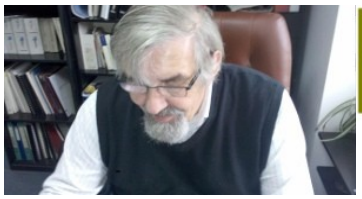


Old Man GURU Magazine

Wychodzi bardzo nieregularnie, kiedy wydaje mi się, że mam coś ciekawego lub pożytecznego do napisania...

Numer 31/2013 16 styczeń 2013

Nasz wieloletni Partner, firma Network Instruments podjęła decyzję o nieodpłatnym udostępnieniu jednego ze swych produktów – OBSERVER Infrastructure (OI).

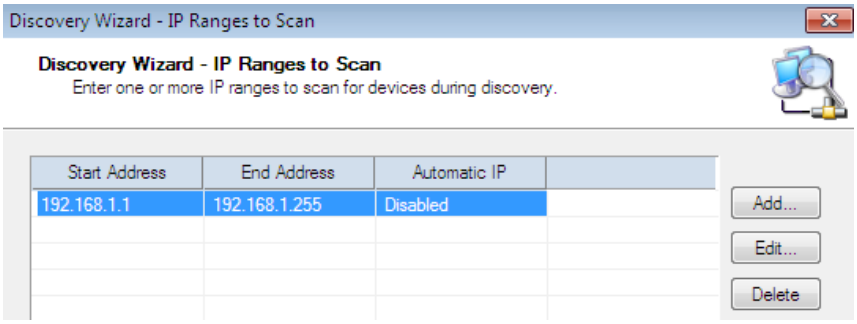
Jest to oprogramowanie przeznaczone dla systemu MS Windows, które zadaniem jest monitorowanie pracy infrastruktury sieciowej. OI monitoruje pracę sieci wykorzystując standardowe narzędzia:

- ICMP (ping, traceroute...),
- Aktywne skanowanie portów IP,
- Skanowanie NetBIOS i NETBEUI,
- Skanowanie adresów IPX,
- Mechanizmy SNMP,
- Zapytania WMI (Windows Management Instrumentation),
- Web Services Data API oraz zapytania definiowane dla poszczególnych protokołów (HTTP, SSH, MySQL, SyBase itp.) oraz definiowane indywidualnie przez użytkownika.

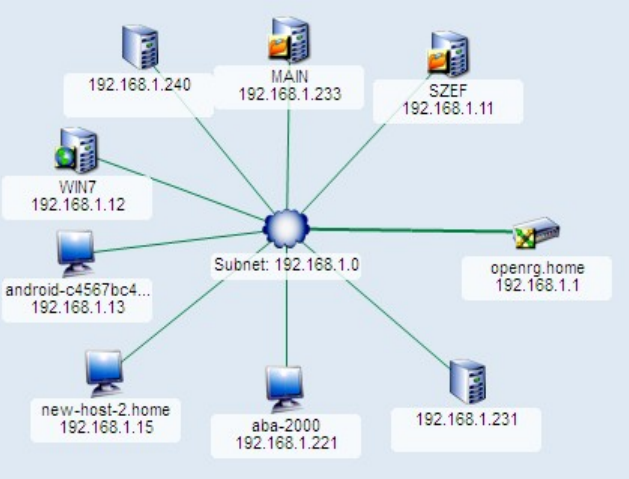
OI jest przykładem, że standardowe, dobrze znane protokoły i narzędzia służące do nadzoru pracy sieci i systemów komputerowych można uzupełnić o wygodny system prezentacyjny, który nie tylko umożliwi administratorowi obserwację pracy sieci, lecz również dzięki obsłudze alertów będzie go informował o ewentualnych problemach (np. za pomocą poczty elektronicznej). Przyjazny, graficzny interfejs użytkownika oraz kontekstowy system pomocy ułatwia konfigurację oprogramowania oraz obserwację stanu sieci na bieżąco lub w dowolnie wybranym momencie. Dostęp do danych „historycznych" zapewnia podsystem tworzenia raportów.

Monitorowanie urządzeń (serwerów, routerów itp.)

Urządzeniem (device) może być dowolne urządzenie podłączone do sieci kablowej lub bezprzewodowej – a więc serwer lub stacja robocza pracująca pod systemem MS Windows, Linux, MacIntosh, Apple, router lub adresowalny rozgałęźnik (Hub), drukarka sieciowa. Urządzenie musi posiadać adres sieciowy – IP, IPX lub Microsoft. Urządzenia nieposiadające adresu nie mogą być monitorowane. Urządzenia są łączone w grupy. Do grupy można dodawać zarówno podsieci, grupy adresów jak i pojedyncze adresy IP.



Po wprowadzeniu adresów (w opisie ograniczę się do sieci IP) uruchamiamy funkcję „Topology Discovery". W wyniku zostanie wyświetlony schemat naszej sieci. Jeśli korzystamy z wersji nieodpłatnej liczba wprowadzonych (lub aktywnych w podsieci lub zakresie) adresów nie może przekraczać 10. Większa ilość urządzeń może być monitorowana przez odpłatne wersje OI. Jeśli jednak ograniczymy się na przykład do monitorowania serwerów i routerów wersja nieodpłatna może być przydatna nawet w sporych sieciach.

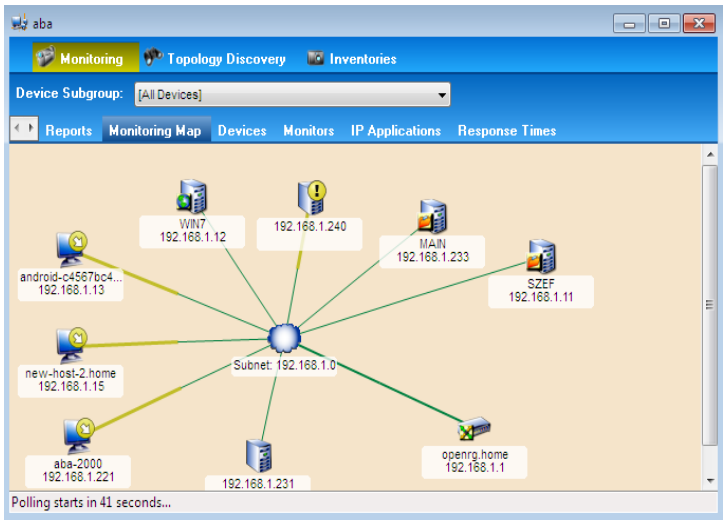


Oczywiście podczas wykrywania urządzeń powinny być one aktywne. Wykryte zostaną zarówno maszyny fizyczne, jak i wirtualne. Na załączonym schemacie maszyny o adresach 221, 233, 240 oraz 11 to komputery fizyczne, 12 i 231 odpowiadają maszynom wirtualnym, 13 to tablet z systemem Android, a 15 to smartphon Sony Ericson Xperia. Routerem (192.168.1.1) jest LiveBox Neostrady.

Wykryte urządzenia (a raczej ich parametry) są zapisywane w odpowiednim pliku, który następnie jest wykorzystywany podczas monitorowania stanu sieci.
Administrator może wprowadzić więcej grup urządzeń.

Po wprowadzeniu urządzeń (można to zrobić zarówno automatycznie, jak i ręcznie) możemy przejść do monitorowania pracy sieci.

Domyślnie system OI sprawdza działanie urządzeń (poll) co 3 minuty i po dokonaniu sprawdzenia ikonka urządzenia jest opatrywana odpowiednim emblematem, na podstawie którego można określić zarówno stan, jak i typ urządzenia. Znaczenie emblematów jest intuicyjne - np. żółte kółko oznacza „yellow alert",(chwilowa niedostępność urządzenia) zaś czerwone „red alert" (dłuższa niedostępność urządzenia). Dzięki temu administrator może błyskawicznie stwierdzić, które urządzenia są aktualnie dostępne.

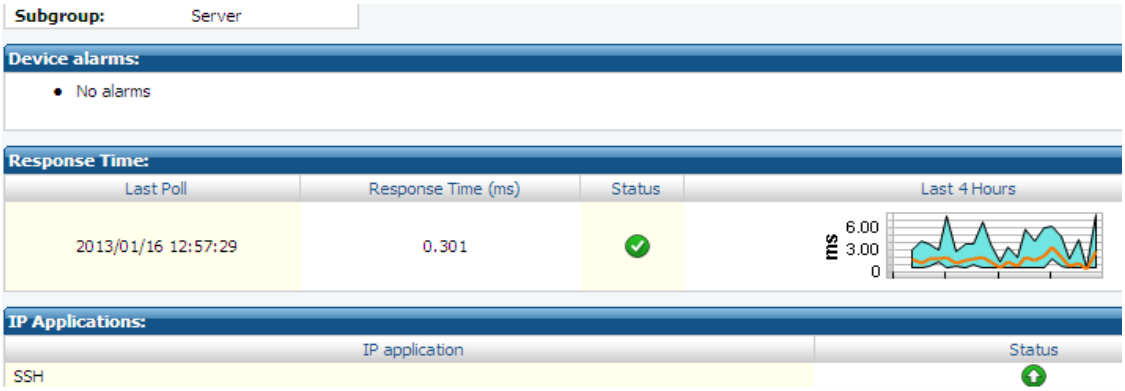


OI pozwala również ocenić czas odpowiedzi urządzeń, co pozwala ocenić stopień ich aktualnego obciążenia (uzyskanie dokładniejszych danych dotyczących czasu odpowiedzi poszczególnych aplikacji wymaga użycia programu Expert OBSERVER lub OBSERVER Suite).

Reports | Monitoring Map | Devices | Monitors | IP Applications | Response Times

	State	Device	IP Address	Response time (ms) Latest	Minimum	Maximum	Average	Polls Total	Failed
1	✓	192.168....	192.168.1.231	8.0	0.2	8.0	1.8	69	0 (00%)
2	✓	192.168....	192.168.1.240	1.4	0.1	5.9	1.0	69	35 (50%)
3	✓	aba-2000	192.168.1.221	0.4	0.1	11.6	1.4	69	22 (31%)
4	✗	android...	192.168.1.13	--	--	--	--	69	69 (100%)
5	✓	MAIN	192.168.1.233	0.3	0.1	6.1	0.9	69	0 (00%)
6	✗	new-ho...	192.168.1.15	--	1.4	219.7	47.0	69	47 (68%)
7	✓	openrg....	192.168.1.1	0.7	0.4	8.2	1.0	69	0 (00%)
8	✓	SZEF	192.168.1.11	0.1	0.1	7.3	0.6	69	0 (00%)
9	✓	WIN7	192.168.1.12	0.0	0.0	0.0	0.0	69	0 (00%)

Pracę każdego urządzenia możemy ocenić indywidualnie. Poniżej umieściłem dane uzyskane za pomocą programu OI dla serwera NoMachine NX (maszyna wirtualna) korzystającego z protokołu SSH:

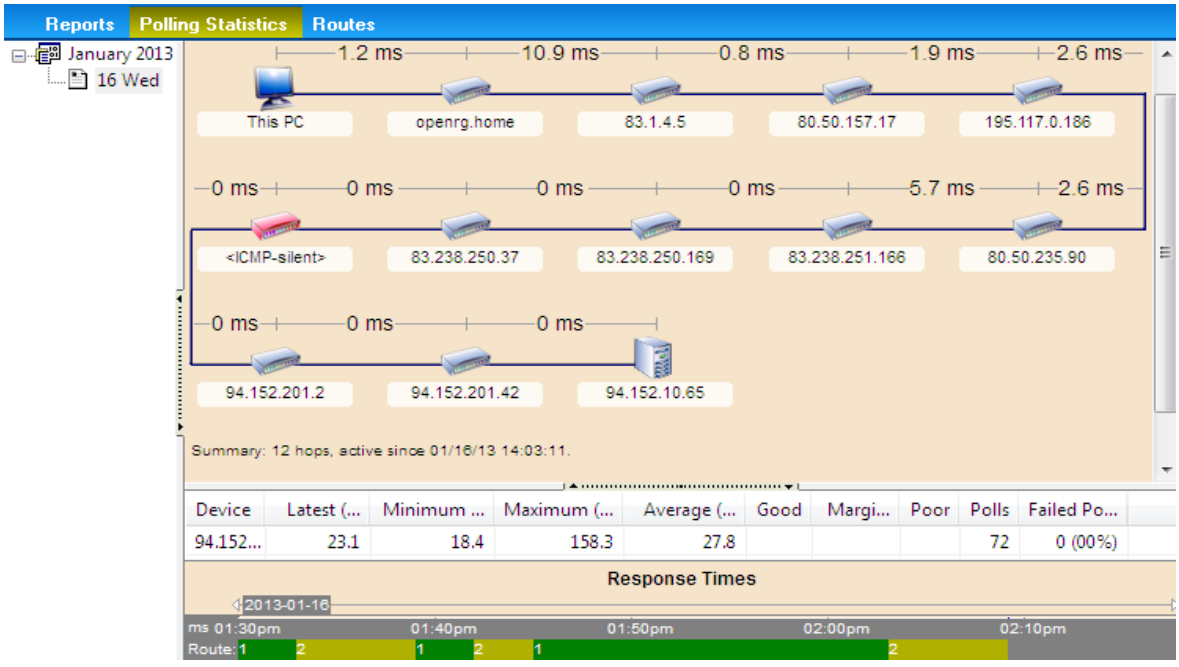


Wykres możemy oczywiście powiększyć oraz w ten sam sposób ocenić obciążenie każdego monitorowanego urządzenia (w tym także routera).

Powyższe przykłady znakomicie ilustrują podejście firmy Network Systems do analizy sieci, które można krótko określić następująco: „Tyle informacji ile w danej chwili jest potrzebne". Jeśli na pierwszy rzut oka widać, że wszystko jest w porządku (brak alertów) i użytkownicy nie skarżą się na żadne nieprawidłowości, to nie ma powodu, aby przeciążać się szczegółami. Jeśli natomiast występują jakieś problemy - to możemy się w te szczegóły zgłębić (Drill Down) korzystając z kolejnych modułów oprogramowania monitorującego.

Monitorowanie połączeń (ścieżek routingu):

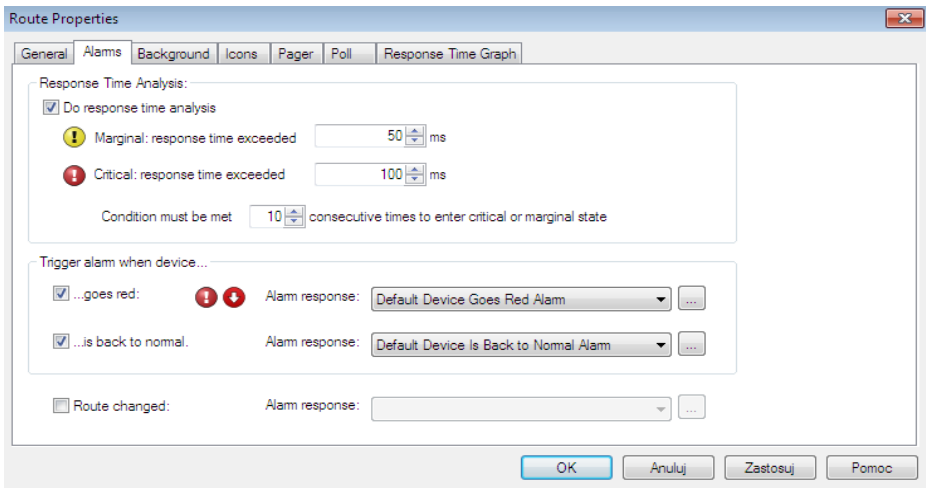
OBSERVER Infrastructure umożliwia również monitorowanie połączeń (wersja Free Forever posiada ograniczenie do 5 ścieżek).



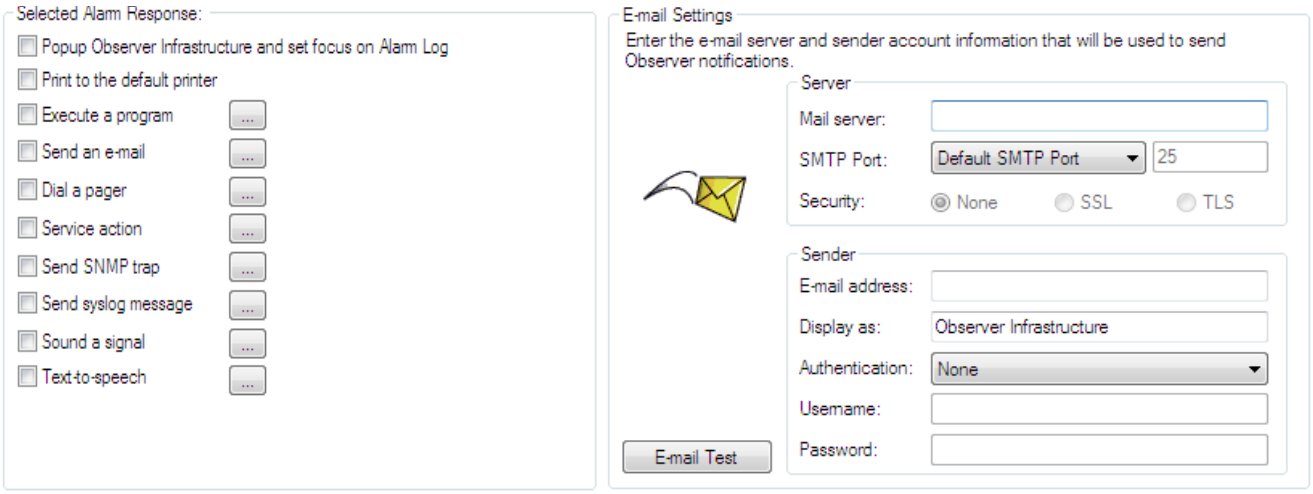
Konfigurowanie alarmów i akcji

Podobnie, jak w przypadku monitorowania urządzeń również dla monitorowania połączeń OI wykorzystuje standardowe, dobrze znane wszystkim administratorom mechanizmy i protokoły sieciowe (głównie ICMP), jednak dzięki starannie opracowanemu interfejsowi prezentuje ich wyniki w sposób umożliwiający natychmiastową ocenę jakości połączenia poprzez obserwację koloru paska pod napisem „Response times". Dane są przechowywane przez (ustawienie domyślne) 14 dni.

OI pozwala również na konfigurację poziomów alarmów (marginal – yellow i critical – red). Po wprowadzeniu poziomów alarmu (zrzut ekranu poniżej):

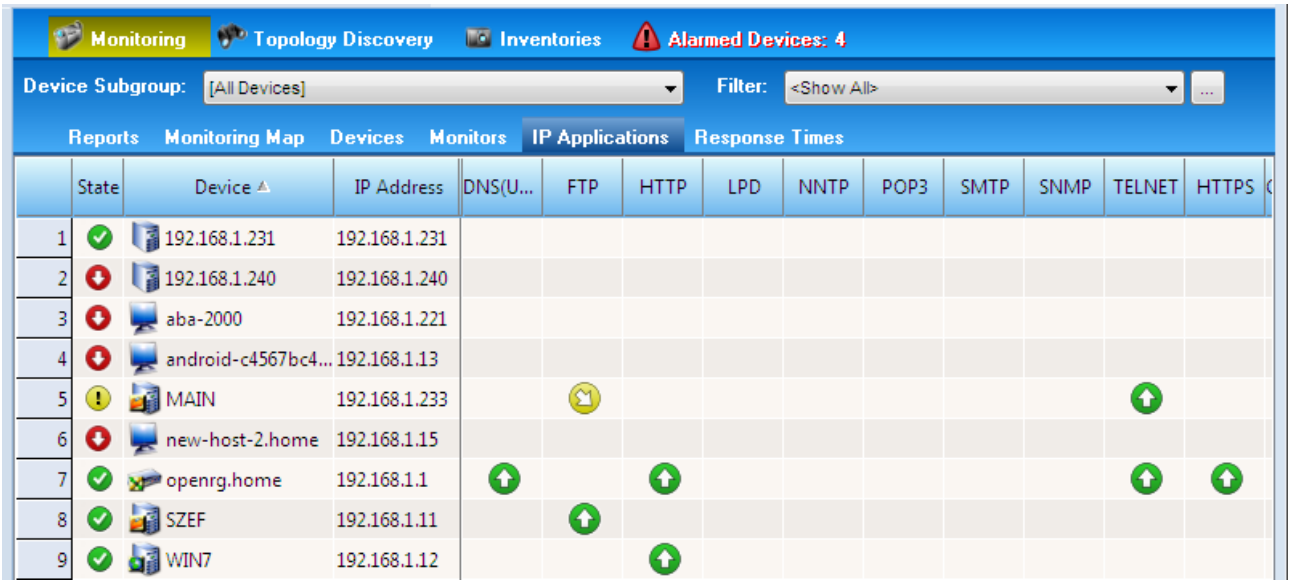


Następnie określamy, jaką akcję OI ma być wykonanać po otrzymaniu alarmu:



Alarmy (oraz ich obsługę) możemy definiować oczywiście nie tylko dla połączeń, ale także dla urządzeń. Dzięki temu możemy otrzymywać ostrzeżenia – a nawet automatycznie realizować akcje serwisowe. Na przykład temu Observer Infrastructure może nas poinformować, że utraciliśmy połączenie z naszym dostawcą Internetu lub połączenie z filią naszej organizacji jest obciążone powyżej założonego krytycznego poziomu. Dzięki temu administratorzy sieci mogą podejmować natychmiastowe działania naprawcze – a nawet wyprzedzające.

Monitorowanie usług i aplikacji



Jeśli jakaś usługa stanie się niedostępna OI to zasygnalizuje. Powyższy zrzut ekranu przedstawia ekran monitora aplikacji IP. Jak widać usługa FTP na serwerze MAIN (192..168.1.233) nie była aktywna w czasie przeprowadzania testu (poll). Jeśli ten stan będzie się utrzymywał w następnych cyklach poll alarm „żółty" zostanie zastąpiony przez „czerwony" i wykonane zaprogramowane wcześniej akcje – np. informacja o braku usługi zostanie przekazana administratorowi, który będzie mógł podjąć odpowiednie działania w celu jej przywrócenia.

OI monitoruje usługi sprawdzając aktywność portów za pomocą wcześniej przygotowanych skryptów, które realizują dwie podstawowe akcje - „Send" oraz „Expect" (szczegółowy opis tworzenia tych skryptów znajduje się w dokumentacji). Administrator może tworzyć własne skrypty, definiować i dodawać nowe usługi udostępniane na dowolnych portach itp. Prosty program konfiguracyjny umożliwia szybkie wprowadzanie, usuwanie lub edycję usług, które mają być monitorowane przez OI.

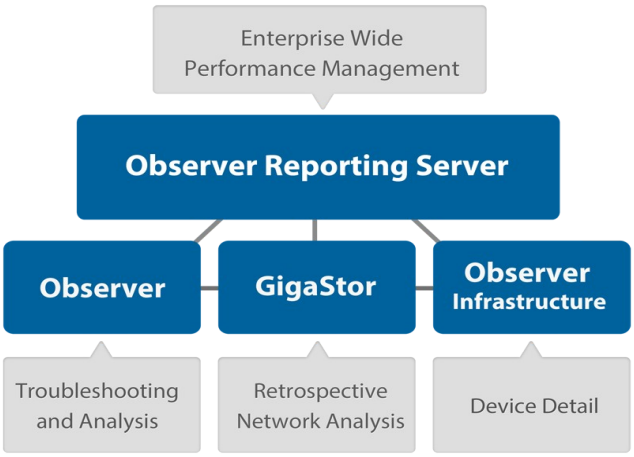
Application	Type	Port	Description	Script
DNS(T...	TCP	53	Domain Name Service(TCP)	
DNS(U...	UDP	53	Domain Name Service(UDP)	
FTP	TCP	21	File Transfer Protocol	Expect="^220";Send="QUIT\r\n";
GOPHER	TCP	70	Internet Gopher Protocol	Send="\r\n";Expect="(.+)";
HTTP	TCP	80	Web Service	Send="HEAD / HTTP/1.0\r\nAccept: *...
HTTPS	TCP	443	HTTP-Secure Sockets Layer (SSL/TLS)	Send="SSL_CLIENT_HELLO";Expe...
IMAP(S...	TCP	993	IMAP-Secure Sockets Layer (SSL/TLS)	Send="SSL_CLIENT_HELLO";Expe...
IMAP4	TCP	143	Internet Message Access Protocol V4	Expect="^* OK";
Lotus N...	TCP	1352	IBM Lotus Notes	
LPD	TCP	515	Printer Connection	
NNTP	TCP	119	USENET News Transfer Protocol	Expect="^2";Send="QUIT\r\n";
POP3	TCP	110	Post Office Protocol	Expect="^\+OK";Send="QUIT\r\n";

Dzięki takiemu podejściu raz zainstalowany Observer Infrastructure będzie nam dobrze służył nawet po wprowadzeniu nowych usług i rozbudowie sieci.

Wielu użytkowników niewielkich systemów – zwłaszcza opartych MS Windows nie dysponuje zaawansowanym narzędziem monitorującym ich pracę. Takie systemy zazwyczaj są administrowane przez osoby z zewnątrz (zatrudnianie administratora na pełny etat nie jest uzasadnione ekonomicznie). Observer Infrastructure – nawet w wersji Free ForEver znakomicie wypełnia tę lukę i stanowi świetną pomoc dla administratorów i osób odpowiedzialnych za pracę systemu teleinformatycznego organizacji bez względu na jej charakter.

Network Instruments - Kompletne i rozszerzalne rozwiązanie

Observer Infrastructure jest jedną z części kompleksowego rozwiązania nadzoru sieci tworzonego od prawie 20 lat przez Network Systems (NI). Istotną cechą tego rozwiązania jest budowa modularna, która pozwala na dostosowanie systemu zarówno do nadzoru małych instalacji (do tego celu służy właśnie Observer Infrastructure), jak i wielkich sieci teleinformatycznych czołowych operatorów telekomunikacyjnych – do klientów, którzy zakupili produkty NI należą takie firmy jak Deutsche Telecom, France Telecom, banki HSBC, ING, Deutsche Bank, PeKaO S.A., Ministerstwo Finansów RP, Boeing, Polskie Porty Lotnicze, WarnerBros, CISCO, IBM szereg Uczelni (również w Polsce) itd. Więcej danych można znaleźć na stronie producenta: http://www.networkinstruments.com/about/customers/index.php



Wersje i wymagania OBSERVER INFRASTRUCTURE

Dla wersji Free (do 10 monitorowanych urządzeń i do 5 ścieżek) optymalny będzie komputer z procesorem DualCore, dyskiem 250 GB i pamięcią 4 GB. W moim przypadku OI pracuje na notebooku HP625 z dwurdzeniowym AMD i 2 GB pamięci RAM i zupełnie dobrze sobie radzi. Niezbędny system operacyjny to Windows XP lub późniejszy.

Dostępne są również wersje komercyjne dla 100 i 500 monitorowanych urządzeń oraz wersja Enterprise dla dowolnej liczby urządzeń i ścieżek. Dla 100 urządzeń zalecany jest procesor czterordzeniowy i 1 TB pamięci dyskowej, zaś dla 500 (lub więcej) dwa procesory czterordzeniowe, 8 GB RAM i macierz dyskowa o łącznej pojemności 2 TB (np. 4 x 500 MB).

Wersje komercyjne mogą być dostarczone w formie licencji na wykorzystywanie oprogramowania (Right to Use) albo jako gotowe do pracy urządzenia sieciowe (Network Appliances) do instalacji w szafach 19". Applance zawiera wszystkie niezbędne elementy – odpowiednio dobraną platformę sprzętową, system operacyjny oraz oprogramowania Observer Infrastructure wraz z licencją.

Informacje końcowe

Nieodpłatną wersję OBSERVER INFRASTRUCTURE (dla 10 użytkowników i 5 ścieżek) można pobrać ze strony http://www.networkinstruments.com/products/observer-infrastructure/index.php .
Program można wykorzystywać na zasadach „Free for Ever" niezależnie od celu – a więc również dla celów komercyjnych, serwisowych itp.

Wersje komercyjne dla 100, 500 i więcej liczby monitorowanych urządzeń i bez większej liczby ścieżek zarówno w postaci licencji na korzystanie z oprogramowania, jak i w postaci Network Appliances są dostępne w firmie ABA – www.aba.krakow.pl (Autoryzowany Dystybutor NI od 1994 r.). ABA udziela również wszystkich informacji handlowych (ceny, warunki dostaw, gwarancji, wsparcia dla oprogramowania) oraz technicznych (dobór produktów, porady konfiguracyjne, wizyty inżynierów, szkolenia itp.).