzenie jest niedostępne, lub jego stan grozi niedostępnością
- Znaczące (Minor) – jedna ze składowych węzła (usługa, interfejs) jest niedostępna
- Ostrzeżenie (Warning) – wystąpiło zdarzenie wymagające uwagi lub odnotowania, jednak nie wymaga natychmiastowej akcji
- Niezdefiniowane (Undefined) – powaga zdarzenia nie jest zdefiniowana
- Normalne (Normal) – zdarzenia informacyjne nie wymagające podejmowania akcji

Rysunek 15 przedstawia widok listy zdarzeń.

33 Powiadamianie

OpenNMS korzysta z koncepcji ścieżek docelowych, która stanowi listę metod powiadamiania, stosowanych kolejno do momentu potwierdzenia alarmu. Umożliwia to przesyłanie powiadomień w określonej kolejności i przy pomocy różnych metod do różnych osób. Standardowo obsługiwane jest przesyłanie powiadomień przy użyciu poczty elektronicznej i komunikatora XMPP, jednak możliwe jest

definiowanie własnych metod, w tym wywoływanie zewnętrznych programów i przekazywanie do nich określonych informacji. W dalszej części tej pracy opisany został proces dodawania własnej ścieżki docelowej, polegającej na wysyłaniu wiadomości SMS przez modem UMTS, podłączony do serwera.



Rys. 15. Lista zdarzeń

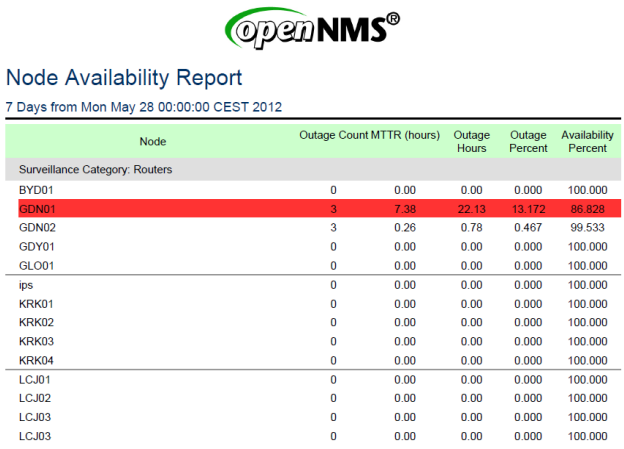
34 Raporty i wykresy

Dane zbierane przez OpenNMS mogą być prezentowane w postaci wykresów i raportów. System oferuje wiele raportów domyślnych (ogólna dostępność usług, dostępność w przedziale czasu, statystyki dla wybranych grup urządzeń itd.) oraz pozwala tworzyć nowe rodzaje raportów. Raporty mogą być opracowywane zgodnie z harmonogramem i automatycznie przesyłane pocztą elektroniczną, można również przygotowywać je na żądanie. Do wyboru są dwa formaty wyjściowe raportów: PDF i CSV [16].

Rysunek 16 przedstawia widok wygenerowanego raportu dostępności węzłów.

Wykresy obrazują zmiany parametrów w czasie dla hostów, dla których zostały zebrane stosowne dane przy pomocy protokołów SNMP i ICMP. Dostępne są tutaj wykresy dla wszystkich parametrów udostępnianych i skonfigurowanych na konkretnym węźle. Do generowania wykresów używany jest pakiet JRobin.

Rysunek 17 przedstawia widok wykresów powiązanych z konkretnym węzłem.

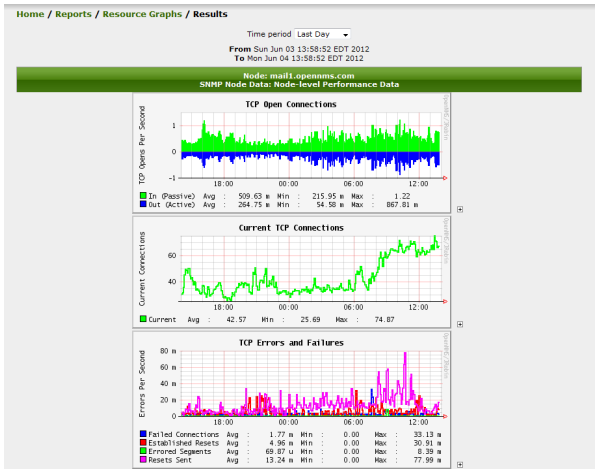


Node Availability Report

7 Days from Mon May 28 00:00:00 CEST 2012

Node	Outage Count	MTTR (hours)	Outage Hours	Outage Percent	Availability Percent
Surveillance Category: Routers					
BYD01	0	0.00	0.00	0.000	100.000
GDN01	3	7.38	22.13	13.172	86.828
GDN02	3	0.26	0.78	0.467	99.533
GDY01	0	0.00	0.00	0.000	100.000
GLO01	0	0.00	0.00	0.000	100.000
ips	0	0.00	0.00	0.000	100.000
KRK01	0	0.00	0.00	0.000	100.000
KRK02	0	0.00	0.00	0.000	100.000
KRK03	0	0.00	0.00	0.000	100.000
KRK04	0	0.00	0.00	0.000	100.000
LCJ01	0	0.00	0.00	0.000	100.000
LCJ02	0	0.00	0.00	0.000	100.000
LCJ03	0	0.00	0.00	0.000	100.000
LCJ03	0	0.00	0.00	0.000	100.000

Rys. 16. Raport dostępności



Rys. 17. Przeglądanie wykresów

35 Podsumowanie

Celem pracy było stworzenie kompleksowego systemu monitorującego infrastrukturę sieciową, który zgromadzi w jednym miejscu informacje o dostępności urządzeń oraz dane statystyczne, przedstawi je w przystępny sposób, oraz powiadomi odpowiednie osoby o wszelkich nieprawidłowościach.

W pracy wykazałem, że dobry system monitorujący wcale nie musi być drogi, a jego wdrożenie trudne i czasochłonne. Przedstawiony przeze mnie system monitorujący OpenNMS jest w pełni darmowy,

dodatkowo może działać na większości systemów operacyjnych, w tym na darmowych dystrybucjach systemu Linux. Jego instalacja i konfiguracja jest na tyle prosta, że każdy administrator sieci będzie w stanie samodzielnie ją wykonać, a w razie problemów do jego dyspozycji będzie obszerna pomoc techniczna, podręczniki oraz kilka for internetowych, na których można spotkać twórców pakietu.

Literatura

[1] Buechler C. M., Pingle J., *The Definitive Guide*. Reed Media Services, 2009

[2] Cihar M., Gammu SMSD Daemon Manual/ http://wammu.eu/docs/pdf/smsd.pdf

[3] Comer D. E., *Sieci komputerowe i intersieci*. Helion, 2012

[4] Dybikowski Z., PostgreSQL / Helion, 2001

[5] Fry C., Nystorm M., Monitoring *i bezpieczeństwo sieci*. Helion 2010

[6] Gentoo Linux Wiki, Huawei E220. http://en.gentoo-wiki.com/wiki/Huawei_E220

[7] Hill Benjamin M., Harris D., Vyas J., *Debian GNU/Linux 3.1. Biblia*. Helion, 2006

[8] ITpedia, RMON, http://itpedia.pl/index.php/RMON

[9] Janus R., Cała prawda o protokole ICMP. http://www.netfocus.pl/raporty/planowanie-zarzadzanie-monitorowanie-sieci/cala-prawda-o-protokole-icmp

[10] Mauro D., Schmidt R., Kevin J., *Essential SNMP*. O'Reilly Media, 2005

[11] Nemeth E., Garth S, Hein Trent R., Whaley Ben, *Unix i Linux*. *Przewodnik administratora systemów*. Helion, 2011

NETWORK INFRASTRUCTURE MONITORING WITH THE USE OF THE "OPENNMS"

Summary – The main topic of the article is to create a comprehensive monitoring system network infrastructure using free tools, in this package of OpenNMS. Described are: installation, configuration and use of the

package, as well as the configuration of network devices to the monitoring system. As runtime package used was a free Linux operating system.