



Marcin Matuszewski
inżynier Pomocy Technicznej w Axence

ABC władcy sieci. O podstawach skutecznego zarządzania infrastrukturą IT

Zasoby informatyczne to prawdziwa kopalnia wiedzy dla administratora sieci. Profesjonalne zarządzanie nimi pomaga zachować ciągłość procesów i bezpieczeństwo IT każdej organizacji. Pozwala również uniknąć wielu awarii i kosztów związanych z ich usunięciem, a także oszczędzi czas, który można poświęcić na rozwijanie biznesu. Na co zwrócić uwagę przy tworzeniu polityk w zakresie monitorowania infrastruktury IT?

Wybór narzędzi

Dobór odpowiedniego narzędzia wspomagającego administrację siecią to kwestia kluczowa. Dedykowane oprogramowanie do monitorowania zasobów sprawdza się nawet, gdy zarządzaniu podlega kilkaset stacji roboczych i urządzeń sieciowych. Zanim jednak podjęta zostanie decyzja o wyborze konkretnego rozwiązania, należy zastanowić się nad potrzebami. Jakie informacje i funkcje są niezbędne, by realnie usprawnić działanie sieci? Wśród narzędzi monitorujących znaleźć można zarówno proste, jak i kompleksowe rozwiązania, pozwalające uzyskać wymierne rezultaty.

Przygotowanie mapy sieci

Aby skutecznie zarządzać infrastrukturą IT trzeba określić, jakie urządzenia i serwisy w niej działają. Kolejną czynnością powinno być pogrupowanie urządzeń (np. według typu: routery, switche, telefony, urządzenia przenośne itd.). Każdemu z urządzeń warto przypisać odpowiednią ikonę reprezentującą typ, co pozwoli na ich szybsze odnajdywanie i usprawni późniejszą pracę. Zwizualizowane powinny zostać również połączenia między urządzeniami. Program Axence nVision umożliwia rozwinięcie tego zadania przez stworzenie inter-

aktywnych map sieci. Każdą ikonę sprzętową można umieścić na schemacie pomieszczeń zgodnie z faktycznym położeniem, co ułatwi dotarcie do zepsutego urządzenia.

Kolejne kroki, dodanie nowych funkcjonalności

Gdy sieć jest zwizualizowana, pora na monitorowanie. Służą do tego m.in. liczniki wydajności, które można konfigurować wedle własnych preferencji i doświadczeń. Warto określić wartości krytyczne, po przekroczeniu których automatycznie wysyłane będą powiadomienia lub akcje korekcyjne (np. restart usługi). Dzięki protokołowi WMI można odczytać informacje o konkretnych podzespołach stacji roboczej, np. obciążeniu procesora lub pamięci. Z kolei SNMP pozwala odczytać ogromną ilość informacji z urządzeń sieciowych np. widok map portów lub obciążenie interfejsów na switchu, a także – przy pomocy dodatkowych czujników – parametry środowiskowe: wilgotność lub temperaturę w serwerowni.

Inne dane, które można uzyskać, to m.in. poprawność i czas odpowiedzi serwisów, statystyki ilości odebranych/utraconych pakietów czy zmiany stanu usług Windows. Bardziej szczegółowe informacje ze stacji

roboczych gromadzić może dodatkowo, zainstalowane na nich oprogramowanie – Agent. W przypadku Axence nVision umożliwia on m.in. zebranie listy zainstalowanego oprogramowania oraz konfiguracji sprzętowej w ramach modułu inwentaryzacji. Pozyskane dane umożliwiają sprawne zarządzanie licencjami, kontrolowanie ich kosztów, a przede wszystkim pozwalają uniknąć kar za posiadanie nielegalnego oprogramowania.

Ile kosztuje bezpieczeństwo?

Monitoring i diagnostyka sieci jest bardzo istotna dla każdego biznesu. Umiejętność skutecznego zarządzania siecią chroni przed wieloma problemami wynikającymi np. z nieodpowiedniej konfiguracji lub działania szkodliwego oprogramowania. Z raportu HP Polska¹ wynika, że aż 59% decydentów IT uważa wdrożenie narzędzi do monitorowania IT za działanie podnoszące poziom bezpieczeństwa ich firm. Ile to kosztuje? Na rynku dostępnych jest wiele programów zawierających opisywane w artykule funkcje. Warto jednak zwrócić uwagę na te rozwiązania, które posiadają bezpłatną licencję również do użytku komercyjnego. Bardzo dobrym przykładem takiego programu jest Axence nVision w wersji Free, który poza omówionymi w artykule funkcjami, wyróżnia się przejrzystym i intuicyjnym interfejsem.