SIECI | CENTRUM DANYCH | KOMUNIKACJA | TESTY I PORÓWNANIA | BEZPIECZEŃSTWO | ROZWIĄZANIA DLA MSP

Networld

PRZEDRUK

WRZESIEŃ 2015 (9/227) INDEKS 328820 CENA 26,90 ZŁ (W TYM 5% VAT) www.networld.pl

SERWERY
POD SPECJALNYM NADZOREM

JAK KONTROLOWAĆ PRACĘ CENTRUM DANYCH

ISSN 1232-8723

SIECIOWI BRUTALE
Dlaczego tak trudno zwalczać ataki sieciowe typu *brute force*

MODERNIZACJA SERWEROWNI
Założenia modernizacji infrastruktury zasilania i chłodzenia serwerowni

SERWERY
POD SPECJALNYM NADZOREM

Tomasz Kowalczyk

W centrum danych nie wystarczy pilnować tylko pracy samych aplikacji. Pracuje tam bowiem wiele innych systemów mających istotny wpływ na poprawne funkcjonowanie całej serwerowni.

Osoby odpowiedzialne za prowadzenie centrów danych wiedzą, jak ważne jest monitorowanie znajdujących się w nim urządzeń, panujących warunków fizycznych oraz poboru prądu. Nie da się zarządzać czymś, czego się nie monitoruje. Systemy monitoringu dają administratorom wgląd w to, co dzieje się w serwerowni, umożliwiając m.in. optymalizację jej pracy czy szybkie wykrywanie problemów. Jednak przy obecnym stopniu skomplikowania centrów danych niezbędne jest dokładne monitorowanie parametrów jej pracy, aby uniknąć różnych zagrożeń informatycznych i fizycznych.

MONITORING SIECI

Obszernym zagadnieniem jest monitorowanie sieci w serwerowniach. Administratorzy muszą śledzić ogólną wydajność sieci, status poszczególnych urządzeń, wydajność serwerów i aplikacji, komunikację w sieci. Zadaniem systemów monitorowania sieci jest wykrywanie awarii urządzeń oraz problemów w komunikacji sieciowej, głównie spadku szybkości transferu danych. Problemy w działaniu sieci wynikają z przeciążania lub awarii serwerów, czy też zakłóceń w komunikacji sieciowej. Mogą być spowodowane awarią sprzętu lub błędami ludzi.

Systemy monitorujące mogą badać wiele komponentów, m.in. aplikacje (serwery pocztowe, WWW itd.), urządzenia końcowe (serwery) oraz samą sieć (np. przełączniki i routery). Administrator powinien przygotować spis urządzeń i aplikacji, które chce monitorować. To pomoże określić, jakie parametry powinny być monitorowane, wskazać, jakie zdarzenia będą sygnalizowane alertami wysyłanymi do administratorów oraz w jaki sposób te alerty będą przesyłane. System monitorowania o wykrytych problemach może powiadamiać administratora, wysyłając mu wiadomość e-mail lub SMS. Narzędzia monitorujące dostarczają dwa typy alertów: czasu rzeczywistego oraz historyczne. Te pierwsze informują administratorów o problemach, które wymagają szybkiej reakcji, np. awarii serwera czy uszkodzeniu okablowania. Historyczne alerty są przechowywane w logach, co pozwala np. przygotować zestawienie najczęściej występujących problemów lub ustalić, kiedy w ciągu dnia występują znaczne wzrosty natężenia ruchu.

Rozwiązania do monitorowania sieci kontrolują stan działania różnych elementów serwerowni, wysyłając w stałych odstępach czasu określone sygnały na różne porty urządzeń i oczekując na odpowiedź (z reguły jest to prosty komunikat ping). Sygnały są wysyłane w bardzo różnych odstępach czasu (liczonym w sekundach, minutach, a nawet godzinach), w zależności od monitorowanego systemu.

Oprogramowanie do monitoringu powinno być na tyle skalowalne, żeby uwzględniać przyszłą rozbudowę sieci. Nie jest to tylko kwestia skalowania wraz z rozbudową serwerowni, ale możliwość obsługi nowych aplikacji, które z czasem mogą pojawić się w firmowej sieci.

Możliwe jest również kontrolowanie poprawności działania różnych protokołów sieciowych, m.in. HTTP, HTTPS, SNMP, FTP, SMTP, POP3, IMAP, DNS, SSH, TELNET, SSL oraz TCP. Jeśli chodzi o serwery WWW, narzędzia monitorujące mogą wysyłać żądania HTTP do serwera, aby określić, czy działa on poprawnie. Z kolei przypadku serwerów pocztowych udaje się periodycznie wysyłać testowe wiadomości e-mail poprzez protokół SMTP, choć będą one odbierane przez protokoły IMAP lub POP3. Wysyłając takie wiadomości, można emulować typową ścieżkę przesyłania wiadomości elektronicznych i sprawdzać stan sieci oraz serwerów, przez które ta wiadomość przechodzi. Najczęściej mierzonym parametrem jest czas odpowiedzi urządzeń, ale na tej podstawie można prowadzić też inne statystyki, np. obliczać poziom dostępności. Jednak narzędzia monitorowania sieci mogą również sprawdzać spójność i niezawodność

Monitoring sieci – wybrane parametry

- RTT (Round-Trip Time) – czas potrzebny do pokonania przez pakiety drogi z punktu A do B i z powrotem,
- czas odpowiedzi aplikacji – zależy od obciążenia samej aplikacji i natężenia ruchu w sieci,
- odsetek utraconych pakietów,
- nieautoryzowane próby dostępu,
- opóźnienia wynikające z kolejkowania pakietów.

działania aplikacji oraz sprzętu IT.

Jeśli narzędzie do monitorowania sieci nie otrzyma odpowiedzi na wysłane żądanie, uzna to za przejaw awarii, która może skutkować np. brakiem odpowiedzi na żądania wysyłane przez użytkowników. Objawy takiej awarii obserwowane przez użytkowników to brak odpowiedzi przy próbach dostępu do usług internetowych czy aplikacji albo problemy z wysłaniem wiadomości e-mail. W takiej sytuacji narzędzie do monitorowania sieci podejmie zdefiniowaną akcję. Mogą to być różne czynności, najczęściej jednak chodzi o wysłanie alertu do administratora sieci. Alternatywnie, automatyczne systemy omijania awarii są w stanie odłączyć problemowy serwer do czasu, aż zostanie naprawiony.

Oprogramowanie do monitoringu powinno być na tyle skalowalne, żeby uwzględniać przyszłą rozbudowę sieci. Nie jest to tylko kwestia skalowania wraz z rozbudową serwerowni, ale możliwość obsługi nowych aplikacji, które z czasem mogą pojawić się w firmowej sieci. Jednak skalowalność ma swoją cenę. Rozwiązania klasy korporacyjnej są bardzo kosztowne, dlatego nie należy wybierać rozwiązań, które oferują większą skalowalność, niż faktycznie jest potrzebna.

Oferowane bezpłatnie lub na licencji *open source* narzędzia do zarządzania siecią są tanie, a jednocześnie stanowią solidną alternatywę do komercyjnych narzędzi do administrowania i monitorowania systemów IT. Dobra wiadomość jest taka, że każdy z tych produktów powinien dobrze sprawdzić się w firmowej sieci. Zła jest taka, że trzeba podjąć wysiłek samodzielnego poznania ich obsługi.

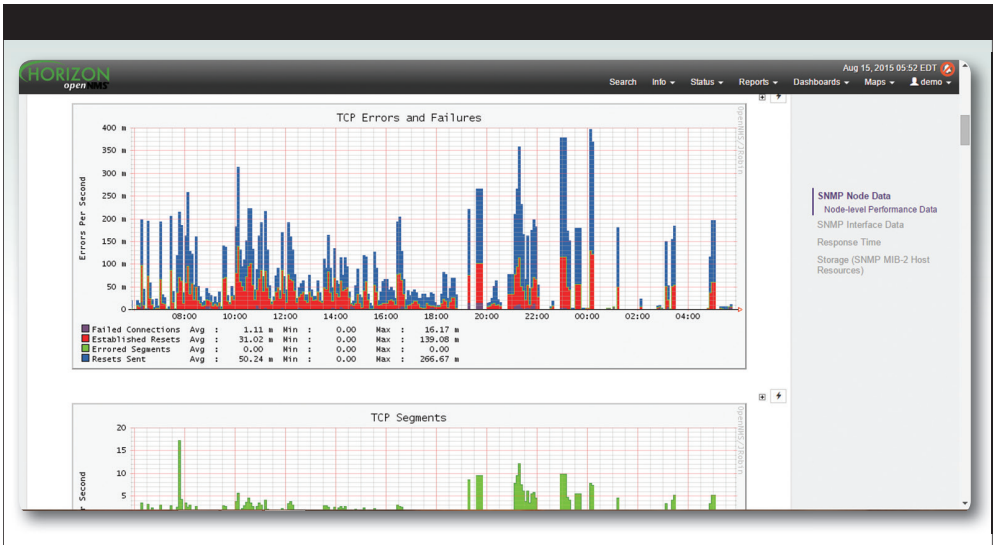
Istotną kwestią jest też podejście producentów do pojęcia *open source*. Z niewielkimi wyjątkami, np. OpenNMS, większość stosuje model *open core*. Nie odnosi się on do licencjonowania oprogramowania, lecz do jego funkcjonalności. W przypadku *open core* producent udostępnia na otwartej licencji tylko podstawowe wersje oprogramowania, a jednocześnie oferuje jeden lub więcej produktów komercyjnych, wyposażonych w dodatkowe funkcje.

Kluczową sprawą, aby system monitorowania działał skutecznie, jest właściwe ustawienie wartości progowych. Producenci sprzętu podają wartości referencyjne, ale nie można stosować ich bezkrytycznie. Często konieczne są inne wartości uwzględniające lokalne czynniki, np. sposób rozmieszczenia sprzętu w serwerowni.

PARAMETRY FIZYCZNE

W centrum danych monitorowania wymaga nie tylko temperatura, ale także wilgotność oraz możliwość pojawienia się mechanicznych uszkodzeń kabli lub przewodów z chłodziwem. Podstawą skutecznego monitorowania tych parametrów jest odpowiednie rozmieszczanie sensorów pomiarowych.

Czujniki temperatury montuje się przede wszystkim przy wlotach powietrza do urządzeń w szafach stelażowych. Często stosowanym rozwiązaniem jest umieszczanie czujników w górnej, dolnej oraz środkowej części przednich drzwi szaf. Temperaturę powietrza w pomieszczeniu regulują klimatyzatory. Wykrycie zbyt



Oprogramowanie OpenNMS można przetestować, korzystając z wersji demo uruchamianej bezpośrednio na stronie tego projektu.

wysokiej temperatury wlotowej może świadczyć o awarii urządzenia chłodzącego, co grozi przegrzaniem serwerów i innych urządzeń znajdujących się w danej szafie, lub skrócić czas ich eksploatacji w wyniku nadmiernego zużycia spowodowanego niekorzystnymi warunkami pracy. Ważne jest również pilnowanie, aby temperatura nie była za niska, ponieważ to powoduje niepotrzebny wzrost kosztów chłodzenia.

Kolejnym parametrem do śledzenia jest wilgotność. Zbyt suche powietrze może powodować gromadzenie się ładunków elektrycznych na urządzeniach i prowadzić do szkodliwych przepięć. Natomiast zbyt duża wilgotność prowadzi do osadzania się pary wodnej, co grozi powstawaniem zwarć. Czujniki wilgotności są domyślnie zamontowane w klimatyzatorach. Żeby dokonywać wiarygodnych pomiarów w większej liczbie miejsc, czujniki należy montować z dala od wylotów powietrza z klimatyzatorów. Wystarczy zamontować jeden czujnik w korytarzu zimnego powietrza na środku rzędu lub w szafie.

Istotnym elementem systemów chłodzenia są kablowe i punktowe czujniki nieszczelności.

Umożliwiają bowiem szybkie zlokalizowanie wycieków płynu chłodzącego, chroniąc pomieszczenia przed zalaniem. W ten sposób można zabezpieczyć infrastrukturę IT przed uszkodzeniem i zminimalizować ewentualne straty finansowe. Kablowe czujniki nieszczelności powinny być porozmieszczane wokół każdego systemu CRAC (Computer Room Air Conditioning) i przy każdym przewodzie, w którym istnieje ryzyko wycieku. Z kolei czujniki punktowe stosuje się w miskach ściekowych i nisko położonych miejscach, aby móc wykryć podwyższony poziom płynu i regulować jego poziom, gdy zajdzie taka potrzeba.

Serwerowni zagraża nie tylko zalanie, ale także pożar, którego szybkie wykrycie umożliwiają czujniki dymu. Montowane są wewnątrz szaf, a więc w obszarach o podwyższonym zagrożeniu wystąpienia dymu i ognia, lub w miejscach, w których nie przewidziano specjalnych sensorów. Czujniki dymu często są standardowym wyposażeniem budynku, ale montowane pod sufitem nie zawsze są w stanie zapewnić wymaganą czułość, nie są również w stanie określić dokładnej lokalizacji źródła zagrożenia.

Jeśli w serwerowni używa się akumulatorów z ogniwami mokrymi, trzeba dodatkowo zamontować czujniki wodoru. Ten gaz może się bowiem wydzielać z tego rodzaju

POWIADAMIANIE O ALARMACH NMS W PRZYPADKU BRAKU POŁĄCZENIA INTERNETOWEGO

WYPOWIEDŹ EKSPERTA

Radosław Janowski
Product Manager

Obecne systemy NMS mają wiele możliwości powiadamiania o zmianie statusu monitorowanych urządzeń. Najczęściej wykorzystywane są powiadomienia typu push (w interfejsie graficznym systemu NMS, w aplikacji mobilnej), wiadomości e-mail, wiadomości SMS. System NMS za pomocą tych kanałów powiadamia odbiorców o wykrytych brakach odpowiedzi, przekroczonych dopuszczalnych progach wykorzystania zasobów lub innych nietypowych sytuacjach w środowisku systemów IT. Ale co się dzieje, kiedy awarii ulega połączenie internetowe? Czy wówczas odbiorcy komunikatów z systemów NMS tracą możliwość reagowania, ponieważ kanały alarmowania zostają przerwane? Czy taka sytuacja może negatywnie wpłynąć na ciągłość procesów biznesowych w firmie?

Jeśli chcemy zredukować do minimum sytuacje, w których alarmy z systemu NMS nie docierają do odbiorców, warto pomyśleć o zdefiniowaniu drugiego kanału powiadamiania jako backupu do głównej metody informowania o krytycznych awariach. Na przykład, jeśli jako głównej metody powiadamiania o alarmach w systemie NMS używamy powiadomień push, warto rozważyć ustawienie drugiej, zapasowej metody powiadamiania wykorzystującej wiadomości SMS. Przy czym, aby taka konfiguracja była niezawodna, wiadomości SMS należy wysyłać bezpośrednio do sieci GSM, wykorzystując do tego celu sprzętową bramkę SMS. Bramka tego typu wysyła wiadomości SMS bezpośrednio do operatora, czyli niepotrzebne jest połączenie internetowe, co pozwala na skrócenie do minimum ścieżki krytycznej pomiędzy serwerem NMS a siecią GSM. Tym samym zwiększamy niezawodność całego kanału powiadamiania. Przy odpowiednim ustawieniu opóźnienia dla drugiego kanału powiadamiania możemy uniknąć podwójnych alarmów, reagując na czas na alarm z pierwszego kanału.

Przykładem sprzętowej bramki SMS jest urządzenie SMSEagle. Bramka polskiego producenta umożliwia automatyczną wysyłkę alertów SMS, tokenów SMS, konwertowanie wiadomości e-mail na SMS. Urządzenie jest wyposażone w zewnętrzną antenę o zysku 3.5dBi, co jest szczególnie ważne w miejscach ze słabym zasięgiem sieci GSM, takich jak serwerownie, centra danych. Wewnętrzny agent SNMP umożliwia monitorowanie wydajności bramki. Urządzenie jest odpowiedzią na zapotrzebowanie profesjonalistów, którzy stawiają na niezawodność i łatwą integrację z istniejącymi systemami IT. Ze względu na gotowe pluginy do 18 systemów NMS jest to niezwykle przydatne narzędzie dla administratora centrum danych.

SMSEagle
hardware sms gateway

akumulatorów. W przypadku akumulatorów VRLA czujniki wodoru nie są potrzebne.

CENTRALA

System zbudowany z samych czujników byłby niekompletny. Potrzebna jest również centrala, która zbiera odczyty. Komunikacja między centralą a czujnikami odbywa się za pośrednictwem protokołu IP. Kluczową sprawą, aby system działał skutecznie, jest właściwe ustawienie wartości progowych. Producenci sprzętu podają pewne wartości referencyjne, ale nie można stosować ich bezkrytycznie. Często konieczne są inne wartości uwzględniające lokalne czynniki, np. sposób rozmieszczenia sprzętu w serwerowni.

Na podstawie zebranych danych centralny system podejmuje różne działania: wysyła alerty (jeśli dojdzie do przekroczenia wartości progowych lub ich kombinacji) lub archiwizuje dane oraz tworzy wykresy i raporty. Administrator systemu może wskazać różne osoby, które będą otrzymywały alerty, np. kierownika czy pracownika przebywającego na miejscu, aby szybko zareagować na powstały problem. Alerty mogą być wysyłane jako wiadomości SMS lub e-mail, ale mogą także mieć inną formę, np. pułapek SNMP czy wiadomości wysyłanych na serwer HTTP. Oprócz alertów system może podejmować też zaprogramowane czynności, np. wyłączać problemowe urządzenia.

POMIAR ZASILANIA

Konsorcjum Green Grid opracowało dwie metryki służące do mierzenia zużycia zasilania przez centrum danych: PUE (Power Usage Effectiveness) oraz DCIE (Data Center Infrastructure Efficiency). Te metryki są używane, aby porównywać ilość prądu, którą centrum danych zużywa na chłodzenie, z ilością prądu zużywaną przez urządzenia IT. Pierwszy z tych parametrów, PUE, to współczynnik określający proporcje całej energii elektrycznej zużywanej na zasilanie centrum danych do energii elektrycznej zużywanej przez urządzenia IT. Jego

Oprogramowanie monitorujące – przegląd narzędzi

GroundWork Monitor Community Edition – narzędzie dostępne od 2004 roku. To pierwsze oprogramowanie *open source* przeznaczone do monitorowania sieci korporacyjnych. Integruje około setki różnych projektów *open source*, w tym Nagios, Apache oraz Nmap, w jedną platformę, oraz wprowadza dodatkowe funkcje, np. webową konsolę administracyjną. Rozwiązanie to umożliwia centralne monitorowanie i zarządzanie siecią korporacyjną, wliczając urządzenia sieciowe, serwery z systemami Windows, Linux i Unix oraz działające w nich aplikacje.

OpenNMS – oprogramowanie napisane w Javie skupia się na zbieraniu danych i zarządzaniu zdarzeniami i powiadomieniami. Aktywna społeczność użytkowników zawsze chętnie pomoże w rozwiązaniu problemów. Aplikacja obsługuje szereg systemów operacyjnych, m.in. Windows, Linux, Solaris i OS X. Testową instalację OpenNMS można wypróbować na stronie producenta.

OpenQRM – rozwiązanie przeznaczone do monitorowania centrów danych, może zarządzać nawet tysiącami serwerów Linux i Windows, jak również śledzić wykorzystanie zasobów. Pozwala na zautomatyzowanie raportowania na podstawie zdefiniowanych reguł. Za monitorowanie odpowiada zintegrowane oprogramowane Nagios.

Zenoss Core – większość kodu tego oprogramowania napisano w Pythonie. Oferuje funkcje zarządzania zdarzeniami, monitorowania wydajności serwerów, urządzeń sieciowych, systemów operacyjnych i aplikacji. Może działać w systemach Linux, FreeBSD oraz Mac OS X. Aby uruchomić je w Windows, należy wykorzystać oprogramowanie VMware Player i wirtualną maszynę z zainstalowanym Zenoss.

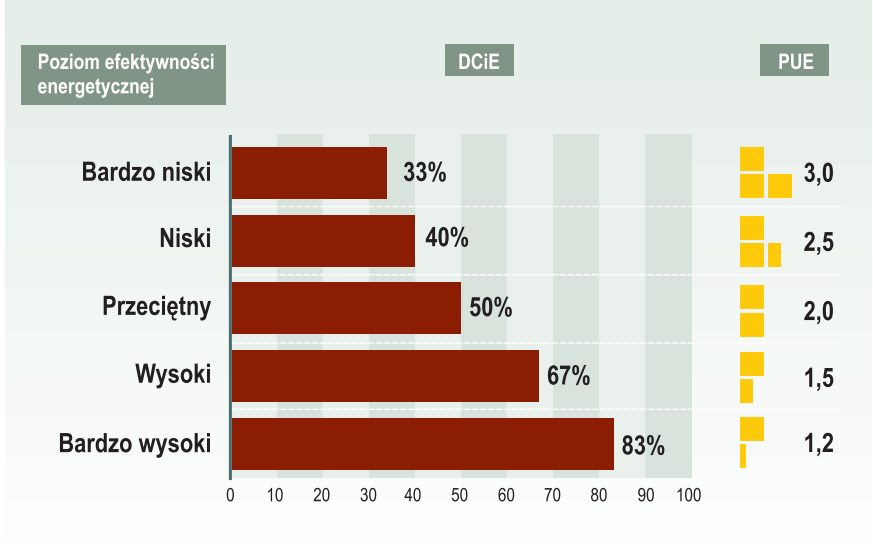
Nagios – program działa w systemie Linux i umożliwia monitorowanie urządzeń sieciowych, aplikacji oraz serwerów. Zaletą tego rozwiązania jest możliwość korzystania z wtyczek rozszerzających jego funkcjonalność. Aplikacja powstała ponad 10 lat temu i w tym czasie dorobiła się dużej liczby użytkowników oraz aktywnej społeczności, wśród której można szukać wsparcia technicznego (na forum internetowym).

MRTG (Multi Router Traffic Grapher) monitoruje i wizualizuje na bieżąco ruch na łączach sieciowych. Tworzy również wykresy dziennie, tygodniowe i miesięczne.

SolarWinds Orion Network Performance Monitor (Orion NPM) to oprogramowanie do monitorowania sieci stworzone z myślą o prostocie obsługi. Firma Solarwinds jest znana z wielu solidnych bezpłatnych narzędzi sieciowych.

Spiceworks IT Management – bezpłatne narzędzie do monitorowania sieci i wykrywania problemów. Ma dużą liczbę aktywnych użytkowników i interfejs, który niemal dowolnie można dostosowywać do własnych potrzeb.

Interpretacja parametrów DCiE i PUE



wartość powinna być mniejsza od 2. Jednocześnie im bliżej 1, tym lepiej. Mniejsza wartość tego współczynnika oznacza bowiem, że mniejszy odsetek energii jest zużywany na zasilanie i chłodzenie. Najbardziej efektywne energetycznie centra danych (Google'a czy Facebooka) chwalą się wartością PUE schodzącą poniżej 1,1. Co istotne, zamierzeniem autorów PUE oraz DCiE nie było stworzenie metryk do porównywania ze sobą różnych centrów danych. Niestety, to nie powstrzymuje niektórych przed publikowaniem wartości PUE, aby zareklamować swoją lokalizację czy skuteczność strategii prowadzenia centrum danych. Wysiłkom mającym na celu poprawę tych współczynników należy przyklasnąć, ale same w sobie nie są one odpowiednie, aby porównywać efektywność działania dwóch różnych centrów danych. W takim porównaniu należałoby jeszcze uwzględnić wiele innych aspektów, m.in. poziom wykorzystania infrastruktury IT i stosowanych technologii. Co bowiem z tego, że centrum danych ma przyzwoite współczynniki efektywności energetycznej, jeśli znajdujące się w nim serwery wykonują niewiele zadań?

Przygotowany przez Green Grid dokument „PUE: A comprehensive examination of the metric" zawiera szczegółowe informacje dotyczące sposobów wykonywania pomiarów, obliczeń, wzorów, metod raportowania itd. Największy wpływ na wartość współczynnika PUE mamy w fazie projektowej, kiedy to można odpowiednio zaplanować i dobrać chłodzenie i zasilanie (główne czynniki mające wpływ na wynik). Pozostałe elementy mają mniejsze znaczenie, co nie oznacza, że nie powinny być przemyślane.

DCiE jest odwrotnością parametru PUE. Jest to wartość procentowa obliczana poprzez podzielenie energii elektrycznej zużywanej przez sprzęt IT, przez całość energii zużywanej przez centrum danych, a następnie pomnożone przez 100. Im większa wartość tego parametru, tym lepiej.

Całkowite zużycie energii można ustalić na podstawie odczytów z liczników elektrycznych, ale zasilanie z nich powinno trafiać wyłącznie do centrum danych. Jest to szczególnie istotne, jeśli centrum danych znajduje się w budynku pełniącym też inne role, np. biurowca. Na to zużycie składa się zasilanie wszelkiego rodzaju sprzętu znajdującego się

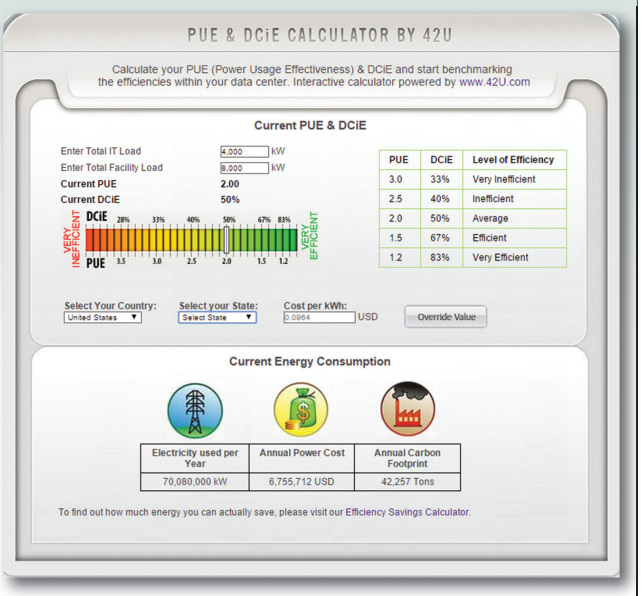
w centrum danych. Oprócz infrastruktury IT są to, m.in.: urządzenie dostarczające prąd (UPS-y, generatory, baterie, moduły PDU, itd.), systemy chłodzenia (agregaty chłodnicze, CRAC, pompy i wieże chłodnicze) oraz inne komponenty, np. oświetlenie. Wymienione urządzenia powodują nadwyżkę zużycia energii ponad to, co jest potrzebne do zasilania sprzętu IT.

Na całkowite zużycie energii składa się zasilanie wszelkiego rodzaju sprzętu znajdującego się w centrum danych. Oprócz infrastruktury IT są to, m.in.: urządzenie dostarczające prąd (UPS-y, generatory, baterie, moduły PDU, itd.), systemy chłodzenia (agregaty chłodnicze, CRAC, pompy i wieże chłodnicze) oraz inne komponenty, np. oświetlenie. Wymienione urządzenia powodują nadwyżkę zużycia energii ponad to, co jest potrzebne do zasilania sprzętu IT.

Z kolei zasilanie sprzętu IT oblicza się jako sumę prądu zużywanego przez urządzenia służące do zarządzania, przetwarzania, przechowywania oraz przesyłania danych w obrębie centrum danych. Są to przede wszystkim serwery, macierze dyskowe i aktywne urządzenia sieciowe, ale mogą to być również przełączniki KVM, monitory, konsola, a nawet stacje robocze wykorzystywane przez administratorów do zarządzania centrum danych.

Pojęcia PUE i DCiE mogą wydawać się proste. Jednak skomplikowany system transformatorów, PDU i agregatów sprawia, że przeprowadzenie pomiarów nie sprowadza się do prostych działań arytmetycznych. Obliczanie tych parametrów ma większą wartość, jeśli proces będzie regularnie powtarzany. Ułatwi to opracowanie powtarzalnej procedury, według której będą dokonywane pomiary.

Częstotliwość obliczeń zależy m.in. od tego, jak łatwy jest dostęp do danych. Jeśli wartości pomiarów są zbierane automatycznie przez oprogramowanie, nic nie stoi na przeszkodzie, żeby wartości tych parametrów obliczać w krótkich odstępach czasu (godzinowych, a nawet minutowych). Obciążenie infrastruktury IT może zmieniać się w ciągu dnia i osoby odpowiedzialne za centrum danych mogą uznać, że warto porównać parametry PUE i DCiE przy największym oraz najmniejszym obciążeniu w ciągu dnia. Sugerowana przez konsorcjum Green Grid częstotliwość pomiarów przewiduje monitoring raz w miesiącu / tygodniu (program podstawowy), codziennie (program średni) lub stałe, cogodzinne badanie w programie zaawansowanym. Niezależnie od częstotliwości regularne powtarzane tej operacji jest krokiem we właściwym kierunku.



Przykład aplikacji do obliczania parametrów PUE i DCiE.

Dane do wyliczeń można zbierać z liczników (pobór prądu dla całego centrum danych) i z zasilaczy awaryjnych UPS (dla urządzeń IT). W ten sposób otrzymamy wartości potrzebne do obliczenia parametrów PUE oraz DCiE. Są to jednak ogólne dane, a na całkowity pobór zasilania wpływa wiele czynników, a czasem warto wiedzieć, ile konkretnie prądu pobierają systemy chłodzenia, zasilania czy oświetlenie. Obecne technologie umożliwiają prowadzenie bardzo dokładnych pomiarów. Systemy zarządzania budynkami mogą monitorować nie tylko całkowitą ilość prądu pobieraną przez centrum danych, ale także przez klimatyzatory czy oświetlenie. Na rynku są rozwiązania, za których

pomocą można monitorować pobór zasilania przez poszczególne urządzenia w szafach stelażowych. Czujniki i oprogramowanie są w stanie zdalnie monitorować zużycie prądu przez systemy CRAC. W efekcie udaje się zidentyfikować, gdzie i kiedy dochodzi do nadmiernego zużycia, i wprowadzać w takich obszarach odpowiednie modyfikacje.

Poziom szczegółowości zależy od instalacji dostępnych w budynku, budżetu oraz celów, jakie chce się osiągnąć. Niezależnie od tego, jak prosty czy skomplikowany będzie system pomiarów, najistotniejszą kwestią jest regularność. Jeśli czegoś się nie mierzy, nie da się tego kontrolować.

ZASILANIE SPRZĘTU IT

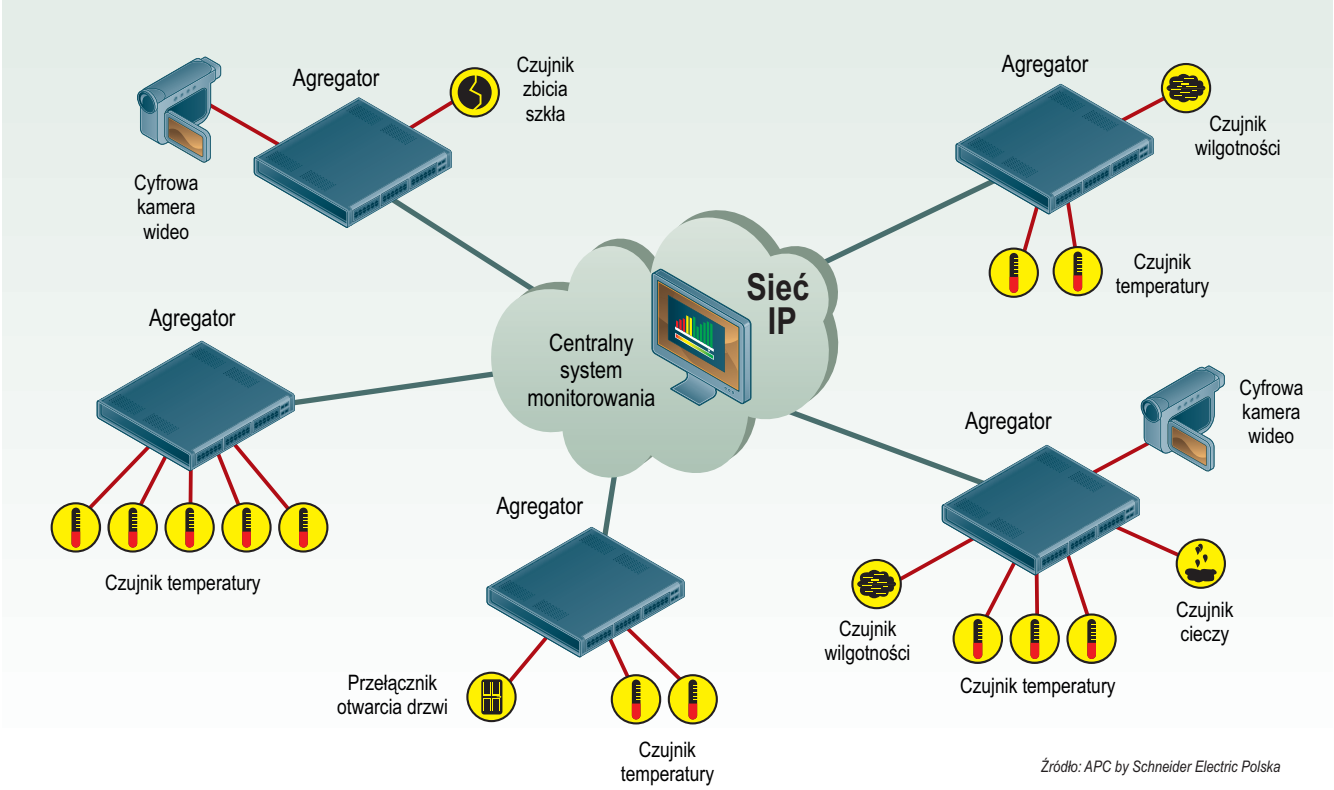
Ilość energii zużywanej przez infrastrukturę informatyczną można mierzyć w dwóch miejscach: na zasilaczach awaryjnych lub modułach dystrybucji zasilania (PDU). Zasilacze UPS to pierwsze logiczne miejsce do przeprowadzenia pomiarów. Nowsze modele mają wbudowane frontowe wyświetlacze lub można uzyskać do nich dostęp za pośrednictwem przeglądarki internetowej, co upraszcza zbieranie danych. W przypadku starszych zasilaczy UPS bez wyświetlaczy czy obsługi protokołu SNMP można zastosować specjalne mierniki.

Kolejnym punktem pomiarowym są moduły PDU. Nowsze są wyposażone w wyświetlacze lub dodatkowe zautomatyzowane obwody monitorujące, co bardzo ułatwia zbieranie danych o zasilaniu pobieranym przez sprzęt IT. Bez mechanizmów automatyzujących zbieranie danych trzeba na każdym gniazdku zamontować czujnik. Moduły PDU mogą mieć jednak nawet 42 gniazdka, co sprawia, że taka operacja jest trudna do przeprowadzenia.

Trzeba też pamiętać, że między punktami pomiarowymi występują różnice wynikające z niedoskonałości zasilaczy UPS i modułów PDU. Można obliczyć te straty, porównując odczyty na wejściu i na wyjściu zasilacza czy modułu PDU.

Prowadząc pomiary, po pewnym czasie można już zaobserwować jakieś trendy lub zidentyfikować komponenty zużywające nadmierne ilości prądu. Przykładowo, jeśli okaże się, że klimatyzacja odpowiada za znaczny odsetek całości energii pobieranej przez centrum danych, należy pochylić się nad optymalizacją chłodzenia. Trzeba przeanalizować ruch powietrza w serwerowni, przejrzeć ustawienia urządzeń chłodzących, sprawdzić temperaturę serwerów. Należy wyeliminować mało obciążone serwery, a jeśli to możliwe, zastosować wirtualizację. Po wprowadzonych zmianach trzeba ponownie dokonać pomiarów.

Schematy budowy systemu monitorowania parametrów fizycznych



Źródło: APC by Schneider Electric Polska