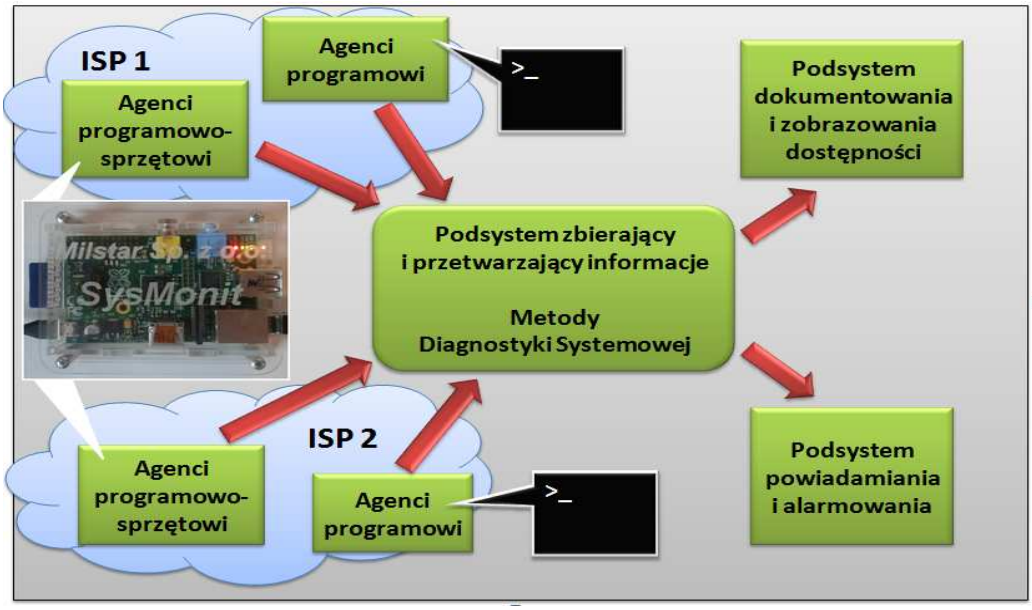
"Wybrane sposoby zapewnienia ciągłości działania oraz wysokiej jakości świadczonych usług na przykładzie Ubezpieczeniowego Funduszu Gwarancyjnego"

Poziom zadowolenia użytkowników (klientów) systemów informatycznych w dużej mierze zależy od ich wysokiej sprawności oraz ciągłości świadczenia usług. Wymagania w tym zakresie stale są podwyższane. Dostępność usług może zostać zaburzona przez awarie systemu informatycznego, łączy sieciowych, czy coraz częściej występujące ataki cybernetyczne. Podwyższanie poziomu dostępności systemów można osiągnąć, między innymi, poprzez zwiększenie wydajności systemów teleinformatycznych, ustawiczne monitorowanie stanu (kondycji) systemów teleinformatycznych oraz badania stabilności i wydajności (zarówno akceptacyjne przed produkcyjnym uruchomieniem systemu, jak również cykliczne w trakcie cyklu życia systemu informatycznego.

W niniejszym wystąpieniu skupiamy uwagę na monitorowaniu stanu (kondycji) systemów teleinformatycznych oraz testach ich stabilności i wydajności.

Odpowiednio prowadzony monitoring "kondycji" systemów i usług, który oprócz stwierdzenia awarii, umożliwia ustalenie jej przyczyn, a także dostarcza dodatkowych danych przydatnych w procesie tworzenia systemów odpornych na ataki zagrażające dostępności usług, staje się powszechnie stosowaną praktyką. Dzięki wcześnie wykrytym symptomom awarii możliwe jest przerwanie jej eskalacji, a przez to minimalizacja strat. Aby to było możliwe, monitorowanie dostępności powinno być wielopoziomowe, co zapewnia szczegółowe sprawdzanie poprawności działania systemu (w tym logiki uzyskiwanych odpowiedzi), przy równoczesnym minimalizowaniu obciążenia związanego z samym monitorowaniem. Monitorowanie powinno być prowadzone z wielu miejsc, zgodnie z zasadami diagnostyki systemowej gwarantującej właściwą interpretację, nie zawsze jednakowych, informacji pozyskiwanych z wielu źródeł oraz wzajemne diagnozowanie sond próbkujących. Dzięki temu można wykluczyć wpływ różnego typu zakłóceń na ocenę funkcjonowania monitorowanych systemów. Powyższe wymagania zostały uwzględnione przy projektowaniu i tworzeniu uniwersalnego systemu służącego do monitorowania dostępności aplikacji i usług internetowych o nazwie ***SysMonit***™*,* który jest wykorzystywany w Ubezpieczeniowym Funduszu Gwarancyjnym. W skład systemu wchodzą agenci wykonujący testy (próbkowanie monitorowanych systemów), podsystem zbierający i przetwarzający informacje od agentów, podsystem zobrazowania dostępności oraz dokumentowania stanu badanych obiektów oraz podsystem powiadamiania i alarmowania (rys. 1).



*Rys.1. Schemat blokowy systemu **SysMonit**™*

SysMonit™ umożliwia zdalne monitorowanie usług i zasobów teleinformatycznych, które są dostępne publicznie, jak również tych, dostępnych jedynie po zalogowaniu (np. przy legitymowaniu się odpowiednim certyfikatem cyfrowym).

Agenci (sondy) ***SysMonit***™ są rozmieszczeni w różnych lokalizacjach, w sieciach należących do różnych dostawców usług internetowych (tzw. Internet Service Provider - ISP). Dzięki temu fluktuacje ruchu sieciowego (lub ewentualne awarie pojedynczych urządzeń sieciowych między monitorowanymi zasobami a węzłami SysMonit) nie mają wpływu na wiarygodność ostatecznie wydawanych opinii. Aby ułatwić uruchamianie agentów w różnych miejscach i środowiskach komputerowych opracowano ich zarówno jako rozwiązanie czysto programowe, które można instalować w ramach już funkcjonujących serwerów (komputerów), jak również jako rozwiązanie sprzętowo-programowe, które do działania wymaga tylko połączenia internetowego i zasilania w energię elektryczną. Warto dodać, iż jest to specjalnie przygotowana platforma sprzętowa, która charakteryzuje się poborem prądu jedynie na poziomie 750 mW. Dzięki zastosowaniu większej niż wymagane minimum liczby sond, w przypadku awarii nawet kilku z nich, ***SysMonit***™ zapewnia ciągłość monitorowania i prawidłowo orzeka o dostępności zasobów.

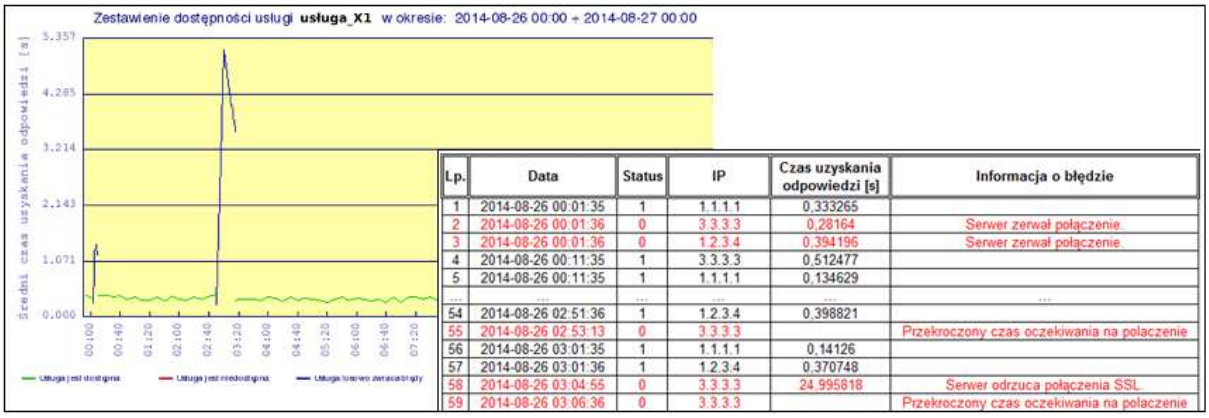
SysMonit™ uwzględnia wielopoziomowe testowanie dostępności zasobów, tzn. rozróżnialna jest poprawność działania serwerów oraz świadczonych przez nie usług na różnym poziomie zaawansowania. Rozwiązanie, poza dostępnością usługi (sprawdzanej np. za pomocą protokołu ICMP), umożliwia m. in. udzielenie odpowiedzi na następujące pytania:

- czy użytkownik może się zalogować do systemu,
- czy może wykonać podstawowe (zdefiniowane przez Klienta) akcje. W tym przypadku możliwe jest opisanie akcji z wykorzystaniem protokołów HTTP, XML, SOAP itd.,
- czy wyniki wykonanych działań są poprawne.

Na życzenie Klienta system może zostać dostosowany do sprawdzania prawidłowości działania dowolnego jego elementu. System umożliwia weryfikację dostępności usług/zasobów Klienta, w dowolnych interwałach czasowych, np. co sekundę.

Niepowodzenie w jakimkolwiek kroku (zdefiniowanym przez Klienta) zostanie odpowiednio wcześnie zgłoszone administratorom.

SysMonit™ udostępnia użytkownikom dwa interfejsy służące przeglądaniu zestawień (raportów) nt. dostępności usług/zasobów. Pierwszym jest interfejs graficzny dostępny poprzez WWW, który w jednym miejscu agreguje i udostępnia zestawienia odnośnie godzinowej, dobowej i miesięcznej dostępności wszystkich monitorowanych zasobów (rys. 2). Możliwe jest również pobranie informacji odnośnie dostępności monitorowanych zasobów poprzez Interfejs WS (Web Service). Wykorzystując go można wysłać zapytanie do systemu ***SysMonit***™, posiadające dodatkowe parametry, np. nazwę usługi, rodzaje błędów itd. W odpowiedzi ***SysMonit***™ wyśle plik XML zawierający przefiltrowane informacje o stanie zasobów w zadanym okresie, który następnie można przetwarzać w programach typu Visual Analytics. Dodatkowo, jeżeli Klient nie ma możliwości wykorzystania raportów we wspomnianych powyżej formatach, ***SysMonit***™ umożliwia wygenerowanie informacji odnośnie dostępności monitorowanych zasobów do pliku w formacie CSV.



Lp.	Data	Status	IP	Czas uzyskania odpowiedzi [s]	Informacja o błędzie
1	2014-08-26 00:01:35	1	1.1.1.1	0,333265	
2	2014-08-26 00:01:36	0	3.3.3.3	0,28164	Serwer zerwał połączenie
3	2014-08-26 00:01:36	0	1.2.3.4	0,394196	Serwer zerwał połączenie
4	2014-08-26 00:11:35	1	3.3.3.3	0,512477	
5	2014-08-26 00:11:35	1	1.1.1.1	0,134629	
...	...	...	...	...	...
54	2014-08-26 02:51:36	1	1.2.3.4	0,398821	
55	2014-08-26 02:53:13	0	3.3.3.3		Przekroczony czas oczekiwania na połączenie
56	2014-08-26 03:01:35	1	1.1.1.1	0,14126	
57	2014-08-26 03:01:36	1	1.2.3.4	0,370748	
58	2014-08-26 03:04:55	0	3.3.3.3	24,995818	Serwer odrzuca połączenia SSL
59	2014-08-26 03:06:36	0	3.3.3.3		Przekroczony czas oczekiwania na połączenie

Rys.2. Widok stanu monitorowanego systemu w interfejsie graficznym ***SysMonit***™

W momencie wykrycia awarii oraz po ponownym wznowieniu świadczenia usług ***SysMonit***™ może powiadomić o tym fakcie odpowiednie osoby wykorzystując system poczty elektronicznej (e-mail) lub wysyłając wiadomość SMS. System w pełni dokumentuje każdą awarię umożliwiając administratorom szybkie znalezienie i usunięcie problemu. W opisie zdarzenia dostępne są m.in. adresy IP sond, które stwierdziły zmianę stanu, treść żądania, pełna odpowiedź serwera itd.

SysMonit™, jako system monitorujący dostępność usług, dobrze współpracuje z narzędziami do zarządzania wydajnością aplikacji. Przykładem jest *Flopsar Suite*. W tym przypadku ***SysMonit***™ zapewnia funkcje związane z monitorowaniem działających usług i zasobów oraz alarmowaniem w momencie wykrycia awarii. Natomiast *Flopsar Suite*, działając wewnątrz monitorowanego systemu, zapewnia funkcje związane ze szczegółowym identyfikowaniem przyczyn problemów i anomalii, umożliwiając wskazanie modułu usługi, czy wręcz fragmentu jej kodu odpowiedzialnego za problemy w działaniu. Wykorzystanie obydwu uzupełniających się systemów pozwala na osiągnięcie efektu synergii, dzięki czemu liczba godzin poświęcanych na obsługę incydentów zdecydowanie maleje, a jednocześnie właściwie ukierunkowane działania optymalizujące prowadzą do eliminacji przyczyn ich występowania.

Rozwiązanie dostarczane jest jako Software as a Service. Oznacza to, że po stronie Klienta nie jest wymagana instalacja żadnych aplikacji, rozszerzeń, dodatków, czy też umieszczanie w serwerowniach dodatkowego sprzętu.

Innym elementem wpływającym pozytywnie na poziom jakości usług świadczonych przez systemy informatyczne jest **sprawdzanie wydajności oraz stabilności** ich działania. W tym zakresie na wiarygodność uzyskanych ocen mają istotny wpływ zastosowana metodyka badań oraz własności specjalizowanych generatorów zapytań, które muszą przede wszystkim zapewnić możliwość obciążenia badanych systemów na wymaganym, niezmiennym w określonych odcinkach czasu, poziomie.

Metodyka badań, której podstawowe, ogólne zasady są wspólne dla wszystkich tego typu testów, w szczegółach musi być dostosowywana do danego obiektu badań, tak aby uwzględniać jego tryby pracy, wymagania wydajnościowe, warunki wykonywania testów (lokalne, zdalne) itp. Prawidłowość założeń prowadzenia badań (metodyki) jest warunkiem koniecznym do uzyskania wiarygodnych, rzetelnych i użytecznych wyników, a następnie wniosków. Jednak sama metodyka nie wystarczy, jeśli do realizacji jej założeń nie zastosuje się odpowiednich narzędzi. Narzędzia te muszą wygenerować odpowiednie zapytania (czasami w trakcie testów zostaje zadanych kilka milionów zapytań), ale również zapisać uzyskane wyniki po stronie generatora (czasy odpowiedzi, zarejestrowane błędy), pozwolić na ich korelację z wynikami odnotowanymi po stronie badanego systemu, przetworzyć całość wyników i zaprezentować je w postaci czytelnej dla odbiorcy.

Najważniejszym narzędziem jest generator zapytań, który musi być dostosowany do obiektu badań, tzn. wiernie odwzorowywać działania klientów badanego systemu. Ważnym jest również to, aby generator dawał możliwość zadawania zapytań na stałym określonym poziomie ich równoległości, tzn. gwarantował, że badany obiekt np. przez 15 minut obsługuje dokładnie 100 zapytań równocześnie. Zdarza się, że w trakcie testów, zgodnie z wymaganiami, poziom równoległości jest bliski 1000 równocześnie przetwarzanych zapytań. W generatorach bardzo istotną kwestią jest również sposób generowania samych zapytań. Należy dążyć do jak najmniejszej ich powtarzalności, co chroni przed udzielaniem odpowiedzi na podstawie wcześniej zapamiętanego wyniku (tzw. cache-owaniu), co przy normalnym wykorzystywaniu rzadko się zdarza. Przy milionach, czy nawet setkach tysięcy zapytań wymaganych do rzetelnej oceny wydajności i/lub stabilności aplikacji (usługi) trudno zbiory danych testowych opracować manualnie. Dlatego wszędzie tam gdzie jest to możliwe należy pola zapytań uzupełniać wartościami opracowywanymi dynamicznie, na podstawie algorytmów opisujących dane formuły, np. składnię numeru PESEL lub nr rejestracyjny samochodu, co zmniejsza prawdopodobieństwo powtarzania się zapytań.

Wnioski uzyskane w wyniku przeprowadzenia badań wydajności i/lub stabilności w przypadku ich cykliczności pozwalają określić nie tylko stan aktualnej wersji badanego systemu, ale również ocenić skutki wprowadzanych zmian w cyklu życia aplikacji/usługi, a przez to, pośrednio wskazywać optymalne kierunki przyszłego ich rozwoju.