Studia i Materiały Informatyki Stosowanej, Tom 12, Nr 2, 2020
str. 10-15

Monitoring urządzeń sieciowych i raportowanie poprzez aplikacje Spektrum oraz Performance Management firmy CA Technologies

Ireneusz Bednorz

Student 1 rok MU Informatyka, Instytut Informatyki
Uniwersytet Kazimierza Wielkiego w Bydgoszczy

Streszczenie: *Artykuł opisuje podstawowe zagadnienia sieciowe, modele warstwowe, protokoły internetowe, główne komponenty oraz integracje miedzy aplikacjami Spektrum oraz Performance Management firmy CA. Głównym celem badania było ukazanie mechanizmu, w jaki sposób Spectrum monitoruje konkretne zdarzenie zwiększenia zużycia pamięci RAM na urządzeniu Router 1, a następnie stworzenie raportu w aplikacji Performance Management w celu ukazania tego zdarzenia na wykresie. Skupiłem się na ukazaniu jak ważny jest monitoring urządzeń sieciowych w obecnym świecie informatyki, aby móc w porę rozwiązać zdarzenie, które potencjalnie może wskazywać usterkę na urządzeniu i przeciwdziałać występowaniu takich problemów w przyszłości.*

Słowa kluczowe: *aplikacja mobilna, niania elektroniczna, IoT.*

Abstract: *The article describes basic network issues, layered models, Internet protocols, main components and integrations between Spectrum and Performance Management applications of CA. The main aim of the study was to show how Spectrum monitors a specific event of increased RAM consumption on Router 1 device, and then to create a report in the Performance Management application to show this event on a graph. I focused on showing how important it is to monitor network devices in the current IT world in order to be able to solve in time an event that potentially indicates a malfunction on the device and counteract the occurrence of such problems in the future.*

Key words: *mobile application, electronic nanny, IoT.*

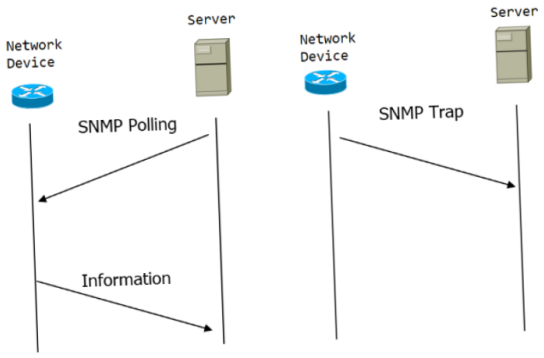
1. Wprowadzenie

Monitoringiem w IT nazywa się proces gromadzenia danych na temat działającego sprzętu i oprogramowania, aby zapewnić, ze wszystko działa zgodnie z oczekiwaniami. Rozwój monitoringu nastąpił w wyniku ogromnego zapotrzebowania na środowisko, w którym jesteśmy w stanie zarządzać ogromna ilością urządzeń sieciowych z jednego komputera centralnego. Daje to możliwość regularnego wykonywania pomiarów na urządzeniach całą dobę, niezależnie od lokalizacji. Możemy odciążyć nasz zespół IT dostosowując aplikacje monitorujące względem naszych potrzeb i stosując automatyzacje, aby informowały nas o tym, co jest najważniejsze. Jeżeli nie chcemy, aby urządzenia się przegrzały. W aplikacji ustawiamy alarmy, i to na wielu stopniach. Dzięki temu nie musimy się martwic o spalone komponenty. Zdarzenia mogą być dostarczane na wiele sposobów np. e-mail czy tez SMS, co pozwala na natychmiastowe działanie. Ulepszenia w monitoringu sieciowym są proste do wykonania, ale niekoniecznie tanie. Obecnie większość urządzeń jest wykonana modularnie, dając możliwość dodawania nowych komponentów na bieżąco. Kluczowym aspektem monitorowania urządzeń jest możliwość wykrycia usterki, zanim wyrządzi ona ogromne szkody i koszta dla firmy. Jest to najważniejszy cel monitoringu w informatyce. CA Technologies stworzyła rozwiązania pomagające w monitoringu sieciowym takie jak Spectrum i Performance Management. CA Technologies, obecnie zwana Broadcom Inc. jest globalnym liderem technologicznym w dziedzinie infrastruktury, opartych na rozwiązaniach inżynieryjnych i współpracy, bazując na zaawansowanych mechanizmach technicznych od AT&T/Bell Labs, Lucent i Hewlett-Packard/Agilent. Broadcom koncentruje się na technologiach, znajdujących się na całym świecie. Dzięki połączeniu liderów branży Avago Technologies, LSI, Broadcom Corporation, Brocade i CA Technologies, firma jest w stanie iść dalej naprzód, gdzie przyszłość stoi otworem. Broadcom Inc. łączy w sobie ogromna ilość rozwiązań, czy to inżynieryjnych, czy tez bazujących na oprogramowaniu dla infrastruktury półprzewodnikowej, daje to możliwości budowania i dalszego rozwoju firm klienckich.

Alternatyw dla wspomnianych wcześniej aplikacji jest wiele: Nagios, SolarWinds czy Intermapper to tylko kilka możliwych. Jednak są to już dosyć przestarzałe rozwiązania. Dla urządzeń sieciowych Spectrum i Performance Management [1, 2] wydają się lepszym rozwiązaniem gdyż mają większe możliwości konfiguracyjne otrzymywanych powiadomień i ich częstotliwości. Można dodawać szczegółowe informacje na temat każdego urządzenia lub typu alarmu, aby rozwiązanie problemu przebiegało jeszcze łatwiej i szybciej. Nie wymagają dodatkowych urządzeń monitorujących działania aplikacji. Topologia urządzeń zapewnia ogólny przegląd architektury sieci. Wykrywanie urządzeń jest proste i bezpieczne dzięki zastosowaniu odpowiednich protokołów.

2. Protokół konfiguracyjno-sterujący Simple Network Management Protocol

SNMP to zbiór protokołów sieciowych, działających w warstwie aplikacji modelu ISO/OSI działający na portach 161/162, które wykorzystuje się do sterowania i konfiguracji urządzeń sieciowych, takich jak routery, switche, komputery, czy centrale telefoniczne. Wszystko funkcjonuje za pośrednictwem sieci IP. Port 161 jest odpowiedzialny za wysyłanie i odbieranie żądań, natomiast 162 za przechwytywanie komunikatów. SNMP posiada komunikat zwany pułapką (ang. trap), można ja utożsamić jako alarm, który będzie monitorować pewna wartość, a gdy wartość monitorowana przekroczy zdefiniowany uprzednio próg, np. użycie pamięci RAM, agent bezzwłocznie powiadomi o tym fakcie zarządcę. Ideą tego działania jest zbieranie informacji z kilku/kilkunastu urządzeń sieciowych jednocześnie, oraz monitorowanie każdej własności urządzenia: liczby użytkowników online, ilość wolnego miejsca na dyskach, obciążenie pamięci, zużycie procesora, temperatury.
SNMP Poll jest drugim sposobem zbierania danych z urządzeń sieciowych. W przeciwieństwie do pułapek gdy urządzenie sieciowe tj. router lub switch posiadają informacje po prostu ją przesyłają nie czekając na zapytanie serwera. Poll działa, gdy serwer żąda informacji, a urządzenia sieciowe musza się podporządkować i ja dostarczyć (rys. 1).



Rysunek. 1. Różnica miedzy trap a poll.

Może to być ustawione czasowo, np. co dziesięć minut wykonaj SNMP Poll do urządzenia serwerowego, odsyłając aktualny pomiar temperatury otoczenia jak i urządzenia badanego, jego obciążenie procesora i pamięci RAM, a te wartości dalej zostaną sprawdzone czy nie przekraczają zakresów bezpieczeństwa.
Wyróżnia się 3 wersje protokołu SNMP:

- SNMPv1 - pierwsza wersja protokołu, opublikowana w 1988 roku w dokumencie RFC 1067, jest najstarsza wersja protokołu, prosta do konfiguracji, lecz jednocześnie najbardziej niebezpieczna przez używane tzw. „communities", czyli nieszyfrowanych haseł, umożliwiających zarządzanie urządzeniem,
- SNMPv2 i jego podwersja SNMPv2c - eksperymentalna wersja protokołu SNMP, opublikowana w dokumencie RFC 1901. Jego atutem względem wersji pierwszej były: poprawiona obsługa błędów, poprawione komendy SET, komenda Inform: w przeciwieństwie do "trap", które są po prostu wysyłane do zarządcy, Inform muszą mieć pozytywna wiadomość zwrotna, a jeśli zarządca nie odpowie na Inform, SNOP wyśle ponownie Inform,
- SNMPv3 - trzecia i zarazem ostatnia wersja protokołu, która umożliwia uwierzytelnianie i szyfrowanie komunikacji.

3. Spectrum

Aplikacja Spectrum firmy CA śluzy głównie do monitorowania w czasie rzeczywistym urządzeń sieciowych, zbierania danych z elementów sieciowych, aktualizowanie statusu urządzeń oraz generowania alarmów poprzez otrzymane z nich trapy, jeśli zostały one certyfikowane wcześniej w Event Configuratorze.

Proces Monitorowania urządzeń oraz generowania alarmów aplikacji Spectrum firmy CA odbywa się w następujących krokach:

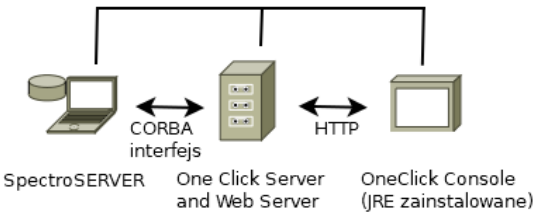
- zbieranie danych zawartych w niej elementów sieciowych równocześnie w bazie danych aktualizując ich status,
- generowanie alarmu z otrzymanej pułapki, który był wcześniej certyfikowany w aplikacji,
- informacje z wygenerowanego alarmu przesyłane są do SANM (ang. Spectrum Alarm Notification Manager), który przy wykorzystaniu polis ustala do jakiej aplikacji przetwarzającej alarmy będzie on przesyłany dalej, jeśli spełni on wymogi zdefiniowane w filtrach.

Sercem aplikacji jest komponent zwany SpectroSERVER. Jest on jednoczesnie serwerem bazodanowym przechowujacym informacje o

procesach zachodzących w aplikacji - silnikiem, który modeluje urządzenia sieciowe oraz menedżerem urządzeń. To dzięki niemu zapewniany jest proces generowania alarmów z wcześniej certyfikowanych wydarzeń (ang. events), czyli główny proces Spectrum. Baza danych SpectroSERVERa znajduje się w katalogu /opt/SS oraz zawarte są w niej następujące informacje: po pierwsze spis modeli wykrytych przez SpectroSERVERa serwera, do których należą;

- informacje na temat modeli oraz relacji zachodzących miedzy nimi potrzebnych do graficznej reprezentacji topologii sieci, w których te urządzenia się znajdują;
- logi z procesami o obecnie generowanych się alarmach, jeśli nastąpi brak komunikacji z Archive Managerem, który jest odpowiedzialny za ich nadzorowanie.

Drugim najważniejszym komponentem jest Archive Manager. Jest on odpowiedzialny za otrzymywanie alarmów oraz dane statystyczne, które otrzymuje od SpectroSERVERa. Dane te ulegają kompresji i przechowywane sa w bazie danych DDM (ang. Distributed Data Manager) - jest to druga najważniejsza baza danych. SpectroSERVER, gdy nie może nawiązać komunikacji z Archive Managerem przejmuje cześć jego funkcji i zaczyna przechowywać wszelkie dane na temat alarmów w swojej bazie danych. Po nastąpieniu ponownego połączenia z Archive Managerem, SpectroSERVER wysyła wszelkie zgromadzone dane do Archive Managera. W katalogu /opt/Spectrum/.vnmrc można określić, ile informacji na temat urządzeń ma przechować baza danych SpectroSERVERa podczas braku połączenia z Archive Managerem. Natomiast to, jak długo dane historyczne będą przechowywane znajdziemy w pliku konfiguracyjnym opt/Spectrum/SS/DDM/.configrc.
Trzecim, ostatnim najważniejszym komponentem jest graficzny interfejs użytkowników aplikacji Spectrum firmy CA nosi on nazwę OneClick. Jest on napisany za pomocą Javy. Korzysta on z dwóch komponentów umożliwiających zdalny dostęp użytkownikom aplikacji JNLP (ang. Java Network Launch Protocol) oraz JWSA (ang. Java Web Start Application). Komunikacja OneClick'a z siecią następuje przy użyciu portu 80 dla systemów Windows lub portu 8080 dla systemów Linux. Poniższy rysunek przedstawia połączenie miedzy SpectroSERVERem przy użyciu interfejsu CORBA wraz z serwerem OneClick'a oraz jego konsola" (rys. 2).



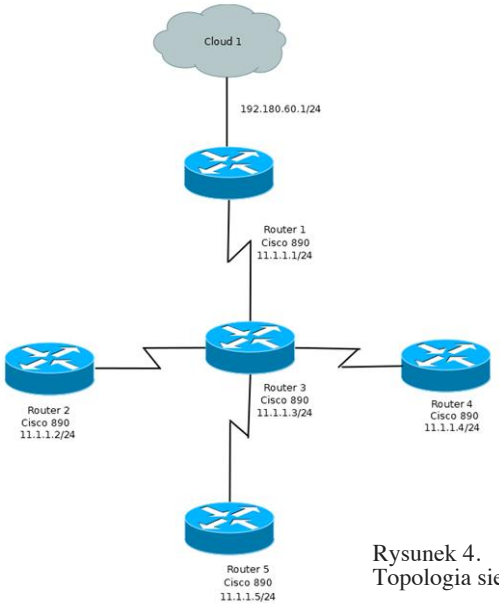
Rysunek 2. Połączenie miedzy SpectroSERVERem przy użyciu interfejsu CORBA wraz z serwerem OneClick oraz jego konsolą

Środowisko, na którym pracowałem, zostało stworzone przy użyciu programu firmy Vmware o nazwie Vmware Workstation Player w wersji 15.0.2 (rys. 3).

Procesor	4 Rdzeniowy
Pamięć RAM	6 GB
System Operacyjny	RedHat 7.0 w wersji 64 bitowej
Graficzny Interfejs użytkownika	Motif (32-bit)
Dysk Twardy	200 GB
Paczki	W wersji 64 bitowej : elfutils-libelf, libaio, ncurses, ncurses-libs, xterm, ksh, xorg-x11-fonts-misc W wersji 32 bitowej oraz 64 bitowej : motif, glibc, nss-softokn-freebl, libICE, libSM, libX11, libXext, libXft, libXmu, libXp, libXrender, libXt, fontconfig, freetype, libjpeg-turbo, libpng, libuuid, libxcb, libXau, expat, zlib, libstdc++, libgcc, libXi, libXtst
Komponenty Java	W 64 bitowej wersji : Java 8.0 Java 2 Run-time Environment (JRE) wersja 1.8.0_31 JCEUnlimited Strength Files wersja 1.8.0_31"[3]

Rysunek 3. Parametry wykorzystanej maszyny wirtualnej

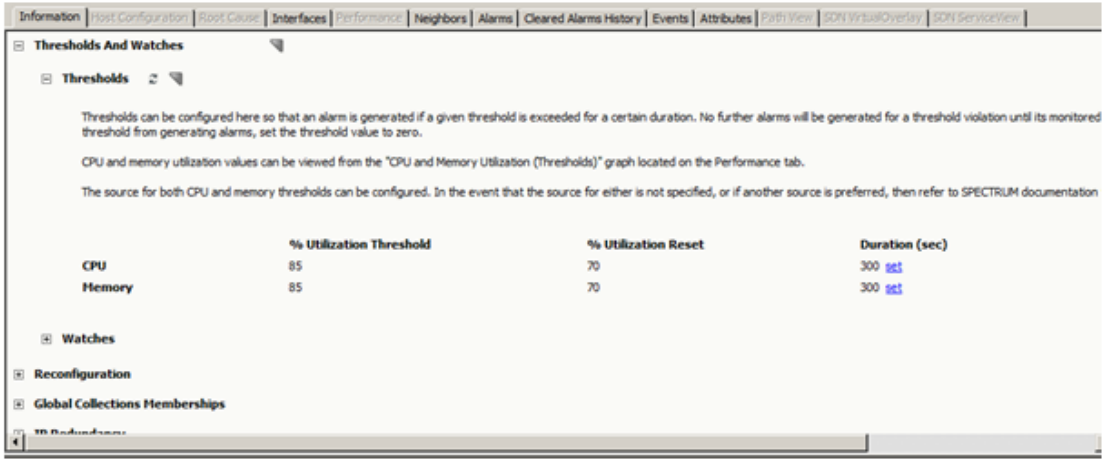
Użyta siec składa się z 5 routerów, z których interfejs maszyny wirtualnej (Cloud 1) jest połączony z jednym z routerów (Router 1), któremu zapewnia ona monitoring poprzez oprogramowanie Spectrum oraz PM firmy CA, reszta urządzeń będzie przedstawiona w oprogramowaniu jako Cloud (rys. 4).



Rysunek 4.
Topologia sieci.

4. Generowanie alarmu na użycie pamięci RAM na urządzeniu Router 1

Aplikacja Spectrum firmy CA umożliwia także generowanie alarmów poprzez polling urządzeń sieciowych przy użyciu protokołu SNMP. Jedna z wielkości, jakie możemy w ten sposób monitorować, jest użycie pamięci RAM (ang. Random Access Memory) monitorowanego urządzenia. W zakładce information urządzenia Router 1 przechodząc do opcji Thresholds And Watches widnieją ustawienia generowania alarmu na podstawie zdefiniowanych opcji (rys. 5).



Rysunek 5. Zakładka Thresholds and Watches urządzenia Router 1

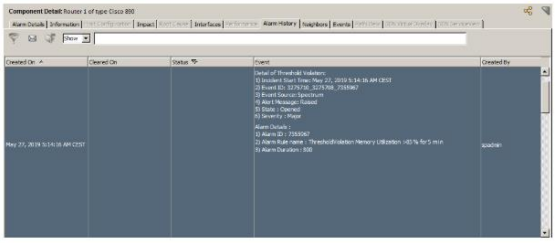
Najważniejszą wartością w zakładce Thresholds and Watches jest Utilization Treshold, który odpowiada procentowej wartości, po której przekroczeniu zostanie wygenerowany event na urządzeniu. Utilization Reset odpowiada za usuniecie alarmu, jeśli wartość spadnie poniżej ustalonej wielkości. Duration to czas podany w sekundach, przez który musi się utrzymać event, aby powstał z niego alarm.
Na urządzeniu Router 1 zostało sztucznie podniesione użycie pamięci RAM w celu wygenerowania alarmu. Użycie pamięci RAM urządzenia Router 1 wyświetlane jest za pomocą komendy show processes memory (rys. 6).

```
Router 1#show processes memory

Total: 5611448, Used: 5330875, Free: 280573
  PID  TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
    0    0     199592       1236        220          0          0 *Init*
    0    0        400      76928        400          0          0 *Sched*
    0    0    5431176     140052     140760     349780          0 *Dead*
    1    0        256        256       1724          0          0 Load Meter
    2    0        264          0       5032          0          0 Exec
    3    0          0          0       2724          0          0 Check heaps
    4    0      97932          0       2852      32760          0 Pool Manager
    5    0        256        256       2724          0          0 Timers
    6    0         92          0       2816          0          0 CXBus hot stall
    7    0          0          0       2724          0          0 IPC Zone Manager
    8    0          0          0       2724          0          0 IPC Realm Manager
    9    0          0          0       2724          0          0 IPC Seat Manager
   10    0        892        476       3256          0          0 ARP Input
   11    0         92          0       2816          0          0 SERIAL A'detect
   12    0        216          0       2940          0          0 Microcode Loader
   13    0          0          0       2724          0          0 RFSS watchdog
   14    0   15659136   15658584       3276          0          0 Env Mon
...
   77    0        116          0       2844          0          0 IPX-EIGRP Hello
                                    2307224 Total
```

Rysunek 6. Użycie pamięci RAM przez urządzenie Router 1

Powstały ze zdarzenia alarm widnieje w polu Alarm History (rys. 7).



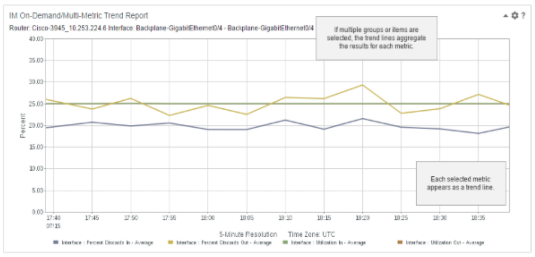
Rysunek 7. Alarm powstały ze zdarzenia odnośnie przekroczenia dopuszczalnego poziomu zużycia pamięci RAM przez urządzenie Router 1

5. Opis CA Performance Management

CA Performance Management to narzędzie, które monitoruje, przechowuje, analizuje i wyświetla ogromna ilość informacji w celu zapewnienia jakości usług w obrębie dużej, złożonej oraz wielopoziomowej infrastruktury sieciowej. Rozwiązanie to pomaga największym sieciom skutecznie kontrolować jakość oferowanych usług, a jednocześnie obniżając koszty monitorowania urządzeń. Dostawcy usług telekomunikacyjnych mogą używać tej aplikacji do poprawy monitorowania sieci i dostarczania usług generujących przychody, takich jak 4G LTE, Voice over LTE i inne. Performance Management wykorzystuje rozszerzalna architekturę wielu serwerów do obsługi monitorowania największych sieci. Gromadzi dane dotyczące wydajności i integruje się z innymi źródłami danych.

6. Raportowanie w CA Performance Management

Jednym z wielu mechanizmów, które udostępnia nam Performance Management jest raportowanie. Raporty te są bardzo przydatne dla klientów, mogą oni dzięki nim sporządzać sprawozdania i monitorować, czy z ich urządzeniem nie działo się nic złego, oraz zapobiegać na przyszłość powstałym anomaliom. Raporty na zadanie pobierają zbiory danych z określonych zestawów elementów lub grup bez tworzenia pulpitów. Można dodać raporty na zadanie do stron kontekstowych grup i urządzeń. W zależności od tego, jaki raport chcemy stworzyć musimy przejść do konkretnych zakładek. Raport na zadanie tworzymy w zakładce Reports - On-Demand Report Templates, gdzie możemy stworzyć nowy szablon albo skorzystać z już istniejących. Wymagane dane do stworzenia szablonu to: tytuł, nazwa, typ szablonu, częstotliwość próbkowania oraz urządzenie bądź wcześniej stworzona grupę, które chcemy monitorować biorąc pod uwagę, jakie dane chcemy uzyskać. To, jakie dane możemy uzyskać, jest zależne od rodzaju monitorowanego urządzenia bądź interfejsu.



Rysunek 8. Przykładowy wykres z strony CA przedstawiający jeden wykres z wieloma danymi.

Dzięki raportowaniu możemy sprawdzić interesujące nas zdarzenia. Alarm, który powstał na urządzeniu Router 1 informuje nas o przekroczeniu progu użycia pamięci RAM. Aby stworzyć dla klienta taki raport (rys. 9), który pokaże mu, ze zdarzenie miało miejsce, używamy wcześniej wspomnianych już narzędzi. Takie raporty są z reguły przygotowywane wcześniej. Są odpowiednio zaplanowane jako codzienne, tygodniowe bądź comiesięczne wysłanie do klienta. Przygotowany tu raport jest z konkretnego dnia, aby pokazać, ze problem zaistniał i aplikacja go zaobserwowała.

Rysunek 9. Raport pokazujący przekroczenie dopuszczalnego progu zużycia RAM na urządzeniu

6. Podsumowanie

Dwie aplikacje Spectrum oraz mechanizm raportowania w Performance Management są tylko częścią możliwości, jakie oferują te aplikacje. Podstawowe działanie dwóch aplikacji, Spectrum oraz Performance Management pokazują jak łatwo zautomatyzować monitoring na urządzeniach oraz jak szybko można uzyskać wszelkie informacje na temat działania urządzenia. Dzięki tak szybkiemu wykrywaniu błędów w działaniu urządzeń oraz możliwości przeglądania raportów, jest możliwe zapobieganie poważniejszym problemom

technicznym, które mogą spowodować zatrzymanie świadczonych usług, co może przełożyć się na ogromne straty dla firm. Alarmowanie w aplikacji Spectrum pozwala na szybka reakcje oraz na zminimalizowanie krytycznych w skutkach awarii urządzeń. Poprzez wykrycie konkretnego problemu na urządzeniach można od razu przystąpić do naprawy zaistniałej usterki. Mechanizm raportowania w Performance Management pozwala na dostarczanie informacji dla użytkowników środowiska, w którym znajdują się monitorowane urządzenia. Następuje to w sposób zaplanowany za pomocą generowania raportów dziennych, tygodniowych czy miesięcznych. Dają one możliwość przeanalizowania statystyk i tego co działo się na urządzeniu z dużą dokładnością w czasie, nawet gdy zdarzenie miało miejsce w przeszłości. Umożliwia to zapobieganie przeciążeniom w planowanych operacjach bądź po prostu dają informacje, ze infrastruktura jest za słaba i trzeba ja rozbudować, aby działała sprawnie.

Bibliografia

1. C. Technologies, “Spectrum,” online: https://techdocs.broadcom.com/us/product-content/recommended-reading/product-documentation/spectrum-900-documentation.html.
2. C. Technologies, “Ca performance management,” online: https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operations-management/performance-management/3-7.html.