Test: WhatsUp – monitorowanie NMS s. 66

Jak atakują przestępcy – ransomware s. 32

3
2021

Miesięcznik informatyków i menedżerów IT

www.it-professional.pl

IT professional

Nr 3 (112) marzec 2021

ZARZĄDZANIE PODATNOŚCIAMI s. 8

Zarządzanie bezpieczeństwem poprzez identyfikację słabych punktów systemów, detekcja zagrożeń i ocena krytyczności podatności, testowanie zabezpieczeń, przegląd i porównanie narzędzi do testowania podatności

OLA w usługach informatycznych s. 48

Funkcjonowanie umów Operational Level Agreement w praktyce

Hurtownia danych z Azure Synapse Analytics s. 18

Hybrydowa analityka danych w chmurze Microsoftu

Windows Package Manager s. 76

Nowa metoda dystrybucji oprogramowania w Windowsie 10

Cena 36,00 zł (w tym 8% VAT)
ISSN 2083-9588

Serwery ▪ Stacje robocze ▪ Bezpieczeństwo ▪ Infrastruktura i sieci ▪ Zarządzanie i prawo IT ▪ Techn

DOSTĘPNE E-WYDANIE

Monitorowanie środowiska sieciowego wymaga zazwyczaj dedykowanego rozwiązania. Ciekawe propozycje znaleźć można zarówno wśród projektów całkowicie darmowych, jak i tych komercyjnych, o czym wielokrotnie pisaliśmy. Dziś test kolejnego rozwiązania komercyjnego.

Oprogramowanie NMS

WhatsUp Gold – zarządzanie siecią

Marcin Jurczyk

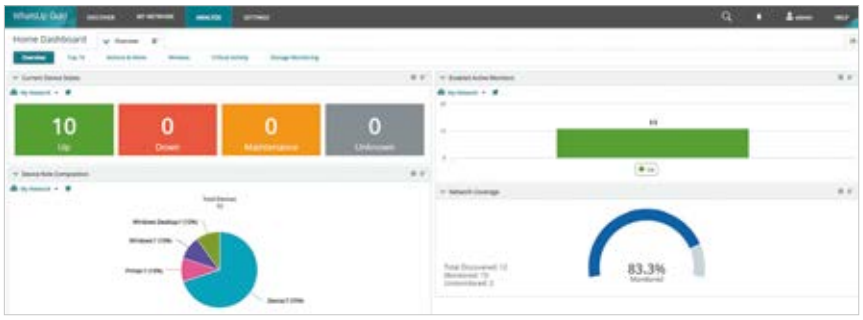
Oprogramowanie typu Network Management System (NMS) to rodzina rozwiązań pozwalających na monitorowanie, zarządzanie i optymalizację sieci przedsiębiorstwa. Produkty tej klasy powinny umożliwiać automatyczne wykrywanie urządzeń podłączonych do sieci wraz z możliwością wizualizacji topologii fizycznej i logicznej na podstawie danych pochodzących ze sprzętu sieciowego. Dla tak zinwentaryzowanego środowiska powinien być także dostępny pełny monitoring, począwszy od weryfikacji dostępności urządzenia w sieci po analizę wykorzystania wszystkich zasobów, takich jak zajętość i utylizacja portów sieciowych wraz z możliwością analizy wydajności w kontekście obciążenia sieci z uwzględnieniem charakterystyki ruchu. Funkcje zarządzania powinny pozwolić także na modyfikację konfiguracji urządzeń sieciowych czy reagowanie na ewentualne zdarzenia w sieci. Ponadto NMS powinien mieć funkcje raportowania i powiadamiania o zdarzeniach. Oprogramowanie WhatsUp Gold firmy Progress Software poza standardowymi cechami NMS pozwala także na monitoring innych elementów infrastruktury, takich jak serwery oraz aplikacje, a także usługi wybranych dostawców chmurowych, o czym w dalszej części testu. Sam produkt na pierwszy rzut oka może się kojarzyć z nieco innym producentem niż firma Progress. Spostrzeżenie to jest jak najbardziej trafne, gdyż za projektem stoi Ipswitch Software, czyli twórca oprogramowania dla firm rynku MŚP z 30-letnią historią. Firma Ipswitch została jednak wchłonięta przez dużo większego Progressa około dwóch lat temu, choć w dalszym ciągu bez większych problemów znaleźć można odwołania do poprzedniego właściciela, przeglądając dokumentację oraz bazę wiedzy dotyczącą WhatsUp Gold.

OTWARTE REST API POZWALA NA INTEGRACJĘ WHATSUP GOLD Z OPROGRAMOWANIEM FIRM TRZECICH

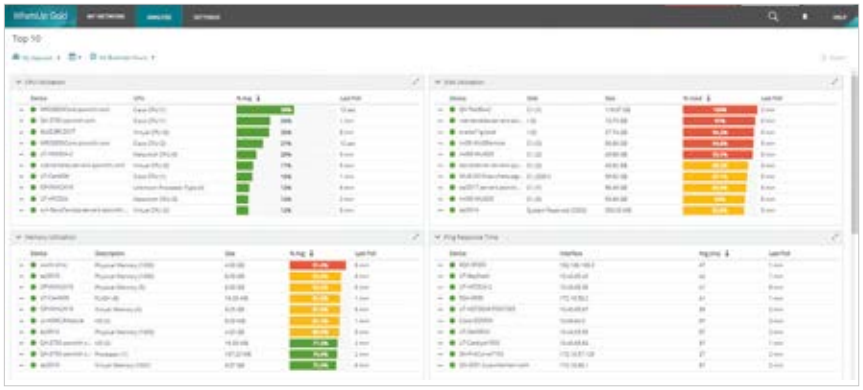
> FUNKCJONALNOŚĆ

Pierwszym i zarazem najbardziej naturalnym krokiem tuż po wdrożeniu WhatsUp Gold jest przeprowadzenie rozpoznania sieci w celu automatycznej detekcji wszystkich podpiętych do niej urządzeń. W tym celu oprogramowanie używa oczywiście protokołu ICMP, a także skanera portów TCP jako podstawowych narzędzi detekcji. Bardziej szczegółowa inwentaryzacja wymaga zdefiniowania własnej biblioteki danych uwierzytelniania dla wszystkich rodzajów urządzeń klienckich pracujących w sieci. Najpopularniejsze mechanizmy szczegółowej detekcji opierają się na protokole SNMP w wersjach od 1. do 3. głównie dla urządzeń sieciowych oraz na obiektach WMI dla systemów rodziny Windows. Ponadto zdefiniować można również dane dostępowe do systemów wykorzystujących protokoły SSH oraz Telnet, dzięki czemu możliwe jest chociażby zdalne wykonywanie poleceń powłoki. WhatsUp Gold wspiera również identyfikację platform wirtualizacyjnych VMware oraz Hyper-V, dzięki czemu na mapie sieci łatwo zidentyfikować maszyny wirtualne przypisane do odpowiednich hostów. Na liście predefiniowanych poświadczeń dla systemów zdalnych znaleźć też można następujące aplikacje: ADO, JMX, Ubiquiti czy SMI-S (wykorzystywany do pobierania danych ze wspieranych rozwiązań typu storage).

WhatsUp Gold to nie tylko monitoring i zarządzanie infrastrukturą lokalną. Oprogramowanie pozwala także monitorować stan oraz wydajność usług dwóch najpopularniejszych dostawców chmurowych – AWS oraz MS Azure, dla których przewidziano dedykowane opcje uwierzytelniania w bibliotece poświadczeń. Dostępna jest także dedykowana opcja dla kontrolera sieci bezprzewodowych w chmurze – Cisco Meraki. WhatsUp Gold pozwala także wykrywać tradycyjną infrastrukturę sieci bezprzewodowej, zarówno z poziomu kontrolerów WLC,



Standardowy Dashboard pozwala szybko ocenić stan pracy monitorowanej sieci.



Gotowe raporty utylizacji zasobów pozwalają namierzyć wąskie gardła.

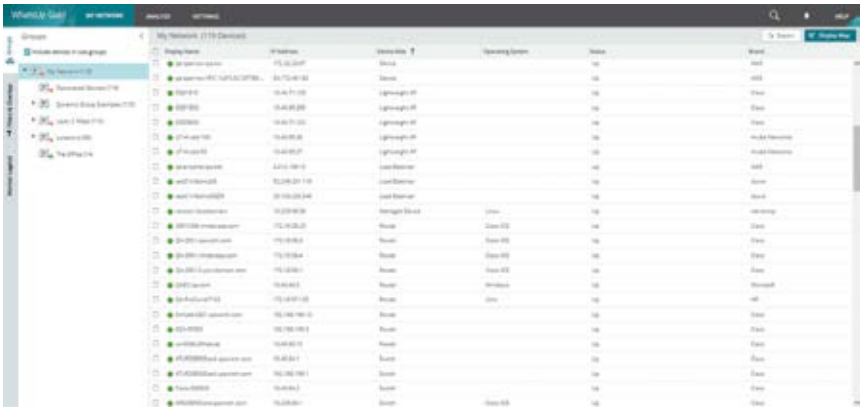
jak też niezależnych punktów dostępowych, dzięki czemu mapa sieci pozwala łatwo zidentyfikować tego typu połączenia wraz z informacjami na temat użytkowników Wi-Fi. W ten sposób z poziomu pojedynczego interfejsu dostępny jest podgląd statusu pracy oraz wydajności zarówno środowiska lokalnego, jak też chmurowego. W przypadku chmury poza standardowymi parametrami wspierane są też raporty dotyczące analizy kosztów.

WhatsUp Gold poza standardowymi cechami NMS pozwala również na monitoring innych elementów infrastruktury, takich jak serwery oraz aplikacje, a także usługi wybranych dostawców chmurowych.

Mając już zdefiniowaną listę poświadczeń dla wszystkich usług i urządzeń, które zamierzamy monitorować, można przystąpić do procedury skanowania. Lista poświadczeń przetwarzana jest sekwencyjnie, zatem istotne jest, aby dane logowania dla hostów wirtualizacji, usług chmurowych czy kontrolerów sieci bezprzewodowej znajdowały się na szczycie listy. Zadania skanowania sieci można dopasować do własnych wymagań czy rozmiaru środowiska, ograniczając zakres adresów IP oraz rodzaju usług. Zbyt szeroka definicja skanowania z uwzględnieniem wszystkich wspieranych typów środowisk i protokołów, szczególnie dla dużych środowisk, może spowodować znaczne obciążenie serwera. W tym celu dostępne są opcje limitowania skanowania do wskazanego zakresu podsieci i liczby urządzeń. Można również wykluczyć ze skanowania

urządzenia wykryte w poprzednich próbach. Proces skanowania można także zaplanować z wykorzystaniem harmonogramów. Wśród dodatkowych opcji zaznaczyć można również powiadamianie mailowe po zakończeniu skanu, rozwiązywanie nazw dla wykrytych hostów czy parametry time out dla skanów ICMP, SNMP oraz WMI.

Wykryta infrastruktura wyświetlana jest w formie wielowarstwowych map sieci lub listy urządzeń. Siatka powiązań tworzona jest na podstawie danych pobranych z urządzeń sieciowych za pomocą protokołu SNMP, więc jeśli nie zdecydujemy się w pierwszym podejściu na użycie właśnie tego protokołu, to wykryte urządzenia będą wizualizowane jako samotne wyspy na mapie sieci. Dostępne są także dynamiczne grupy pozwalające kategoryzować wykryte urządzenia pod kątem przynależności do danej klasy sprzętu czy rodzaju usługi. Każdemu wykrytemu urządzeniu przypisywana jest w sposób automatyczny główna rola oraz role pomocnicze. Kategoryzacja bazuje na informacjach pozyskanych w trakcie skanu. Oczywiście administrator systemu ma możliwość modyfikacji roli w sposób ręczny, tak aby odzwierciedlała ona rzeczywistą funkcję danego urządzenia. Automatyczne wskazanie głównej roli dla serwera hostującego zarówno silnik bazodanowy, jak też usługi SMTP, HTTP czy FTP nie zawsze musi być celne. Rola urządzenia zazwyczaj determinuje także rodzaj domyślnie dostępnych monitorów i tak np. dla predefiniowanego serwera DNS sprawdzane są odpowiedź na ping, działanie wentylatorów serwera, temperatura czy stan zasilania. Listę elementów do sprawdzenia, podobnie jak pozostałe atrybuty wbudowanych ról, można dowolnie modyfikować. Można także tworzyć własne definicje ról, tak aby odwzorować potrzeby własnego środowiska, przypisując odpowiednie monitory. Domyślnie dostępna biblioteka predefiniowanych ról zawiera kilkadziesiąt pozycji, wśród których znaleźć można



Informacje o wykrytych urządzeniach można wyświetlić tabelarycznie lub w formie mapy sieci.

tak popularne pozycje jak routery, firewalle, load balancery, serwery email, FTP, vCenter itd.

Nieco bardziej rozbudowana jest biblioteka wbudowanych monitorów, czyli zróżnicowanych testów, za pomocą których sprawdzane są dostępność i stan usług na monitorowanych urządzeniach. Dostępne są trzy kategorie monitorów: aktywne, pasywne oraz wydajnościowe. Pierwsza grupa reprezentuje testy symulujące zachowanie użytkowników różnego rodzaju usług sieciowych, takich jak chociażby HTTP, FTP czy SMTP. W tym celu nawiązywane jest połączenie z badaną usługą i wykonywany skrypt pozwalający na sprawdzenie statusu działania aplikacji. W ten sposób sprawdzić można chociażby ważność certyfikatu SSL, parametry SLA usługi VoIP czy czas odpowiedzi na kwerendę SQL. Możliwości są spore dzięki wsparciu dla PowerShella, REST API czy VBScript oraz JScript. Testy pasywne z kolei nie generują ruchu sieciowego symulującego zachowanie użytkowników i nie są wyzwalane z poziomu serwera WhatsUp Gold. Mowa tu o tradycyjnych logach systemowych oraz trapach SNMP. Pasywny monitoring to także przesyłanie informacji o przepływach sieciowych z routerów z wykorzystaniem jednego ze wspieranych protokołów typu NetFlow czy sFlow. Ostatnia grupa testów to monitory wydajności poszczególnych parametrów pracy w funkcji czasu, czyli wszelkiego rodzaju utylizacja zasobów, takich jak CPU, zajętość dysku czy obciążenie interfejsów.

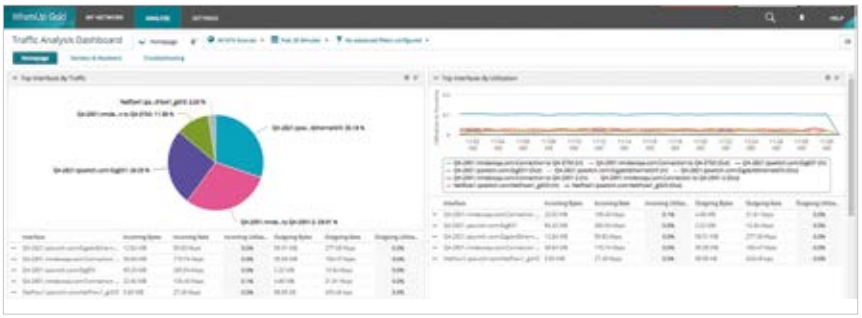
Dysponując już pełnym skanem sieci, wraz z dostępną mapą połączeń i zależności, uzupełnioną o monitoring wybranych usług i parametrów pracy, potrzebowalibyśmy interfejsu pozwalającego w łatwy sposób uzyskać wgląd w najbardziej kluczowe informacje o stanie sieci. W tym celu dostępne jest menu analityki zebranych informacji, które umożliwia wgląd w zebrane dane na różnych płaszczyznach. Standardowy Dashboard pozwala w szybki sposób zorientować się co do liczby aktywnych urządzeń w sieci oraz statusu dostępności i zakresu monitoringu. Zestaw wyświetlanych informacji można w prosty sposób personalizować, dodając kolejne, predefiniowane widgety. Aranżacja widoku realizowana jest na zasadzie drag & drop. Panel sterowania przystosowany jest do wyświetlania wielu statystyk, związanych chociażby z utylizacją zasobów obliczeniowych, obciążeniem interfejsów sieciowych czy alertami wyzwolonymi poprzez przekroczenie wartości progowych wybranych parametrów. Dostęp do raportów skategoryzowano na podstawie wydajności, sieci, urządzeń, alertów oraz danych inwentaryzacyjnych. Dostępne jest także wbudowane menu pozwalające na rozszerzoną analizę zebranych logów.

Ponadto dostępne jest dedykowane menu monitoringu aplikacji, co umożliwia śledzenie parametrów dostępności i wydajności dla monitorowanego software'u. WhatsUp Gold pozwala rozpoznać aplikacje, których działanie bazuje na wielu uruchomionych w tle programach. Takie podejście pozwala na dokładne określenie przyczyny potencjalnego problemu z dostępnością usługi. Dobrym przykładem jest sam WhatsUp, którego poprawne działanie uzależnione jest od dostępności wielu usług, takich jak chociażby serwer SQL czy usługa IIS. Wbudowana biblioteka profili aplikacyjnych obejmuje najpopularniejsze produkty, jak chociażby bazy danych MySQL w różnych wersjach, programy Microsoftu, takie jak Exchange czy SQL, produkty Oracle lub serwer Apache. Dla każdej profilowanej aplikacji zdefiniowano wymagania co do wymaganych ról i uruchomionych monitorów.

Kolejnym przydatnym modułem WhatsUp jest Configuration Management, za pośrednictwem którego administrator może zarządzać konfiguracją monitorowanych urządzeń sieciowych. Poza standardową archiwizacją historycznych plików konfiguracyjnych dostępna jest także biblioteka najczęściej wykorzystywanych skryptów oraz zadań, które mogą być wykonywane w sposób periodyczny. Inną ciekawą funkcją jest analiza plików konfiguracyjnych pod kątem zgodności z politykami konfiguracyjnymi obowiązującymi w danym przedsiębiorstwie. Dzięki temu łatwo zidentyfikować urządzenia, które chociażby zezwalają na dostęp z wykorzystaniem protokołu Telnet lub nie mają skonfigurowanego hasła do trybu uprzywilejowanego.

Uzupełnieniem danych pozyskanych z poziomu różnego rodzaju monitorów omówionych dotychczas jest funkcja Network Traffic Analysis, pozwalająca na analizę wzorców ruchu sieciowego i statystyk pochodzących z wielu źródeł. WhatsUp Gold może być kolektorem informacji o przepływach sieciowych zbieranych z poziomu routerów, przełączników czy firewalli w formatach NetFlow, NetFlow-Lite, sFlow, J-FLow lub IPFIX. Na podstawie zgromadzonych danych dostępne są rozbudowane statystyki oraz raporty pozwalające zidentyfikować podejrzaną aktywność w sieci. Poza standardową analizą przepływów sieciowych można także skorelować zebrane informacje z bazą danych reputacji IP. Domyślnie wraz z aplikacją skonfigurowana jest jedynie lista węzłów wyjściowych sieci Tor, dzięki czemu administrator może zidentyfikować „własne" hosty komunikujące się z tą siecią. Nic nie stoi na przeszkodzie, aby dodać własne listy, chociażby definiujące dobrze znane serwery spamujące.

Inna ciekawa funkcja WhatsUpa to scentralizowane zarządzanie logami Windows Event Log oraz Syslog. Dzięki integracji w ramach tego samego interfejsu użytkownika możliwe jest szybkie reagowanie i generowanie alertów w oparciu o zebranych logów. W celu efektywnego zarządzania logami aplikacja przechowuje je w dedykowanej instancji Elasticsearch.



Moduł analizy przepływu danych jest opcjonalny, ale warto dopłacić za tę opcję.

> WYMAGANIA I INSTALACJA

Test WhatsUp Gold zbiegł się w czasie z premierą najnowszej wersji v21.0, która trafiła na nasz redakcyjny stół testowy. Wersja ewaluacyjna, którą można pobrać ze strony producenta, pozwala na testowanie możliwości aplikacji przez 14 dni. Ze względu na szeroki wachlarz możliwości programu posiłkowaliśmy się również wersją demonstracyjną, ogólnodostępną na serwerze producenta. W tym przypadku środowisko testowe było zdecydowanie większe niż to, które można wykreować we własnym zakresie na potrzeby testu. Najnowsza wersja to również kilka nowości. Jedną z najważniejszych jest integracja wspomnianej już funkcjonalności Log Management w ramach tego samego interfejsu zarządzania WhatsUp. Druga najważniejsza opcja to wsparcie dla publicznie dostępnego interfejsu REST API, dzięki któremu możliwa jest niemal dowolna integracja z produktami firm trzecich.

Wspominając wszystkie dostępne opcje, nie sposób nie wspomnieć o dostępnych wersjach i sposobie licencjonowania. WhatsUp Gold można nabyć zarówno w modelu subskrypcyjnym z corocznym odnowieniem licencji, jak i w formie licencji wieczystej. Obie opcje dostępne są dla wersji PREMIUM, która w standardzie pozwala na korzystanie z podstawowego zestawu funkcji, takich jak: monitoring urządzeń, automatyczne wykrywanie węzłów, mapy sieci, monitoring dostępności i wydajności, alerty i powiadomienia, personalizowane raporty, a także monitoring sieci bezprzewodowych, macierzy dyskowych i usług w chmurze. Pozostałe funkcje wspomniane w tekście, czyli Network Traffic Analysis, Application Monitoring, Virtualization Monitoring, Configuration Management, Log Management oraz Scalability Pollers, dostępne są w formie dodatków opcjonalnych i wymagają dokupienia osobnych licencji. Ponadto dla licencji wieczystej wersji PREMIUM dostępna jest funkcja umożliwiająca pracę w klastrze failover. Wersja PREMIUM to +

także licencjonowanie zgodnie z liczbą zarządzanych urządzeń końcowych. Dostępna jest także wersja TOTAL PLUS, która zawiera już wszystkie płatne dodatki poza funkcją klastra failover, płatną osobno. W tym przypadku zmienia się również sposób licencjonowania. Zamiast prostej kalkulacji opartej na liczbie urządzeń płacimy za punkty licencyjne, przeliczane odpowiednio względem wykorzystywanych funkcji. Dla przykładu, 1 punkt pozwala na standardowy monitoring jednego urządzenia typu serwer, router czy maszyna wirtualna, ale już skorzystanie z zaawansowanych funkcji typu Log Management czy NTA będzie kosztowało nas 10 punktów za źródło logów lub pojedyncze źródło analizy przepływów sieciowych (flow). Producent przewiduje też sprzedaż dedykowanych edycji dla rozproszonych środowisk.

WhatsUp Gold ma wsparcie tylko dla platformy systemowej Microsoftu. Na potrzeby testów wspierana jest nawet wersja desktopowa systemu Windows 10, choć wdrożenie produkcyjne powinno odbyć się już na MS Windows Server 2012+. Wraz z wersją instalacyjną dostarczany jest silnik bazy danych. Domyślnie jest to wersja MSSQL 2017 Express. Nic nie stoi na przeszkodzie, aby skorzystać z osobnego serwera bazodanowego w pełnej wersji. W tym przypadku wspierane są wersje Standard lub Enterprise, począwszy od wydania 2012. Minimalne wymagania sprzętowe to cztero-rdzeniowy procesor taktowany z częstotliwością co najmniej 2,6 GHz, a także 8 GB pamięci operacyjnej oraz 25 GB przestrzeni dyskowej. Takie parametry serwera powinny wystarczyć na efektywny monitoring środowiska składającego się ze 100 urządzeń i 500 aktywnych monitorów. Powyżej 20 tys. urządzeń producent rekomenduje odseparowanie instancji WhatsUp Gold od serwera bazodanowego. Ponadto zalecane jest co najmniej 16 GB pamięci operacyjnej dla aplikacji oraz 64 GB RAM dla serwera bazodanowego. Co ciekawe – wymagania co do stacji roboczej, z której będziemy zarządzali WhatsUpem za pośrednictwem webGUI, nie należą do najmniejszych. Producent sugeruje procesor klasy i5 oraz 8 GB RAM. W naszym środowisku testowym spełnione zostały wszystkie wymagania zarówno co do serwera, jak i stacji roboczej, a pomimo to niektóre elementy menu ładowały się relatywnie długo, biorąc pod uwagę fakt, iż monitorowaliśmy raptem 11 urządzeń. Sam interfejs użytkownika jest nieźle zaprojektowany, szczególnie patrząc przez pryzmat mnogości dostępnych funkcji. W niektórych widokach zauważyć jednak można brak konsekwencji – menu kontekstowe pod prawym klawiszem myszy jest dostępne tylko dla wybranych opcji, a próba wywołania go w innych oknach kończy się wywołaniem domyślnych opcji przeglądarki, co może nieco frustrować.

Sama instalacja, co charakterystyczne dla większości ówczesnych aplikacji, jest prosta i sprowadza się do przeklikania kilku okien instalatora. Konfiguracja SQL Express czy usługi IIS nie wymaga kompletnie żadnej uwagi użytkownika. Oczywiście można również zmodyfikować domyślne ustawienia instalacji dla scenariuszy w topologii rozproszonej lub kiedy chcemy skorzystać z zewnętrznego serwera bazodanowego. Specjalna uwaga będzie również wymagana w przypadku instalacji drugiej instancji w konfiguracji failover. IT

Autor jest architektem w międzynarodowej firmie z branży IT. Zajmuje się infrastrukturą sieciowo-serwerową, wirtualizacją infrastruktury i pamięcią masową.

PODSUMOWANIE

WhatsUp Gold to potężne narzędzie, którego możliwości wykraczają poza standardowy zestaw funkcji charakteryzujący typowe produkty NMS. Uporządkowany i relatywnie prosty w obsłudze interfejs pozwala na łatwą nawigację w gąszczu funkcji. Podstawowa wersja programu zaspokoi większość wymagań małych i średnich przedsiębiorstw w kontekście efektywnego monitorowania całej infrastruktury sieciowo-serwerowej. Bardziej wymagający użytkownicy docenią z pewnością możliwości pracy w trybie failover wraz z opcją implementacji rozwiązania w środowisku rozproszonym geograficznie. Pomimo relatywnie niewielkiej rozpoznawalności produktu na polskim rynku WhatsUp Gold nie ustępuje konkurencji pod względem funkcjonalności, szczególnie jeśli weźmiemy pod uwagę dodatki licencjonowane osobno. Na pochwałę zasługuje także świetna i obszerna dokumentacja, w której znaleźć można wszystkie niezbędne informacje dotyczące instalacji, obsługi, a także potencjalnego troubleshootingu.

Werdykt

WhatsUp Gold

Zalety

- funkcjonalność wykraczająca poza ramy NMS
- proste i elastyczne licencjonowanie
- możliwość pracy w trybie failover
- różnorodność wbudowanych raportów
- wyczerpująca dokumentacja
- Network Traffic Monitoring

Wady

- responsywność webGUI

Ocena **9**/10