AdRem NetCrunch

Wersja 4.x

Podręcznik użytkownika

System monitorowania i zarządzania sieciami

AdRem Software, sp. z o.o.
ul. Wadowicka 8a
30-415 Kraków
Polska

tel.: +48 (12) 252 83 00
faks: +48 (12) 252 83 01
e-mail: sales@adrem.com.pl

witryna internetowa: www.adrem.com.pl

Spis treści

Wstęp

Niniejszy podręcznik użytkownika przeznaczony jest dla administratorów sieci oraz innych specjalistów odpowiedzialnych za zarządzanie firmowymi sieciami komputerowymi. Przedstawione w nim zostały metody wykorzystania rozbudowanych funkcji programu AdRem NetCrunch – takich jak wizualizacja, monitorowanie, alertowanie oraz raportowanie – do nadzorowania sieci firmowej w sposób efektywny zarówno pod względem osiąganych oszczędności czasowych, jak i odpowiednio niskich nakładów finansowych. Ponieważ w przeważającej mierze podręcznik ten odnosi się do sieci opartych na protokole TCP/IP, począwszy od tego miejsca termin „sieć" będzie oznaczać sieć działającą w oparciu o protokół TCP/IP, chyba że w danym przypadku zostanie wyraźnie określone, że chodzi o inny rodzaj sieci.

Ogólna charakterystyka

Szkoda czasu na przestoje. Tak najkrócej można streścić główny motyw zastosowania programu NetCrunch firmy AdRem. Utrzymanie najwyższego poziomu dostępności sieci oraz oferowanych usług staje się w oczywisty sposób czynnikiem krytycznym w każdej firmie, która dąży do osiągnięcia rynkowego sukcesu. Globalizacja rynku, nowe formy działalności, technologiczne innowacje, a także rosnąca potrzeba sprostania wymaganiom stale rozbudowującego się Internetu, tworzą dziś zapotrzebowanie na bezpieczne, niezawodne i odporne na błędy rozwiązania gwarantujące wysoką dostępność usług i aplikacji sieciowych.

Nie dysponując specjalistycznymi i dającymi się łatwo przystosować rozwiązaniami służącymi do monitorowania, alertowania czy diagnozowania, łatwo jest przeoczyć awarie kluczowych urządzeń, usług sieciowych lub aplikacji. Pracownicy, partnerzy biznesowi czy klienci stają się w coraz to większym stopniu zależni od nieprzerwanego, całodobowego dostępu do danych udostępnianych za pośrednictwem firmowej sieci. Każdy przestój lub niedostępność usługi mogą mieć niekorzystny wpływ na wydajność pracy poszczególnych pracowników i mogą prowadzić do znaczącego zmniejszenia ogólnej efektywności działania. Co gorsza, jeżeli awaria sieci nastąpi w czasie dni świątecznych lub podczas weekendu, wówczas usługi o istotnym znaczeniu lub nawet cała firmowa sieć mogą pozostawać niedostępne dla klientów lub dostawców przez wiele godzin, a nawet dni – zanim problem zostanie wykryty. W najgorszej wersji takiego scenariusza potencjalny klient, nie mogąc skontaktować się z przedstawicielem danej firmy, zniechęci się i wybierze ofertę konkurencji.

Korzystając z programu NetCrunch 4.x firmy AdRem Software administrator sieci już nie musi martwić się taką perspektywą, gdyż w przypadku przestoju lub sytuacji awaryjnej to właśnie on będzie powiadomiony w pierwszej kolejności. Program AdRem NetCrunch w sposób ciągły, w odpowiednich odstępach czasu, próbkuje poszczególne zasoby sieci, sprawdzając w ten sposób ich dostępność. Wyświetla tworzony w czasie rzeczywistym czytelny obraz wydajności sieci oraz przedstawia działanie systemu i poszczególnych dostępnych w nim usług na przejrzystych mapach graficznych. W sytuacji awarii lub wyraźnego pogorszenia parametrów działania, program NetCrunch automatycznie powiadamia o tym za pośrednictwem poczty e-mail lub pagera, odpowiednich,

przewidzianych w harmonogramie administratorów, dostarczając im równocześnie niezbędnych informacji diagnostycznych.

Ponadto dla poszczególnych urządzeń generowane mogą być szczegółowe raporty dotyczące ich wydajności w dowolnym okresie czasu – zarówno bieżącym, jak i przeszłym (raporty historyczne). Inną pożyteczną funkcją programu jest zbieranie zapisu trendów. Umożliwia ona zachowanie odpowiedniej jakości funkcjonowania sieci firmowych oraz wydłuża czasu ich prawidłowego działania.

Program AdRem NetCrunch stanowi doskonałe narzędzie do nieustannego sprawdzania stanu firmowej sieci lub może być wykorzystywany jako dedykowany instrument do monitorowania określonych podsieci, krytycznych usług sieciowych albo aplikacji rozproszonych. Jest on również polecany konsultantom jako pomoc w rozwiązywaniu problemów z sieciami obejmującymi kilka różnych lokalizacji. Ponieważ NetCrunch jest klientem systemu Windows, mogą oni instalować go na komputerach przenośnych i mieć go zawsze do dyspozycji. Opracowany z myślą o zastosowaniu w małych i średnich sieciach, program ten został wyposażony w szereg użytecznych funkcji umożliwiających monitorowanie sieci w dłuższym okresie czasu.

Podstawowe zastosowania programu

Graficzna prezentacja sieci

Typowa infrastruktura informatyczna we współczesnej firmie stanowi skomplikowany zbiór systemów, procesów, danych, oprogramowania i sprzętu. Od sprawnego współdziałania wszystkich zasobów składających się na daną sieć uzależnione jest niezakłócone dostarcza nie przez nią usług informatycznych i właściwa obsługa procesów związanych z działalnością firmy. Z tego powodu kluczowego znaczenia dla każdego działu informatyki w przedsiębiorstwie nabiera graficzna prezentacja zasobów sieciowych i zachodzących pomiędzy nimi współzależności. Każda informacja staje się z reguły bardziej zrozumiała, gdy jest przekazywana w formie graficznej, na przykład w postaci map. Mapy pozwalają w odpowiedni sposób skonfigurować i dostosować prezentowane widoki sieci, tak aby użytkownicy mogli szybko i skutecznie dotrzeć do interesujących ich informacji.

W rzeczywistych zastosowaniach mapy mogą ilustrować zarówno całą fizyczną i logiczną strukturę sieci, jak i różne ujęcia funkcjonalne jej topologii. W tym ostatnim przypadku graficzna reprezentacja sieci może być oparta na takich kryteriach jak lokalizacja geograficzna, struktura jednostek organizacyjnych lub odpowiadać innym uwarunkowaniom, wynikającym ze specyfiki danej firmy. Ta różnorodność i elastyczność w prezentowaniu struktury sieci pozwala lepiej rozumieć różne elementy jej topologii, a w rezultacie bardziej skutecznie ją nadzorować i serwisować. Oprogramowanie NetCrunch obsługuje w pełnym zakresie funkcję automatycznego wykrywania sieci i udostępnia prawie nieograniczoną liczbę opcji wykorzystywanych przy tworzeniu różnych rodzajów jej wizualizacji.

Alertowanie

System powiadamiania administratorów sieci lub kierowników działów o zakłóceniach w dostępności lub wydajności zasobów sieciowych wpływa w istotny sposób na ogólną sprawność sieci, a w rezultacie na kondycję całej firmy. Jest oczywiste, że reakcja na sytuację awaryjną powinna nastąpić możliwie jak najszybciej, angażując możliwie jak najmniej środków. Nie ulega więc wątpliwości, że alertowanie stanowi integralną część procesu monitorowania sieci. Dzięki niemu możliwe jest stałe otrzymywanie informacji na temat bieżących problemów występujących w monitorowanej sieci i podejmowanie natychmiastowych działań zmierzających do ich usunięcia lub zapobieżenia im – w pewnych sytuacjach program może nawet przeprowadzić takie działania naprawcze w sposób automatyczny. Alertowanie ułatwia administratorom wykonywanie powierzonych im zadań, pomagając w wykrywaniu i rozpoznawaniu potencjalnych źródeł problemów, jakie mogą w przyszłości pojawić się w nadzorowanej sieci lub w poszczególnych jej składnikach.

W programie NetCrunch reguły alertowania mogą być określane dla pojedynczych węzłów sieci lub dla grup węzłów (na które składają się poszczególne mapy sieci bądź cały atlas). Możliwe jest również definiowanie schematów eskalacji alertów, polegających na tym, iż pewne zdarzenia w sieci – w zależności od ich priorytetu – uruchamiają określony zestaw akcji podejmowanych w różnych odstępach czasowych i obejmujących dodatkowy ciąg poleceń o różnej randze. W ten sposób gdy pierwsza podejmowana w wyniku określonego zdarzenia akcja – wymagająca zaangażowania najmniejszych zasobów – nie przynosi w założonym czasie pożądanego skutku, może zostać uruchomiona inna, bardziej zaawansowana akcja (powiadomienie lub procedura automatycznego przywracania stanu normalnego), wykorzystująca bardziej zaawansowane metody rozwiązywania problemów. Program może podjąć różnego rodzaju akcje – od powiadomienia (na przykład poprzez wysłanie wiadomości pocztą e-mail, wysłanie trapu SNMP lub wyświetlenie okna dialogowego na pulpicie), do lokalnego lub zdalnego uruchomienia programu lub skryptu, a nawet zapisania informacji związanych z danym alertem do odpowiedniego pliku.

Raportowanie

Kolejnym priorytetowym zadaniem każdego administratora sieci jest stałe zbieranie i wykorzystanie informacji o historii jej działania oraz o jej wydajności. Zasadniczo, najważniejszym celem raportowania jest dostarczanie informacji na temat wydajności zarówno samej sieci, jak i poszczególnych jej elementów – takich jak usługi czy aplikacje – uzyskanych w dłuższym horyzoncie czasowym. Ich analiza w istotny sposób pomaga administratorom i kadrze kierowniczej w planowaniu rozwoju sieci, jak również w eliminowaniu wąskich gardeł obniżających jej wydajność. Tak więc funkcja raportowania to kluczowe narzędzie dostarczające ważnych wskaźników wykorzystywanych przy planowaniu obciążeń oraz zarządzaniu zasobami.

Na podstawie informacji uzyskanych w wyniku przetwarzania zdarzeń oraz zebranych zapisów trendów NetCrunch może tworzyć zestaw typowych raportów, dotyczących zarówno pojedynczego węzła, jak i grup węzłów należących do danej mapy lub do całego atlasu. W dowolnej chwili możliwe jest wygenerowanie któregokolwiek ze wstępnie zdefiniowanych typów raportów, a nawet zażądanie przesłania w odpowiednim czasie przedstawionych w nim wyników innym użytkownikom.

Monitorowanie sieci

Podstawowe pojęcia

Ponieważ sieć ze swej natury jest strukturą niezwykle złożoną, trudno jest ustalić jedyny właściwy sposób jej opisu. Jedną z możliwości jest skupienie się na najbardziej podstawowych elementach składowych sieci czyli na węzłach wraz z przypisanymi do nich adresami sieciowymi. Tak więc w naszym podręczniku opis elementów sieciowych rozpoczynać się będzie od warstwy drugiej modelu OSI. A to oznacza, że węzły traktowane tu będą jako elementy reprezentujące pojedyncze unikatowe adresy TCP/IP. Poziom ten posłuży jako punkt wyjścia do opisu elementów należących do wyższych warstw modelu OSI, np. warstwy usług sieciowych (takich jak PING, FTP, POP3, HTTP), warstwy interfejsów sieciowych, warstwy usług i procesów systemu Windows oraz warstwy wydajności aplikacji każdego monitorowanego elementu sieciowego.

Monitorowanie aktywne

Monitorowanie aktywne oznacza, że program w sposób ciągły testuje węzły zdalne oraz mierzy czas ich odpowiedzi.

Najprostszym rodzajem monitorowania przeprowadzanym przez program NetCrunch jest monitorowanie dostępności, które określa wyłącznie aktualny stan obiektu (czyli to, czy dany węzeł lub usługa odpowiadają, czy też nie).

Stan węzła ustalany jest na podstawie stanu udostępnianych przez ten węzeł usług sieciowych, które poddawane są monitorowaniu. Aby ułatwić sprawdzanie dostępności węzła, program NetCrunch w sposób domyślny testuje usługę PING, wysyłając komunikaty ICMP.

Jednakże w niektórych sytuacjach informacje uzyskane w ten sposób nie są wystarczające, gdyż nie mówią nic o jakości połączeń w sieci. Dlatego też program może także mierzyć liczbę utraconych pakietów oraz czas odpowiedzi każdej usługi sieciowej.

Monitorowanie inteligentne

Ograniczanie ruchu związanego z monitorowaniem

NetCrunch służy do monitorowania bezagentowego. W programach bezagentowych bardzo często sam proces monitorowania może wywoływać dodatkowy niepożądany ruch w sieci. Aby ograniczyć generowanie takiego dodatkowego ruchu, program NetCrunch został wyposażony w unikalną technologię monitorowania inteligentnego. Polega ona na ustalaniu górnych wartości progowych ruchu w sieci, których podczas jej monitorowania program nie może przekroczyć. Innym elementem tej technologii jest automatyczne dostosowywanie przez program NetCrunch czasu monitorowania sieci do zdefiniowanego w ten sposób progu. Przykładowo, jeśli monitorowanie pewnej sieci wymaga przesłania 1 MB danych,

a użytkownik ustali górny próg ruchu na 5 kB/s, to wówczas przesłanie takiej ilości danych zajmie około 3 minuty, i taki będzie właśnie oczekiwany czas monitorowania węzłów tej sieci.

Określanie zależności sieciowych

Zależności sieciowe stanowią wygodny sposób na uniknięcie niepożądanych zdarzeń oraz ograniczenie ruchu związanego z monitorowaniem.

Wybiórcze monitorowanie nieodpowiadających węzłów

W sytuacji gdy dany węzeł nie odpowiada, w celu ustalenia stanu połączenia z takim węzłem NetCrunch może monitorować jedynie usługę określoną jako usługę wiodącą. W tym czasie wszystkie pozostałe monitory znajdują się w stanie *Oczekiwanie na odpowiedź*.

Mechanizm wstrzymywania zdarzeń

Program umożliwia określenie, które zdarzenia dotyczące zmiany stanu węzła lub usługi sieciowej będą generowane lub wstrzymywane na wyłączonych przez współzależność węzłach podrzędnych w momencie, gdy węzeł nadrzędny z jakiegoś powodu przestaje odpowiadać. Funkcja ta jest dostępna wyłącznie w edycji Premium XE programu.

Priorytety monitorowania usług sieciowych

Opcja przyznawania węzłom krytycznym wyższego priorytetu umożliwia monitorowanie w pierwszej kolejności działających na nich usług sieciowych, a dopiero później usług na innych rodzajach węzłów. Dla mniej istotnych węzłów możliwe jest także obniżanie priorytetu monitorowania. Funkcja ta jest dostępna wyłącznie w edycji Premium XE programu.

Monitorowanie wydajności

W przypadku usług sieciowych wydajność można wyznaczyć w prosty sposób – poprzez pomiar czasu odpowiedzi oraz liczby utraconych pakietów. Jednak przeważnie istnieje potrzeba monitorowania także innych elementów, takich jak interfejsy sieciowe (porty) lub aplikacje działające w danym węźle. Jedynym sposobem na osiągnięcie tego celu jest śledzenie statystyk zbieranych w danym węźle. Rodzaj zastosowanych statystyk jest uzależniony od rodzaju węzła. Przykładowo, węzły działające pod kontrolą systemu Windows udostępniają pewną ilość liczników mierzących wykorzystanie różnego rodzaju zasobów (np. liczniki związane z procesorem, sieciami, wątkami, obiektami systemowymi oraz liczniki właściwe dla danej aplikacji). Ponadto wiele urządzeń sprzętowych, takich jak drukarki, rutery czy przełączniki, udostępnia pewną liczbę statystyk charakterystycznych dla wykonywanych przez nie zadań. Program NetCrunch ułatwia uzyskanie dostępu do tych różnorodnych informacji poprzez zdefiniowanie powszechnie stosowanych raportów i zdarzeń z wykorzystaniem wstępnie zdefiniowanych liczników i progów. W większości przypadków do uzyskania tych informacji program używa protokołu SNMP, jednakże w przypadku komputerów działających pod kontrolą systemów Windows lub NetWare oprogramowanie NetCrunch może również korzystać z protokołów właściwych dla danego systemu operacyjnego.

Reprezentacja sieci

Węzły

Jak już wspomniano, węzeł jest podstawowym obiektem, poprzez który uzyskujemy dostęp do jego zasobów, usług i aplikacji. Ponieważ węzeł reprezentuje pojedynczy adres TCP/IP, może się zdarzyć, że jedno urządzenie fizyczne może być przedstawione w programie za pomocą kilku węzłów. W tym przypadku zalecane jest wprowadzenie w jednym z takich węzłów monitorowania wydajności i usług, a dla pozostałych węzłów reprezentujących to urządzenie – wybranie opcji *uproszczonego monitorowania*.

Mapy

Mapy umożliwiają łączenie węzłów w grupy, co okazuje się niezwykle pomocne w przypadku zarządzania dużą ilością węzłów. Inną zaletą – natury estetycznej – jest możliwość tworzenia takich map graficznych, które pozwalają na uzyskanie eleganckich strukturalnych map sieci, wyposażonych w odsyłacze do innych map.

Logiczna sieć IP

Na tego rodzaju mapie przedstawiane są logiczne sieci IP zarządzane przez program. Użytkownik może umieszczać na niej wyłącznie węzły należące do danej sieci. Mapa tego typu może być tworzona ręcznie przez użytkownika bądź automatycznie przez sam program – poprzez dodawanie do niej kolejnych nowo wykrywanych węzłów.

Topologia fizyczna

NetCrunch może także przedstawiać na mapach schemat fizycznych połączeń między komputerami i zarządzanymi przełącznikami. Aby było to możliwe, urządzenia muszą obsługiwać bazę MIB mostu SNMP. Zawartość map topologii fizycznej jest zarządzana wyłącznie przez program, a użytkownicy nie mogą dokonywać zmian w ich wyglądzie.

Widok filtrowany

Program NetCrunch umożliwia tworzenie map zarządzanych automatycznie, powstających na podstawie określonych kryteriów filtrowania. Przykładem takiego widoku może być mapa zawierająca urządzenia tego samego rodzaju lub zlokalizowane w tym samych miejscu.

Widok własny

Jest to najprostszy rodzaj mapy tworzonej przez program. Widoki własne wstawiają na pustą mapę dowolne wykryte w sieci węzły, odpowiednio je przy tym rozmieszczając. Widoki takie są w pełnym zakresie zarządzane przez użytkowników.

Wykresy

Wykresy stanowią w programie graficzną reprezentację określonych liczników wydajności monitorowanych w dowolnym węźle atlasu. Widoki wykresów mogą być na bieżąco aktualizowane przez program lub zarządzane ręcznie przez użytkownika.

Atlas sieci

Atlas jest obiektem znajdującym się najwyżej w hierarchii obiektów w programie – zawiera on zbiór wszystkich monitorowanych obiektów i ich widoków. Atlas to swego rodzaju dokument, w którym przechowywana jest zarówno sama jego treść, jak i style oraz wszelkie inne związane z nim ustawienia. Tuż pod obiektem atlasu znajduje się specjalny *Wykaz węzłów* umożliwiający łatwy dostęp do wszystkich monitorowanych węzłów sieciowych. Kolejne sekcje atlasu zawierają mapy i widoki monitorowanej sieci.

Atlas sieci został podzielony na dwie sekcje zarządzane przez program automatycznie (*Sieci IP* oraz *Topologia fizyczna*) oraz dwie kolejne sekcje zarządzane przez użytkownika (*Widoki własne* oraz *Widoki wydajności*).

Podstawowe sekcje atlasu sieci:

Sieci IP	Zawiera mapy sieci IP. Mapy te mogą być w dowolny sposób przenoszone w ramach sekcji *Sieci IP*.
Topologia fizyczna	Zawiera listę map przedstawiających fizyczną topologię sieci. Linie połączeń umieszczane na mapach topologii fizycznej reprezentują rzeczywiste, fizyczne kable sieciowe, łączące poszczególne urządzenia. Mapy należące do tej sekcji nie mogą być zarządzane przez użytkownika, jednakże można modyfikować ich układ.
Widoki własne	Ta sekcja może zawierać dowolną ilość różnego rodzaju widoków sieci. Tworzenie takich widoków pozwala na oglądanie i analizowanie sieci z wielu różnych punktów widzenia.
Widoki wydajności	Zawiera wykresy (liniowe, słupkowe lub w postaci wskaźników wychyłowych) przedstawiające dane pochodzące z określonych liczników wydajności monitorowanych w węzłach SNMP, NetWare lub Windows.

Rodzaje map (w poszczególnych sekcjach atlasu sieci):

	**Wykaz węzłów**	Tabela wszystkich węzłów należących do aktualnie otwartego atlasu – wykrytych przez program lub dodanych ręcznie przez użytkowników.
	**Mapa logiczna**	Mapa utworzona na podstawie logicznego adresowania IP. Należy do sekcji *Sieci IP*.
	**Mapa routingu**	Mapa routingu monitorowanej sieci. Należy do sekcji *Widoki własne*.
	**Mapa współzależności monitorowania**	Mapa wyświetlająca węzły, które posiadają co najmniej jeden zależny od nich węzeł, a także występujące między nimi rzeczywiste współzależności monitorowania.

	**Mapa widoku filtrowanego**	Mapa własna, której zawartość jest automatycznie aktualizowana przez program.
	**Mapa własna**	Mapa własna, której zawartość jest statyczna, czyli może być aktualizowana wyłącznie w sposób ręczny, przez użytkownika.
	**Mapa segmentów**	Mapa należąca do sekcji *Topologia fizyczna*, tworzona na podstawie fizycznej topologii sieci.
	**Mapa portów**	Mapa należąca do sekcji *Topologia fizyczna*, przedstawiająca wszystkie elementy, które są aktualnie podłączone do określonego portu. Mapa ta również jest tworzona na podstawie fizycznej topologii sieci.

Alertowanie

Funkcja alertowania to funkcja powszechnie udostępniana w narzędziach do monitorowania sieci. Pozwala ona użytkownikom w szybki sposób wykrywać i diagnozować powstające problemy, zarówno te krytyczne, jak i te mniej istotne, a docelowo – usuwać je. Alertowanie jest integralną częścią procedury testowania sieci oraz reagowania na wszelkie zmiany, jakie wykrywane są albo w jej działaniu, albo w ogólnej wydajności poszczególnych jej składników. Bez możliwości monitorowania sieci w czasie rzeczywistym nie byłoby możliwe uzyskanie istotnych danych pomiarowych, wykorzystywanych przez proces alterowania.

Mówiąc najprościej, alertowanie to ogólny proces zbierania informacji o stanie sieci i reagowania na określone warunki i zdarzenia. A uściślając – alertowanie polega na definiowaniu przez użytkownika zdarzeń, jakie w pewnych warunkach mogą wystąpić w dowolnym miejscu monitorowanej sieci, oraz akcji uruchamianych w odpowiedzi na te zdarzenia. Zwykle wystąpienie takiego zdarzenia związane jest z wykorzystaniem pewnych danych, uzyskanych wcześniej w wyniku prowadzenia monitorowania sieci, takich jak zmiana stanu urządzenia bądź przekroczenie wartości progowej w licznikach wydajności. Z kolei sama akcja alertująca może przybrać wiele form, takich jak na przykład powiadomienie wysłane do użytkownika bądź automatyczne uruchomienie określonej procedury.

Uwaga

Odpowiednie skonfigurowanie alertowania pozwala wyeliminować niepotrzebny ruch w danej sieci oraz zbędne akcje alertujące.

Podstawowe pojęcia

Istotne jest w tym miejscu rozróżnienie między alertami a zdarzeniami. Zdarzenia można określić jako pewne warunki, jakie mogą zachodzić w sieci, i jakie w związku z tym mogą być rejestrowane w danym systemie komputerowym (lub w określonych systemach komputerowych) przez program monitorujący. Ogrywają one zasadniczą rolę zarówno w procesie alertowania, jak i raportowania. Podczas monitorowania sieci zdarzenia są gromadzone i przechowywane w bazie danych będącej dziennikiem zdarzeń. Zdarzenia

stają się alertami wówczas, gdy zostaną skojarzone z określonymi akcjami. Mogą wtedy posłużyć na przykład do powiadomienia właściwych użytkowników, bądź wywołania procedury naprawczej.

Klasy zdarzeń

Ponieważ każdy warunek wystąpienia zdarzenia może zostać opisany za pomocą różnego rodzaju zestawów parametrów, z tego względu wszystkie zdarzenia zostały podzielone na odpowiednie klasy. Taka klasyfikacja ułatwia definiowanie zdarzeń, gdyż z każdą klasą zdarzeń może być związany dedykowany edytor zdarzeń. Aby ułatwić odnalezienie właściwej klasy zdarzeń zostały one pogrupowane następujące pięć kategorii.

Zdarzenia ogólne

Heartbeat	Zdarzenie informujące użytkownika, czy program NetCrunch jest uruchomiony i działa poprawnie.

Zdarzenia w węźle

Zdarzenie stanu węzła	Zdarzenie polegające na zmianie stanu węzła (ODPOWIADA lub NIE ODPOWIADA).
Zdarzenie związane z monitorem stanu węzła	Zdarzenie informujące użytkownika, czy w określonym czasie węzeł niezmiennie znajduje się w żądanym stanie (ODPOWIADA lub NIE ODPOWIADA) .
Stan interfejsu sieciowego	Zdarzenie polegające na zmianie stanu interfejsu sieciowego (ODPOWIADA lub NIE ODPOWIADA).
Akcje na węźle	Zdarzenie polegające na *wykryciu*, *usunięciu*, *wyłączeniu monitorowania* lub *włączeniu monitorowania* węzła.
Akcje na mapie	Zdarzenie polegające na dodaniu lub usunięciu węzła z określonej mapy.
Komunikat Syslog	Zdarzenie polegające na nadejściu komunikatu Syslog ze zdalnego węzła.

Usługi sieciowe

Stan usługi sieciowej	Zdarzenie polegające na zmianie stanu usługi sieciowej (np. PING, HTTP lub FTP) w określonym węźle.
Próg dostępności usługi sieciowej	Zaawansowany rodzaj zdarzenia polegającego na przekroczeniu wartości progowej w liczniku wydajności dowolnej usługi sieciowej (np. PING, HTTP, FTP) w danym węźle.

Progi i trapy SNMP

Próg wydajności SNMP	Zaawansowany rodzaj zdarzenia polegającego na przekroczeniu wartości progowej w dowolnym liczniku wydajności SNMP w węźle zarządzanym za pomocą agenta SNMP.
Trap SNMP	Zdarzenie polegające na nadejściu z danego węzła trapu SNMP.

Windows

Próg wydajności aplikacji	Zaawansowany rodzaj zdarzenia polegającego na przekroczeniu wartości progowej w dowolnym liczniku wydajności systemu Windows NT w węźle (dotyczy tylko węzłów Windows).
Stan usługi Windows	Zdarzenie polegające na zmianie stanu usługi systemu Windows w węźle (*zatrzymana, uruchomiona, wstrzymana*).

NetWare

Próg wydajności Novell NetWare	Zaawansowany rodzaj zdarzenia polegającego na przekroczeniu wartości progowej w dowolnym liczniku wydajności systemu NetWare w węźle (dotyczy tylko węzłów NetWare).

Progi

Progi są integralnym, zaawansowanym elementem procesu alertowania. Złożone definicje zdarzeń są z reguły powiązane z określonymi wartościami progowymi. Wartości te uzyskiwane są przeważnie w wyniku monitorowania różnego rodzaju liczników wydajności, uzależnionych od systemu operacyjnego zainstalowanego w danych węźle. Choć wartości progowe są trudniejsze do zdefiniowania, umożliwiają one zarządzanie procesem alertowania w sposób o wiele bardziej elastyczny. Korzystanie z mechanizmu wartości progowych pozwala uzyskać pełniejszy wgląd w to, co dzieje się w monitorowanej sieci.

Aby ułatwić definiowanie progów, w programie NetCrunch udostępniony został specjalny kreator, w którym można określać wszystkie rodzaje wartości progowych. W praktyce kreator ten służy do definiowania wszystkich rodzajów zdarzeń – zarówno tych opartych na prostej zmianie stanu, jak i tych polegających na przekroczeniu pewnych wartości progowych.

Definiowanie

Dla potrzeb procesu alertowania próg można zdefiniować jako górną lub dolną wartość graniczną, której przekroczenie wywołuje określony rodzaj odpowiedzi (na przykład pewną akcję). Istnieją dwa rodzaje progów – narastający i opadający. Próg narastający polega na tym, że jeśli ustalona wartość graniczna zostanie przekroczona, nastąpi określona akcja, jeżeli natomiast wartość monitorowanego parametru spadnie poniżej tej wartości granicznej, wówczas nie zostanie podjęta żadna akcja. Próg opadający działa analogicznie, przy czym założenie jest takie, że określona akcja zostanie wykonana wówczas, gdy wartość monitorowanego parametru spadnie poniżej ustalonej wartości granicznej. W sytuacji

gdy wartość śledzonego parametru przekroczy tę wartość graniczną, nie jest podejmowana żadna akcja. Tak więc skutecznie korzystanie z mechanizmu progów wymaga monitorowania pewnego rodzaju liczników wydajności w funkcji czasu. Zanim program zareaguje podjęciem jakiejś akcji lub szeregu akcji, musi wcześniej śledzić – przez odpowiedni okres czasu – zmiany wartości określonego licznika w celu wykrycia momentu, kiedy przekroczona zostanie uprzednio zdefiniowana dla tego licznika wartość progowa. Poza podstawowym rodzajem progu NetCrunch udostępnia także trzy inne klasy wartości progowych; należy je jednak traktować w kategoriach przypadków nadzwyczajnych, gdyż w dużej mierze znajdują one zastosowanie jedynie w bardzo konkretnych sytuacjach.

Aby progi mogły skutecznie wspomagać proces alertowania, należy zdefiniować następujące właściwości (to, które z nich mają zastosowanie, uzależnione jest od konkretnego rodzaju warunku progowego):

Typ warunku progu	Typ warunku progowego może mieć postać jednej z następujących par: podstawowy (narastający/opadający), nagła zmiana (narastający/opadający), stan (jest równe/jest różne), obecność (odebrano dowolną wartość/nie odebrano żadnej wartości).
Licznik wydajności	Określa parametr, który ma być mierzony w funkcji czasu w celu określenia, czy jego wartość przekroczyła wartość graniczną lub spadła poniżej niej (odpowiednio dla progu narastającego lub opadającego). Licznik wydajności może być związany z dowolnym obiektem Windows, NetWare lub SNMP, bądź z dowolną usługą sieciową monitorowaną na danym węźle.
Czas monitorowania	Określa, jak często dany licznik wydajności będzie sprawdzany w celu uzyskania jego aktualnej wartości. Możliwość zmiany częstotliwości odpytywania ma istotne znaczenie dla całego procesu alertowania przeprowadzanego z wykorzystaniem progów.
Wartość (graniczna)	*(dotyczy wyłącznie progów podstawowych i progów kategorii „stan")* Określa górną lub dolną wartość graniczną dla danego progu (w zależności od tego, czy jest to próg narastający, czy opadający). Jeżeli na liczniku wydajności aktualnie monitorowany parametr przekracza zdefiniowaną wartość krytyczną lub, odpowiednio, spadnie poniżej niej, następuje wygenerowanie właściwego zdarzenia.
Wartość resetująca (Resetuje się przy)	*(dotyczy wyłącznie progów podstawowych*) – Określa graniczną wartość resetującą dla danego progu. W przypadku progu narastającego, gdy monitorowany licznik wydajności spadnie poniżej wartości resetującej, próg zostanie zresetowany. Analogicznie w przypadku progu opadającego, próg ten zostanie zresetowany, gdy wartość licznika wydajności przekroczy wartość resetującą. Aby uprościć definiowanie progu, można ustawić wartość resetującą identyczną z ze zdefiniowaną wartością graniczną.

Okres uśredniania wartości)	(*dotyczy wyłącznie progów podstawowych i progów kategorii „nagła zmiana”*) – określa czas (w minutach), jaki powinien upłynąć od momentu naruszenia wartości granicznej do uznania faktu naruszenia danego warunku progowego. W tym czasie wartość licznika wydajności będzie nadal odczytywana z częstotliwością odpowiadającą ustalonemu wcześniej czasowi monitorowania, a po upływie zdefiniowanego czasu opóźnienia UŚREDNIONA wartość dokonanych w międzyczasie odczytów posłuży do podjęcia decyzji, czy dany próg został faktycznie przekroczony.
Opóźnienie	*(dotyczy wyłącznie warunków progowych kategorii „stan” i „obecność”)* – określa czas (w minutach), jaki powinien upłynąć od momentu naruszenia wartości granicznej do uznania faktu naruszenia danego warunku progowego. Z reguły opóźnienie ma wartość nieco wyższą od czasu monitorowania, dzięki czemu uwzględniane są zmiany zachodzące w dłuższym przedziale czasu.
Tolerancja (%)	*(dotyczy wyłącznie warunków progowych kategorii „nagła zmiana”)* – określa w procentach odchylenie mierzonej wartości w porównaniu do uśrednionej wartości w określonym przedziale czasu. Jeśli aktualna wartość przekroczy poza zdefiniowaną wartość tolerancji, zostanie wygenerowane zdarzenie związane z powyższym rodzajem progu.
Margines błędu (%)	*(dotyczy wyłącznie warunków progowych kategorii „nagła zmiana”)* – określa margines błędu, w granicach którego może spaść aktualna mierzona wartość – w stosunku do średniej wartości – aby powodować zresetowanie progu. Oznacza to, że gdy aktualna wartość spada do przedziału marginesu błędu średniej wartości, ten rodzaj progu jest resetowany.
Generuj lub Nie Generuj (Przy resetowaniu)	Określa, czy należy generować zdarzenie w sytuacji, gdy warunki określonego typu progu są spełnione i jest on resetowany.

Uwaga

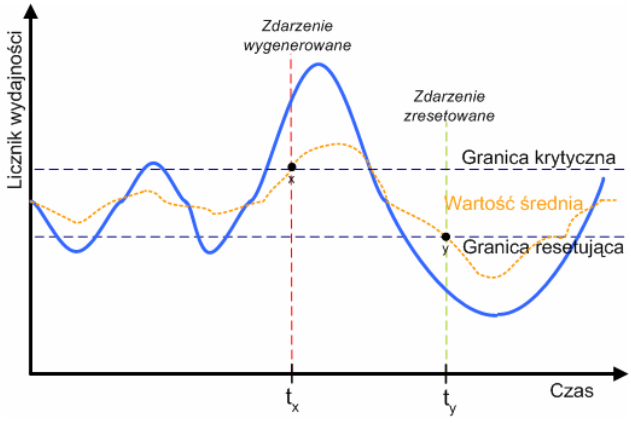
Używanie okresu uśredniania wartości lub opóźnienia zalecane jest w sytuacji, gdy mierzony ma być parametr, który ma tendencję do przypadkowych oscylacji w funkcji czasu (tzn. do nagłych i skrajnych wahań następujących w stosunkowo krótkich przedziałach czasowych). W takiej sytuacji, jeżeli nie zostanie zastosowany czas opóźnienia, istnieje znaczne prawdopodobieństwo, iż wartość graniczna będzie w stosunkowo krótkim odstępie czasu wielokrotnie przekraczana. Za każdym razem spowoduje to wygenerowanie zdarzenia polegającego na przekroczeniu wartości progowej, przez co uzyskane w ten sposób odczyty nie będą pomocne. Natomiast zastosowanie czasu opóźnienia bądź uśrednianie odczytu w czasie ułatwia ocenę odczytów pochodzących z danego licznika wydajności, a także stwierdzenie, czy wykazują one tendencję do przekraczania przyjętych wartości progowych.

Typ podstawowy

Typ podstawowy warunku progowego może mieć postać narastającą bądź opadającą – są one względem siebie przeciwstawne. Próg narastający wykorzystywany jest w alertowaniu do reagowania na sytuacje, gdy średnia mierzonych w funkcji czasu wartości licznika wydajności przekracza pewien punkt krytyczny (gdy to nastąpi, generowane jest odpowiednie zdarzenie oraz ewentualnie podejmowane są stosowne akcje). Kiedy zaś średnia wartości aktualnie monitorowanego parametru w przedziale czasu spadnie poniżej innego punktu (zwanego wartością resetującą) – lub zrówna się z nim – wówczas próg jest resetowany. Wartość krytyczna (graniczna) wyznacza zatem górną granicę progu narastającego, zaś wartość resetująca wyznacza jego granicę dolną.

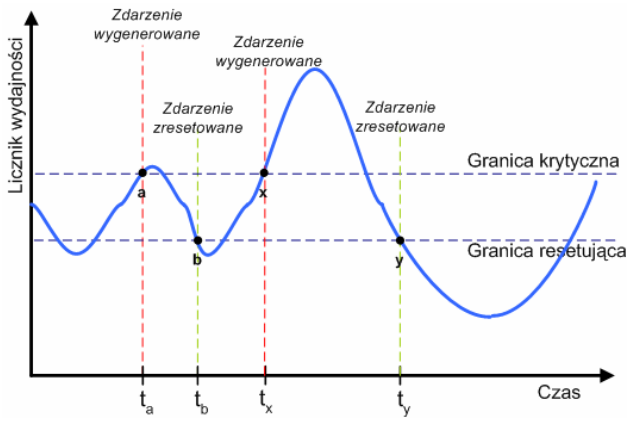
Definicja podstawowego progu narastającego wygląda następująco:

```
Wygeneruj zdarzenie związane z progiem, jeśli wartość „LICZNIKA WYDAJNOŚCI” przekroczy
krytyczną granicę „WARTOŚCI”. Zresetuj stan progu i „GENERUJ LUB NIE GENERUJ”
zdarzenia, jeśli wartość odczytu jest zrówna się lub spadnie poniżej granicy o wartości
„Wartość resetująca”. Wartość licznika zostanie obliczona jako średnia wartości
odczytanych podczas „OKRESU UŚREDNIANIA WARTOŚCI” w minutach.
```



Rys. 1 Przykład progu narastającego

Aby ułatwić procedurę ustalania progu, można zawsze używać aktualnej wartości odczytywanej dla licznika wydajności – zamiast wartości uśrednionej w funkcji czasu – w celu weryfikacji, czy warunki progu są spełnione. W takim wypadku podczas tworzenia definicji progu ustaw właściwość OKRES UŚREDNIANIA WARTOŚCI na wartość 0 minut; w zasadzie spowoduje to wyłączenie mechanizmu uśredniania wartości w przedziale czasu w celu sprawdzenia istnienia warunku. Poniżej zamieszczono przykład uproszczonego progu narastającego.

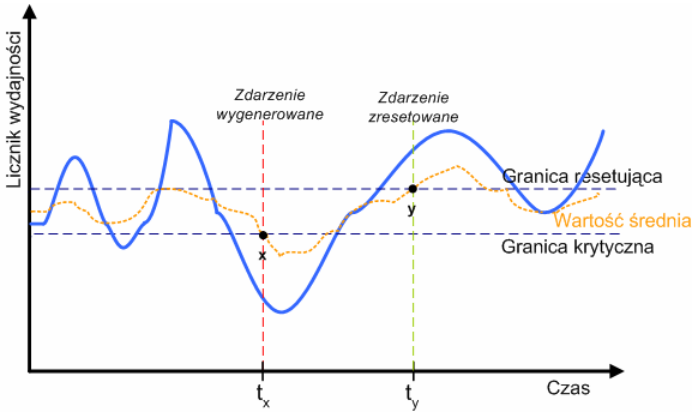


Rys. 2 Przykład uproszczonego progu narastającego

Podstawowy próg opadający stanowi dokładne przeciwieństwo progu narastającego. Próg opadający wykorzystywany jest w alertowaniu do reagowania na sytuacje, gdy wartość mierzona w przedziale czasu przez licznik wydajności spadnie poniżej pewnego punktu krytycznego (gdy to nastąpi, generowane jest odpowiednie zdarzenie oraz ewentualnie podejmowane są stosowne akcje). Kiedy zaś średnia mierzonych na bieżąco wartości parametru zrówna się w przedziale czasu z innym punktem (zwanym wartością resetującą) – lub podniesie się powyżej niego – wówczas próg zostanie zresetowany. W tym przypadku wartość krytyczna (graniczna) wyznacza dolną granicę progu opadającego, zaś wartość resetująca wyznacza jego granicę górną.

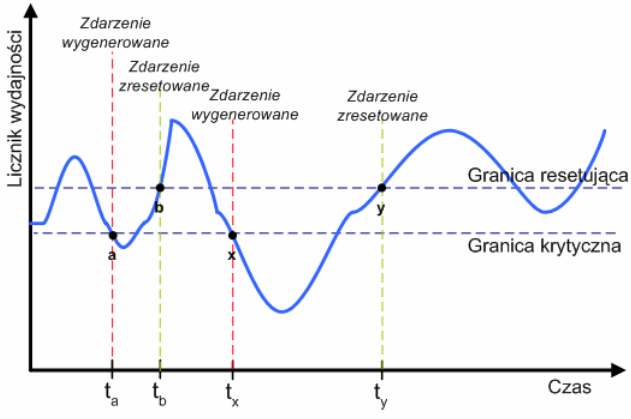
Definicja podstawowego progu opadającego wygląda następująco:

„Wygeneruj zdarzenie związane z progiem, jeśli wartość „LICZNIKA WYDAJNOŚCI” spadnie poniżej krytycznej granicy „WARTOŚCI”. Resetuj stan progu i „GENERUJ LUB NIE GENERUJ” zdarzenia, jeśli wartość odczytu zrówna się lub przekroczy granicę o wartości „Wartość resetująca”. Wartość licznika zostanie obliczona jako średnia wartości odczytanych podczas „OKRESU UŚREDNIONIANIA WARTOŚCI” w minutach.



Rys. 3 Przykład progu opadającego

Aby ułatwić procedurę ustalania progu, można zawsze używać aktualnej wartości odczytywanej dla licznika wydajności – zamiast wartości uśrednionej w funkcji czasu – w celu weryfikacji, czy warunki progu są spełnione. W takim wypadku podczas tworzenia definicji progu ustaw właściwość OKRES UŚREDNIANIA WARTOŚCI na wartość 0 minut; w zasadzie spowoduje to wyłączenie mechanizmu uśredniania wartości w przedziale czasu w celu sprawdzenia istnienia warunku. Poniżej zamieszczono przykład uproszczonego progu opadającego.



Rys. 4 Przykład uproszczonego progu opadającego

Uwagi

- *Z powyższego rysunku wynika, że gdy używany jest okres wartości uśrednionej, próg zostanie wygenerowany jedynie w momencie* **t(x),** *gdy średnia odczytów wartości licznika wydajności (uzyskanych w zdefiniowanym okresie) znajdzie się poniżej krytycznej (dolnej) wartości granicznej. Analogicznie później, w momencie* **t(y)**, *jeśli średnia odczytów wartości licznika wydajności (uzyskanych w zadanym okresie) przekroczy krytyczną (górną) wartość graniczną (wartość resetującą),*

próg zostanie zresetowany. Warto jednakże zauważyć, że na powyższym Rys. 4 zdarzenie zostanie wygenerowane dwukrotnie – mianowicie w momentach **t(a)** *i* **t(x)**, *jeśli nie zostanie użyta wartość uśredniona (dla identycznego zestawu danych licznika wydajności).*

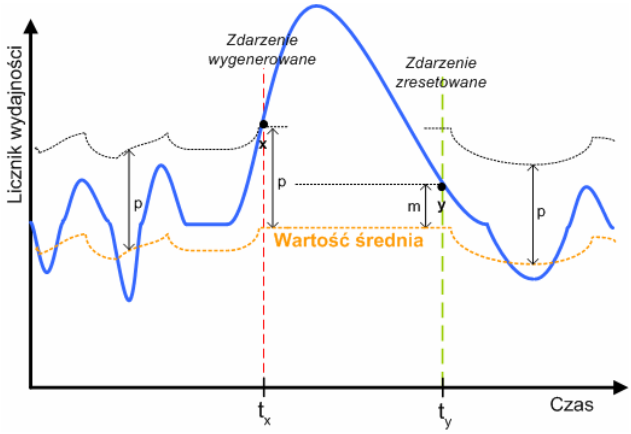
- *Należy pamiętać, że istnieje możliwość dalszego uproszczenia definicji progu narastającego lub opadającego poprzez ustawienie krytycznej wartości granicznej na poziomie identycznym z graniczną wartością resetującą.*
- *Dobrym przykładem zastosowania prostego progu opadającego jest pomiar na określonym komputerze parametru „Procent dostępnej pamięci". W przypadku serwera NetWare można wykorzystać licznik* **% *Dostępnej pamięci*** *dla obiektu* ***Serwer***. *Jest oczywiste, że zdarzenie i akcja powinny nastąpić w momencie, gdy wartość tego parametru spadnie poniżej pewnej procentowej wartości krytycznej. Wartości graniczne – górna i dolna – mogą być ustawione na przykład na wartość 10%. W takim wypadku, gdy dostępna pamięć serwera w procentach spadnie poniżej 10%, zostanie wygenerowane zdarzenie polegające na przekroczeniu wartości progowej, a także uruchomiona zostanie odpowiednia akcja lub zestaw akcji przypisanych temu progowi. Gdy z kolei wartość tego parametru podniesie się i przekroczy poziom 10%, próg zostanie zresetowany.*

Typ „nagła zmiana"

Próg typu „nagła zmiana" może mieć postać progu narastającego lub wznoszącego – są one względem siebie przeciwstawne. Próg narastający typu „nagła zmiana" jest szczególnym rodzajem scenariusza wykorzystywanego w alertowaniu w celu wywołania reakcji w momencie, gdy mierzona wartość notuje nieoczekiwany wzrost do znacznie wyższej wartości niż standardowo zakładano. Uściślając, zdarzenie związane z progiem jest generowane (i ewentualnie podejmowane są stosowne akcje), gdy przyrost odczytywanej na bieżąco wartości licznika wydajności przekracza w sposób nagły spodziewany poziom tolerancji w porównaniu do uśrednionych wartości odczytanych w przedziale czasu. Z tego względu punkt krytyczny jest zawsze obliczany na podstawie aktualnej wartości uśrednionej w stosunku do znajdującej się powyżej niej spodziewanej wartości tolerancji. Zdarzenie zostanie zresetowane, gdy aktualnie odczytana wartość wróci do oczekiwanego poziomu mieszczącego się w granicach względnego marginesu błędu w porównaniu do uśrednionej wartości otrzymanej w danym okresie. Zdarzenie może również zostać zresetowane, gdy odczytana wartość spadnie do dowolnego poziomu znajdującego się poniżej wartości uśrednionej uzyskanej w danym okresie bądź do 0.

Definicja progu narastającego typu „nagła zmiana" przedstawia się następująco:

```
Wygeneruj zdarzenie związane z progiem, jeśli bieżąca wartość „LICZNIKA WYDAJNOŚCI"
zwiększy się o wartość „PROCENTOWEJ TOLERANCJI" w stosunku do uśrednionych wartości
odczytanych podczas ostatniego „OKRESU UŚREDNIANIA WARTOŚCI" w minutach. Zresetuj stan
progu i „GENERUJ LUB NIE GENERUJ" zdarzenia, jeśli aktualna wartość powróci
do poprzedniej wartości uśrednionej o maksymalnym „PROCENTOWYM MARGINESIE BŁĘDU"
marginesu błędu. Poprzednia wartość uśredniona jest obliczana w okresie, w którym
został wygenerowany próg.
```



Rys. 5 Przykład progu narastającego typu "nagła zmiana"

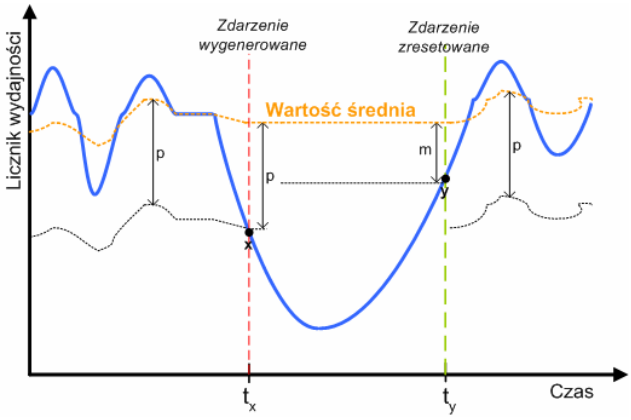
Powyższy Rys. 5 ilustruje omawiany rodzaj progu. **P** to dopuszczalna wartość tolerancji w odniesieniu do wartości uśrednionej obliczonej w określonym przedziale czasu. Warto zauważyć, że gdy poziom tolerancji zostaje naruszony w momencie **t(x)**, zdarzenie jest generowane. Z drugiej strony **m** jest dopuszczalnym marginesem błędu w porównaniu do bieżącej wartości uśrednionej obliczonej w przedziale czasu. W momencie **t(y)** próg zostaje zresetowany, ponieważ aktualnie odczytywana wartość wraca do ustalonego marginesu błędu w porównaniu do wartości uśrednionej obliczonej w danym przedziale czasu.

Próg opadający typu „nagła zmiana" jest uzupełnieniem progu identycznego typu w wersji narastającej. Także ta kategoria progu jest szczególnym rodzajem scenariusza wykorzystywanego w alertowaniu w celu wywołania reakcji w momencie, gdy mierzona wartość notuje nieoczekiwany spadek w stosunku do wartości zwyczajowo oczekiwanej. Uściślając, zdarzenie związane z progiem jest generowane (i ewentualnie podejmowane są stosowne akcje), gdy odczytywana na bieżąco wartość licznika wydajności w krótkim czasie spada o wartość przekraczającą oczekiwany poziom tolerancji w porównaniu do uśrednionych wartości odczytanych w przedziale czasu. Z tego względu punkt krytyczny jest zawsze obliczany na podstawie aktualnej średniej wartości w stosunku do znajdującego się poniżej niej poziomu tolerancji. Zdarzenie zostanie zresetowane, gdy aktualnie odczytywana wartość wróci do oczekiwanego poziomu mieszczącego się w granicach względnego marginesu błędu w porównaniu do uśrednionej wartości otrzymanej w danym okresie. Zdarzenie może również zostać zresetowane, gdy odczytywana wartość wzrośnie do dowolnego poziomu powyżej wartości uśrednionej uzyskanej w danym okresie.

Definicja progu opadającego typu „nagła zmiana" brzmi:

```
Wygeneruj zdarzenie związane z progiem, jeśli bieżąca wartość „LICZNIKA WYDAJNOŚCI"
zmniejszy się o wartość „PROCENTOWEJ TOLERANCJI" w stosunku do uśrednionych wartości
odczytanych podczas ostatniego „OKRESU UŚREDNIANIA WARTOŚCI" w minutach. Zresetuj stan
progu i „GENERUJ LUB NIE GENERUJ" zdarzenia, jeśli aktualna wartość powróci
do poprzedniej wartości uśrednionej o maksymalnym „PROCENTOWYM MARGINESIE BŁĘDU"
```

marginesu błędu. Poprzednia wartość uśredniona jest obliczana w okresie, w którym został wygenerowany próg.



Rys. 6 Przykład progu opadającego typu "nagła zmiana"

Powyższy Rys. 6 ilustruje omawiany rodzaj progu. **P** to dopuszczalna wartość tolerancji w odniesieniu do wartości uśrednionej w określonym przedziale czasu. Warto zauważyć, że gdy poziom tolerancji zostaje naruszony w momencie **t(x)**, zdarzenie jest generowane. Z drugiej strony **m** jest dopuszczalnym marginesem błędu w porównaniu do bieżącej wartości uśrednionej obliczonej w przedziale czasu. W momencie **t(y)** próg jest resetowany, ponieważ aktualnie odczytywana wartość wraca do ustalonego marginesu błędu w porównaniu do wartości uśrednionej obliczonej w danym przedziale czasu.

Uwaga

- *Gdy zdarzenie jest generowane w ramach definicji progu typu „nagła zmiana", aktualna wartość uśredniona w danym okresie nie ulegnie zmianie i będzie używana do sprawdzania, czy aktualnie odczytywana wartość mieści się w marginesie błędu. Na rysunku 7, pokazującym prób opadający, sytuacja taka ma miejsce między momentem **t(x)** a **t(y)**. Gdy zachodzi ten warunek, zdarzenie związane z progiem zostanie zresetowane, a średnia wartość dla danego okresu zostanie obliczona ponownie – na rysunku jest to widoczne po momencie **t(y)**.*
- *Dobrym przykładem zastosowania progu narastającego typu „nagła zmiana" jest licznik wydajnościowy na ruterze wychodzącym związanym z ruchem w sieci. Uściślając, NetCrunch pozwala w ten sposób weryfikować, czy liczba błędów związanych z ruchem w sieci notuje nagłe przeskoki.*

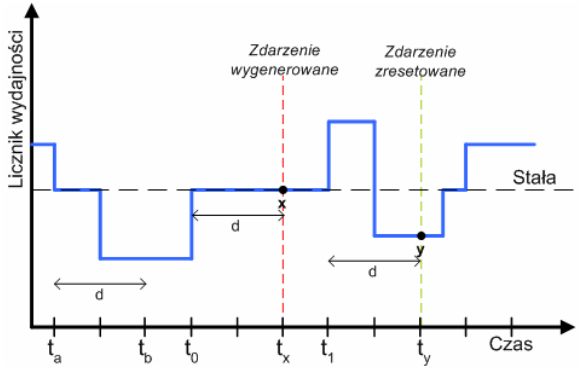
Typ „stan"

Na próg kategorii „stan" składają się dwa komplementarne przypadki. Zasadniczo warunek o treści „stan jest równy (równa się stanowi)" jest stosowany w alertowaniu w celu wywołania odpowiedzi w momencie, gdy mierzona wartość pozostaje przez określony czas na poziomie zdefiniowanej stałej. Zdarzenie z wykorzystaniem progu jest generowane (oraz ewentualnie wykonywane są akcje), kiedy aktualnie odczytana wartość jest identyczna ze zdefiniowaną

stałą krytyczna co najmniej przez wskazany czas opóźnienia. Próg zostanie zresetowany, kiedy ów warunek przestaje zachodzić.

Definicja progu kategorii „stan" („jest równy") brzmi następująco:

```
Wygeneruj zdarzenie z wykorzystaniem progu, jeśli wartość „LICZNIKA WYDAJNOŚCI" jest
równa stałej „WARTOŚCI" co najmniej przez okres „CZAS OPÓŹNIENIA" w minutach. Zresetuj
stan progu i WYGENERUJ LUB NIE GENERUJ" zdarzenia, jeśli powyższy warunek nie zostanie
spełniony w określonym przedziale czasu.
```



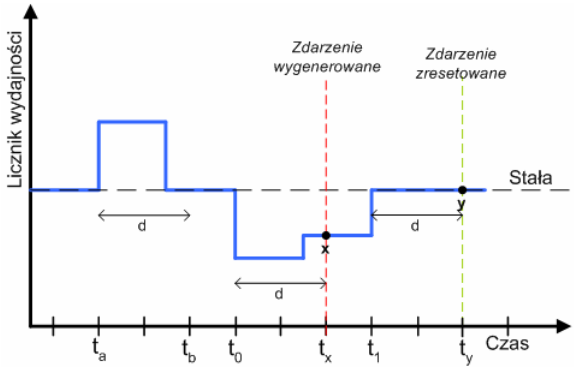
Rys. 7 Przykład progu typu „Stan (Jest równy)"

W ukazanej na powyższym Rys. 7 sytuacji zdarzenie zostanie wygenerowane w momencie **t(x)**, ponieważ odczytana wartość dla licznika wydajności pozostała równa ustanowionej stałej co najmniej przez okres czasu d (czas opóźnienia). Warto odnotować, że w momencie **t(b)** zdarzenie nie zostanie wygenerowane, ponieważ odczytana wartość nie była równa stałej przez okres d.

Uzupełnieniem warunku „jest równy – stan" jest próg typu „jest różny". Warunek rodzaju „jest równy" jest stosowany w alertowaniu w celu wywołania odpowiedzi, gdy mierzona wartość w danym okresie czasu odbiega od przyjętej granicy. Zdarzenie z zastosowaniem progu jest generowane (oraz ewentualnie uruchamiane są akcje), gdy aktualnie odczytana wartość jest różna od zadanej przyjętej stałej co najmniej przez określony czas opóźnienia. Próg jest resetowany, gdy warunek ten przestaje zachodzić.

Definicja progu kategorii „stan" („jest różny") wygląda następująco:

```
Wygeneruj zdarzenie z wykorzystaniem progu, jeśli wartość „LICZNIKA WYDAJNOŚCI" jest
różna od stałej „WARTOŚCI" co najmniej przez okres „CZAS OPÓŹNIENIA" w minutach.
Zresetuj stan progu i WYGENERUJ LUB NIE GENERUJ" zdarzenia, jeśli powyższy warunek nie
zostanie spełniony w określonym przedziale czasu.
```



Rys. 8 Przykład progu kategorii „stan (jest różny)"

W ukazanej na powyższym rysunku Rys. 8 sytuacji zdarzenie zostanie wygenerowane w momencie **t(x)**, ponieważ odczytana wartość dla licznika wydajności pozostała różna od ustanowionej stałej co najmniej przez okres czasu **d** (czas opóźnienia).Należy pamiętać, że w momencie **t(b)** zdarzenie nie zostanie wygenerowane, ponieważ odczytana wartość nie odbiegała od stałej przez okres **d**.

Uwagi

- *Warunek progu typu „jest równy – stan" jest stosowany w szczególnych wypadkach, gdy istotne jest śledzenie konkretnego licznika wydajności, o którym wiadomo, że zawsze powinien być różny od pewnej wartości (stałej).*
- *Z kolei warunek progu typu „jest różny – stan" jest przydatny w przypadku, gdy pewien licznik wydajności standardowo kształtuje się na jakimś stałym poziomie i gdy z tego powodu istotne jest natychmiastowe wykrywanie przypadków, w których taki stan rzeczy ulega zmianie. Dobrym przykładem zastosowania tego rodzaju progu jest utrzymywanie stałej temperatury pomieszczenia w budynku – w momencie, gdy temperatura ulega jakiemukolwiek odchyleniu, odbiegając od stanu pożądanego (stałej), następuje wygenerowanie zdarzenia.*

Typ "obecność"

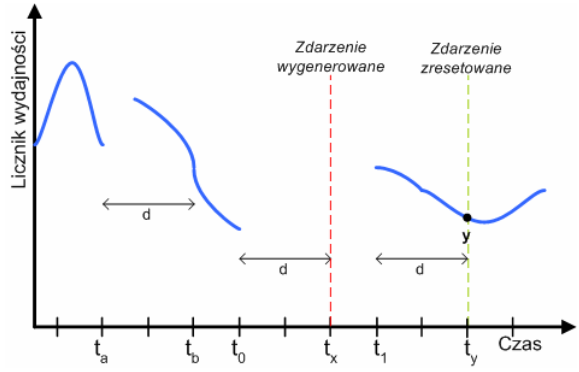
Warunek typu „obecność" jest używany do weryfikowania, czy w danych okresie czasu otrzymano – bądź nie otrzymano – określone dane dotyczące licznika wydajności.

Warunek typu „nie otrzymano wartości" jest stosowany w alertowaniu w celu wywołania odpowiedzi w momencie, gdy przez wskazany okres czasu nie została odebrana żadna wartość dla danego licznika wydajności. Zdarzenie oparte na progu jest generowane (i ewentualnie podejmowane są akcje), gdy co najmniej przez wskazany okres nie zostaje odczytana żadna wartość. Z drugiej strony zdarzenie z zastosowaniem progu jest resetowane, gdy co najmniej przez wskazany okres następuje odczyt jakiejkolwiek wartości.

Definicja warunku typu „nie otrzymano wartości" wygląda następująco:

```
Wygeneruj zdarzenie oparte na progu, jeśli co najmniej przez okres „CZAS OPÓŹNIENIA"
w minutach nie zostanie odebrana wartość „LICZNIKA WYDAJNOŚCI". Zresetuj stan progu
```

i „WYGENERUJ LUB NIE GENERUJ” zdarzenia, jeśli w tym czasie zostanie odczytana dowolna wartość licznika.



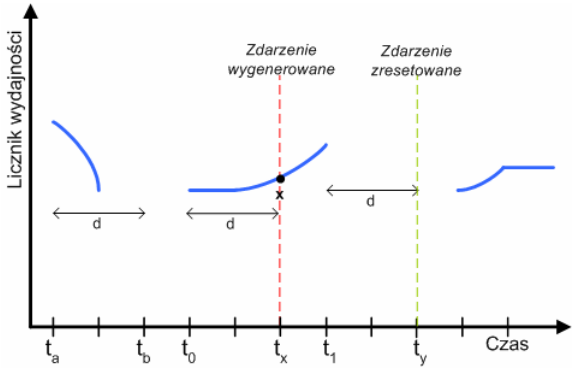
Rys. 9 Przykład progu typu „obecność” („nie otrzymano wartości”)

W przedstawionej na powyższym rysunku sytuacji zdarzenie zostanie wygenerowane w momencie **t(x)**, gdy nie zostanie odebrana żadna wartość licznika wydajności przez okres **d**. Zdarzenie zostanie zresetowane w momencie **t(y)**, gdy dla danego licznika wydajności zostaną odczytane jakiekolwiek wartości. Na uwagę zasługuje fakt, iż w momencie **t(b)** zdarzenie nie zostanie wygenerowane, ponieważ w okresie **d** dane zostały odebrane.

Warunek progu typu „otrzymano dowolną wartość” jest stosowany w alertowaniu w celu wywołania odpowiedzi w sytuacji, kiedy dla licznika wydajności zostanie odebrana dowolna wartość we wskazanym przedziale czasu. Zdarzenie zostanie zresetowane w momencie **t(y)**, gdy dla danego licznika wydajności nie zostaną odczytane żadne wartości w określonym interwale czasowym.

Definicja warunku typu „obecność” (otrzymano dowolną wartość) brzmi następująco:

Wygeneruj zdarzenie oparte na progu, jeśli zostanie odebrana jakakolwiek wartość „LICZNIKA WYDAJNOŚCI” co najmniej przez okres „CZAS OPÓŹNIENIA” w minutach. Zresetuj stan progu i „WYGENERUJ LUB NIE GENERUJ” zdarzenia, jeśli w tym czasie nie zostanie odczytana żadna wartość licznika.



Rys. 10 Przykład progu typu „obecność – otrzymano dowolną wartość"

W zilustrowanej na powyższym rysunku sytuacji zdarzenie zostanie wygenerowane w momencie **t(x)**, ponieważ w okresie **d** odczytano wartość licznika wydajności. Zdarzenie zostanie zresetowane w momencie **t(y)**, gdy dla danego licznika wydajności nie zostaną odczytane żadne wartości. Należy pamiętać, że w momencie **t(b)** zdarzenie nie zostanie wygenerowane, ponieważ w okresie **d** nie zostały odebrane żadne dane.

Uwagi

- *Dobrym przykładem zastosowania warunku „nie otrzymano wartości" jest sprawdzanie, czy konkretny proces (np. związany z istotną usługą sieciową, taką jak aplikacja bazodanowa) odpowiada czy nie. Monitorując nieprzerwanie jeden z jego liczników wydajności i ustawiając warunek typu „nie otrzymano wartości" można wykrywać momenty, w których dana aplikacja bazodanowa przestaje odpowiadać.*
- *Typowym przykładem zastosowania warunku „otrzymano dowolną wartość" jest weryfikowanie, kiedy określony proces (np. związany z aplikacją, które ze względów bezpieczeństwa nie powinna być uruchomiona)zaczyna odpowiadać. Monitorując na bieżąco jeden z jego liczników wydajności i definiując warunek typu „otrzymano dowolną wartość" można wykrywać momenty, w których dana aplikacja bazodanowa zaczyna działać.*

Zastosowanie progów w NetCrunchu

Podczas korzystania w programie z funkcji alertowania istotne jest rozróżnianie poszczególnych rodzajów urządzeń, dla których definiowane są określone progi, gdyż każdy rodzaj urządzeń wyposażony jest w charakterystyczne dla niego liczniki wydajności. Zasadniczo możliwe jest skonfigurowanie progów w czterech różnych kategoriach:

Dostępność usług sieciowych	Użytkownik może wybrać jeden z dwóch liczników wydajności określających dostępność usług sieciowych – procent utraconych pakietów lub czas odpowiedzi.
Wydajność SNMP	Użytkownik ma możliwość wyboru różnych liczników wydajności obiektów SNMP. Dokładna ilość takich liczników uzależniona jest od rodzaju urządzenia zarządzanego za pomocą agenta SNMP.

Wydajność aplikacji Windows	Użytkownik ma możliwość wyboru różnych liczników wydajności obiektów działających w oparciu o system Windows. Ich liczba jest uzależniona od wersji systemu operacyjnego Windows działającego w monitorowanym urządzeniu.
Wydajność Novell NetWare	Użytkownik ma możliwość wybrania różnych liczników wydajności obiektów działających w oparciu o system NetWare.

Uwaga

Wszystkie wyżej wymienione kategorie progów są zdefiniowane w programie NetCrunch jako oddzielne klasy zdarzeń. Oznacza to, że mogą one być wybierane już w pierwszym oknie kreatora definicji zdarzenia.

Definiowanie, włączanie, reagowanie

Procedura uruchamiania alertowania odbywa się w trzech etapach:

1. **Definiowanie** – Pierwszy krok polega na opisaniu zdarzenia, które ma być monitorowane w sieci. Jest to, innymi słowy, dokładne określenie zdarzenia poprzez podanie parametrów opisujących warunki jego wystąpienia.
2. **Włączenie** – Krok drugi to uaktywnienie zdefiniowanego zdarzenia dla danego obiektu w programie. W szczególności może to nastąpić dla całego atlasu (a więc dla każdego monitorowanego węzła), jedynie dla określonej mapy lub dla pojedynczego węzła. Warto zwrócić uwagę, że możliwość przypisywania zdarzeń na trzech różnych poziomach jest bardzo skutecznym narzędziem i umożliwia tworzenie zaawansowanych reguł alertowania. Przy tworzeniu reguł dla atlasów lub map użytkownik może także definiować wyjątki odnoszące się do poszczególnych węzłów.

Uwaga

Tylko włączone zdarzenia są monitorowane i zapisywane do dziennika zdarzeń.

3. **Reagowanie** – Ostatni krok polega na przypisaniu akcji, jakie mają zostać podjęte w wyniku wystąpienia poszczególnych włączonych zdarzeń. W chwili gdy w sieci rzeczywiście wystąpi określone zdefiniowane zdarzenie (zostanie ono wykryte przez program monitorujący), automatycznie uruchomiona zostanie również przypisana mu akcja lub grupa akcji, przy czym nastąpi to albo natychmiast, albo po upływie określonego czasu. Więcej informacji na ten temat można znaleźć w rozdziale *Eskalacja alertów* na stronie 46.

Definiowanie nowych zdarzeń

Aby ułatwić proces definiowania zdarzeń w programie udostępniony został kreator definicji zdarzenia. Aby dodać nowe zdarzenie do listy zdarzeń, należy w oknie **Konfiguracja alertów** kliknąć ikonę ***Dodaj zdarzenie***. Po pojawieniu się okna **Wybierz zdarzenie** należy wybrać obszar zastosowania, do której ma być dodane nowe zdarzenie, a następnie kliknąć ikonę ***Dodaj nowe zdarzenie***. Kreator definicji zdarzenia pomoże zdefiniować warunki wystąpienia

nowego zdarzenia. Należy przy tym pamiętać, że występowanie nowo utworzonego zdarzenia będzie sprawdzane jedynie wówczas, gdy zostanie ono przypisane do jakiegoś atlasu, mapy lub węzła. Więcej informacji na ten temat można znaleźć w rozdziale *Włączanie zdarzeń* na stronie 36.

Z każdą klasą zdarzeń związane są charakterystyczne dla niej parametry warunków. Zazwyczaj jednak wszystkie definicje zdarzeń zawierają co najmniej trzy pola, które muszą być zawsze określone, bez względu na klasę zdarzeń, do której należy zdefiniowane zdarzenie.

Opis	W polu tym określana jest nazwa nowego zdarzenia, służąca do odróżniania go od innych zdarzeń. Ten opis zdarzenia jest widoczny na liście zastosowań wyświetlanej w oknie **Konfiguracja alertów** – pod określonym zastosowaniem, do której przypisane jest dane zdarzenie.
Ranga	Opisuje rangę, jaką ma dane zdarzenie w chwili, gdy występuje ono w określonym węźle (czyli gdy jest ono generowane przez program). Dostępne są następujące stopnie ważności: **KRYTYCZNA** – generowane zdarzenie jest niezwykle istotne i może mieć poważne konsekwencje wpływające na stan całej sieci, **OSTRZEŻENIE** – zdarzenie jest stosunkowo istotne i może mieć pewien wpływ na wydajność sieci, **INFORMACYJNA** – zdarzenie jest istotne tylko w pewnym stopniu; musi zostać przynajmniej zgłoszone i przyjęte w celach informacyjnych, **NIEISTOTNA** – zdarzenie ma niewielkie znaczenie i nie ma prawie żadnego wpływu na bieżącą wydajność i stabilność sieci.
Stan	Informuje czy generowane przez program zdarzenie powoduje przejście węzła, dostępnej w nim usługi lub jakiegokolwiek innego zasobu w stan niesprawności czy też nie. Możliwymi wartościami w tym polu są: SPRAWNY oraz NIESPRAWNY.

Otwieranie okna Konfiguracja alertów

Okno **Konfiguracja alertów** może zostać otwarte dla węzła, mapy lub atlasu. W każdym z tych przypadków okno to ma taką samą funkcjonalność.

Aby otworzyć okno Konfiguracja alertów

1. Aby otworzyć okno **Konfiguracja alertów** dla węzła, kliknij prawym przyciskiem myszy odpowiedni węzeł w oknie **Widok sieci**, w menu podręcznym wskaż pozycję **Alerty**, a następnie kliknij polecenie **Konfiguruj**.
   Aby otworzyć okno dla mapy, zaznacz odpowiednią mapę w oknie **Atlas sieci**, w menu **Mapa** wskaż pozycję **Alerty**, a następnie kliknij polecenie **Reguły**.
   Aby otworzyć okno dla atlasu, z menu **Atlas** wybierz polecenie **Reguły alertów**.

Uwagi

- *Okno **Konfiguracja alertów** otwarte dla atlasu ma tytuł **Właściwości atlasu**.*
- *Okno **Konfiguracja alertów** otwarte dla mapy ma tytuł **Właściwości mapy**.*
- *Okno **Konfiguracja alertów** otwarte dla węzła ma tytuł **Konfiguruj alerty dla <nazwa węzła>**.*

Włączanie zdarzeń

Aby włączyć zdarzenie wyszczególnione na liście pod zastosowaniem, należy po prostu zaznaczyć to zdarzenie i z listy rozwijanej, znajdującej się w górnej części ekranu, wybrać opcję *Zawsze generuj zdarzenie*. Włączanie zdarzeń odbywa się w ten sam sposób zarówno dla pojedynczego węzła, dla mapy jak i dla całego atlasu (jest to czynność wchodząca w zakres tworzenia reguł alertowania). Oczywiście w każdym z tych przypadków zakres przetwarzania danego zdarzenia jest różny. W przypadku włączenia danego zdarzenia dla mapy, jeśli w pewnych węzłach mapy zachodzą warunki wystąpienia tego zdarzenia, zdarzenie będzie przetwarzane w każdym z tych węzłów.

Aby włączyć generowanie zdarzenia dla węzła, mapy lub atlasu

1. Otwórz okno **Konfiguracja alertów** dla węzła, mapy lub atlasu. Więcej informacji na temat tego, jak to zrobić, można znaleźć w rozdziale *Otwieranie okna Konfiguracja alertów* na stronie 35.
2. Na wyświetlanej po lewej stronie liście zdarzeń zaznacz to, dla którego chcesz włączyć generowanie zdarzenia.
3. Z listy rozwijanej znajdującej się w prawej górnej części okna wybierz opcję **Zawsze generuj zdarzenie**.

Uwaga

*Aby wyłączyć zdarzenie dla węzła, należy po prostu zaznaczyć to zdarzenie, a następnie z listy rozwijanej znajdującej się w górnej części okna wybrać opcję **Nie generuj zdarzenia dla węzła**. Aby wyłączyć zdarzenie dla mapy, należy po prostu zaznaczyć to zdarzenie, a następnie z listy rozwijanej znajdującej się w górnej części okna wybrać opcję **Nie generuj zdarzenia dla mapy**. Aby wyłączyć zdarzenie dla atlasu, należy po prostu zaznaczyć to zdarzenie, a następnie z listy rozwijanej znajdującej się w górnej części okna wybrać opcję **Nie generuj zdarzenia dla atlasu**.*

Wprowadzanie wyjątków od reguł zdarzeń

Oprogramowanie NetCrunch umożliwia wprowadzanie wyjątków od reguł zdarzeń, które zostały przez użytkownika określone dla mapy lub dla całego atlasu. Odbywa się to poprzez wybranie dla obiektu należącego do niższego poziomu w hierarchii programu (czyli dla mapy lub węzła) innej opcji generowania zdarzenia. Jeśli na przykład pewne zdarzenie zostało wyłączone dla mapy, można otworzyć okno **Konfiguracja alertów** dla pojedynczego węzła należącego do tej mapy i włączyć to zdarzenie wyłącznie dla tego węzła. Spowoduje to dla tego jednego węzła uchylenie reguł zdarzeń, zgodnie z którymi zdarzenie to miało być wyłączone, i ustanowienie nowej definicji – nadrzędnej w stosunku do reguł zdarzeń określonych dla całej mapy. Dla wszystkich innych węzłów należących do tej mapy generowanie danego zdarzenia będzie wyłączone, natomiast w węźle, dla którego zdefiniowano taki wyjątek, generowanie tego zdarzenia będzie możliwe.

Uwaga

Do nietypowej sytuacji dochodzi w momencie, gdy dany węzeł należy do dwóch różnych map, przy czym na poziomie węzła pozostawione zostały dla niego domyślne reguły zdarzeń (nie zostały wprowadzone żadne wyjątki od tych reguł). Reguły zdarzeń dla każdej z tych map są różne – dla jednej mapy generowanie danego zdarzenia jest włączone, dla drugiej – wyłączone. Czy zatem zdarzenie to zostanie wygenerowane, gdy w danym węźle spełnione zostaną warunki jego wystąpienia? W takim przypadku, jeżeli zdarzenie jest włączone dla co najmniej jednego obiektu wyższego rzędu, do którego należy dany węzeł, będzie ono również włączone – na zasadzie dziedziczenia – dla tego węzła.

Alerty – odpowiedź na zdarzenie

Alerty to zdefiniowane zdarzenia, z którymi skojarzono co najmniej jedną akcję (podejmowaną po wygenerowaniu zdarzenia). W dalszej części podręcznika zostaną opisane różne rodzaje akcji alertujących, jakie użytkownik może kojarzyć z wybranym zdarzeniem. Przypisanie akcji do zdarzenia przeprowadzane jest w oknie **Konfiguracja alertów** i jest to czynność dość prosta.

Aby przypisać akcję do zdarzenia

1. Otwórz okno **Konfiguracja alertów** dla węzła, mapy lub atlasu. Więcej informacji na temat tego, jak to zrobić, zawiera rozdział *Otwieranie okna Konfiguracja alertów* na stronie 35.
2. Z listy zdarzeń znajdującej się po lewej stronie wybierz zdarzenie, któremu chcesz przypisać daną akcję.
3. Kliknij ikonę ***Dodaj akcję*** znajdującą się w środkowej części okna.
4. Przejdź do kreatora *Utwórz akcję*, w którym możesz wybrać jedną z uprzednio zdefiniowanych akcji lub zdefiniować nowy rodzaj akcji.
5. Po wybraniu lub zdefiniowaniu akcji w polu **Uruchom po** określ czas, jaki ma upłynąć pomiędzy wygenerowaniem zdarzenia a podjęciem danej akcji.

Uwaga

Jeżeli w punkcie 4. ma być definiowany nowy rodzaj akcji, wówczas w kreatorze Utwórz akcję *należy kliknąć ikonę* **Zdefiniuj nową akcję**. *Na ekranie wyświetlone zostanie wówczas okno kreatora* Zdefiniuj akcję, *w którym będzie można określić jeden ze sposobów powiadamiania lub inne opisanej poniżej rodzaje akcji alertujących.*

Akcje alertujące

NetCrunch umożliwia podejmowanie szerokiej gamy akcji alertujących. Zostały one podzielone na następujące kategorie, wyszczególnione w poniższej tabeli.

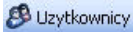
Powiadomienie	Umożliwia szybkie określenie odbiorców powiadomienia poprzez wybór uprzednio zdefiniowanego profilu użytkownika lub grupy.
Powiadomienie proste	Umożliwia przeprowadzenie powiadomienia za pośrednictwem poczty e-mail, pagera, wiadomości tekstowej wysłanej na telefon komórkowy (SMS), komunikatu ICQ, trapu SNMP lub komunikatu Syslog.
Powiadomienie na pulpicie	Umożliwia przeprowadzenie powiadomienia na pulpicie poprzez wyświetlenie paska alertów lub okna dialogowego alertów albo przez odtworzenie sygnału dźwiękowego lub alertu głosowego.
Akcja sterująca	Pozwala na zmianę stanu serwisu systemu Windows, ponowne uruchomienie/wyłączenie komputera, uruchomienie programu lub skryptu, ustawienie stanu monitorowania węzła lub zmiennej SNMP, zakończenie procesu bądź wykonanie polecenia „Wake on LAN".
Akcja diagnostyczna	Umożliwia dodanie wyników testu Traceroute lub statusu usługi sieciowej do treści komunikatu alertu.
Akcja rejestrująca	Pozwala na zapisanie informacji o zdarzeniu w pliku lub w dzienniku zdarzeń systemu Windows.

Uwagi

- *Wszystkie dostępne w programie akcje zostały opisane w kolejnych rozdziałach podręcznika.*

Powiadamianie

Aby skorzystać z możliwości powiadamiania wystarczy po prostu z uprzednio zdefiniowanej listy wybrać użytkownika lub grupę, do których ma być skierowane powiadomienie. Ustawienia dla poszczególnych użytkowników lub grup definiowane są już wcześniej i zawierają wszelkie niezbędne informacje o tym, kiedy i w jaki sposób odbywać się ma ich powiadamianie. Lista użytkowników i grup, dostępna po kliknięciu ikony ***Użytkownicy*** na głównym pasku narzędzi, umożliwia zarządzanie użytkownikami lub grupami (tj. dodawanie nowych użytkowników lub grup, wybór metody powiadamiania – pocztą e-mail, komunikatem ICQ, na pager lub za pomocą SMS – oraz określanie czasu powiadomienia).



Uwaga

Więcej informacji na temat definiowania użytkowników dla potrzeb powiadamiania i dostępu przez WWW można znaleźć w rozdziale Zarządzanie powiadamianiem użytkowników i grup *na stronie 237*.

Powiadomienie proste

W przypadku powiadomienia prostego należy zdefiniować parametry określające, kto ma być powiadamiany. Są one zróżnicowane w zależności od rodzaju wybranego powiadomienia prostego (czy ma ono być przesłane za pośrednictwem poczty e-mail, na pager, z wykorzystaniem wiadomości SMS, alertu SNMP lub komunikatu ICQ).

Poczta e-mail

Wybranie tego rodzaju powiadomienia wskazuje, że zostanie ono wysłane pocztą e-mail. Konfigurując tego typu powiadomienie proste należy podać adres e-mail odbiorcy. Możliwe jest również wprowadzenie zmian w polu *Temat*, które określa temat wiadomości e-mail.

Pager

Powiadomienie na pager może zostać przeprowadzone za pośrednictwem modemu lub Internetu. W każdym z tych przypadków należy określić numer pagera, na który ma być kierowane powiadomienie o alercie.

Ponadto przed rozpoczęciem korzystania z tego rodzaju powiadomienia należy skonfigurować odpowiednie ustawienia pagera – odbywa się to poprzez wybranie z menu **Narzędzia** polecenia **Opcje**, a następnie przejście do strony **Powiadomienia – Pager**. W przypadku korzystania z powiadomienia na pager za pośrednictwem modemu należy wybrać modem i usługę TAP. TAP (Telocator Alphanumeric Protocol) to protokół używany do przesyłania maksymalnie tysiąca znaków na pager. W przypadku korzystania z powiadomienia na pager za pośrednictwem Internetu należy określić nazwę i numer portu serwera SNPP (Simple Network Paging Protocol).

Wiadomość tekstowa na telefon komórkowy – SMS

Istnieją trzy metody wysyłania powiadomienia na telefon komórkowy w formie wiadomości SMS: za pośrednictwem bramki e-mail, za pomocą telefonu lub trybu GSM albo z wykorzystaniem komunikatu ICQ. W każdym z tych przypadków należy określić numer telefonu odbiorcy wiadomości SMS. Dla każdej z metod, która ma być wykorzystywana, należy przeprowadzić odpowiednią konfigurację programu. W tym celu należy z menu **Narzędzia** wybrać polecenie **Opcje**, a następnie przejść do strony **Powiadomienia – Urządzenie GSM** lub **Powiadomienia – ICQ**. Każdą z metod można również konfigurować na bieżąco, podczas definiowania powiadomienia (wystarczy w tym celu kliknąć przycisk **Konfiguracja**).

Bramka e-mail

Metoda ta polega na wysyłaniu powiadomienia pocztą e-mail na bramkę SMS, która następnie przekierowuje ją do odbiorcy w formie krótkiej wiadomości tekstowej (SMS). Aby móc z niej korzystać, należy skonfigurować i wybrać odpowiednią bramkę SMS tak, aby wysyłanie wiadomości było właściwie obsługiwane. Ponieważ NetCrunch będzie wysyłał wiadomości e-mail, należy więc również odpowiednio skonfigurować obsługę poczty (na przykład podając adres zwrotny i włączając obsługę za pomocą zewnętrznego serwera pocztowego zamiast wbudowanego w program serwera).

Telefon lub tryb GSM

Aby korzystać z powiadamiania w formie wiadomości SMS wysyłanych za pośrednictwem telefonu GSM, należy najpierw podłączyć i skonfigurować telefon lub urządzenie pracujące jako telefon. Zwykle wykorzystuje się do tego celu jeden ze standardowych portów COM w komputerze, na którym działa NetCrunch. Następnie można przystąpić do konfigurowania opcji w programu związanych z korzystaniem z telefonu komórkowego GSM.

ICQ

Do powiadomienia w formie wiadomości SMS może również posłużyć komunikat ICQ. W takim przypadku w programie należy skonfigurować odpowiednie opcje ICQ, takie jak serwer ICQ, unikatowy numer, nazwa oraz hasło.

Trap SNMP

Chcąc przesyłać (przekierowywać) powiadomienia dalej, do innych zewnętrznych aplikacji, można do tego celu wykorzystać opcję alertu SNMP. Należy wówczas określić nazwę lub adres IP docelowego urządzenia, numer portu do komunikacji oraz wykorzystywaną wspólnotę trapów SNMP.

Komunikat ICQ

Powiadomienie może zostać przeprowadzone poprzez wysłanie komunikatu na unikatowy numer ICQ. Podczas definiowania tego rodzaju akcji wystarczy podać ten właśnie numer ICQ. Oczywiście przed wysłaniem wiadomości ICQ w opcjach programu należy określić serwer ICQ, własny numer ICQ, nazwę i hasło – w przeciwnym przypadku skorzystanie z tego rodzaju akcji nie będzie możliwe.

Komunikat Syslog

Kolejny rodzaj powiadomienia prostego to wysyłanie komunikatu Syslog. Podczas jego definicji należy określić nazwę lub IP docelowego urządzenia, numer portu oraz kategorię i rangę komunikatu Sysloga.

Powiadomienia na pulpicie

Powiadomienia na pulpicie następują wyłącznie na stacji roboczej lub serwerze, na których uruchomiony jest NetCrunch. Przeznaczone są one dla użytkowników programu chcących otrzymywać natychmiastowe krótkie powiadomienia o zdarzeniach. W ten sposób mogą oni szybciej reagować na sygnalizowane przy użyciu alertów różnego rodzaju problemy z siecią.

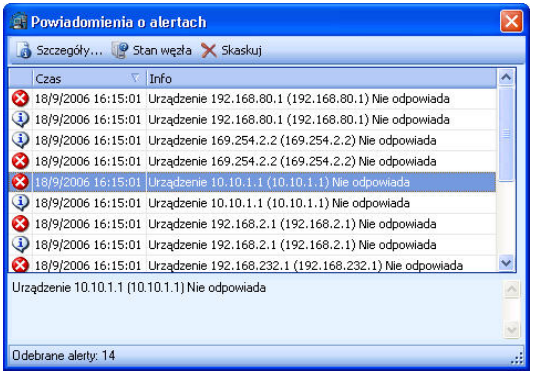
Pasek alertów

Ten rodzaj powiadomienia polega na wyświetlaniu – w górnej części pulpitu – paska alertów, zawierającego zwięzłe informacje na temat zaistniałego problemu w sieci. Podczas definiowania tego rodzaju alertu możliwe jest wybranie jednego z trzech stylów tekstu przesuwającego się na pasku. Natomiast klikając przycisk **Test**, można zobaczyć, jak wygląda aktualnie wybrany styl.

Wyświetlanie okna dialogowego alertów

Okno dialogowe alertów to specjalne okno programu, służące do wyświetlania przetwarzanych alertów. Ten rodzaj powiadomienia na pulpicie umożliwia szybki przegląd nowych nieprzyjętych alertów, zestawionych w postaci przejrzystej tabeli. Okno dialogowe alertów pozwala również wykonać szereg zadań związanych z alertem:

- przeglądnąć istotne informacje dotyczące alertu (z menu podręcznego dla wybranego zdarzenia należy wybrać polecenie **Szczegóły**),
- natychmiast wyświetlić stan węzła, w którym wystąpiło dane zdarzenie (z menu podręcznego dla wybranego zdarzenia należy wybrać polecenie **Stan węzła**),
- usunąć zdarzenie z tabeli wyświetlanej w oknie dialogowym (z menu podręcznego dla wybranego zdarzenia należy wybrać polecenie **Skasuj**).



Uwagi

- *Aby dodatkowo wyświetlić niewielkie, tymczasowe okno dialogowe powiadomień dla wygenerowanych zdarzeń, należy zaznaczyć pole wyboru* ***Pokaż powiadomienie*** *we właściwościach edycji akcji dla akcji polegającej na wyświetlaniu okna dialogowego alertu.*
- *Wybranie z menu podręcznego polecenia* ***Skasuj wszystkie*** *umożliwia usunięcie z tabeli w oknie dialogowym alertów wszystkich wyświetlanych w niej zdarzeń.*
- *Szybki odczyt liczby nowych alertów w oknie dialogowym alertów jest możliwy dzięki paskowi statusu. Kliknij na link* ***Odebrane alerty****, aby wyświetlić samo okno dialogowe.*

Sygnał dźwiękowy

Kolejnym rodzajem powiadomienia na pulpicie jest sygnał dźwiękowy uruchamiany na stacji roboczej lub serwerze, na których – w chwili obsługi określonego zdarzenia – uruchomiony jest NetCrunch. Konfiguracja tej akcji polega na wybraniu z dysku lokalnego lub sieciowego odpowiedniego pliku dźwiękowego (zapisanego np. w standardowym formacie `.WAV`).

Alert głosowy

Do generowania komunikatu głosowego opisującego dany alert można wykorzystać oprogramowanie służące do syntezy mowy. Aby rozwiązanie takie mogło prawidłowo działać, na komputerze, na którym uruchomiony jest NetCrunch, wymagane jest poprawne zainstalowanie oprogramowania do syntezy mowy oraz karty dźwiękowej. Ponadto konieczne jest skonfigurowanie w programie opcji głosowych, a w szczególności wybranie odpowiedniego rodzaju syntezatora mowy (w tym celu należy z menu **Narzędzia** wybrać polecenie **Opcje**, a następnie przejść do strony **Powiadomienia – Alert głosowy**). Podczas definiowania tego rodzaju akcji alertującej możliwe jest natychmiastowe sprawdzenie,

czy działa ona poprawnie – w tym celu w oknie kreatora *Zdefiniuj akcję* należy kliknąć przycisk **Test**.

Akcje sterujące

Zmiana stanu usług systemu Windows

W przypadku węzłów działających w oparciu o system operacyjny Windows (węzłów będących źródłem zdarzenia lub dowolnych innych węzłów znajdujących się w atlasie sieci), możliwe jest wykonanie procedury sterującej dowolnymi usługami systemu Windows. Akcja tego typu może polegać na uruchomieniu, zatrzymaniu, wstrzymaniu, ponownym uruchomieniu lub kontynuowaniu działającego na węźle serwisu Windows.

Ponowne uruchomienie lub wyłączenie komputera

Kolejnym przydatnym rodzajem akcji jest opcja ponownego uruchamiania lub wyłączania komputera. Także w tym przypadku możliwe jest wykonanie akcji bezpośrednio na węźle będącym źródłem zdarzenia lub na innym węźle w atlasie. W przypadku węzłów działających w oparciu o system operacyjny Linux możliwe jest wybranie jednego z dwóch rodzajów połączenia z węzłem w celu wykonania omawianej akcji (dostępne rodzaje połączeń to Secure Shell oraz Telnet).

Uruchomienie programu lub skryptu

Uruchomienie programu lub skryptu może zostać ustawione na węźle lokalnym, na którym jest uruchomiony program NetCrunch, na węźle, na którym wygenerowane zostało zdarzenie lub na jakimkolwiek innym węźle zdalnym. W przypadku alertu polegającego na uruchomieniu programu lub skryptu lokalnie – tzn. na komputerze, na którym uruchomiony jest NetCrunch – możliwe jest natychmiastowe wykorzystanie innych aplikacji w celu wystosowania do niego powiadomienia lub wykonania innych przydatnych zadań. Z kolei ustawienie akcji alertującej polegającej na uruchomieniu zdalnego programu lub skryptu umożliwia podejmowanie działań zapobiegawczych lub naprawczych, np. zmierzających do diagnozy i usunięcia problemu na węźle, na którym wystąpiło dane zdarzenie.

Scenariusz lokalny

Jeżeli program lub skrypt ma być uruchamiany lokalnie, to akcja alertująca zostanie wykonana na komputerze pracującym pod kontrolą systemu Windows, na którym uruchomiony jest NetCrunch. Podczas definiowania tego rodzaju akcji należy wypełnić kilka pól w kreatorze *Zdefiniuj akcję*:

Nazwa pliku	Określa nazwę programu lub skryptu, który zostanie uruchomiony na lokalnym komputerze pracującym pod kontrolą systemu Windows.

Parametry	Określa wszelkie parametry, które użytkownik może przekazać do programu lub skryptu. Użytkownik może albo kliknąć to pole prawym przyciskiem myszy i dokonać wyboru spośród parametrów zaproponowanych przez program, albo wpisać bezpośrednio swoje własne parametry. Pełna lista możliwych do wybrania pól znajduje się w rozdziale *Zmiana domyślnych szablonów wiadomości* na stronie 251.
Plik z wiadomością alertu jako parametr	Zaznaczenie tego pola wyboru spowoduje, że dana wiadomość alertu zostanie przekazana do programu lub skryptu działającego w środowisku systemu Windows jako jego parametr.

W przypadku skryptów wykorzystywane są również następujące pola:

Komputer skryptów	Określa urządzenie aparatu skryptów systemu Windows na komputerze lokalnym (tj. `wscript.exe`).
Limit czasu	Określa maksymalny dozwolony czas wykonywania skryptu (w sekundach). Jeśli przewidziany limit czasu zostanie przekroczony, a skrypt będzie wciąż wykonywany, komputer skryptów przerwie działanie aparatu skryptów i automatycznie zakończy proces.
Interaktywny	Jeżeli zaznaczone zostanie to pole wyboru, aparat skryptów umożliwi wykonywanemu skryptowi wyświetlanie – na komputerze lokalnym, pracującym pod kontrolą systemu Windows – podpowiedzi dla użytkownika oraz komunikatów o błędach wykonania skryptu. Odznaczenie tego pola wyboru spowoduje, że aparat skryptów wyłączy wyświetlanie podpowiedzi dla użytkownika oraz komunikatów o błędach podczas wykonywania danego skryptu.

Scenariusz zdalny

Możliwość uruchamiania zdalnego programu lub skryptu nie jest ograniczona tylko do węzłów działających pod kontrolą systemu Windows. Zdalne programy lub skrypty mogą być uruchamiane także na komputerach działających pod kontrolą systemów Linux lub NetWare. W każdym z tych przypadków użytkownik powinien upewnić się, że ma odpowiednie uprawnienia do uruchamiania programu lub skryptu w takim zdalnym węźle. W tym celu we właściwościach monitorowania danego węzła należy określić nazwę i hasło logowania użytkownika (karty **Wydajność Windows**, **Wydajność NetWare** lub **Linux**).

Windows

Dla zdalnych węzłów Windows należy określić te same pola, co w opisanym powyżej scenariuszu lokalnym. Udostępniane w tym przypadku dodatkowe pole wyboru pozwala skopiować program lub skrypt do zdalnego komputera Windows. W oknie kreatora *Zdefiniuj akcję* należy więc określić następujące pola:

Nazwa pliku	Określa nazwę programu lub skryptu, który zostanie wykonany na zdalnym komputerze pracującym pod kontrolą systemu Windows.

Skopiuj program do zdalnego komputera	Zaznaczenie tego pola wyboru sprawi, że dodatkowo NetCrunch, przed uruchomieniem wybranego programu, przekopiuje go do zdalnego komputera Windows (opcja ta jest dostępna tylko w przypadku, gdy program ma być wykonywany zdalnie).
Parametry	Określa wszelkie parametry, które użytkownik może przekazać do programu lub skryptu. Użytkownik może albo kliknąć to pole prawym przyciskiem myszy i dokonać wyboru spośród parametrów zaproponowanych przez NetCruncha, albo wpisać bezpośrednio swoje własne parametry. Pełna lista możliwych do wybrania pól znajduje się w rozdziale *Zmiana domyślnych szablonów wiadomości* na stronie 251.
Plik z wiadomością alertu jako parametr	Zaznaczenie tego pola wyboru spowoduje, że dana wiadomość alertu zostanie przekazana do programu lub skryptu jako jego parametr.

W przypadku zdalnego skryptu Windows należy dodatkowo określić następujące pola:

Skopiuj skrypt do zdalnego komputera	Zaznaczenie tego pola wyboru sprawi, że NetCrunch, przed uruchomieniem skryptu Windows, dodatkowo przekopiuje go do zdalnego węzła Windows.
Komputer skryptów	Określa mechanizm aparatu skryptów systemu Windows na komputerze zdalnym (tj. `wscript.exe`).
Limit czasu	Określa maksymalny dozwolony czas wykonywania skryptu (w sekundach). Jeśli przewidziany limit czasu zostanie przekroczony, a skrypt będzie wciąż wykonywany, komputer skryptów przerwie działanie aparatu skryptów i automatycznie zakończy proces.
Interakcyjny	Jeżeli zaznaczone zostanie to pole wyboru, aparat skryptów umożliwi wykonywanemu skryptowi wyświetlanie – na komputerze zdalnym, pracującym pod kontrolą systemu Windows – podpowiedzi dla użytkownika oraz komunikatów o błędach wykonania skryptu. Odznaczenie tego pola wyboru spowoduje, że aparat skryptów wyłączy wyświetlanie podpowiedzi dla użytkownika oraz komunikatów o błędach podczas wykonywania danego skryptu.

Linux/Unix

Zdefiniowanie tego rodzaju akcji spowoduje wykonanie skryptu na tym zdalnym węźle działającym w oparciu o system operacyjny Linux lub Unix, który jest odpowiedzialny za wywołanie alertu. W tym przypadku należy określić następujące pola:

Nazwa pliku	Określa nazwę skryptu, jaki zostanie wykonany na zdalnym komputerze Linux lub Unix.

Skopiuj skrypt do zdalnego komputera	Zaznaczenie tego pola wyboru sprawi, że NetCrunch dodatkowo, przed uruchomieniem skryptu, przekopiuje go do zdalnego urządzenia Linux.
Parametry	Określa wszelkie parametry, które użytkownik może przekazać do skryptu w systemie Linux/Unix. Użytkownik może albo kliknąć to pole prawym przyciskiem myszy i dokonać wyboru spośród parametrów zaproponowanych przez NetCruncha bądź wpisać bezpośrednio własne parametry. Pełna lista możliwych do wybrania pól znajduje się w rozdziale *Zmiana domyślnych szablonów wiadomości* na stronie 251.
Plik z wiadomością alertu jako parametrem	Zaznaczenie tego pola wyboru spowoduje, że dana wiadomość alertu zostanie przekazana do skryptu jako jego parametr.
Użyj polecenia su	Zaznaczenie tego pola wyboru spowoduje, że zdalny skrypt Linux zostanie uruchomiony z uprawnieniami nadzorcy systemu. Konieczne jest przy tym określenie hasła administratora systemu (*su*) – w odpowiednim dla danego węzła oknie **Monitorowanie** na karcie **Linux/Unix**.
Rodzaj połączenia	Umożliwia wybór spośród dwóch następujących rodzajów połączenia z komputerem Linux/Unix: Secure Shell (SSH) lub Telnet.

NetWare

Podczas definiowania zdalnej akcji dla urządzenia NetWare jedyne wykorzystywane pole to **Nazwa pliku**. Określa ono nazwę skryptu NetWare, który będzie uruchamiany zdalnie w tym węźle, który wywołał dany alert. Skrypty NetWare mają z reguły rozszerzenie `.NCF`. Przykładowo, skrypt NetWare może posłużyć do ładowania lub usuwania modułów NLM w zdalnym hoście.

Ustaw stan monitorowania węzła

W niektórych sytuacjach pomocna okaże się akcja polegająca na zmianie stanu monitorowania węzła (węzła będącego źródłem zdarzenia lub innego węzła w atlasie). Możliwe jest włączenie monitorowania węzła, wyłączenie monitorowania węzła na określony czas lub na stałe.

Ustaw zmienną SNMP

Powyższy rodzaj akcji służy do ustawiania konkretnej wartości zmiennej SNMP na węźle będącym źródłem zdarzenia lub innym węźle w atlasie. W szczególności możliwy jest wybór określonego obiektu OID docelowej zmiennej SNMP z bazy danych MIB-ów lub bezpośrednie wpisanie wartości. Ponadto istnieje opcja ustawienia zmiennej SNMP w formacie szesnastkowym zamiast liczby całkowitej.

Zakończ proces
W aktualnej wersji program oferuje możliwość zatrzymywania dowolnie wskazanego procesu działającego na węźle Windows. Wykonywanie tego zadania jest możliwe wyłącznie na węźle będącym źródłem zdarzenia lub na pozostałych węzłach atlasu.

Wykonaj polecenie „Wake on LAN"
Ten rodzaj akcji umożliwia zdalne włączenie komputera poprzez wykonanie polecenia „Wake on LAN", przesyłanego do interfejsu sieciowego danego komputera w postaci zestawu specjalnych pakietów sieciowych.

Akcje diagnostyczne

Dodanie do alertu polecenia Traceroute
Tego rodzaju akcja wykorzystywana jest wówczas, gdy informacja związana z danym alertem ma być poszerzona o dane przydatne do diagnostyki i usuwania problemów. W takim przypadku przed podjęciem innych zdefiniowanych akcji przeprowadzany jest dodatkowy test diagnostyczny. Podczas definiowania tego rodzaju akcji można określić następujące parametry: maksymalną liczbę przeskoków, jaka może nastąpić podczas wykonywania polecenia *traceroute*, maksymalny czas oczekiwania (w minutach) oraz to, czy ma być stosowane rozpoznawanie nazw adresów ruterów.

Dodanie statusu usług sieciowych do alertu
Powyższa odmiana akcji umożliwia zamieszczanie informacji o stanie usług sieciowych w komunikacie alertu w celach diagnostycznych.

Akcje rejestrujące

Zapis alertu do pliku
NetCrunch umożliwia zapisywanie alertów bezpośrednio do pliku na dysku lokalnym komputera, na którym program ten został uruchomiony. Zdefiniowanie tego rodzaju akcji umożliwia gromadzenie informacji o określonych węzłach w jednym pliku. Podczas definiowania takiej akcji użytkownik może określić nazwę pliku (wraz z jego ścieżką), format pliku (tekstowy, XML lub HTML), a nawet ograniczyć jego rozmiar (gdy przekroczy on określoną wartość, dane dotyczące najstarszych alertów zostaną z niego usunięte).

Zapis alertu do dziennika zdarzeń systemu Windows
Dzięki powyższej funkcji możliwe jest ustawianie zapisywania informacji o wygenerowanym w NetCrunchu zdarzeniu w dzienniku zdarzeń systemu Windows.

Eskalacja alertów
NetCrunch umożliwia definiowanie akcji, które mają być podejmowane w różnych momentach czasu, począwszy od chwili wystąpienia skojarzonego z nimi zdarzenia. Procedura ta nazywana jest eskalacją alertów. Kiedy początkowy zestaw podjętych akcji nie

przynosi pożądanego skutku, uruchamiane są kolejne akcje, przewidziane w definicji alertu do wykonania w późniejszym czasie. Akcje te odbywają się na następnym poziomie hierarchii ważności i mogą służyć albo do powiadomienia o utrzymującym się problemie albo do jego rozwiązania przez program. W ten sposób, w ramach definiowania alertu, możliwe jest utworzenie dowolnej ilości akcji, które mają zostać podjęte w różnych momentach (w tym również takie ich skonfigurowanie, aby kilka różnych akcji podejmowanych było w tym samym momencie).

Uwagi

- *Istnieje możliwość takiego skonfigurowania ostatniego zestawu akcji (zestawu zdefiniowanego w grupie akcji jako ostatni), aby był on powtarzany cyklicznie (do momentu, w którym przestaną zachodzić warunki wystąpienia danego zdarzenia, albo gdy użytkownik ręcznie skasuje dany alert).*
- *Różne grupy akcji służących do eskalacji alertu ustawiane są automatycznie podczas konfigurowania danej akcji (należy przy tym określić czas opóźnienia, po jakim określona akcja ma zostać podjęta, wykorzystując do tego celu pole* ***Uruchom po*** *w oknie kreatora* Utwórz akcję*).*

Alerty oczekujące

Z alertami oczekującymi mamy do czynienia wówczas, gdy z wygenerowanym zdarzeniem, które wywołało już określone akcje, związane są akcje, które jeszcze nadal oczekują na uruchomienie w zaplanowanym, późniejszym czasie. Alert oczekujący występuje zazwyczaj wtedy, gdy odpowiadająca mu lista eskalacji alertu zawiera różne akcje, które mają zostać podjęte w różnych momentach (może ona nawet obejmować grupę akcji końcowych, która ma być powtarzana cyklicznie).

Kasowanie alertów oczekujących

Akcje oczekujące związane z alertem są kasowane albo automatycznie przez program, albo ręcznie przez użytkownika (poprzez wybranie odpowiedniego polecenia z podręcznego menu dla danego węzła). Każdy z tych przypadków został opisany w kolejnych rozdziałach podręcznika.

Automatyczne kasowanie alertów

Automatyczne kasowanie alertów następuje wówczas, gdy warunki, które doprowadziły do wygenerowania danego zdarzenia, ulegają zmianie i przestają zachodzić. Wówczas związane z danym alertem akcje oczekujące zostaną przez program automatycznie usunięte, czyli po prostu nie nastąpią.

Zilustrujmy to na przykładzie. Załóżmy, że w programie zdefiniowano zdarzenie, które ma nastąpić wówczas, gdy stan określonego węzła zmieni się na *Nie odpowiada*. Ze zdarzeniem tym zostały skojarzone dwie akcje – jedna ma zostać podjęta bezpośrednio po wystąpieniu zdarzenia, druga po upływie 15 minut. Gdy w węźle nastąpi awaria i zmieni on swój stan na *Nie odpowiada*, NetCrunch natychmiast wygeneruje tak zdefiniowane zdarzenie i uruchomi pierwszą ze skojarzonych z nim akcji (druga z tych akcji stanie się wówczas akcją oczekującą). Jeśli w ciągu kolejnych 15 minut stan węzła zmieni się na *Odpowiada* (czyli węzeł zacznie z powrotem działać poprawnie), alert automatycznie sam się skasuje. Oznacza to, że ta druga akcja nie zostanie przez program uruchomiona, ponieważ w danym węźle

warunki wystąpienia tego zdarzenia już nie zachodzą. Oczywiście taki oczekujący alert może w każdej chwili zostać skasowany ręcznie przez użytkownika.

Ręczne kasowanie alertów

Aby ręcznie skasować alert oczekujący związany z danym węzłem, należy wybrać odpowiednie polecenie z menu podręcznego tego węzła.

Aby skasować alert

1. W oknie **Widok sieci** otwórz menu podręczne dla węzła, z którym związane są akcje oczekujące.
2. Wskaż pozycję **Alerty**, a następnie wybierz z menu polecenie **Kasuj oczekujące**.

Potwierdzanie alertów

Aby potwierdzić przyjęcie danego zdarzenia należy wprowadzić odpowiednią zmianę w polu **Status zdarzenia** i zamiast stanu *Nowy* wybrać stan inny (np. *Przyjęty*). W tym celu należy otworzyć okno **Dziennik zdarzeń** (przez wskazanie w menu podręcznym dla danego węzła pozycji **Alerty**, a następnie wybranie z kolejnego menu polecenia **Przeglądaj**), zaznaczyć odpowiednie zdarzenie i za pomocą menu podręcznego zmienić status.

Uwaga

Jeżeli w momencie przyjęcia zdarzenia związane były z nim jakieś akcje oczekujące, operacja ta nie będzie miała na nie żadnego wpływu (nie zostaną one wykasowane i wciąż będą czekać na uruchomienie). Aby nie dopuścić do ich wykonania, należy wykasować je ręcznie lub poczekać, aż program zrobi to automatycznie.

Śledzenie zmian w strukturze sieci

Wykrywanie nowo dodanych węzłów możliwe jest w programie NetCrunch dzięki funkcji automatycznego wykrywania sieci, która jest procesem uruchamianym i działającym w tle. Jednocześnie, bez względu na to, czy opcja automatycznego wykrywania sieci jest uruchomiona, program stale uaktualnia informacje o fizycznej topologii sieci pochodzące z tablic przełączników.

NetCrunch może automatycznie wykrywać nowe węzły w monitorowanej sieci. Aby uruchomić tę funkcję, należy dla danej mapy sieci otworzyć okno **Właściwości mapy** i kliknąć kartę **Automatyczne wykrywanie**. Następnie należy zaznaczyć pole wyboru **Włącz automatyczne wykrywanie węzłów** i określić częstotliwość, z jaką ma być przeprowadzane automatyczne skanowanie tej mapy (np. co godzinę, codziennie lub co tydzień). Ponadto można zawęzić zakres skanowania sieci, zmieniając odpowiednie kryteria filtrowania w oknie *Kreatora wykrywania sieci*, tak aby wykrywane i dodawane do monitorowanej sieci były tylko określone rodzaje węzłów.

Oprócz ustawiania regularnego reskanowania automatycznego, zgodnie z przyjętym harmonogramem, użytkownik może także przeprowadzić skanowanie określonej sieci w dowolnym momencie. W tym celu z menu podręcznego, które udostępniane jest

po zaznaczeniu danej mapy w drzewie **Atlas sieci**, należy wybrać polecenie **Wykryj nowe węzły**.

Uwagi

- *Gdy do sieci dodawane są nowe węzły, można skonfigurować program tak, aby rozmieszczał je na mapie według określonych kryteriów. W tym celu z menu* ***Mapa*** *należy wybrać polecenie* ***Rozmieść węzły****.*
- *Funkcja skanowania automatycznego może zostać włączona dla dowolnej mapy należącej do sekcji* Sieci IP *w drzewie* Atlas sieci.

Monitorowanie aplikacji

Monitorowanie wydajności systemu

NetCrunch udostępnia szereg metod monitorowania wydajności systemu. Ich faktyczna ilość jest uzależniona od rodzaju systemu operacyjnego, liczby aplikacji zainstalowanych w węźle oraz od tego, czy dany węzeł jest zarządzany za pomocą agenta SNMP.

Aby monitorować wydajność systemów Windows albo NetWare, lub wykorzystywać agenta SNMP, należy określić klasę danego zdarzenia. W tym celu należy dla danego węzła wybrać z menu **Alerty** polecenie **Konfiguruj** i w nowo otwartym oknie kliknąć ikonę ***Dodaj zdarzenie***. Następnie w oknie **Wybierz zdarzenie** należy kliknąć ikonę ***Dodaj nowe zdarzenie***, co spowoduje wyświetlenie okna **Edytuj warunek zdarzenia**.

Windows

Monitorowanie wydajności sytemu w węzłach działających pod kontrolą systemu Windows może odbywać się na kilka sposobów. Po pierwsze, w tabeli zestawionej dla systemu **Windows NT** można uzyskać szybki podgląd związanych z danym węzłem liczników *% Obciążenia procesora* i *% Wykorzystania pamięci*.

Po drugie, można zdefiniować zdarzenia oparte na usługach sieciowych związanych z daną aplikacją. W oknie **Edytuj warunek zdarzenia** należy rozwinąć sekcję *Usługi sieciowe* i wybrać klasę *Próg dostępności usługi sieciowej*. Przykładowo, w celu monitorowania aplikacji Microsoft Exchange, można ustawić monitorowanie liczników wydajności *% Utraconych pakietów* i/lub *Czas odpowiedzi (RTT)* dla usług sieciowych POP3 i SMTP (dla każdej z nich należy zdefiniować osobne zdarzenie).

Po trzecie, dla potrzeb monitorowania można wykorzystać zdarzenia oparte na udostępnianych w danym węźle licznikach systemowych Windows. W oknie **Edytuj warunek zdarzenia** należy rozwinąć sekcję *Windows* i wybrać klasę *Próg wydajności aplikacji Windows*. Kolejnym krokiem podczas definiowania tego rodzaju zdarzenia jest wybór systemowego licznika wydajności Windows, który ma być monitorowany. Następnie w oknie **Dodaj liczniki** należy wybrać obiekt wydajności oraz charakterystyczny dla niego licznik (liczba dostępnych liczników jest uzależniona od rodzaju systemu operacyjnego i liczby zainstalowanych aplikacji).

NetWare

Monitorowanie wydajności może być przeprowadzane również dla węzłów działających pod kontrolą systemu NetWare. Wygląda ono podobnie jak w przypadku węzłów Windows – dla potrzeb monitorowania należy zdefiniować zdarzenia, wykorzystując do tego celu dostępne w danym węźle liczniki NetWare. W oknie **Edytuj warunek zdarzenia** należy rozwinąć sekcję *Novell* i wybrać klasę *Próg Novell NetWare*. Następnym krokiem podczas definiowania tego rodzaju zdarzenia jest wybór licznika wydajności NetWare, który ma być monitorowany. Polega to na wybraniu w oknie **Dodaj liczniki** obiektu wydajności oraz odpowiedniego, należącego do niego licznika.

SNMP

Jeżeli w węźle, dla którego monitorowana ma być wydajność systemu, włączony jest agent SNMP, możliwe jest również skorzystanie z liczników wydajności odczytywanych bezpośrednio za pomocą takiego agenta SNMP. Procedura uruchamiania monitorowania wygląda tak samo jak w przypadkach opisanych w poprzednich rozdziałach. W oknie **Edytuj warunek zdarzenia** należy rozwinąć sekcję *Progi i trapy SNMP* i wybrać klasę *Próg wydajności SNMP*. Następnie należy określić żądany licznik wydajności, co można uczynić na dwa sposoby – albo wybierając go z listy, albo przeglądając bazę MIB-ów.

Monitorowanie wydajności sieci

Komunikacja sieciowa spełnia kluczową rolę w systemie informatycznym każdej organizacji. Analiza wydajności sieci poprzez monitorowanie wykorzystania jej zasobów lub ruchu sieciowego może przyczynić się do zapewnienia optymalnego działania całego systemu. Monitorowanie wydajności sieci za pomocą programu NetCrunch może być przeprowadzane na kilka sposobów. W szczególności odnosi się to do tego typu węzłów jak rutery czy przełączniki.

W celu przeprowadzenia takiego monitorowania należy dla danego węzła wybrać z menu **Alerty** polecenie **Konfiguruj** i w nowo otwartym oknie kliknąć ikonę ***Dodaj zdarzenie***. Następnie w oknie **Wybierz zdarzenie** należy kliknąć ikonę ***Dodaj nowe zdarzenie***, co spowoduje wyświetlenie okna **Edytuj warunek zdarzenia**.

Windows

W węzłach Windows można definiować zdarzenia oparte na licznikach Windows związanych z wydajnością sieci. Tak jak w przypadku monitorowania wydajności systemu, w oknie **Edytuj warunek zdarzenia** należy rozwinąć sekcję *Windows* i wybrać klasę *Próg wydajności aplikacji Windows*. Następnym krokiem podczas definiowania tego rodzaju zdarzenia jest wybór licznika związanego z wydajnością sieci (na przykład dla obiektu wydajności, którym jest interfejs sieciowy). Odbywa się to w oknie dialogowym **Dodaj liczniki**.

NetWare

Dla węzłów NetWare można definiować zdarzenia wykorzystujące liczniki NetWare związane bezpośrednio z wydajnością sieci. W oknie **Edytuj warunek zdarzenia** należy rozwinąć sekcję *Novell* i wybrać klasę *Próg Novell NetWare*. Następnym krokiem podczas definiowania tego

rodzaju zdarzenia jest wybór licznika wydajności NetWare, który ma być monitorowany. Odbywa się to w oknie dialogowym **Dodaj liczniki**.

SNMP

Gdy w danym węźle uruchomiony jest agent SNMP, możliwe jest odczytywanie dodatkowych istotnych informacji o wydajności sieci. Można na przykład monitorować zmiany w interfejsie sieciowym w takim węźle. W tym celu w oknie **Edytuj warunek zdarzenia** należy rozwinąć sekcję *Zdarzenia w węźle* i wybrać klasę *Reguły stanu interfejsu sieciowego*. W następnym wyświetlanym oknie należy wybrać ten interfejs sieciowy oraz jego stan, które mają być monitorowane. Można ponadto rozwinąć sekcję *Progi i trapy SNMP* i wybrać klasę *Próg wydajności SNMP*. Jeśli w przypadku określonego węzła baza MIB-ów danego producenta została skompilowana za pomocą NetCruncha, możliwe będzie teraz jej przeglądanie. Dotyczyć to będzie również informacji SNMP właściwych dla danego producenta.

Monitorowanie serwera Microsoft SQL

Monitorowanie serwera MS SQL za pomocą programu NetCrunch może być przeprowadzane na klika sposobów. Jednym z nich jest dodanie usługi sieciowej `MSSQL` do listy usług monitorowanych w danym węźle (w tym, w którym usługa ta jest uruchomiona). Można wówczas dla takiej usługi sieciowej zdefiniować alert, który byłby związany ze zdarzeniem polegającym albo na zmianie stanu usługi sieciowej, albo na przekroczeniu próg dostępności usługi, i skonfigurować go w taki sposób, aby odpowiednie akcje podejmowane były wówczas, gdy usługa ta przestaje odpowiadać, odpowiada zbyt wolno, lub gdy zbyt duża liczba wysłanych pakietów zostaje utracona.

Innym sposobem monitorowania serwera SQL jest skonfigurowanie alertu dla usługi systemu Windows związanej z serwerem MS SQL (czyli `MSSQLSERVER` lub `MSSQLServerAdHelper`), tak aby w momencie, gdy usługa ta zostanie zatrzymana lub wstrzymana, wystosowane zostało odpowiednie powiadomienie lub podjęta właściwa akcja naprawcza.

Jeszcze innym sposobem jest skonfigurowanie alertu polegającego na przekroczeniu progu wydajności aplikacji Windows w licznikach jednego lub kilku obiektów wydajności, bezpośrednio związanych z serwerem MS SQL (np. SQLServer:Databases, SQLServer:GeneralStatistics, SQLServer:SQLStatistics, SQLServer:AccessMethods).

Monitorowanie Microsoft IIS

Monitorowanie serwera Microsoft IIS może odbywać się na kilka sposobów. W pierwszej kolejności do listy usług monitorowanych w danym węźle, w którym działa serwer IIS, należy dodać usługę sieciową HTTP. Po wykonaniu tej czynności możliwe jest skonfigurowanie alertu dla tej określonej usługi sieciowej (związanego ze zdarzeniem polegającym na przykład na zmianie stanu tej usługi na ODPOWIADA lub NIE ODPOWIADA, jej zbyt długiej odpowiedzi lub zbyt dużej ilości traconych pakietów). W tym celu podczas definiowania zdarzenia należy wybrać klasę *Zmiana stanu usługi sieciowej* lub *Próg dostępności usługi sieciowej*.

Kolejną metodą monitorowania serwera IIS jest skonfigurowanie alertu dla usługi systemu Windows związanej z tym serwerem WWW. Podczas definiowania odpowiedniego zdarzenia należy wybrać klasę *Stan usługi Windows*, a następnie na przykład usługę Windows o nazwie *IIS Admin Service*. Istnieje możliwość wyboru takiego sposobu generowania alertu, aby następował on w sytuacji, gdy usługa ta zostanie z jakiegokolwiek powodu zatrzymana, wstrzymana lub uruchomiona, w wyniku czego wystosowywane będzie odpowiednie powiadomienie lub podejmowana właściwa akcja naprawcza.

Ostatnim możliwym sposobem jest definiowanie alertu z wykorzystaniem klasy *Próg wydajności aplikacji Windows*. Możliwe jest przy tym skonfigurowanie dowolnej ilości obiektów spośród wymienionych poniżej obiektów typu licznik związanych z serwerem IIS (dla każdego z nich należy wybrać określone liczniki):

Strony ASP (Active Server Pages)	Liczniki związane ze skryptami i aplikacjami ASP uruchomionymi na serwerze
Usługa FTP	Liczniki odpowiadające usłudze FTP
Usługa indeksowania HTTP	Liczniki związane z usługą indeksowania witryn WWW, aktywnych kwerend i rezultatów buforowania
Usługa indeksowania	Liczniki usługi indeksowania związane z indeksowaniem procesów, list roboczych i zapytań
Filtr usługi indeksowania	Liczniki udostępniające dodatkowe informacje o wydajności związanej z filtrami treści oraz o ich szybkości indeksowania
Ogólne informacje o usługach IIS	Liczniki dostarczające dodatkowych informacji o wydajności związanej z filtrami treści oraz o ich szybkości indeksowania
Polecenia NNTP	Liczniki odpowiadające poleceniom NNTP wykonywanym na serwerze przez użytkowników
Serwer NNTP	Liczniki używane do monitorowania ogólnej wydajności serwera NNTP, np. liczby przesyłanych, odbieranych lub publikowanych artykułów na sekundę
Sterownik pamięci SMTP NTFS	Liczniki służące do śledzenia całkowitej liczby wiadomości i strumieni wiadomości
Serwer SMTP	Liczniki śledzące całkowitą wydajność usługi SMTP, np. liczbę wysyłanych i odbieranych wiadomości na sekundę
Usługa sieci WWW	Liczniki związane z usługą World Wide Web Publishing Service

Optymalizacja monitorowania

Do modyfikowania sposobu monitorowania aktualnie otwartego atlasu służy specjalny kreator programu. Okno tego kreatora pojawia się po wybraniu z menu **Atlas** polecenia

Optymalizacja monitorowania. Można w nim wybrać jedną z następujących strategii optymalizacji monitorowania:

Uproszczona	W ramach tej strategii program monitoruje w pełnym zakresie jedynie serwery i rutery. Pozostałe rodzaje węzłów monitorowane są w trybie monitorowania uproszczonego, co oznacza, że nie są zbierane żadne dane dotyczące wydajności – ani na potrzeby związane z alertowaniem, ani na potrzeby związane z raportowaniem.
Szczegółowa	Wybór tej opcji powoduje, że program określa ustawienia parametrów monitorowania poszczególnych węzłów na podstawie ich właściwości. Na przykład węzły krytyczne będą monitorowane częściej, a dla innych węzłów włączone zostaną jedynie wybrane kategorie monitorów.

Wspomniany kreator umożliwia również pomijanie dowolnie wybranych węzłów atlasu w optymalizacji monitorowania. W tym celu należy dodać odpowiednie węzy do listy węzłów wyłączonych z optymalizacji monitorowania w drugim oknie kreatora.

Uwaga

Dany węzeł można wyłączyć z optymalizacji monitorowania także poprzez zaznaczenie w oknie ***Monitorowanie*** *(na karcie* ***Ogólne****) pola wyboru* ***Wyklucz z optymalizacji monitorowania****.*

Widoki wydajności

W oknie **Widok sieci** możliwe jest tworzenie wykresów wydajności związanych z określonymi węzłami w atlasie. Umożliwiają one obserwację dowolnie wybranego parametru wydajności, który z różnych względów powinien być monitorowany. Wykresy mogą przybierać jedną z trzech postaci: wykresu liniowego, wykresu słupkowego lub wskaźnika wychyłowego. Zatem w zależności o tego, jakie liczniki wydajności mają być śledzone, istnieje możliwość wybrania takiej postaci wykresu, która najlepiej nadaje się do prawidłowej wizualizacji danych dostarczanych przez te liczniki. Możliwy jest wybór następujących czterech rodzajów liczników wydajności: liczniki związane z usługami sieciowymi, liczniki wydajności systemu Windows NT, liczniki wydajności SNMP oraz liczniki wydajności systemu NetWare.

Tworzenie widoków wydajności

Przed przystąpieniem do tworzenia widoków wydajności należy zdecydować, czy ma zostać tworzony pusty widok wykresów czy też filtrowany widok wykresów. Pusty widok wykresów zawiera wykresy wydajności tych węzłów, które zostały ręcznie naniesione na mapę. Z kolei filtrowany widok wykresów zawiera listę tych węzłów wraz z odpowiednimi wykresami wydajności, które zostały dodane automatycznie, na podstawie wcześniej ustalonych reguł filtrowania. W przypadku tego typu widoku nie ma możliwości ręcznego dodawania wykresów wydajności nowych węzłów.

Aby utworzyć dynamiczny widok wykresów

1. W oknie **Atlas sieci** kliknij prawym przyciskiem myszy sekcję *Widoki wydajności* lub którykolwiek należący do niej folder.
2. W menu podręcznym wskaż pozycję **Nowy**, a następnie wybierz opcję **Dynamiczny widok wykresów**.
3. W oknie **Właściwości mapy** wpisz nazwę widoku wykresów, a w polu **Kryteria filtrowania węzłów** określ odpowiednie kryteria filtrowania.
4. Kliknij pole **Licznik**, aby wybrać żądany licznik wydajności. Możesz go wybrać z dostępnej listy lub dodać nowy.

Aby utworzyć pusty widok wykresów

1. W oknie **Atlas sieci** kliknij prawym przyciskiem myszy sekcję *Widoki wydajności* lub którykolwiek należący do niej folder.
2. W menu podręcznym wskaż pozycję **Nowy**, a następnie wybierz opcję **Pusty widok wykresów**.
3. W oknie **Widok sieci** kliknij prawym przyciskiem myszy dowolne wolne miejsce, wskaż w menu podręcznym polecenie **Wstaw**, a następnie w kolejnym otwartym menu kliknij pozycję **Wykres**.
4. W polu **Monitorowany węzeł** wybierz węzeł, dla którego będą wyświetlane dane wydajności udostępniane przez licznik.
   Następnie należy kliknąć ikonę ***Wybierz węzeł*** i w nowym oknie wskazać żądany węzeł.
5. Kliknij przycisk **Dalej**.
6. Kliknij ikonę **Dodaj węzeł** i wybierz rodzaj licznika, którego dane chcesz prezentować na wykresie.
7. Powtórz czynność opisaną w punkcie 6, ilekroć chcesz wyświetlić na wykresie – dla węzła wybranego w punkcie 4 – dodatkowe dane licznika w postaci osobnego panelu wykresu.
8. Kliknij przycisk **OK**.
   Powtórz czynności opisane w punktach 3-7 dla każdego kolejnego węzła, dla którego chcesz utworzyć wykres.

Uwaga

W punkcie 6 można wybrać jeden z następujących rodzajów liczników: wydajność NetWare, wydajność SNMP (przy zastosowaniu niestandardowego OID-a licznika, bazy danych MIB-ów lub rodzaju predefiniowanego), wydajność Windows oraz wydajność usługi sieciowej.

Zmiana właściwości wykresów wydajności

Modyfikacja właściwości wyświetlanego wykresu odbywa się w oknie **Właściwości panelu wydajności**, które można otworzyć wybierając polecenie z podręcznego menu. W ten sposób można ustawiać następujące właściwości wykresów:

Tytuł	Określa tytułowy tekst, który pojawia się tuż nad wykresem.
Stopka	Określa dowolny dodatkowy tekst, który pełni rolę stopki.
Rodzaj panelu	Określa, czy wyświetlany będzie wykres liniowy, wykres słupkowy czy też wskaźnik wychyłowy.
Schemat kolorystyczny	Definiuje kolory używane przy różnych zakresach wartości na wykresie. Możliwe jest tworzenie własnych zestawień kolorów.
Jednostki skali	Określa jednostki skali pomiaru automatycznie dobierane dla wartości, w formacie K, KB, M, MB, G lub GB.
Przedział wartości	Określa minimalny i maksymalny przedział wartości, jaki będzie wyświetlany na wykresie. Powyższe wartości wyznaczają skalę wykresu. Przy wpisaniu wartości 0 dla obu wielkości, program będzie stosował domyślne wartości maksymalne i minimalne.

Aby zmienić właściwości wykresu

1. Wskaż docelowy widok wykresów w folderze **Widoki wydajności** w oknie **Atlas sieci**.
2. Kliknij prawy przyciskiem myszy wykres, którego właściwości chcesz zmienić, a następnie wybierz kartę **Właściwości**.
   Wówczas zostanie uruchomione okno **Właściwości panelu wydajności**.
3. W polu **Tytuł** umieść opisowy tytuł wykresu.
4. W polu **Stopka** wpisz dodatkowy tekst, który ma figurować w dolnej części wykresu.
5. Aby zmienić rodzaj panelu, wybierz wykres kołowy, słupkowy bądź wskaźnik wychyłowy w rozwijanej liście **Rodzaj panelu**.
6. Użyj rozwijanej listy **Schemat kolorystyczny**, aby wybrać schemat kolorów dla różnych wartości prezentowanych na wykresie
7. Kliknij kartę **Skala**.
8. Używając rozwijanej listy **Skala** oraz sąsiadującego z nią pola, zdefiniuj jednostki skali i przyrostu dla wykresu.
9. W polu **Wyświetl wartości w przedziale** podaj minimalne i maksymalne wartości, które będą wyznaczać punkty graniczne skali na wykresie.

Uwagi:

- *W punkcie 6 można ponadto kliknąć ikonę* **Właściwości** *znajdującą się na prawo od rozwijanej listy, a następnie w oknie* ***Właściwości schematu kolorów*** *określić własne kolory, jakie będą stosowane dla różnych przedziałów wartości na wykresach. Po zakończeniu tej operacji można kliknąć przycisk* ***Zapisz jako****, aby zapisać zmiany definiujące nowy kolor schematów (wówczas pojawi się on automatycznie w rozwijanej liście* ***Schemat kolorystyczny****).*

- *Istnieje również możliwość zmiany rozmiaru lub stylu wyświetlanych wykresów (wskaźników lub słupków). W tym celu wystarczy kliknąć prawym przyciskiem myszy dowolne miejsce w oknie **Widok sieci**, z menu podręcznego wybrać polecenie **Rozmiar** lub **Styl**, a następnie wybrać odpowiednią opcję.*

Przeglądanie historii licznika

Dla każdego licznika wyświetlanego w danym widoku wydajności możliwe jest odczytanie historii wydajności określonego licznika. Zadanie to można wykonać za pomocą menu podręcznego dla wykresu.

Aby przeglądać historię licznika wydajności

1. W Atlasie sieci wybierz widok wydajności, którego historia ma zostać pokazana. Zdefiniowane dla niego wykresy zostaną wyświetlone w oknie **Widok sieci**.
2. Prawym przyciskiem myszy kliknij wybrany wykres widoku i z podręcznego menu wybierz opcję **Historia licznika**.
   W nowym oknie wyświetli się program o nazwie **Przeglądarka trendów**.

Wirtualne liczniki wydajności

Wirtualne liczniki wydajności są szczególnym rodzajem licznika swoistym dla programu NetCrunch. Noszą one miano wirtualnych, ponieważ nie odnoszą się bezpośrednio do rzeczywistych liczników wydajności, jakie są monitorowane w programie. Ich głównym przeznaczeniem jest umożliwianie użytkownikowi tworzenie własnych liczników zdefiniowanych za pomocą prostego lub złożonego wyrażenia arytmetycznego składającego się ze zmiennych (z wykorzystaniem funkcji dodawania, odejmowania, mnożenia, dzielenia, maks. i min.). Licznikom tym przypisywane są rzeczywiste dane zbierane z monitorowanych liczników urządzeń (rodzaju SNMP, NT i NetWare). Jednakże w definicji licznika wirtualnego, w charakterze zmiennych wyrażenia arytmetycznego można używać wyłącznie monitorowanych liczników wydajności jednego typu (czyli SNMP, NetWare lub NT).

Wirtualne liczniki wydajności definiuje się przy użyciu udostępnionego w programie kreatora. Jeśli w trakcie definicji wirtualnego licznika wydajności używane są wystąpienia, należy wskazać na wirtualne wystąpienie wybranego rzeczywistego monitorowanego licznika o nazwie '_VCounter', który zostanie użyty w wyrażeniu arytmetycznym w charakterze zmiennej. Stworzony w ten sposób licznik wirtualny można regularnie używać – tak jak każdy inny licznik w programie – w definicji progów, przeglądarce trendów, raportów i zdarzeniach. Licznik taki zawsze zaczyna się przedrostkiem '.NCVC' odróżniającym go od zwykłych liczników urządzeń. Warto zauważyć, że nie można usuwać definicji wirtualnego licznika wydajności, jeśli jest on już używany w innym miejscu w programie.

Otwieranie okna Wirtualne liczniki wydajności

Zarządzanie licznikami wirtualnymi w programie odbywa się w oknie **Wirtualne liczniki wydajności**. Można w nim w łatwy sposób dodawać nowe liczniki wirtualne, edytować ich wyrażenie arytmetyczne złożone ze zmiennych przypisanych rzeczywistym licznikom urządzeń a także całkowicie je usuwać.

Aby otworzyć okno Wirtualne liczniki wydajności

1. W menu **Atlas** wskaż **Monitorowanie** i wybierz opcję **Wirtualne liczniki wydajności**. Okno **Wirtualne liczniki wydajności** wyświetli listę aktualnie zdefiniowanych w programie liczników wirtualnych wraz z krótkim opisem każdego z nich.

Uwagi

- *Lista liczników wirtualnych dzieli się na trzy sekcje związane odpowiednio z licznikami wydajności rodzaju NT, NetWare i SNMP.*
- *Możliwe jest rozwijanie lub zwijanie listy liczników wirtualnych dla każdego rodzaju licznika należącego do sekcji.*

Definicja nowego wirtualnego licznika wydajności

Przy definiowaniu licznika wirtualnego należy w pierwszej kolejności wybrać jedną z następujących kategorii liczników rzeczywistych, które posłużą do jego utworzenia: wydajność NT, wydajność SNMP lub wydajność NetWare. Następnie należy wskazać obiekt wydajności, do którego będzie przynależał (można wybrać obiekt już istniejący lub utworzyć nowy dla rodzaju wydajności SNMP). W kolejnym kroku należy określić nazwę nowego licznika wirtualnego oraz jego krótki opis. Ostatnia czynność polega na zbudowaniu wyrażenia arytmetycznego złożonego ze zmiennych przypisanych rzeczywistym licznikom urządzeń, odpowiadającym kategorią wybranemu licznikowi wirtualnemu (NT, SNMP lub NetWare).

Aby zdefiniować wirtualny licznik wydajności

1. Otwórz okno **Wirtualne liczniki wydajności**.

2. Kliknij ikonę ***Dodaj licznik***.
   Wyświetli się okno **Definicja licznika wirtualnego**.
3. Wybierz rodzaj monitora wydajności dla nowego wirtualnego licznika: NT, SNMP lub NetWare.
4. Kliknij **Dalej**.
5. Z rozwijanej listy **Nazwa obiektu wydajności** wybierz obiekt wydajności, któremu ma podlegać nowy licznik wirtualny.
6. W polu **Nazwa licznika wydajności** wpisz nazwę nowego licznika wirtualnego.
7. W polu **Opis** wpisz krótki tekst opisujący nowy licznik wirtualny.
8. Kliknij **Dalej**.
9. Dodaj żądane zmienne licznika (por. sekcję *Dodawanie zmiennej licznika* na stronie 58, w celu uzyskania dodatkowych informacji).
10. W polu **Wyrażenie licznika** użyj właśnie zdefiniowanych zmiennych do zbudowania wyrażenia arytmetycznego dla nowego licznika wirtualnego (stosując dodawanie, odejmowanie, dzielenie i mnożenie).

Uwagi

- *W punkcie 5 można kliknąć przycisk **Edytuj**, aby utworzyć nowy obiekt wydajności SNMP dla tworzonego aktualnie wirtualnego licznika wydajności. W oknie **Właściwości obiektu wydajności SNMP** konieczne stanie się określenie źródła wystąpienia liczników, czyli kolumny tabeli SNMP, która będzie źródłem wystąpienia liczników określonego obiektu. Następnie kliknij **Zapisz jako**, aby utworzyć nową nazwą dla obiektu wydajności SNMP.*
- *W punkcie 5 w trakcie budowania wyrażenia arytmetycznego można w polu sekcji **Zmienne licznika** dwukrotnie kliknąć określoną zmienną, aby automatycznie dodać ją do pola **Wyrażenie licznika**.*

Dodawanie zmiennej licznika

Możliwe jest dodawanie dowolnej ilości zmiennych licznika. Później można włączyć nazwę każdej zmiennej licznika do wyrażenia arytmetycznego dla tworzonego wirtualnego licznika wydajności. Procedury dodawania zmiennych kategorii „licznik SNMP" i zmiennych kategorii „licznik NT/NetWare" nieco się od siebie różnią. Mianowicie przy dodawaniu licznika SNMP jako zmiennej, można go wybrać na trzy następujące sposoby:

Predefiniowany licznik SNMP	Należy wybrać węzeł źródłowy, obiekt wydajności do którego należy, licznik i ewentualnie skorygować jego wystąpienie ('_VCounter').
Licznik bazy MIB-ów	Należy użyć okna **Przeglądarki MIB-ów** w celu wyszukania żądanego licznika SNMP, który ma zostać użyty w charakterze zmiennej.
Licznik niestandardowego OID-a	Należy bezpośrednio wpisać OID licznika SNMP mającego pełnić rolę zmiennej.

Aby dodać zmienne licznika NT/NetWare

1. W oknie Definicja liczników wirtualnych (ekran Definicja wyrażenia licznika), kliknij ikonę ***Dodaj***.
2. Wybierz opcję **Licznik wydajności**.
   Otworzy się okno **Dodaj liczniki**.
3. Z rozwijanej listy **Źródło** wybierz węzeł źródłowy.
4. Z rozwijanej listy **Obiekt wydajności** wybierz obiekt wydajności.
5. Wybierz licznik z listy, a jeśli posiada wystąpienia, wybierz wystąpienie '_VCounter'.
6. Kliknij **Dodaj**.
7. Określ nazwę dla zmiennej, której przypisany jest wybrany rzeczywisty licznik urządzenia (punkty 3-5) i kliknij **OK**.
   Pojawi się nowa zmienna w liście **Zmienne licznika**.
8. Powtórz kroki od 1 do 7, jeśli chcesz dodać kolejny rzeczywisty licznik urządzenia w charakterze zmiennej.

Uwagi

- *W punkcie 1 po kliknięciu ikony* **Dodaj** *można także wybrać funkcję* ***Maks.*** *lub* ***Min.****, która umożliwia wybór wartości minimalnej i maksymalnej znajdującej się między dwoma porównywanymi wartościami zmiennych. Zostanie ona natychmiast dodana do wyrażenia licznika wyświetlanego w polu* ***Wyrażenie licznika****. Użyj dwóch przedzielonych przecinkiem nazw zmiennych umieszczonych w nawiasach funkcji* `MAX()` *lub* `MIN()` *(tj.* `MAX[var1, var2]`*).*
- *Po wykonaniu kroku z punktu 8 wszystkie zdefiniowane zmienne zostaną w przystępny sposób wyszczególnione w sekcji pola* ***Zmienne liczników****.*
- *Po dodaniu wszystkich zmiennych można przystąpić do formułowania wyrażenia arytmetycznego dla nowego wirtualnego licznika wydajności. Por. ostatni punkt sekcji* Definicja nowego wirtualnego *licznika na stronie 57 w celu uzyskania dodatkowych informacji.*

Aby dodać zmienną licznika SNMP

1. W oknie **Definicja liczników wirtualnych** (ekran **Definicja wyrażenia licznika**) kliknij ikonę ***Dodaj***.
2. Wybierz opcję Predefiniowany licznik SNMP, Licznik bazy MIB-ów, lub Niestandardowy licznik OID-a.
3. Jeśli wybrałeś opcję **Predefiniowany licznik SNMP**, wykonaj czynności opisane w punktach od 3 do 7 opisanych w poprzedniej sekcji.
   Jeśli wybrałeś opcję **Licznik bazy MIB-ów**, otworzy się okno **Dodaj licznik**. Użyj okna **Przeglądarka MIB-ów**, aby znaleźć licznik SNMP i wskazać jego wystąpienie (w stosownych przypadkach). Kliknij **Dodaj**.
   Jeśli wybrałeś opcję **Niestandardowy licznik OID-a**, otworzy się okno **Dodaj licznik**. Wpisz OID żądanego licznika SNMP w polu **OID** i kliknij **Dodaj**.
4. Powtórz czynności opisane w punktach 1—3, aby dodać kolejny licznik SNMP jako zmienną.

Uwagi

- *Jeśli w punkcie 3 wybrałeś opcję* ***Licznik z bazy MIB-ów*** *lub* ***Niestandardowy licznik OID-a****, w oknie* ***Dodaj licznik*** *możesz dodatkowo zaznaczyć opcję* ***Wartość/Sek****. Oznacza to, że zmiany zachodzące w dwóch ostatnich odczytanych wartościach wybranego licznika SNMP zostaną obliczone w sekundach.*
- *Po dodaniu wszystkich zmiennych można przystąpić do formułowania wyrażenia arytmetycznego dla nowego wirtualnego licznika wydajności. Por. ostatnią czynność opisaną w sekcji* Definicja nowego wirtualnego *licznika na stronie 57 w celu uzyskania dodatkowych informacji.*

Edycja właściwości licznika wirtualnego

Po zdefiniowaniu wirtualnego licznika wydajności można jedynie modyfikować jego wyrażenie arytmetyczne złożone ze zmiennych przypisanych rzeczywistym licznikom urządzenia oraz krótki tekst opisujący licznik wirtualny. Nie można natomiast zmienić nazwy licznika wirtualnego ani zmodyfikować obiektu wydajności, do którego przynależy.

Aby edytować właściwości licznika wirtualnego

1. Otwórz okno Wirtualne liczniki wydajności.

2. Wybierz z listy licznik i kliknij ikonę ***Zmień właściwości***.
   Otworzy się okno **Definicja liczników wirtualnych**.
3. Dokonaj zmian w wyrażeniu arytmetycznym lub zdefiniowanych zmiennych skojarzonych z rzeczywistymi licznikami urządzenia.

Uwaga

Aby zmienić krótki opis licznika wirtualnego, kliknij przycisk ***Wstecz*** *i dokonaj zmian w polu* ***Opis****.*

Usuwanie licznika wirtualnego

Możliwe jest usunięcie jedynie wirtualnego licznika wydajności, który aktualnie nie jest używany w NetCrunchu (tj. nie znajduje się w progach, zdarzeniach, raportach lub przeglądarce trendów).

Aby usunąć wirtualny licznik wydajności

1. Otwórz okno **Wirtualne liczniki wydajności**.
2. Wybierz z listy licznik wirtualny do usunięcia. Konieczne może okazać się rozwinięcie sekcji licznika (NT, SNMP lub NetWare).

3. Kliknij ikonę ***Usuń licznik***. Wskazany licznik wirtualny zostanie usunięty.

Zarządzanie urządzeniami przy użyciu agentów SNMP

Przeglądanie i konfigurowanie zmiennych SNMP

Przeglądanie i konfigurowanie ustawień SNMP może odbywać się na dwa sposoby – albo bezpośrednio w programie NetCrunch, albo za pomocą dostępnej w pakiecie NetCrunch zewnętrznej aplikacji o nazwie **Narzędzia IP i SNMP** (która może być także uruchamiana z poziomu interfejsu programu). Posługiwanie się obiema metodami odbywa się w taki sam sposób – zmienne SNMP mogą być przeglądane, a ponadto ich poszczególne wartości mogą być zmieniane.

Aby skorzystać z jednej z tych metod, należy – odpowiednio – albo z menu podręcznego dla węzła, dla którego chcemy przeglądać lub konfigurować ustawienia SNMP, wybrać polecenie **SNMP**, a następnie polecenie **Przeglądaj**, albo kliknąć od razu ikonę ***Narzędzia IP i SNMP*** na pasku narzędzi. Oczywiście, aby móc w danym węźle oglądać i modyfikować zmienne SNMP, należy prawidłowo określić parametry *Wspólnota odczytu* oraz *Wspólnota zapisu*.

Zewnętrzna przeglądarka SNMP wyświetla te informacje, które wyszczególnione zostały w pliku SNMPVIEW.XML, znajdującym się w katalogu, w którym został zainstalowany sam program. Jeśli przeglądarka ma wyświetlać dodatkowe informacje SNMP właściwe dla danego węzła, należy ten plik XML odpowiednio zmodyfikować.

W oknie **Narzędzia IP i SNMP** można także przeglądać lub wprowadzać zmiany w informacjach SNMP korzystając z wbudowanej przeglądarki MIB-ów. W tym celu wystarczy w obszarze **SNMP** wybrać przycisk opcji **Przeglądarka MIB-ów**.

Rozbudowywanie baz MIB

Kompilator MIB-ów

Kompilator MIB-ów to praktyczny program narzędziowy udostępniony w NetCrunchu. Umożliwia on wykonywanie następujących zadań:

- edycja treści modułów MIB,
- kompilacja modułów MIB,
- przeglądanie zawartości modułów MIB – drzew, zdefiniowanych zmiennych oraz trapów,
- tworzenie aliasów dla określonych modułów MIB,
- usuwanie modułów MIB.

Poza powyższymi opcjami Kompilator MIB-ów oferuje poręczne metody sortowania i filtrowania listy załadowanego modułu MIB. Przede wszystkim jednak Kompilator MIB-ów pozwala na dodawanie do bazy programu MIB-ów producentów, dzięki czemu możliwe jest poprawne przeglądanie zawartych w nich informacji z poziomu programu lub jego modułu ITools.

Typowe problemy podczas kompilacji baz MIB-ów oraz sposoby ich rozwiązywania

Podczas korzystania z **Kompilatora MIB-ów** pojawić się może kilka problemów związanych z kompilacją. Problemy te oraz sposoby ich rozwiązywania zostały opisane w kolejnych podrozdziałach.

Brakujące aliasy

Ponieważ w chwili obecnej na rynku nie przyjęto żadnych standardów nazewnictwa plików MIB, podczas kompilacji mogą wystąpić błędy. Aby tego uniknąć, przed rozpoczęciem kompilacji bazy MIB (która zazwyczaj jest uzależniona od innych baz MIB), należy określić zestaw aliasów dla importowanych baz MIB.

Na przykład baza MIB o nazwie `RFC1155-SMI` może być także nazywana, w różnych odwołaniach do niej, jako `RFC-1155`, `RFC1155` lub `RFC1155SMI`. Jeżeli wszystkie te różniące się konwencje nazewnictwa danej bazy MIB zostaną zadeklarowane w obszarze aliasów, wówczas możliwa będzie jej pomyślna kompilacja.

Kilka deklaracji bazy MIB w jednym pliku

W sytuacji, gdy dany plik zawiera kilka sekcji definiujących bazę MIB, ograniczonych słowami kluczowymi BEGIN i END, kompilator zasygnalizuje wystąpienie błędów. Rozważmy przykładowy plik o nazwie `RFCXXFDDI-MIB.MIB` i następującej zawartości:

```
RFCXXFDDI-MIB DEFINITIONS ::= BEGIN
```

```
…

…

…

END


TEST-MIB DEFINITIONS ::= BEGIN

…

…

…

END
```

Jak widać, w tym samym pliku znajdują się dwie definicje bazy MIB, co dla kompilatora jest sytuacją nieprawidłową. Aby uniknąć problemu kilku deklaracji bazy MIB w jednym pliku, należy przed kompilacją umieścić każdą taką deklarację w oddzielnym pliku. Dla przykładu, aby uniknąć sygnalizowania błędów podczas kompilacji przedstawionego powyżej pliku MIB, jego zawartość powinna zostać rozdzielona w następujący sposób:

Plik `RFCXXFDDI-MIB.MIB`:

```
RFCXXFDDI-MIB DEFINITIONS ::= BEGIN

…

…

…

END
```

Plik `TEST-MIB.MIB`:

```
TEST-MIB DEFINITIONS ::= BEGIN

…

…

…

END
```

Nieprawidłowa definicja obiektu

Kompilator baz MIB nie akceptuje definicji obiektów o następującej składni:

```
iso(1) org(3) dod(6) internet(1) …
```

Dotyczy to zwłaszcza przypadku trapu właściwego dla producenta – umieszczany jest on wówczas w niewłaściwym miejscu drzewa. Poniżej przedstawiony został przykład zapisu pochodzącego z pliku MIB, zawierającego nieprawidłową definicję obiektu (co podczas kompilowania takiego pliku spowoduje zasygnalizowanie błędu):

```
fddirmon-mib OBJECT IDENTIFIER ::= { iso(1) org(3) dod(6) internet(1) private(4)
     enterprises(1) novell(23) mibDoc(2) 69 }
```

Aby temu zaradzić, należy tak zmienić składnię definicji obiektu, aby tylko przedostatni wpis odpowiadający identyfikatorowi OID nie zawierał liczby w nawiasach. Tak więc poprawna definicja obiektu z przykładu powyżej powinna przedstawiać się następująco:

```
fddirmon-mib OBJECT IDENTIFIER ::= { mibDoc 69 }
```

Po wprowadzeniu takiej zmiany kompilator nie powinien sygnalizować błędu.

Gdzie szukać baz MIB-ów

Jeśli poszukujemy bazy MIB dla urządzenia pochodzącego od określonego producenta, najlepszym wyjściem jest odwiedzenie jednej ze wielu witryn WWW zawierających katalogi baz MIB. Można również spróbować pobrać bazę MIB producenta bezpośrednio z jego oficjalnej witryny, zwłaszcza że może ona okazać się bardziej aktualna niż bazy dostępne w witrynach będących katalogami baz MIB. Poniżej podana została lista najbardziej popularnych stron udostępniających bazy MIB różnych producentów:

www.mibdepot.com/cgi-bin/downloads.cgi

www.oidview.com/mibs/detail.html

www.somix.com/software/mibs

www.hdopp.de/S-ManageWise.html#mwmibs

Otrzymywanie trapów SNMP i odpowiadanie na nie

Tryby nasłuchu

Aby uruchomić w programie NetCrunch procedurę nasłuchu i otrzymywania trapów SNMP, konieczne jest ustawienie odpowiednich opcji w programie – w tym celu z menu **Narzędzia** należy wybrać polecenie **Opcje**, a następnie kliknąć stronę **Monitorowanie – SNMP**. W otwartym w ten sposób oknie można włączyć nasłuchiwanie przez program trapów SNMP (określając numer portu, na którym będzie się to odbywało) oraz ustawić przekierowywanie przychodzących trapów SNMP (należy w tym celu określić odpowiedniego urządzenia i numer portu, na którym będzie on prowadzić nasłuch).

Program udostępnia dwa niezależne tryby nasłuchu – jeden wykorzystuje usługę systemu Windows o nazwie Trap SNMP, a drugi korzysta z wewnętrznego mechanizmu nasłuchiwania. W danym momencie tylko jeden z tych trybów może być aktywny. Jeśli w chwili uruchomienia programu NetCrunch działa usługa Windows SNMP Trap, program domyślnie użyje jej do prowadzenia nasłuchu. Jeśli zaś usługa ta nie jest uruchomiona, NetCrunch automatycznie ją uruchomi i wykorzysta do nasłuchu. Gdy jednak usługa ta nie będzie dostępna (nie została zainstalowana), zamiast niej program automatycznie skorzysta z wewnętrznej metody nasłuchu. Należy pamiętać, że gdy określony w opcjach programu port nasłuchu jest zajęty przez inną aplikację (np. usługę trapową HP OpenView), NetCrunch wyświetli okno ostrzegające o tym problemie. Aby go usunąć, należy w ustawieniach programu wskazać inny port nasłuchu i odpowiednio zmienić ustawienia agenta SNMP w węzłach, tak aby generowane przez nie trapy były kierowane do portu o nowym numerze.

Definiowanie zdarzenia polegającego na nadejściu trapu

W programie NetCrunch przewidziana została specjalna klasa zdarzeń – właśnie dla potrzeb przychodzących trapów SNMP. Zdarzenie takie może zostać przez użytkownika zdefiniowane albo dla ogólnych (standardowych) trapów SNMP, albo dla trapów właściwych dla danego producenta.

Aby zdefiniować zdarzenie polegające na nadejściu trapu

1. W oknie Konfiguracja alertów kliknij ikonę ***Dodaj zdarzenie.***
2. W oknie Wybierz zdarzenie kliknij ikonę ***Dodaj nowe zdarzenie***.
3. W sekcji *Progi i trapy SNMP* wybierz klasę **Zdarzenie trap SNMP**, a następnie kliknij przycisk **Dalej**.
4. Wpisz nazwę nowo tworzonego zdarzenia (w polu **Opis**), jego rangę oraz stan, który następuje po wystąpieniu takiego zdarzenia (odpowiednio w polach **Ranga** i **Stan**).
5. Wykorzystaj następujące cztery pola (omówione w poniższej tabeli) do opisania danego trapu, a następnie potwierdź wprowadzone ustawienia, klikając przycisk **OK**.

NAZWA POLA	OPIS POLA
Rodzaj podstawowy	Umożliwia wybór pomiędzy ogólnym rodzajem trapu (Cold Start, Warm Start, Link Down, Link Up, Błąd uwierzytelnienia, Neighbor Loss) a rodzajem trapu właściwym dla producenta
Wspólnota	Umożliwia wybór wspólnoty trapów wykorzystywanej podczas nasłuchu
Producent	Określa producenta, dla którego ma być prowadzone nasłuchiwanie trapów
Szczególny rodzaj trapu	Umożliwia wybór nasłuchiwanego rodzaju trapu właściwego dla producenta

Uwagi

- *W polach **Rodzaj podstawowy**, **Wspólnota** lub **Producent** można wybrać opcję 'dowolny lub 'dowolna'. Jeśli opcja ta zostanie wybrana w pierwszym z pól, oznacza to, że dane zdarzenie będzie generowane dla każdego rodzaju przychodzącego trapu SNMP (ogólnego lub właściwego dla producenta). Jeśli w polu **Wspólnota** wybierana zostanie opcja 'dowolna', program będzie nasłuchiwał trapów we wszystkich wspólnotach SNMP. W przypadku pola **Producent** program NetCrunch będzie nasłuchiwał trapów od wszystkich producentów.*
- *Po zdefiniowaniu zdarzenia polegającego na otrzymaniu trapu SNMP można mu przypisać określone akcje. W tym celu w oknie **Konfiguracja alertów** należy wybrać to konkretne zdarzenie i kliknąć ikonę* **Dodaj akcję***).*

Przekierowywanie trapów SNMP (Trap forwarding)

Jeżeli chcemy, aby w programie NetCrunch trapy SNMP przychodzące z dowolnego węzła były przekazywane dalej do innego urządzenia, należy wprowadzić odpowiednie ustawienia w opcjach programu.

Aby przekazywać trapy SNMP dalej, do innego urządzenia

1. Z menu **Narzędzia** wybierz polecenie **Opcje**.
2. W nowo otwartym oknie wybierz stronę **Monitorowanie – SNMP**.
3. Zaznacz pole wyboru **Nasłuchuj trapów SNMP**.
4. W znajdującym się poniżej polu **Port** wpisz numer portu, na którym program NetCrunch będzie prowadził nasłuch.
5. Zaznacz pole wyboru **Przekierowuj trapy SNMP**.
6. W polu **Nazwa lub adres IP węzła** wpisz adres IP lub nazwę urządzenia, do którego NetCrunch będzie przekazywał przychodzące trapy SNMP.
7. W znajdującym się poniżej polu **Port** wpisz numer portu, na jakim zdalny komputer będzie nasłuchiwał trapów SNMP.
8. Zatwierdź zmiany, klikając przycisk **OK**.

Zamiana alertu programu NetCrunch na trap SNMP

Aby umożliwić taką zamianę, należy do listy akcji związanych z określonym alertem dodać akcję o nazwie *Alert SNMP*. Wymaga to wskazania docelowego komputera, numeru portu oraz wspólnoty trapów SNMP, którą zdalny węzeł będzie wykorzystywał do nasłuchu.
Po zdefiniowaniu dla danego zdarzenia akcji polegającej na wysłaniu trapu SNMP można wyeksportować bazę MIB-ów NetCruncha (wraz ze zdefiniowanymi parametrami dla zdarzenia/trapu SNMP) do pliku. Plik taki może zostać później skompilowany i włączony do bazy danych aplikacji nasłuchującej na tym hoście, który będzie odbierać trapy SNMP wygenerowane przez program NetCrunch. Więcej informacji na ten temat zawiera rozdział *Korzystanie z bazy MIB-ów programu NetCrunch* na stronie 66.

Aby dla danego zdarzenia utworzyć akcję polegającą na wysłaniu trapu SNMP

1. W oknie **Konfiguracja alertów** wybierz zdarzenie polegające na otrzymaniu trapu SNMP.
2. Kliknij ikonę ***Dodaj akcję***.
3. Kliknij ikonę ***Zdefiniuj nową akcję***.
4. Wybierz opcję Wyślij powiadomienie proste.
5. Ze znajdującej się nieco poniżej listy rozwijanej wybierz opcję *Alert SNMP*.
6. Określ docelowego komputera (wpisując jego nazwę lub adres IP).
7. Wpisz numer portu, na którym komputer będzie nasłuchiwał przychodzących alertów SNMP.

8. Określ wspólnotę trapów SNMP, która będzie wykorzystywana przez komputer.
9. Kliknij przycisk **OK**.
10. Kliknij przycisk **Dalej**, aby określić właściwości definiowanej akcji.
11. Klikając odpowiednią opcję zdecyduj, czy wysłane mają być wszystkie czy tylko wybrane informacje o trapie.
12. Jeżeli w poprzednim punkcie podjęta została decyzja o wysyłaniu tylko wybranych informacji, odznacz pola wyboru odpowiadające tym zmiennym, których nie chcesz wysyłać.
13. Kliknij przycisk **OK**.

Uwaga

Podczas wybierania akcji polegającej na wysłaniu trapu SNMP istnieje możliwość precyzyjnego określenia, które spośród informacji o trapie mają być wysłane do komputera. Zmienne związane z trapem można ogólnie podzielić na trzy kategorie: ogólne (opisują ogólne warunki zdarzenia), właściwości (opisują właściwości węzła generującego zdarzenie) oraz charakterystyczne dla danej klasy (opisują dane charakterystyczne dla określonej klasy zdarzeń). Użytkownik ma możliwość wyboru tylko tych, które chce, aby były włączone do przekazywanego trapu alertującego SNMP.

Korzystanie z bazy MIB-ów programu NetCrunch

Baza MIB-ów w NetCrunchu jest generowana automatycznie podczas dodawania do określonego alertu akcji polegającej na wysłaniu trapu SNMP i zawiera listę trapów SNMP zdefiniowanych w programie. Taką bazę MIB-ów można w prosty sposób zaimportować i skompilować dla potrzeb zewnętrznego monitora SNMP. Aby ją wyeksportować, należy w menu **Plik** wskazać polecenie **Eksportuj**, a następnie wybrać polecenie **NetCrunch MIB**. Następnie należy po prostu skompilować tak wyeksportowany plik, łącząc go z bazą danych tej aplikacji na komputerze, która będzie nasłuchiwać alertów SNMP programu NetCrunch – w ten sposób program monitorujący SNMP będzie wiedział w jaki sposób prawidłowo przetwarzać wszystkie przychodzące z programu NetCrunch informacje.

Korzystanie z narzędzi systemu Windows

NetCrunch wyposażony jest w niezależny program narzędziowy o nazwie **WinTools**. WinTools to zestaw przydatnych aplikacji, które umożliwiają zarządzanie dowolnym węzłem działający w oparciu o system, operacyjny Windows (wersja Windows 2000 i nowsze). Umożliwia wykonywanie następujących czynności:

- wyświetlanie podstawowych informacji na temat komputera z zainstalowanym systemem Windows,
- przeglądanie i wyłączanie dowolnych procesów uruchomionych na węźle
- przeglądanie usług systemu Windows na komputerze, a także uruchamianie ich, wyłączanie i wstrzymywanie,
- zarządzanie plikami dziennika systemu Windows: Application, Security i System,
- weryfikowanie zasobów sprzętu na komputerze Windows,

- weryfikowanie zasobów oprogramowania na węźle,
- tworzenie i nawigowanie przestrzeni nazw i klas WMI dostępnych na danym komputerze.

Aby urruchomić program WinTools oraz zawarte w nim narzędzie

1. Z menu **Narzędzia** wybierz pozycję **Narzędzia systemu Windows**. Otworzy się program **WinTools**.
2. W oknie przycisków nawigacji w lewej, dolnej części wybierz narzędzie, którym chcesz się posłużyć.
3. W pasku narzędzi wyboru węzła wybierz adres IP lub nazwę użytkownika węzła Windows.
4. Kliknij **Połącz**.

Przeglądanie sieci

Po otwarciu okna **Ruch monitorowania** program umożliwia oglądanie statystyk generowanego przez siebie ruchu w dowolnej monitorowanej sieci. Aby uzyskać taką możliwość należy z menu **Widok** wybrać polecenie **Statystyka monitorowania**. W oknie tym można dodatkowo, dla danej sieci, określać górne limity jej obciążania przez ruch monitorujący, których program podczas monitorowania nie powinien przekraczać. Można to również zrobić podczas określania właściwości mapy sieci należącej do sekcji *Sieci IP*.

Wyszukiwanie węzła

Gdy wyświetlana mapa zawiera dużą liczbę węzłów, znalezienie określonego węzła może okazać się trudne. Jeszcze trudniejszym zadaniem może być zlokalizowanie węzła na mapie topologii fizycznej. Aby w obu powyższych przypadkach ułatwić użytkownikowi szybkie dotarcie do określonego węzła, program udostępnia okno **Znajdź węzeł**. Umożliwia ono ponadto wyświetlenie listy wszystkich map, na których występuje dany węzeł, a także przeglądanie wyników wyszukiwania w oddzielnym oknie.

Aby znaleźć węzeł na aktualnie wyświetlanej mapie

1. Naciśnij klawisze **Ctrl+F** lub z menu **Edycja** wybierz polecenie **Znajdź**. Spowoduje to wyświetlenie okna **Znajdź węzeł**.
2. Kliknij kartę **Znajdź** znajdującą się w górnej części okna.
3. W polu **Nazwa lub adres IP węzła** wpisz ciąg znaków do wyszukania (wchodzących w skład nazwy lub adresu IP węzła).

W wyniku tego na mapie aktualnie wyświetlanej w oknie **Widok sieci** zaznaczone zostaną te węzły, które spełniają tak określone kryteria wyszukiwania.

Uwagi

- *W punkcie 3 można we wpisywanym ciągu znaków wprowadzić dowolną ilość symboli wieloznacznych *, co przyczyni się do rozszerzenia listy wyników wyszukiwania.*
- *Jeżeli wyszukiwanie nie przyniesie rezultatu (nie zostaną znalezione żadne węzły pasujące do zadanych kryteriów), program wyświetli niewielkie okno dialogowe informujące o takiej sytuacji.*
- *Jeżeli nie została zaznaczona opcja **Zaznacz wszystkie węzły spełniające kryteria**, to wówczas na aktualnie wyświetlanej mapie odnaleziony zostanie tylko pierwszy węzeł spełniający dane kryteria wyszukiwania. Aby znaleźć na tej mapie kolejny węzeł spełniający dane kryteria, należy nacisnąć klawisz **F3** lub z menu **Edycja** wybrać polecenie **Znajdź następny**.*

Aby znaleźć węzeł na dowolnej mapie atlasu

1. Naciśnij klawisze **Ctrl+F** lub z menu **Edycja** wybierz polecenie **Znajdź**. Spowoduje to wyświetlenie okna **Znajdź węzeł**.
2. Kliknij w górnej części okna kartę **Znajdź na mapach**.

3. W polu **Nazwa lub adres IP** wpisz ciąg znaków do wyszukania (wchodzących w skład nazwy lub adresu IP węzła).
4. W obszarze wyświetlanego okna zatytułowanym **Gdzie** zaznacz odpowiednie pola wyboru przy sekcjach lub mapach, które powinny zostać objęte wyszukiwaniem.
5. Jeśli chcesz, aby program wyświetlił wyniki wyszukiwania w oddzielnym oknie, możesz w obszarze **Dane wyjściowe** zaznaczyć pole wyboru **Wyświetl wyniki w oddzielnym oknie**.

Jeżeli wybrana została opcja wyświetlania wyników wyszukiwania w oddzielnym oknie, a program znajdzie co najmniej jeden węzeł spełniający dane kryteria, wówczas wyświetlone zostanie okno **Wyniki wyszukiwania**. Wszystkie nazwy map, na których zlokalizowany został wybrany węzeł (węzeł spełniający określone kryteria wyszukiwania), będą wyświetlone kolorem czarnym. Natomiast nazwy map, na których poszukiwany węzeł nie występuje, będą wyszarzone).

Uwagi

- *W punkcie 3 można we wpisywanym ciągu znaków wprowadzić dowolną ilość symboli wieloznacznych *, co przyczyni się do rozszerzenia listy wyników wyszukiwania.*
- *Jeśli wyszukiwanie nie przyniesie rezultatu, wyświetlone zostanie niewielkie okno dialogowe informujące o tej sytuacji.*
- *Jeżeli w punkcie 5 nie zostało zaznaczone pole wyboru **Wyświetl wyniki w oddzielnym oknie**, wówczas odnaleziony zostanie tylko pierwszy węzeł należący do pewnej mapy i spełniający zadane kryteria wyszukiwania (mapa, na której występuje znaleziony w ten sposób węzeł, zostanie automatycznie wyświetlona w oknie **Widok sieci**, a węzeł spełniający zadane kryteria wyszukiwania zostanie na niej wyróżniony). Aby znaleźć w atlasie kolejny węzeł spełniający zadane kryteria, należy nacisnąć klawisz **F3** lub z menu **Edycja** wybrać polecenie **Znajdź następny**.*

Określanie stanu węzła

Określenie aktualnego stanu węzła przedstawionego na dowolnym widoku to jedna z najprostszych, a zarazem najważniejszych czynności w programie. Aby to umożliwić, program wykorzystuje różne kolory do oznaczania aktualnego stanu monitorowania danego węzła (widoki **Mapa** i **Szczegóły**) lub aktualny stan połączenia z tym węzłem (widoki Windows NT, NetWare i SNMP).

Widok mapy graficznej

Domyślnie ikony węzłów na mapie wyświetlane są w różnych kolorach, z których każdy oznacza inny stan węzła. Pozwala to szybko określić aktualny stan węzła na dowolnej mapie należącej do określonej grupy w drzewie **Atlas sieci**. Jeżeli w programie wybrana została karta **Mapa**, stan każdego z węzłów może być wyrażony za pomocą następujących kolorów (przedstawione poniżej ikony zostały wybrane jednie jako przykład – ikony symbolizujące inne rodzaje węzłów mogą również zmieniać kolory zgodnie z opisanymi poniżej zasadami):

Normalny – ***OK*** – węzeł odpowiada na monitorowanie, co oznacza, że w danym momencie działa poprawnie. Wszystkie monitorowane w nim usługi również

odpowiadają poprawnie.

Żółty – ***OSTRZEŻENIE*** – sygnalizuje stan ostrzegawczy. Niektóre monitorowane usługi sieciowe w danym węźle nie odpowiadają prawidłowo, pomimo że sam węzeł działa poprawnie. Zwykle naprowadzenie kursora myszy na węzeł oznaczony kolorem żółtym powoduje wyświetlenie nazw nieodpowiadających usług sieciowych.

Czerwony – ***NIE ODPOWIADA*** – węzeł nie działa i w ogóle nie odpowiada. Żadna usługa sieciowa w tym węźle nie odpowiada.

Szary – ***NIEZNANY*** – monitorowanie węzła zostało wyłączone. A zatem jego aktualny stan nie jest znany – zarówno możliwe jest, że węzeł działa, jaki i to, że niektóre z jego usług są niedostępne, albo że węzeł i wszystkie usługi nie działają. Jeśli program został właśnie uruchomiony lub zupełnie nowy węzeł został właśnie dodany do mapy, węzły mogą przejściowo znajdować się w stanie NIEZNANY – aż do chwili sprawdzenia ich stanu przez program. Dzieje się tak dlatego, że w danej sytuacji program jeszcze nie odpytał takich węzłów z informacji o ich stanie. Gdy to już zrobi, ikony takich węzłów zmienią kolor na odpowiadający jednemu z trzech pozostałych stanów – OK, OSTRZEŻENIE lub NIE ODPOWIADA.

Oprócz stosowania różnych kolorów wyświetlania, ikony poszczególnych węzłów mogą również przez chwilę migotać, zwracając uwagę na zmianę stanu danego węzła.

Dodatkowe znaki na ikonie

Trwa wykrywanie węzła. Na ikonie węzła znajduje się niewielka lupa umieszczona w jej prawym dolnym rogu (tak jak to zostało pokazane na przykładowej ikonie). Zwykle węzeł pozostaje w tym stanie przez klika sekund.

Urządzenie zarządzane za pomocą agenta SNMP. W prawym górnym rogu ikony urządzenia zarządzanego za pomocą agenta SNMP umieszczona jest mała żółta gwiazdka (uzależniona od rodzaju węzła, który ikona ta reprezentuje). Ikona ta wskazuje, że program będzie mógł odczytywać i ustawiać parametry tego węzła za pomocą agenta SNMP (pod warunkiem, że została określona prawidłowa wspólnota).

Niepotwierdzone rzyjęte alerty. Jeśli z danym węzłem na mapie związane są jakiekolwiek alerty, które nie zostały przyjęte, do ikony reprezentującej taki węzeł przyczepiony będzie w prawym dolnym rogu niewielki dzwonek. Dzwonek ten zniknie, gdy dla danego węzła status wszystkich nowo wygenerowanych zdarzeń zostanie przez użytkownika zmieniony na inny niż *nowy* lub gdy wszystkie takie zdarzenia zostaną z tego węzła usunięte.

Wyłączony przez przedział czasowy. Sytuacja ta ma miejsce wówczas, gdy dla danego węzła użytkownik określił w których godzinach w ciągu dnia i/lub w które dni tygodnia ma on być (lub nie być) monitorowany. W takim przypadku, gdy nadejdzie odpowiednia chwila, ikona węzła zmieni kolor na szary, a w jej prawym dolnym rogu pojawi się niewielki zegar informujący, że monitorowanie tego węzła jest w danej chwili wyłączone.

Wyłączony przez współzależność. Gdy określony węzeł jest zdefiniowany jako zależny od innego węzła, a ten ostatni w danym momencie nie odpowiada, taki węzeł zależny zostanie również wyłączony. Jego ikona zmieni kolor na czerwony, a w prawym dolnym rogu ikony pojawi się obraz wyłączonej wtyczki, wskazujący, że dany węzeł został wyłączony na skutek występujących zależności sieciowych.

Stan nieznany. Gdy z listy usług sieciowych monitorowanych w danym węźle usunięte zostaną wszystkie usługi, ikona zmieni stan na NIEZNANY, a jej kolor zmieni się na szary. Dodatkowo w prawym dolny rogu takiej ikony pojawi się niewielki znak zapytania, informujący, że w danym węźle nie są monitorowane żadne usługi sieciowe.

Węzeł z NetCrunchem. Węzeł, na którym uruchomione jest oprogramowanie NetCrunch, oznaczony jest ikoną opatrzoną napisem „NC" umieszczonym w lewym górnym rogu. Ikona ta nie może być usunięta z atlasu; wszystkie inne węzły są niezmiennie zależne od węzła z NetCrunchem. Co więcej, przy tworzeniu pustego atlasu węzeł, na którym jest uruchomiony NetCrunch zostanie do niego automatycznie dodany. W momencie przenoszenia atlasu na inny komputer, węzeł z NetCrunchem zostanie automatycznie uaktualniony, aby odzwierciedlić dokonaną zmianę.

Uwaga

W programie istnieje również możliwość zmiany sposobu sygnalizacji aktualnego stanu węzła – zamiast stosowania domyślnej metody oznaczania ikon odpowiednimi kolorami, można wprowadzić odpowiednie tło za ikoną lub otaczać ikonę kolorową ramką. Przy wyborze którejkolwiek z tych alternatywnych opcji możliwa jest także zmiana kolorów służących do oznaczania stanu węzła (domyślnie kolor szary oznacza stan NIEZNANY, kolor żółty – OSTREŻENIE, a czerwony to stan NIE ODPOWIADA). Modyfikowanie powyższych opcji zostało szerzej opisane w sekcji Sygnalizacja stanu węzła *na stronie 213.*

Widok szczegółowy

Jeśli w oknie **Widok sieci** została wybrana karta **Szczegóły**, to w położonej najbardziej na lewo kolumnie tabeli wyświetlanej na tej karcie do oznaczania stanu węzła stosowane są następujące kolory (na tym widoku nie są wykorzystywane ikony, które odzwierciedlałyby odpowiedni stan węzła):

Zielony – ***OK*** – węzeł w danym momencie odpowiada na monitorowanie i działa poprawnie. Oznacza to, że jego wszystkie monitorowane usługi sieciowe odpowiadają.

Żółty – ***OSTRZEŻENIE*** – stan sygnalizujący, że niektóre usługi sieciowe w węźle nie odpowiadają poprawnie. Jednakże niektóre inne usługi sieciowe w tym węźle nadal odpowiadają na monitorowanie.

Czerwony – ***NIE ODPOWIADA*** – węzeł nie działa prawidłowo i w ogóle nie odpowiada, gdyż żadna z jego usług sieciowych nie odpowiada poprawnie.

Szary – ***NIEZNANY*** – monitorowanie usług sieciowych w węźle zostało wyłączone lub

w danej chwili żadna usługa sieciowa nie została wyznaczona do monitorowania. Węzeł może także znajdować się w tym stanie zanim wyniki monitorowania dotrą do programu.

 **Zegar – *WYŁĄCZONY PRZEZ PRZEDZIAŁ CZASOWY*** – ten symboliczny obrazek wyświetlany jest wówczas, gdy monitorowanie węzła zostało wyłączone w wyniku wprowadzonego przez użytkownika ograniczenia czasu, w którym ma się ono odbywać.

 **Wtyczka – *WYŁĄCZONY PRZEZ WSPÓŁZALEŻNOŚĆ*** – monitorowanie usług w węźle zostało wyłączone, ponieważ inny węzeł, od którego dany węzeł jest zależny, znajduje się w danej chwili w stanie ***NIE ODPOWIADA***.

Uwaga

*Różne stany węzłów wyświetlane w tabelach w widoku **Szczegóły** są dokładnie takie same, jak wyświetlane w widoku **Mapa** (i opisane w poprzednim rozdziale). Oczywiście w widoku **Mapa** ikony zmieniają kolor, by zasygnalizować zmianę stanu węzła, natomiast w widoku **Szczegóły** zmiany takie sygnalizowane są przez wyświetlanie kolorowych wskaźników w lewej skrajnej kolumnie tabeli.*

Widoki Windows NT i NetWare

Do sygnalizowania aktualnego stanu połączenia z monitorem systemu operacyjnego danego węzła wykorzystywane są następujące kolory:

 **Zielony – *UWIERZYTELNIONY*** – nawiązane jest połączenie z węzłem i nastąpiło do niego zalogowanie.

 **Niebieski – *POŁĄCZONY*** – program nawiązał połączenie z węzłem, ale jeszcze nie zalogował się do tego węzła.

 **Czerwony – *BŁĄD*** – program nie może poprawnie połączyć się z węzłem (ponieważ prawdopodobnie została użyta nieprawidłowa nazwa lub hasło logowania). Jednakże węzeł działa poprawnie i odpowiada w oczekiwany sposób.

 **Szary – *NIEZNANY*** – w danej chwili węzeł nie jest dostępny. Program w ogóle nie może nawiązać z nim połączenia. Najprawdopodobniej węzeł taki nie działa.

 **Zegar – *WYŁĄCZONY PRZEZ PRZEDZIAŁ CZASOWY*** – ten symbol wyświetlany jest wówczas, gdy węzeł został wyłączony w wyniku wprowadzonych przez użytkownika ograniczeń czasowych.

 **Wtyczka – *WYŁĄCZONY PRZEZ WSPÓŁZALEŻNOŚĆ*** – węzeł został wyłączony, ponieważ inny węzeł, od którego dany węzeł jest zależny, znajduje się w danej chwili w stanie ***NIE ODPOWIADA***.

Widok SNMP

Do sygnalizowania aktualnego stanu połączenia SNMP z danym węzłem wykorzystywane są następujące kolory:

Zielony – ***UWIERZYTELNIONY*** – w danej chwili ustanowione jest połączenie z węzłem, na którym uruchomiony jest agent SNMP. NetCrunch może więc czytać informacje SNMP przychodzące z takiego węzła, a prawdopodobnie również zapisywać je do tego węzła.

Szary – ***ROZŁĄCZONY*** – NetCrunch nie może uzyskać odpowiedzi SNMP od danego węzła. Program nie może zatem czytać informacji SNMP przychodzących z wybranego węzła, ani zapisywać ich do takiego węzła.

Zegar – ***WYŁĄCZONY PRZEZ PRZEDZIAŁ CZASOWY*** – symbol ten wyświetlany jest wówczas, gdy węzeł został wyłączony w wyniku wprowadzonych przez użytkownika ograniczeń czasowych.

Wtyczka – ***WYŁĄCZONY PRZEZ WSPÓŁZALEŻNOŚĆ*** – węzeł został wyłączony, ponieważ inny węzeł, od którego dany węzeł jest zależny, znajduje się w danej chwili w stanie ***NIE ODPOWIADA***.

Okno stanu węzła

NetCrunch umożliwia szybkie otwarcie okna stanu węzła, służącego do przeglądania szczegółowych informacji o danym węźle i działających w nim usługach. Okno to otwierane jest przez dwukrotne kliknięcie danego węzła lub kliknięcie danego węzła prawym przyciskiem myszy i wybranie z menu podręcznego polecenia **Stan**.

Karty z informacjami o stanie węzła:

Podsumowanie	Na tej karcie wyświetlane są ogólne informacje o stanie węzła, w tym m.in. dotyczące ustawień monitorowania, SNMP oraz systemów Windows i NetWare.
Usługi sieciowe	Na tej karcie wyświetlane są usługi sieciowe aktualnie monitorowane w danym węźle oraz związane z nimi informacje.
Interfejsy	Jeśli węzeł wyposażony jest w jakiekolwiek interfejsy sieciowe, ich aktualny stan jest wyświetlany na tej karcie okna. Karta ta będzie wyświetlana poprawnie jedynie wówczas, gdy w danym węźle jest uruchomiony agent SNMP, a w programie NetCrunch jest włączone monitorowanie z wykorzystaniem agentów SNMP.
Usługi Windows NT	Karta ta jest dostępna jedynie wtedy, gdy w danym węźle jest uruchomiony system Windows (NT/2000/XP). Służy ona do monitorowania usług systemu Windows.

Uwaga

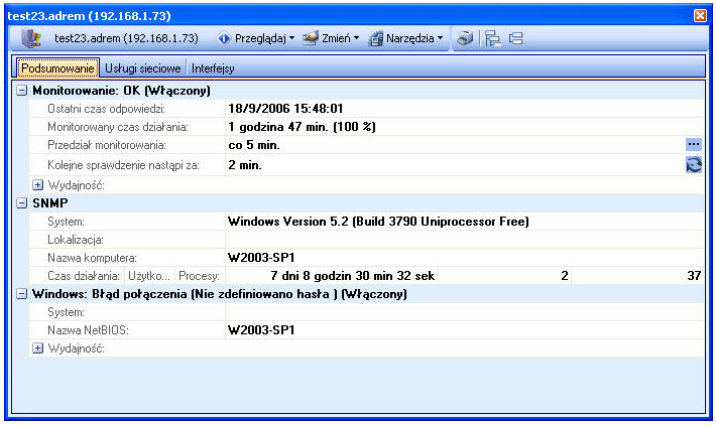
Okno stanu węzła nie daje się otworzyć, gdy na mapie zaznaczony został więcej niż jeden węzeł. W takiej sytuacji można jednak otworzyć kilka okien stanu – każde dla pojedynczego węzła.

Podsumowanie

Po kliknięciu karty **Podsumowanie**, znajdującej się w górnej części okna stanu, wyświetlone zostaną – w dogodnej postaci – ogólne informacje na temat danego węzła.

Sekcje na karcie Podsumowanie:

Monitorowanie	Wyświetla aktualne informacje związane z monitorowaniem węzła, w tym: informację o tym, czy węzeł ten jest sprawny, ostatnią odpowiedź, czas prawidłowego działania, częstotliwość sprawdzania stanu węzła, czas następnego sprawdzenia oraz dane dotyczące wydajności, uzyskane w wyniku monitorowania (średni i maksymalny czas odpowiedzi, procent utraconych pakietów). W sekcji tej może być również wyświetlana lista nieodpowiadających usług, a także podawana liczba nieodpowiadających interfejsów oraz liczba nieprzyjętych alertów (o ile takie w danej chwili istnieją).
SNMP	Wyświetla informacje odczytywane z węzła za pośrednictwem agenta SNMP, takie jak np. pełna nazwa systemu, lokalizacja, nazwa komputera, czas prawidłowego działania, liczba zalogowanych użytkowników oraz procesy aktualnie uruchomione w tym węźle.
Windows NT	Wyświetla informacje związane z systemem Windows, takie jak np. rodzaj systemu, nazwa NetBIOS czy liczniki wydajności systemu Windows.
NetWare	Wyświetla informacje związane z systemem NetWare, takie jak np. wersja systemu operacyjnego czy liczniki wydajności NetWare (liczba aktywnych połączeń, ilość żądań na sekundę oraz procentowe wykorzystanie systemu).



Uwagi

- *Aby rozwinąć informacje zamieszczone we wszystkich sekcjach, należy kliknąć ikonę* **Rozwiń wszystkie**. *Aby ukryć informacje zamieszczone we wszystkich sekcjach, należy kliknąć ikonę* **Zwiń wszystkie**.

- *Jeśli z danym węzłem związane są jakiekolwiek nieprzyjęte alerty, to aby szybko uzyskać o nich więcej informacji, należy kliknąć ikonę* **Zobacz info** *(spowoduje to otwarcie dla danego węzła okna* ***Dziennik zdarzeń****).*

- *Aby dla danego węzła zmienić czas monitorowania, należy kliknąć ikonę* **Wybierz** *(spowoduje to otwarcie okna* ***Monitorowanie*** *z wybraną kartą* ***Ogólne****).*

Stan usług sieciowych

Na karcie **Usługi sieciowe** przedstawione są wszystkie usługi sieciowe aktualnie monitorowane w danym węźle. W górnej części okna znajduje się lista monitorowanych usług, natomiast w jego dolnej części umieszczony jest panel, w którym podawane są szczegółowe informacje o danej usłudze. Lista monitorowanych usług ma postać tabeli, w której zestawione zostały podstawowe parametry poszczególnych usług monitorowanych w danym węźle – ich stan, czas odpowiedzi (RTT, ang. *round-trip time*) oraz procentowy udział pakietów otrzymanych.

Sekcje w panelu szczegółowych informacji o usłudze:

Informacje podstawowe	Wyświetla nazwę zaznaczonej usługi sieciowej, stan jej monitorowania, czas odpowiedzi (RTT) oraz procentowy udział pakietów otrzymanych
Ostatnie odpytanie	Informuje o tym, kiedy miało miejsce ostatnie odpytanie monitorowanego węzła i jaki był jego rezultat
Suma pakietów	Wyświetla całkowitą liczbę pakietów wysłanych do monitorowanego węzła i odebranych z niego
Konfiguracja	Wyświetla parametry związane z danym węzłem – czas monitorowania, timeout i liczbę powtórzeń przy jego odpytywaniu

Uwaga

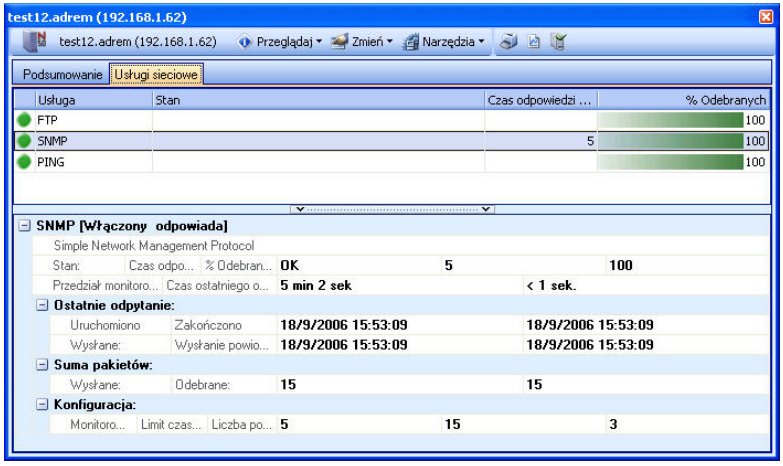
Ponadto w górnej części okna, w lewej skrajnej kolumnie tabeli, za pomocą specjalnych kolorowych znaczników sygnalizowany jest aktualny stan poszczególnych usług sieciowych w danym węźle. Dla potrzeb sygnalizowania bieżącego stanu usług sieciowych w węźle wykorzystywane są następujące kolory:

Kolory sygnalizujące stan usługi sieciowej:

Zielony – ***ODPOWIADA*** – usługa sieciowa odpowiada poprawnie.

Szary – ***NIEZNANY*** – monitorowanie usługi sieciowej zostało wyłączone lub nie dotarły jeszcze żadne wyniki monitorowania.

Czerwony – ***NIE ODPOWIADA*** – usługa sieciowa nie odpowiada lub została wyłączona.



Uwagi

- *Aby szybko sprawdzić stan monitorowanej usługi sieciowej, należy zaznaczyć ją na liście, a następnie kliknąć ikonę* **Sprawdź teraz**.
- *Aby przeglądnąć dane historyczne dotyczące aktualnie zaznaczonej usługi sieciowej, należy kliknąć ikonę* **Historia**, *znajdującą się w górnej części okna. Warto również zapoznać się z rozdziałem* Historia wydajności usługi sieciowej *na stronie 77.*
- *Istnieje również możliwość przeglądania listy monitorowanych usług sieciowych w danym węźle – w tym celu należy otworzyć okno* ***Monitorowanie*** *i wybrać kartę* **Usługi sieciowe**. *Więcej informacji na ten temat zawiera rozdział* Przeglądanie aktualnie monitorowanych usług sieciowych w danym węźle *na stronie 151.*

Historia wydajności usługi sieciowej

W oknie historii określonej usługi sieciowej monitorowanej w danym węźle wyświetlane są trzy wykresy przedstawiające trendy obserwowane podczas działania tej usługi: Czas odpowiedzi, Dostępność oraz Procent utraconych pakietów. Ponadto można zdecydować, dla jakiego okresu czasu mają być przedstawione wyświetlane wyniki – mogą to być na przykład ostatnie 24 godziny albo dowolna liczba dni, tygodni lub miesięcy. Ponadto w górnej części okna można wybrać jedną z następujących czterech kart:

Trendy	Wyświetla na trzech wykresach informacje dotyczące wybranego okresu czasu
Godziny	Wyświetla na trzech wykresach informacje dotyczące okresu jednego dnia
Dni	Wyświetla na trzech wykresach informacje dotyczące okresu jednego tygodnia
Zdarzenia	Wyświetla wszelkie wygenerowane zdarzenia związane z daną usługą sieciową w danym węźle

Interfejsy sieciowe

NetCrunch monitoruje interfejsy sieciowe dla dowolnego węzła zarządzanego za pomocą agenta SNMP. Interfejsy takie zestawione są w przejrzystej tabeli zawierającej następujące informacje:

Stan	Informuje o bieżącym stanie interfejsu. Możliwymi wartościami w tej kolumnie tabeli są: ODPOWIADA (znacznik zielony), NIE ODPOWIADA (znacznik czerwony) lub NIEZNANY (znacznik szary).
Opis	Podaje opisową nazwę interfejsu.
Szybkość	Określa szybkość interfejsu sieciowego.
Adres	Określa adres IP interfejsu, o ile ma on zastosowanie.
Maska sieciowa	Określa maskę sieciową, którą używa dany interfejs.

Uwaga

Informacja o stanie wszystkich interfejsów węzła dostępna jest również w widoku ***Szczegóły*** *związanym z daną mapą, a ściślej – w kolumnie* Interfejsy. *O wiele więcej informacji o interfejsach wyświetla okno* ***Widok SNMP****. Aby je otworzyć, należy w menu podręcznym węzła wskazać pozycję* ***SNMP****, a następnie wybrać polecenie* ***Przeglądaj****.*

Usługi Windows NT

Program umożliwia nie tylko przeglądanie stanu usług systemu Windows NT w węźle, ale również zarządzanie nimi. W szczególności użytkownik może uruchomić, zatrzymać, uruchomić ponownie lub wstrzymać dowolną związaną z danym węzłem usługę systemu Windows, tak jakby odbywało się to lokalnie – z poziomu tego węzła.

Na karcie **Usługi Windows NT** wyświetlane jest zestawienie wszystkich usług systemu Windows dostępnych w danym węźle.

Kolumny tabeli usług:

Stan	Określa aktualny stan usługi systemu Windows (uruchomiona czy zatrzymana).
Nazwa	Podaje nazwę usługi systemu Windows.
Rodzaj uruchomienia	Informuje, w jaki sposób (automatycznie czy ręcznie) uruchomiona została dana usługa systemu Windows po uruchomieniu danego węzła.
Uruchom jako	Określa jak uruchamiana jest dana usługa systemu Windows, np. zy na systemie lokalnym, czy nie.
Plik obrazu	Podaje ścieżkę i nazwę pliku z daną usługą systemu Windows na dysku lokalnym węzła.
Opis	Podaje zwięzły opis danej usługi systemu Windows.

Uwagi

- *Jeżeli karta **Usługi Windows NT** nie jest widoczna w oknie stanu węzła, oznacza to, że węzeł nie jest urządzeniem Windows, lub użytkownik programu nie podał odpowiednich uprawnień do zalogowania się do niego, lub pole wyboru **Monitoruj usługi Windows NT** w karcie **Wydajność Windows** okna **Monitorowanie** dla węzła jest odznaczone.*
- 
W celu dodania lub usunięcia kolumn tabeli należy kliknąć ikonę **Dostosuj kolumny**. *Wówczas wyświetli się okno **Dostosuj**, w którym można przeciągnąć wybrane kolumny z lub do tabeli.*
- *Za pomocą ikon znajdujących się w górnej części okna można także uruchamiać, zatrzymywać, uruchamiać ponownie lub wstrzymywać dowolną aktualnie zaznaczoną w tabeli usługę systemu*
- *Windows NT.*

Korzystanie z dziennika zdarzeń

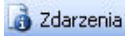
Do zapamiętywania zdarzeń w programie NetCrunch służy dziennik zdarzeń, będący bazą danych SQL. Zdarzenie przedstawione jest w nim za pomocą określonej liczby wstępnie zdefiniowanych kolumn oraz dowolnej ilości parametrów dodatkowych. Dziennik zdarzeń służy również do analizy przebiegu akcji alertujących wywołanych przez dane zdarzenie.

Możliwość otwierania dowolnej ilości okien dziennika zdarzeń pozwala na wygodne zarządzanie zdarzeniami w programie NetCrunch. W każdym takim oknie można w prosty sposób określić, które kolumny mają być wyświetlane oraz jak ma być sortowana lista zdarzeń.

Ponieważ program jest wykorzystywany do alertowania w dłuższym horyzoncie czasowym, baza danych dziennika zdarzeń może w praktyce zawierać informacje o tysiącach zdarzeń. Aby ułatwić ich przeglądanie program udostępnia okno **Dziennik zdarzeń**, które umożliwia tworzenie zapytań dotyczących zdarzeń zapamiętanych w bazie przy wykorzystaniu do tego celu widoków predefiniowanych. W szczególności użytkownik może tworzyć widoki własne. Dla takiego widoku można ponadto określić zakres wyświetlanego obiektu – poprzez wybranie atlasu, mapy lub węzła. Program umożliwia także określenie zakresu czasowego związanego z danym zapytaniem.

Gdy w danym węźle wystąpi jakieś zdarzenie, które jest monitorowane, program NetCrunch zapisze je w dzienniku zdarzeń jako nowe zdarzenie (wyświetlane na liście zdarzeń pogrubioną czcionką). Można wówczas zmienić jego status i np. zaliczyć je do zdarzeń przyjętych lub przypisać to zdarzenie określonej osobie w celu jego zamknięcia.

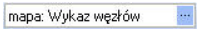
Okno dziennika zdarzeń



Aby otworzyć okno **Dziennik zdarzeń**, należy albo kliknąć prawym przyciskiem myszy określony węzeł, wskazać w menu podręcznym pozycję **Alerty**, a następnie wybrać polecenie **Przeglądaj** – albo od razu kliknąć ikonę ***Zdarzenia*** na głównym pasku narzędzi.
W pierwszym przypadku wyświetlone zostaną tylko zdarzenia wygenerowane dla danego węzła. W drugim przypadku w oknie pokazane zostaną zdarzenia dla wszystkich węzłów, a użytkownik będzie mógł wówczas odpowiednio zmienić zakres zapytania.

Pasek narzędzi dziennika zdarzeń

Oprócz udostępniania typowych funkcji związanych z zarządzaniem zdarzeniami, pasek narzędzi dziennika zdarzeń umożliwia również wybór rodzaju wyświetlanych obiektów, rodzaju prezentowanego widoku oraz jego zakresu czasowego. W tabeli zamieszczonej poniżej omówione zostały poszczególne elementy paska narzędzi, służące do wykonywania wyżej wymienionych czynności:

	Służy do określenia zakresu wyświetlanych obiektów poprzez umożliwienie wyboru określonej mapy, grupy lub pojedynczego węzła, w których wygenerowane zostały zdarzenia. Aby zawęzić zakres wyświetlanych danych, należy skorzystać z ikony ***Wybierz zakres danych***.
	Pole to informuje o aktualnie wybranym rodzaju widoku, a także umożliwia utworzenie lub wybranie innego rodzaju widoku. Aby wybrać istniejący widok, należy skorzystać z ikony ***Wybierz widok***. Natomiast do tworzenia lub edytowania widoków własnych użytkownika służy ikona ***Edytuj widok*** (można przy tym określić własne filtry, aby zawęzić listę zdarzeń).
	Pole to pokazuje aktualnie wybrany przedział czasu, stanowiący kryterium zawężania liczby wyświetlanych zdarzeń. Aby określić zakres czasowy wyświetlanych zdarzeń (ostatnie 24 godziny, dzień, tydzień lub miesiąc), należy skorzystać z ikony ***Zakres czasu***. Aby zmienić dany zakres czasowy na poprzedni lub następny w kolejności (tzn. na poprzedni lub następny dzień, tydzień lub miesiąc), należy skorzystać, odpowiednio, z ikony ***Wstecz*** lub ***Dalej***.

W tabeli poniżej przedstawione zostały pozostałe ikony dostępne na tym pasku narzędzi:

	**Eksportuj**	Eksportuje aktualnie wyświetlaną tabelę z listą zdarzeń do pliku (w formacie tekstowym rozdzielanym przecinkami, HTML, XML lub MS Excel).
	**Drukuj**	Drukuje aktualnie wyświetlaną tabelę z listą zdarzeń.
	**Synchronizuj z atlasem sieci**	Synchronizuje zawartość dziennika zdarzeń z tym, co wyświetlane jest w oknie **Atlas sieci** (to znaczy, jeżeli w oknie **Atlas sieci** została wybrana określona mapa, w tabeli **Dziennik zdarzeń** wyświetlane będą wyłącznie zdarzenia związane z węzłami należącymi do tej mapy).
	**Odśwież**	Odświeża wyświetlaną tabelę z listą zdarzeń.
	**Pokaż panel podglądu**	Ukrywa lub pokazuje panel podglądu zawierający szczegółowe informacje o alercie związanym ze zdarzeniem, które zostało zaznaczone w tabeli.

	**Zmień status zdarzenia**	Zmienia status wybranego zdarzenia (możliwe stany to: *Przyjęty, Przekazany działowi pomocy technicznej, Przekazany ekspertowi w danej dziedzinie, Wymaga regularnego serwisowania, Przekazany grupie zewnętrznej* lub *Zamknięty*).
	**Przypisz zdarzenie do**	Przypisuje zdarzenie określonemu użytkownikowi.
	**Automatyczna szerokość kolumn**	Zaznaczenie tej ikony powoduje użycie przez program automatycznej szerokości kolumn w tabeli z listą zdarzeń.
	**Usuń**	Usuwa wybrane zdarzenie z bazy danych.

Pola związane ze zdarzeniami

Na liście zdarzeń może zostać przedstawione dowolne zestawienie zdarzeń zapisanych w bazie danych. Każde takie zdarzenie opisane jest za pomocą kilku wstępnie zdefiniowanych pól, wymienionych w poniższej tabeli według hierarchii ich ważności:

Czas wystąpienia	Data i czas wystąpienia zdarzenia wywołującego alert (dokładna data, godzina, minuta i sekunda). Należy pamiętać o tym, że zdarzenie mogło zostać zapisane w dzienniku zdarzeń z pewnym opóźnieniem.
Ranga	Stopień ważności zdarzenia, zgodnie z tym, który został podany podczas definiowania danego zdarzenia (ranga zdarzenia może przyjąć takie wartości jak KRYTYCZNA, OSTRZEŻENIE, INFORMACYJNA lub NIEISTOTNA). Więcej informacji na ten temat zawiera rozdział *Definiowanie nowych zdarzeń* na stronie 34.
Stan urządzenia	Pole to informuje, czy wystąpienie danego zdarzenia spowodowało przejście węzła, w którym miało ono miejsce, względnie zasobów zainstalowanych w tym węźle, do stanu sprawności, czy też nie.
Rodzaj	Nazwa opisująca rodzaj zdarzenia, zgodnie z określeniem, które zostało podane w polu **Opis** podczas definiowania danego zdarzenia.
Nazwa urządzenia	Nazwa urządzenia, w którym nastąpiło zdarzenie.
Adres urządzenia	Adres IP urządzenia, w którym nastąpiło zdarzenie.
Status zdarzenia	Aktualny status zdarzenia. Stan taki może przybierać następujące wartości – tuż po wystąpieniu zdarzenia określane jest ono jako *Nowy*, jednak później, podczas korzystania z okna **Dziennik zdarzeń**, jego stan może zostać zmieniony i na przykład może ono przybrać status *Przyjęty* lub *Zamknięty*.

Zastosowanie	Nazwa obszaru zastosowania – czyli niejako wyższej kategorii obiektu– do której należy zdarzenie. Jest to ten sam obszar zastosowania, w którym zdefiniowane zostało dane zdarzenie.
Rodzaj zdarzenia	Określa klasę zdarzeń, do której należy dane zdarzenie (np. *Stan węzła* lub *Stan usługi sieciowej*). Pełna lista dostępnych klas zdarzeń w programie zawiera rozdział *Klasy zdarzeń* na stronie 20.
Właściciel	Nazwa użytkownika, któremu zostało przypisane dane zdarzenie. W momencie wystąpienia zdarzenia pole to jest puste, natomiast jest ono zmieniane wyłącznie podczas korzystania z okna **Dziennik zdarzeń**.
Nazwa użytkownika	Nazwa użytkownika, którego akcja spowodowała wystąpienie danego zdarzenia. Zazwyczaj w polu tym zostaje zapisana nazwa tego użytkownika, który jest aktualnie zalogowany do określonego systemu operacyjnego, w którym nastąpiło dane zdarzenie.
Źródło	Nazwa podsystemu, który wygenerował dane zdarzenie w węźle (np. serwer DNS lub serwer sieci WWW).
Info	Opis zdarzenia.
Opis	Krótki tekst opisujący zdarzenie. Jest on określany przez użytkownika podczas definicji danego zdarzenia.
Identyfikator zdarzenia	Numer identyfikacyjny zdarzenia, odróżniający go od innych zdarzeń (pochodzących z aplikacji zewnętrznych). W aktualnej wersji programu, wszystkie zdarzenia wewnętrzne, wygenerowane przez program NetCrunch, mają identyfikator równy 0.
Kategoria	Dodatkowa kategoria, do której należy wygenerowane zdarzenie (np. Inicjalizacja, Sieć lub Pamięć).

Uwaga

Zawartość każdego z powyższych pól może być wyświetlana w osobnej kolumnie na liście zdarzeń. Kolejność wyświetlania kolumn może być dowolnie zmieniana, a niektóre z nich mogą zostać usunięte.

Funkcje dziennika zdarzeń

W oknie **Dziennik zdarzeń** możliwe jest wykonywanie różnego rodzaju operacji. Zasadniczo można je podzielić na trzy kategorie:

Dostosowywanie zapytań o informacje dotyczące zdarzeń, pochodzące z bazy danych SQL	Możliwe jest wykonanie kilku czynności związanych z formułowaniem zapytań o informacje dotyczące zdarzeń. Program pozwala wybrać zakres atlasu, dla którego tworzona ma być lista zdarzeń (określoną mapę lub węzeł). Można również utworzyć i wybrać widoki własne zawierające dane dotyczące zdarzeń. Ponadto można wybrać zakres czasowy, w ramach którego zdarzenia mają być wyświetlane.
Operacje na liście zdarzeń	Za pomocą tych operacji można wybrać kolumny oraz zmienić sposób sortowania lub grupowania. Możliwe jest również eksportowanie lub drukowanie aktualnie wyświetlanych danych zdarzeń.
Operacje na zdarzeniach	Za pomocą tych operacji można zmienić informacje związane z danym zdarzeniem poprzez zmianę jego statusu, przypisanie go jakiemuś użytkownikowi lub jego usunięcie.

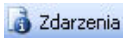
Zapytania o zdarzenia

Program umożliwia tworzenie zapytań o zdarzenia z bazy danych programu w oparciu o trzy różne kryteria:

Zakres atlasu	Program umożliwia tutaj wybór dowolnej pojedynczej mapy (spośród map wyświetlanych w oknie **Atlas sieci**), pod warunkiem, że należy ona do sekcji *Widoki własne* lub *Sieci IP*. Ponadto można wybrać zbiorczą mapę `Wykaz węzłów`, która stanowi listę wszystkich węzłów zdefiniowanych w atlasie. Wreszcie możliwy jest także wybór dowolnego pojedynczego węzła na mapie. Wówczas na liście zdarzeń będą wyświetlane tylko zdarzenia wygenerowane dla tego węzła. Natomiast w przypadku wyboru określonej mapy lista ta będzie zawierać zdarzenia wygenerowane dla dowolnego z węzłów należących do zaznaczonej mapy.
Wybrany widok	Program umożliwia wyświetlanie na liście zdarzeń jedynie tych zdarzeń, które należą do określonego zastosowania lub do dowolnego widoku zdefiniowanego przez użytkownika (widoku własnego).
Zakres czasu	Program umożliwia wybór dokładnego przedziału czasowego, w którym nastąpiły zdarzenia. Na liście zdarzeń zostaną w takim przypadku wyświetlone tylko zdarzenia mieszczące się w tak określonych ramach czasowych. Dostępne zakresy czasu to ostatnie 24 godziny, dowolny dzień, tydzień lub miesiąc.

Wybór zakresu atlasu

Podczas otwierania okna **Dziennik zdarzeń** zakres obiektu (określona mapa lub węzeł), dla którego wyświetlane będą zdarzenia, jest wybierany automatycznie. Kliknięcie ikony



Zdarzenia na głównym pasku narzędzi programu powoduje wybranie domyślnej mapy `Wykaz węzłów`.

Aktualnie wybrany zakres atlasu podany jest w polu **Zakres danych**, znajdującym się na pasku narzędzi dziennika zdarzeń. (Na przestawionej poniżej ilustracji pole **Zakres danych** informuje o tym, że wyświetlane będą zdarzenia dla węzła o nazwie a*lexandra.sf.ca.aacme.com*).

Aby zmienić zakres wyświetlanych zdarzeń

1. Kliknij ikonę ***Zakres danych***, znajdującą się w obszarze **Zakres danych** w lewej skrajnej części paska narzędzi dziennika zdarzeń.
   Spowoduje to wyświetlenie okna dialogowego **Wybierz węzeł lub mapę**.
2. Wybierz mapę lub węzeł, dla których chcesz wyświetlić listę wygenerowanych zdarzeń. Aby wyświetlić zawartość dowolnej grupy lub mapy wyświetlonej w omawianym oknie, kliknij ją dwukrotnie.

Uwagi

- *W oknie **Wybierz węzeł lub mapę**, zamiast określonej mapy lub węzła, można również wybrać folder. Wówczas na wyświetlanej liście zdarzeń pojawią się wszystkie zdarzenia, które wystąpiły w węzłach należących do którejkolwiek z map tego folderu.*
- *Bez względu na to, jaki zakres atlasu został wybrany, lista wyświetlanych zdarzeń zależy również od dwóch dodatkowych czynników – wybranego widoku oraz zadanego zakresu czasu. Więcej informacji na ten temat zawiera rozdział* Wybór widoku *na stronie 86 oraz rozdział* Wybór zakresu czasu *na stronie 87.*

Wybór widoku

Na lewo od pola **Zakres danych** na pasku narzędzi w oknie **Dziennik zdarzeń** znajduje się pole **Widok aktualny**.

Po kliknięciu strzałki skierowanej w dół, znajdującej się obok pola **Widok aktualny**, pojawi się drzewo widoków zdarzeń, z którego można wybrać dowolny zdefiniowany widok. Drzewo widoków zdarzeń podzielone jest na dwie oddzielne sekcje:

Własny	Sekcja ta zawiera wykaz wszystkich widoków własnych utworzonych wcześniej przez użytkownika na podstawie zdefiniowanych kryteriów filtrowania. Więcej informacji na temat tworzenia, modyfikowania i usuwania widoków własnych zawiera rozdział *Zarządzanie widokami własnymi* na stronie 87.
Zastosowania	Sekcja zawiera obszary zastosowań oraz należące do nich rodzajów zdarzeń. Zaznaczenie obszaru zastosowania powoduje wyświetlenie na liście zdarzeń, które należą do określonego obiektu (np. aplikacji) lub związanej z nim wielkości (np. wydajność urządzenia). Jeśli natomiast zostanie zaznaczony określony rodzaj zdarzenia, lista będzie zawierać wyłącznie wygenerowane zdarzenia danego rodzaju.

Wybór zakresu czasu

Program pozwala określić dokładny zakres czasu, dla którego mają być wyświetlane zdarzenia w aktualnie wybranym widoku zdarzeń. Innymi słowy, na liście zdarzeń będą w tym przypadku wyświetlane tylko takie zdarzenia, które wystąpiły w zadanym przedziale czasu. Użytkownik ma do wyboru następujące zakresy:

- ostatnie 24 godziny,
- wybrany dzień,
- wybrany tydzień,
- wybrany miesiąc.

Aktualnie wybrany zakres czasowy zawsze podawany jest w polu **Zakres czasu**, znajdującym się na pasku narzędzi dziennika zdarzeń.

Aby zmienić zakres czasu, należy skorzystać z ikony ***Data*** oraz z odpowiadającej jej ikony oznaczonej skierowaną w dół strzałką, znajdującej się na pasku narzędzi dziennika zdarzeń. Jeżeli wybrany został dzienny, tygodniowy lub miesięczny zakres czasu, możliwe jest także przechodzenie do analogicznego poprzedniego lub następnego w kolejności okresu czasu, przy wykorzystaniu do tego celu ikony – odpowiednio – ***Dalej*** lub ***Wstecz***.

Zarządzanie widokami własnymi

Oprócz możliwości wybrania widoku zdarzeń z sekcji *Zastosowanie* w drzewie widoków zdarzeń, użytkownik ma w tym samym miejscu możliwość wybrania dowolnego utworzonego wcześniej widoku własnego. Widoki te, po ich zdefiniowaniu, wyświetlane są w rozwiniętym drzewie widoków zdarzeń, na odpowiednich pozycjach w sekcji *Własne*.

Procedura tworzenia własnego widoku zdarzeń przewiduje wykonanie kilku czynności. Należy określić dogodną nazwę opisującą dany widok oraz ustalić zestaw kryteriów filtrowania, jaki ma zostać zastosowany podczas kierowania zapytania do bazy danych dziennika zdarzeń. Ostatnim krokiem tej procedury jest wybór kolumn, jakie mają być wyświetlane w tabeli z listą zdarzeń, po wybraniu danego widoku własnego. W przypadku dużej ilości prezentowanych zdarzeń wygodnie będzie pogrupować je według zawartości określonego pola (parametru) opisującego zdarzenie.

Właściwości każdego utworzonego w ten sposób własnego widoku zdarzeń mogą być w późniejszym czasie dowolnie zmieniane. Można na przykład zmienić nazwę takiego widoku lub dowolne z jego kryteriów filtrowania. A ponadto każdy utworzony wcześniej własny widok zdarzeń można w późniejszym czasie usunąć.

Tworzenie widoku własnego

Utworzenie nowego własnego widoku zdarzeń okazuje się przydatne w przypadku, gdy żaden z widoków zdarzeń zamieszczonych w sekcji *Zastosowania* nie spełnia naszych oczekiwań. Na widoku własnym wyświetlane są wszystkie zdarzenia spełniające pewne ściśle określone warunki.

Tworzenie własnych widoków zdarzeń pozwala użytkownikowi na określenie dokładnych kryteriów filtrowania, które mają być wykorzystywane przez program podczas kierowania danego zapytania do bazy danych dziennika zdarzeń. Określanie kryteriów filtrowania jest ułatwione, ponieważ program korzysta z wyrażeń powszechnie używanych w języku polskim. Możliwe jest definiowanie zarówno bardzo prostego rodzaju filtrowania, jak i bardziej rozbudowanego, wykorzystującego wyrażenia złożone. Przykładowo można utworzyć bardzo przydatny własny widok zdarzeń, w którym wyświetlane będą wyłącznie zdarzenia o krytycznym stopniu ważności (czyli w ich polu **Ranga** zapisana jest wartość KRYTYCZNA), które ponadto są zdarzeniami nowymi (czyli w ich polu **Status zdarzenia** zapisana jest wartość NOWY), oraz wystąpiły w dwóch węzłach o określonym adresie IP.

Tworzenie nowych własnych widoków zdarzeń odbywa się w oknie **Nowy widok**. Zostało ono podzielone na cztery oddzielne obszary, z których każdy opisuje osobne zagadnienie związane z definiowaniem takiego widoku:

Nazwa	Nazwa własnego widoku zdarzeń, odróżniająca go od innych widoków znajdujących się na liście widoków własnych lub na rozwiniętym widoku drzewa zdarzeń.
Filtr	W tym obszarze określa się reguły filtrowania, według których program kieruje zapytania do bazy danych dziennika zdarzeń związane z generowaniem własnego widoku zdarzeń. Więcej informacji na ten temat zawiera rozdział *Określanie kryteriów filtrowania* na stronie 89.
Kolumny	W tym obszarze określa się, które kolumny mają być wyświetlane na liście zdarzeń w przypadku, gdy wybrany został własny widok zdarzeń.
Grupuj wg	Obszar ten służy do dodatkowego grupowania zdarzeń wyświetlanych na liście, która pojawia się na własnym widoku zdarzeń, według zawartości jednego z wybranych pól opisujących zdarzenie.

Aby utworzyć własny widok zdarzeń w oknie Dziennik zdarzeń

1. Kliknij na pasku narzędzi ikonę ***Edytuj widoki***.

2. Kliknij ikonę ***Dodaj*** lub kliknij prawym przyciskiem myszy dowolne miejsce na liście w sekcji *Widoki własne*, a następnie z menu podręcznego wybierz polecenie **Dodaj**.
3. W polu **Nazwa** wpisz nazwę nowego widoku własnego.
4. W polu **Filtr** określ pożądane reguły filtrowania. Więcej informacji na ten temat zawiera rozdział *Określanie kryteriów filtrowania* na stronie 89.
5. W polu **Kolumny** wybierz kolumny (odpowiadające polom opisującym zdarzenia), które mają być wyświetlane na liście zdarzeń po zaznaczeniu określonego własnego widoku zdarzeń. W tym celu zaznacz odpowiednie pola wyboru, znajdujące się na lewo od każdej nazwy pola opisującego zdarzenie.
6. Na rozwijanej liście **Grupuj wg** wybierz to pole opisujące zdarzenie, według którego zdarzenia powinny być grupowane na liście wyświetlanej na widoku zdarzeń. Wybranie

takiego pola nie jest konieczne. Domyślnie program nie przeprowadzi grupowania zawartości listy zdarzeń wyświetlanej na własnym widoku zdarzeń.

Uwaga

*Każdy nowo utworzony widok własny będzie zawsze umieszczany na końcu listy widoków własnych (widocznej w oknie **Okno edycji widoków własnych**).*

Określanie kryteriów filtrowania

Określanie kryteriów filtrowania dla nowego własnego widoku zdarzeń lub zmienianie ich w już zdefiniowanym widoku własnym odbywa się w przystępny sposób. Obie te czynności przeprowadza się w polu **Filtr** podczas wyświetlania albo okna **Nowy widok**, albo okna **Edytuj widok**.

We wszelkich kryteriach filtrowania wykorzystywane są jedynie wyrażenia powszechnie używane w języku polskim, a zatem nie jest konieczne wcześniejsze dysponowanie jakąś specjalistyczną wiedzą na temat ich definiowania. Użytkownik ma przy tym możliwość dodawania dowolnej ilości następujących dwóch rodzajów wyrażeń:

Warunek	Wyraża regułę filtrowania; np. `Ranga jest równe Informacyjna`. Na podstawie tego prostego warunku filtrowania program NetCrunch wyszuka w bazie danych dziennika zdarzeń wyłącznie te zdarzenia, które w polu *Ranga* mają zapisaną wartość *Informacyjna*.
Nawias	Jest wykorzystywany do łączenia w grupę dowolnej ilości warunków filtrowania; przykładem takiego nawiasu jest `Zachodzą dowolne z następujących warunków`. Po dodaniu nowego nawiasu zostaje pod nim również dodany nowy warunek filtrowania.

Kliknięcie numeru któregokolwiek wyrażenia (znajdującego się po lewej stronie samego wyrażenia) powoduje wyświetlenie menu podręcznego ze wszystkimi operacjami, które mogą być przeprowadzone na takim wyrażeniu. Należą do nich następujące operacje:

Dodaj warunek	Dodaje pod zaznaczonym wyrażeniem nowy warunek.
Dodaj nawias	Dodaje, bezpośrednio pod zaznaczonym wyrażeniem, nowy nawias wraz z umieszczonymi pod nim nowymi warunkami.
Usuń aktualny wiersz	Usuwa zaznaczone wyrażenie oraz wszelkie inne zdefiniowane pod nim warunki i nawiasy.

W każdym wyrażeniu wyświetlanym w polu **Filtr** (nawiasie lub warunku) pewne jego elementy mogą być zmieniane poprzez kliknięcie określonej części składowej takiego wyrażenia, a następnie wybranie z listy rozwijanej jednego z dostępnych na niej elementów lub, w niektórych przypadkach, przez bezpośrednie wpisanie w to miejsce określonej wartości.

W przypadku nawiasu zmieniać można tylko operator logiczny wyrażenia. Kliknięcie odpowiedniego wyrazu w wyrażeniu stanowiącym nawias powoduje wyświetlenie menu

podręcznego, z którego można wybrać jeden z następujących operatorów: ***wszystkie***, ***dowolne***, ***żadne*** lub ***nie wszystkie***.

Natomiast wyrażenie stanowiące warunek jest zdaniem logicznym składającym się z trzech modyfikowalnych części:

1. **Podmiot** – umożliwia wybór jednej z kolumn opisujących zdarzenie. Kliknięcie pierwszej części wyrażenia stanowiącego warunek powoduje wyświetlenie menu podręcznego, z którego można wybrać żądaną kolumnę opisującą zdarzenie.
2. **Operator** – operator logiczny związany z parametrem i argumentem. Kliknięcie tej części wyrażenia stanowiącego warunek umożliwia wybór jednego z następujących operatorów (dla określonego wyrażenia niektóre z tych operatorów mogą być niedostępne): ***jest równe***, ***jest różne od***, ***zawiera***, ***nie zawiera***, ***jest na liście*** oraz ***nie jest na liście***.
3. **Argument** – argument wyrażenia, odpowiedni do wybranego parametru i operatora. Może nim być wartość lub lista. Zmiana argumentu w wyrażeniu stanowiącym warunek może być przeprowadzona na kilka sposobów, w zależności od rodzaju wybranego parametru oraz operatora.

W przykładowym wyrażeniu `Stan jest równy niesprawny` element *Stan* jest podmiotem, element *jest równy* jest operatorem, a element *niesprawny* jest argumentem tego wyrażenia.

Drukowanie listy zdarzeń

Lista aktualnie wyświetlanych zdarzeń może być drukowana. Przed wydrukowaniem listy zdarzeń można dla niej wybrać dowolny widok zdarzeń, pogrupować zdarzenia w odpowiednich sekcjach, a nawet zmienić układ kolumn.

Aby wydrukować listę zdarzeń wyświetlanych w oknie dziennika zdarzeń

1. Kliknij ikonę **Drukuj**, znajdującą się na pasku narzędzi, lub kliknij prawym przyciskiem myszy dowolne miejsce na liście zdarzeń, a następnie z menu podręcznego wybierz polecenie **Drukuj**.
   Spowoduje to wyświetlenie okna **Podgląd wydruku**.
2. Korzystając z opcji udostępnionych na pasku narzędzi, dostosuj wygląd drukowanej strony odpowiednio do swoich potrzeb.

3. Kliknij ikonę ***Drukuj***.
   Lista zostanie wydrukowana w takiej postaci, w jakiej wyświetlana jest w oknie programu.

Eksportowanie listy zdarzeń

Lista zdarzeń wyświetlana w oknie dziennika zdarzeń może zostać wyeksportowana do pliku w dowolnym z następujących trzech formatów:

- Plik tekstowy rozdzielany przecinkami

- Plik HTML
- Plik XML

Przed ostatecznym wyeksportowaniem danych można oczywiście w oknie podglądu odpowiednio pogrupować zdarzenia lub zmienić zastosowany układ kolumn.

Aby wyeksportować listę zdarzeń z okna dziennika zdarzeń

1. Kliknij ikonę ***Eksportuj*** na pasku narzędzi dziennika zdarzeń lub kliknij prawym przyciskiem myszy dowolne miejsce na liści zdarzeń, a następnie z menu podręcznego wybierz polecenie **Eksportuj**.
   Spowoduje to otwarcie okna **Zapisz jako**.
2. Zmień odpowiednio ścieżkę katalogu, w którym ma zostać zapisany eksportowany plik.
3. Z listy rozwijanej **Zapisz jako typ** wybierz format pliku, w jakim ma zostać zapisana lista zdarzeń (tekstowy rozdzielany przecinkami, HTML lub XML).
4. Kliknij przycisk **Zapisz**.
   Okno **Zapisz jako** zostanie zamknięte, a lista zdarzeń zostanie zapisana w pliku o określonym formacie.

Uwaga

Każda wyeksportowana lista zdarzeń zapisana w pliku HTML lub XML może być następnie oglądana za pomocą standardowej przeglądarki internetowej (przeglądarki WWW).

Zarządzanie zdarzeniami

W oknie **Dziennik zdarzeń** istnieje możliwość wykonywania różnego rodzaju operacji bądź na pojedynczym zdarzeniu, bądź na wielu zaznaczonych zdarzeniach. W szczególności można:

- zmienić status zdarzenia,
- przypisać zdarzenie właścicielowi,
- usunąć zdarzenie,
- przeglądać informacje o alercie.

Uwagi

- *Można skorzystać z funkcji jednoczesnego wyboru wielu elementów i zaznaczyć kilka zdarzeń, a następnie wykonać na nich jedną z powyższych operacji, np. równocześnie usunąć wszystkie zaznaczone zdarzenia lub zmienić ich status. Aby zaznaczyć więcej niż jedno zdarzenie, należy przytrzymać wciśnięty klawisz **Ctrl** i kliknąć każde zdarzenie, na którym ma zostać przeprowadzona dana operacja.*
- *Aby zaznaczyć wszystkie zdarzenia aktualnie wyświetlane na danym widoku, należy kliknąć prawym przyciskiem myszy dowolnym miejsce tabeli, a następnie z menu podręcznego wybrać polecenie **Zaznacz wszystko**.*

Zmiana statusu zdarzenia

W oknie **Dziennik zdarzeń** wykorzystywane jest pojęcie statusu zdarzenia, służące do ścisłego rozróżniania poszczególnych etapów, w jakich może się znaleźć każde wygenerowane w programie zdarzenie. W rzeczywistości status jest jednym z pól bazy danych dziennika zdarzeń, służących do opisu poszczególnych zdarzeń. Początkowo, tuż po wystąpieniu danego zdarzenia i zapisaniu go w bazie danych dziennika zdarzeń, jego statusowi nadawana jest wartość *Nowy*, co oznacza, że zdarzenie to nie zostało jeszcze przyjęte do obsługi. Podczas wyświetlania jakiegokolwiek widoku zdarzeń te zdarzenia, które nadal są nowe (w polu statusu mają zapisaną wartość *Nowy*), zaznaczone są pogrubioną czcionką w celu odróżnienia ich od zdarzeń o innym statusie. Ponadto każdy widok zdarzeń w rozwiniętym drzewie widoków zdarzeń, który zawiera nowe zdarzenia, będzie także wyróżniony pogrubioną czcionką wraz z podaniem ilości takich nowych zdarzeń (będzie ona wyświetlana w nawiasach, na prawo od nazwy danego widoku zdarzeń).

W programie NetCrunch użytkownik może zmienić status dowolnego zdarzenia na jeden z następujących:

Przyjęty	Zgłoszenie zdarzenia zostało przyjęte przez użytkownika.
Przekazany działowi pomocy technicznej	Zdarzenie zostało skierowane do działu obsługi technicznej w celu znalezienia rozwiązania problemu, który wywołał to zdarzenie.
Przekazany ekspertowi w danej dziedzinie	Zdarzenie zostało powierzone odpowiedniemu specjaliście.
Wymaga regularnego serwisowania	Zdarzenie wymaga uruchomienia zadania lub zadań obsługi zgodnie z określonym harmonogramem.
Przekazany grupie zewnętrznej	Zdarzenie zostało przekazane do obsługi grupie zewnętrznej w celu znalezienia rozwiązania problemu.
Zamknięty	Problem, który wywołał zdarzenie, został pomyślnie rozwiązany.

Aktualny status zdarzenia może oczywiście zostać przez użytkownika zmieniony na dowolny inny spośród wymienionych w powyższej tabeli.

Korzystanie z pola opisującego status zdarzenia jest szczególnie przydatne w sytuacji, gdy baza danych dziennika zdarzeń zawiera dużą ilość zdarzeń, przez co ich obsługa jest znacznie utrudniona. Można na przykład tworzyć własne widoki zdarzeń o określonym statusie (np. *Nowy* lub *Przekazany ekspertowi w danej dziedzinie*), a nawet grupować aktualnie wyświetlane zdarzenia w sekcjach odpowiadających statusom tych zdarzeń. Pozwala to na znacznie wygodniejsze zarządzanie bazą danych dziennika zdarzeń.

Aby zmienić status zdarzenia na liście zdarzeń

1. Zaznacz widok zdarzeń za pomocą paska narzędzi dziennika zdarzeń.

2. Kliknij strzałkę skierowaną w dół, znajdującą się obok ikony ***Zmień status zdarzenia***, otwierając w ten sposób odpowiednie menu rozwijane.
   Można też to zrobić w inny sposób – otwierając menu podręczne i wybierając z niego polecenie **Zmień status zdarzenia**.

Uwagi

Jeżeli zdarzenie jest wyświetlone pogrubioną czcionką, oznacza to, że jego status to Nowy. *Bezpośrednie kliknięcie ikony* **Zmień status zdarzenia** *(bez klikania znajdującej się na prawo od niej strzałki skierowanej w dół) automatycznie zmienia status zdarzenia na* Przyjęty.

Przypisywanie zdarzenia użytkownikowi

Zdarzenia, które zostały wygenerowane i zapisane w bazie danych dziennika zdarzeń, mogą być ze względów organizacyjnych przypisywane określonemu użytkownikowi. Służy do tego kolumna *Właściciel*.

Aby przypisać użytkownikowi zdarzenie z listy zdarzeń

1. Wybierz zdarzenie, które chcesz przypisać określonemu użytkownikowi.
2. Kliknij prawym przyciskiem myszy dane zdarzenie, a następnie z menu podręcznego wybierz polecenie **Przypisz zdarzenie do**. Zamiast tego możesz kliknąć ikonę ***Przypisz zdarzenie do***, znajdującą się na pasku narzędzi dziennika zdarzeń.
   Spowoduje to wyświetlenie okna **Wybierz właściciela zdarzenia**.
3. Wybierz nazwę użytkownika z listy lub dodaj nowego użytkownika, korzystając z ikony ***Dodaj***.

Uwagi

- *Jeżeli na liście zdarzeń wyświetlana jest kolumna* Właściciel*, można szybko określić, komu dane zdarzenie zostało przypisane.*
- *Jeżeli w punkcie 3. do listy* ***Właściciel*** *ma być dodany nowy użytkownik, należy w tym celu kliknąć ikonę* **Dodaj**. *Otwarte zostanie wówczas niewielkie okno, w którym należy wpisać nazwę nowego użytkownika i kliknąć przycisk* ***OK***.
- *W punkcie 3. można również zmienić nazwę dowolnego użytkownika na liście, klikając ikonę* **Zmień**..

Korzystanie z raportów

Integralną częścią programu NetCrunch jest funkcja gromadzenia informacji uzyskanych podczas procesu monitorowania, a następnie wykorzystywania ich do tworzenia raportów. Sam proces zbierania niezbędnych danych prowadzony jest przez program w sposób niezależny od tworzenia końcowych, gotowych do przeglądania raportów. W programie, który otrzymuje użytkownik, zostały już wstępnie zdefiniowane najbardziej popularne rodzaje raportów, dzięki czemu nie trzeba tracić czasu na tworzenie ich od podstaw.

Generowanie raportów jest jedną z kluczowych funkcji dostępnych w programie. Jej znaczenie wynika z faktu, że jednym z podstawowych celów realizowanych przez tego rodzaju program do monitorowania sieci jest raportowanie – czyli na przykład wykazywanie, że coś w sieci nie działa poprawnie, lub umożliwianie natychmiastowego dostrzeżenia sygnałów ostrzegawczych, informujących o spadającej wydajności sieci.

Rodzaje raportów

NetCrunch jest wyposażony w zestaw predefiniowanych popularnych raportów. Warto zauważyć, że raporty o powyższej kategorii (określane w programie oraz w niniejszym dokumencie mianem raportów predefiniowanych) nie mogą być modyfikowane ani tworzone przez użytkownika. Aby je generować i przeglądać, należy posłużyć się programem o nazwie **Przeglądarka raportów**. Por. sekcję *Przeglądarka raportów* na stronie 100 w celu uzyskania dodatkowych informacji.

Ponadto NetCrunch oferuje dodatkowy zestaw raportów o nazwie własne raporty trendów (określane tym mianem w programie oraz niniejszym dokumencie w celu odróżnienia od raportów predefiniowanych). Raporty tego rodzaju związane są z dowolnie wybieranym przez użytkowników zestawem wybranych liczników wydajności (systemów NetWare, Windows NT, SNMP, baz MIB-ów SNMP i/lub usług sieciowych). W przeciwieństwie do raportów predefiniowanych, istnieje opcja tworzenia całkowicie od podstaw własnych raportów trendów – w pierwszym rzędzie tworzy się wówczas szablon raportu. Do tworzenia, edycji, usuwania oraz ewentualnie generowania takich raportów służy zawarty w NetCrunchu program Kreator raportów wydajności. Por. sekcję *Kreator raportów wydajności* na stronie 103 w celu uzyskania dodatkowych informacji.

Włączanie raportów

Włączenie raportu jest czynnością niezwykle ważną, gdyż od tego momentu rozpoczyna się w programie zbieranie danych niezbędnych do wygenerowania określonego raportu. Do innych ważnych czynności należy ustalenie harmonogramu raportowania, czyli określenie jak często program będzie automatycznie generował dany raport (codziennie, co tydzień, co miesiąc), oraz wybranie odbiorców, którzy będą go otrzymywać (dotyczy tylko raportów predefiniowanych). Wszystkie te operacje przeprowadzane są w oknie **Konfiguracja raportów**. Podobnie jak w przypadku zdarzeń, raport można włączyć dla pojedynczego węzła, mapy lub dla całego atlasu. Do przeglądania wygenerowanego raportu służy **Kreator**

raportów wydajności lub funkcja dostępu przez WWW (dotyczy tylko raportów predefiniowanych).

Co istotne, program będzie zbierał wyłącznie dane potrzebne do wygenerowania określonego raportu. Jest to znaczące udogodnienie, gdyż dzięki temu, aby wygenerować dany raport, użytkownik nie musi włączać w programie każdego licznika i zdarzenia z osobna.

Przydzielanie raportów

Okno **Konfiguracja raportów** składa się z dwóch paneli. W lewym panelu wyświetlane są wybrane rodzaje raportów dla danego węzła, mapy lub atlasu (mogą być włączone, wyłączone lub znajdować się w stanie domyślnym). Po zaznaczeniu dowolnego raportu w prawym panelu wyświetlone zostają informacje na temat jego generowania. Należą do nich częstotliwość generowania raportu oraz użytkownicy i grupy, do których ma zostać wysłany.

Okno **Konfiguracja raportów** może zostać otwarte dla pojedynczego węzła, mapy lub dla całego atlasu, w zależności od zakresu sieci, którego ma dotyczyć. Przykładowo, włączenie określonego rodzaju raportu dla danej mapy oznacza, że program będzie gromadził niezbędne dane tylko dla węzłów należących do tej mapy. Następnie na ich podstawie może generować odpowiedni raport, zawierający wszystkie informacje pochodzące z węzłów należących do takiej mapy.

Uwagi

- *Aby otworzyć okno **Konfiguracja raportów** dla węzła, należy w menu podręcznym danego węzła wskazać pozycję **Raporty**, a następnie wybrać polecenie **Konfiguruj**.*
- *Aby otworzyć okno **Konfiguracja raportów** dla mapy, należy w menu **Mapa** wskazać pozycję **Raporty**, a następnie wybrać polecenie **Reguły**.*
- *Aby otworzyć okno **Konfiguracja raportów** dla atlasu, należy w menu **Atlas** wskazać pozycję **Raporty**, a następnie wybrać polecenie **Reguły**.*
- *Po otwarciu okna **Konfiguracja raportów** dla mapy lub atlasu będzie ono włączone, jako jedna z kart, do okna właściwości. Pomimo to, w naszym podręczniku będzie ono nazywane oknem **Konfiguracja raportów**.*

Włączanie generowania raportów

Włączenie generowania raportu dla pojedynczego węzła oznacza, że program będzie automatycznie zbierał wszystkie niezbędne dane, które mają być wykorzystywane do wygenerowania takiego raportu. Włączenie generowania raportu dla całego atlasu oznacza, że program będzie automatycznie zbierał wszystkie niezbędne dane, które mają być wykorzystywane do wygenerowania takiego raportu, a które związane są ze wszystkimi węzłami należącymi do tego atlasu.

Aby włączyć generowanie raportów dla węzła, mapy lub atlasu

1. Otwórz okno **Konfiguracja raportów** dla węzła, mapy lub atlasu.
2. Kliknij ikonę ***Dodaj***, znajdującą się na lewo od listy włączonych raportów.
3. Zaznacz wybrany raport i kliknij przycisk **OK**.

4. Wybrany raport zostanie natychmiast włączony (na rozwijanej liście w górnej części prawego panelu zostanie wybrana opcja *Zawsze generuj raport*).

Uwagi

Po wykonaniu czynności opisanych w punkcie 3. można przystąpić bezpośrednio do określenia częstotliwości generowania danego rodzaju raportu oraz jego odbiorców. Więcej informacji na ten temat zawiera rozdział Tworzenie harmonogramów raportów *na stronie 97 oraz w rozdziale* Rozsyłanie raportów *na stronie 98.*

Zarządzanie regułami generowania raportów

Sposób generowania zaznaczonego rodzaju raportu może zostać pozostawiony jako taki, który jest dla danej mapy lub węzła sposobem domyślnym. W takim przypadku program zastosuje ustawienia określone na poziomie wyższym.

Wyjątki

Określony raport może zostać dla danego węzła wyłączony, nawet jeżeli raport ten został włączony dla mapy lub atlasu, do którego należy ten węzeł. W wyniku tego program dla tak wybranego węzła nie będzie zbierał danych związanych z wyłączonym w ten sposób raportem.

Lista raportów

Otwarcie okna **Konfiguracja raportów** powoduje wyświetlenie przydzielonych raportów, pogrupowanych według obszarów ich zastosowania. Aby dodać do listy inne wstępnie zdefiniowane raporty, należy otworzyć okno **Wybierz raport** i w nim dokonać odpowiedniego wyboru.

Aby wybrać rodzaj raportu ze zdefiniowanej listy

1. Otwórz okno Konfiguracja raportów.
2. Kliknij ikonę ***Dodaj***, znajdującą się po lewej stronie okna.
3. Zaznacz wybrany raport.
4. Po zamknięciu okna **Wybierz raport** dany raport pojawi się na liście przydzielonych raportów.

Uwaga

Po dodaniu wybranego rodzaju raportu, czyli po wykonaniu punktu 4., można przystąpić do zmiany stanu jego generowania i określić go jako włączony, wyłączony lub domyślny. Można również ustalić jak często zaznaczony rodzaj raportu ma być generowany oraz do kogo i jak często powinien być wysyłany.

Tworzenie harmonogramów raportów

Po przydzieleniu i włączeniu przez użytkownika określonego rodzaju raportu, NetCrunch rozpoczyna zbieranie danych niezbędnych do jego wygenerowania. Raport taki może następnie zostać wygenerowany na żądanie, tuż przed jego przeglądaniem, lub automatycznie we wstępnie określonych momentach. Samo generowanie raportu, ze względu na dużą ilość

danych do przetworzenia, może okazać się zadaniem dość czasochłonnym, a zatem automatyczne generowanie raportu w tle pozwala użytkownikowi na uzyskanie takiego raportu w bardziej wygodny dla niego sposób. Raporty są bowiem wówczas generowane w nocy, według określonego przez użytkownika harmonogramu – codziennie, co tydzień lub co miesiąc.

Uwagi

- *Gdy użytkownik określi, jak często ma być generowany dany raport (codziennie, co tydzień lub miesiąc), wybrany rodzaj raportu zostanie automatycznie włączony oraz rozpocznie się proces zbierania danych koniecznych do jego wygenerowania.*
- *Jednakże, aby dla danego atlasu mogło nastąpić automatyczne generowanie raportu, spełnione muszą być dwa warunki: program NetCrunch musi być uruchomiony, a sam atlas musi być otwarty. Raporty będą generowane tylko dla aktualnie otwartego atlasu.*

Rozsyłanie raportów

Każdy przydzielony i włączony raport może być wysyłany do dowolnej liczby odbiorców. Aby określić odbiorców, należy skorzystać z tych samych profilów użytkowników i grup, które zostały już wcześniej zdefiniowane w celu alertowania. Odbiorca raportu musi mieć określony aktualny adres e-mail.

Aby dodać odbiorcę lub grupę odbiorców do listy *Wyślij raport do*

1. W oknie **Konfiguracja raportów** kliknij ikonę ***Dodaj***, znajdującą się na lewo od listy.
2. W oknie **Opcje dostarczania** kliknij ikonę ***Wybierz***, a następnie wybierz odbiorcę lub grupę.
3. W obszarze **Wyślij** zaznacz jak często ma być wysyłany wygenerowany raport – codzienne, co tydzień lub miesiąc.

Uwagi

- *Po dodaniu co najmniej jednego odbiorcy raportu, wybrany rodzaj raportu zostanie automatycznie włączony oraz rozpocznie się proces zbierania danych koniecznych do jego wygenerowania.*
- *Więcej informacji na temat definiowania, zmieniania właściwości oraz usuwania użytkowników lub grup zawiera rozdział* Zarządzanie powiadamianiem użytkowników i grup *na stronie 237.*

Dostępne rodzaje raportów

Raporty udostępniane w programie można podzielić na cztery grupy, odpowiadające czterem podstawowym obszarom zastosowania. W tabeli poniżej zostały pokrótce przedstawione wszystkie możliwe rodzaje raportów, które mogą być generowane za pomocą programu.

NAZWA RAPORTU	*OBSZAR ZASTOSOWANIA*	*KRÓTKI OPIS RAPORTU*
Dostępność węzła	Dostępność urządzenia	Informuje o stanie węzła – czy dany węzeł odpowiada, czy nie odpowiada.
Dostępność węzła – procent utraconych pakietów	Dostępność urządzenia	Informuje o procentowym udziale pakietów traconych w danym węźle.
Raport dostępności węzłów mapy	Dostępność urządzenia	Informuje o dziesięciu najbardziej lub najmniej dostępnych węzłach – w rozumieniu sprawności ich odpowiadania.
Dostępność interfejsów	Interfejsy sieciowe	Informuje o dostępności interfejsów sieciowych w węzłach, a także o rejestrowanym w nich ruchu sieciowym (w oparciu o uzyskane informacje SNMP).
Ruch sieciowy na interfejsach	Interfejsy sieciowe	Informuje o całkowitym ruchu sieciowym, na każdym interfejsie węzła.
Raport dostępności usługi na mapie[1]	Usługi sieciowe	Informuje o dziesięciu najbardziej dostępnych lub niedostępnych usługach sieciowych na danej mapie.
Raport dostępności usługi[1]	Usługi sieciowe	Informuje o dostępności usług sieciowych w węźle.
Rzeczywisty czas odpowiedzi usługi[1]	Usługi sieciowe	Porównuje czas odpowiedzi usługi sieciowej i czas odpowiedzi usługi PING w danym węźle.
Czas działania usługi[1]	Usługi sieciowe	Informuje, jak długo dana usługa odpowiadała lub nie odpowiadała; podaje statystykę czasową, czyli rozkład godzin, w których usługa ta odpowiadała.
Wykorzystanie i wydajność dysku	Windows NT Server	Informuje o wykorzystaniu dysku oraz wydajności w węźle Windows.
Podstawowy raport - planowanie wydajności i historia obciążeń	Windows NT Server	Informuje o parametrach pracy systemu Windows w danym węźle.
Analiza wykorzystania pamięci	Windows NT Server	Informuje o wykorzystaniu pamięci w węźle Windows.

NAZWA RAPORTU	*OBSZAR ZASTOSOWANIA*	*KRÓTKI OPIS RAPORTU*
Raport wykorzystania interfejsów sieciowych	Windows NT Server	Informuje o wykorzystaniu interfejsów sieciowych w węźle Windows (na podstawie odczytu wskazań liczników wydajności Windows NT).
Analiza obciążenia procesora	Windows NT Server	Informuje o parametrach pracy procesora w węźle Windows.

[1] - W aktualnej wersji NetCrunch umożliwia tworzenie raportów wyłącznie dla następujących usług sieciowych: DNS, FTP, HTTP, MSSQL, ORACLE, PING, POP3, SMTP oraz SNMP.

Raporty mogą być generowane albo dla mapy, albo dla węzła. W przypadku usług sieciowych mamy trzy rodzaje raportów generowanych dla map i jeden rodzaj raportów generowanych dla węzła. Informacje niezbędne do wygenerowania raportu uzyskiwane są na podstawie zapisów trendów oraz, w niektórych przypadkach, zebranych informacji o zdarzeniach. Z tego względu oprogramowanie NetCrunch powinno być stale uruchomione podczas całego procesu generowania wybranego raportu. Wykresy w poszczególnych raportach przedstawiają następujące zakresy czasu: dzienny z podziałem na godziny, tygodniowy z podziałem na dni lub miesięczny z podziałem na dni.

Przeglądarka raportów

Przeglądarka raportów programu NetCrunch obsługuje wyłącznie raporty predefiniowane. Umożliwia ona oglądanie albo wygenerowanych już wcześniej raportów tego typu, albo raportów generowanych „na żądanie".

Chcąc oglądnąć dany raport w przeglądarce raportów, należy podać trzy podstawowe parametry:

Zakres atlasu	Określa węzły lub mapy, dla których ma być generowany raport. W przypadku każdego z tych obiektów generowany jest całkowicie oddzielny rodzaj raportu.
Żądany raport	Określa raport, który ma być przeglądany. Program wyświetla wyłącznie raporty dostępne dla wybranego obiektu.
Zakres czasu	Określa zakres czasu, dla którego raport ma być przeglądany lub generowany.

Program udostępnia osobne zestawy raportów dla map i węzłów, gdyż niektóre raporty mogą być generowane tylko dla pojedynczych węzłów, a inne tylko dla wielu węzłów. Gdy zachodzi potrzeba tworzenia raportów dla określonej grupy węzłów, należy utworzyć mapę własną zawierającą te właśnie węzły.

Uwaga

Program będzie zbierał dane wyłącznie wówczas, gdy będzie to możliwe. Na przykład, jeżeli użytkownik włączy określony raport dla węzła Windows NT (rozpocznie się generowanie zdarzeń dla

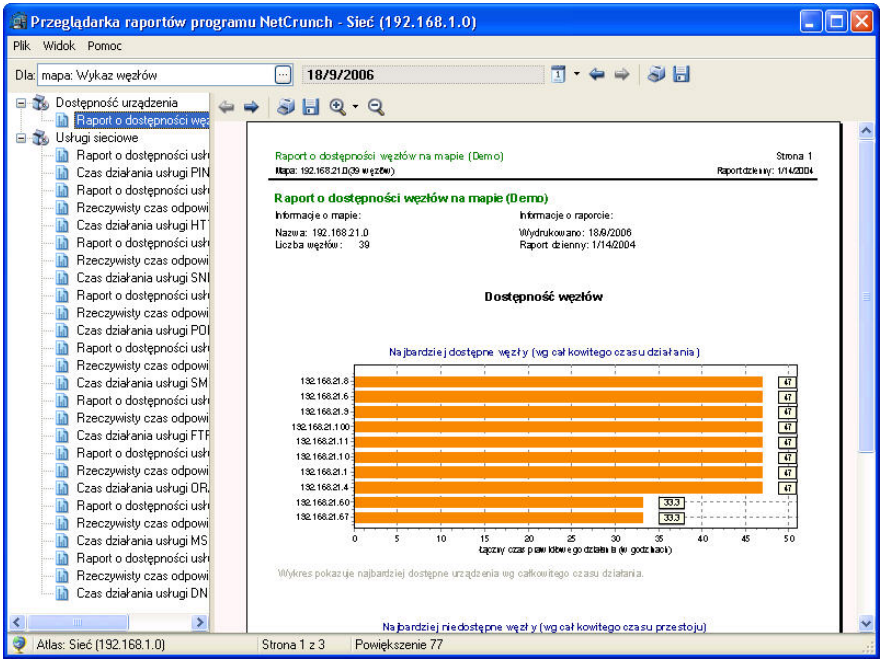
potrzeb tego raportu oraz zbierane będą dane o trendach), a w danej chwili na komputerze w tym węźle jest uruchomiony system NetWare, wówczas właściwe zbieranie danych będzie praktycznie niemożliwe.

Omówienie programu

Przeglądarka raportów to łatwy w użyciu program, stanowiący uzupełnienie podstawowego programu NetCrunch. Umożliwia ona przeprowadzanie prostych operacji związanych z analizą i przeglądaniem raportów wygenerowanych na podstawie danych zebranych przez program NetCrunch.

Sposób korzystania z programu

Okno **Przeglądarka raportów NetCruncha** składa się z drzewa raportów, znajdującego się po lewej stronie, oraz sąsiadującego z nim okna raportów, w którym przedstawiane są wygenerowane wyniki.



Rys. 11 Przeglądarka raportów

Uruchamianie programu

Przeglądarka raportów NetCruncha może być wykorzystywana do generowania nowych raportów jedynie wtedy, gdy równocześnie uruchomiony jest główny program NetCrunch, jako że ten ostatni zawiera pewne procedury, które są niezbędne do uzyskania dostępu do bazy danych NetCruncha. Natomiast przeglądanie już wcześniej wygenerowanych

raportów jest możliwe zawsze, bez względu na to czy w danej chwili sam program NetCrunch działa, czy też nie. Okno **Przeglądarka raportów** można w NetCrunchu otworzyć bezpośrednio za pomocą menu podręcznego danego węzła (przez wskazanie pozycji **Raporty**, a następnie wybranie polecenia **Przeglądaj**), bezpośrednio za pomocą ikony ***Raporty***, znajdującej się na głównym pasku narzędzi, lub przez wybranie z menu **Narzędzia** polecenia **Raporty**.

Aby wygenerować raport

1. Określ zakres danych, jaki ma zostać objęty raportem.
2. W drzewie raportów wybierz rodzaj raportu.
3. Wybierz zakres czasowy raportu.
4. Kliknij przycisk **Generuj**, aby natychmiast wygenerować dany raport.
   Przez krótki okres czasu na ekranie widoczne będzie okno postępu. Gdy generowanie raportu zostanie ukończone, wyświetlona zostanie jego zawartość.

Uwagi

- *Zamiast generować raport na żądanie, można wybrać do przeglądania raport, który został już wygenerowany wcześniej. W tym celu należy kliknąć przycisk* ***Pokaż****.*
- *Jeśli w oknie raportów przycisk* ***Pokaż*** *nie jest widoczny, oznacza to, że dany raport nie został jeszcze wygenerowany.*

Nawigacja na stronach raportu

Informacje zamieszczone w wygenerowanym raporcie mogą obejmować kilka stron. Poruszanie się między poszczególnymi stronami raportu i przechodzenie do strony poprzedniej lub następnej jest bardzo proste – wystarczy w tym celu kliknąć odpowiednią ikonę na pasku narzędzi.

Drukowanie

Każdy raport wygenerowany za pomocą **Przeglądarki raportów NetCruncha** i widoczny w oknie raportów może zostać wydrukowany. Kompletna treść raportu, obejmująca wszystkie jego strony, jest drukowana dokładnie w takiej postaci, w jakiej widoczna jest ona na ekranie. Tuż przed rozpoczęciem drukowania wyświetlone zostaje standardowe okno dialogowe **Ustawienia wydruku**, umożliwiające wybór drukarki oraz związanych z nią właściwości.

Eksportowanie predefiniowanego raportu

Zamiast drukowania, wygenerowany raport może zostać zapisany w pliku o jednym z następujących formatów:

- Quick Report (rozszerzenie `.QRP`),
- dokument Adobe Acrobat (rozszerzenie `.PDF`),
- arkusz Microsoft Excel (rozszerzenie `.XLS`),
- Rich Text Format (rozszerzenie `.RTF`),
- dokument HTML lub XHTML (rozszerzenie `.HTM`),

- dokument tekstowy (rozszerzenie `.TXT`),
- plik graficzny JPEG (rozszerzenie `.JPG`).

Aby wyeksportować raport

1. Upewnij się, że raport został wcześniej wygenerowany.
2.  Kliknij ikonę ***Eksportuj*** lub z menu **Plik** wybierz polecenie **Eksportuj**.
3. Wpisz nazwę pliku, w którym chcesz zapisać eksportowany raport.
4. Wybierz odpowiedni format pliku, korzystając z listy rozwijanej **Zapisz jako typ**.
5. Kliknij przycisk **Zapisz**, aby wyeksportować raport do pliku o określonym formacie.
6. Spowoduje to otwarcie okna **Eksportuj**, w którym możesz określić wszelkie ustawienia związane z eksportowaniem (liczba opcji dostępnych w tym oknie uzależniona jest od wybranego formatu pliku).
7. Kliknij przycisk **OK**, aby utworzyć plik zawierający treść raportu.

Kreator raportów wydajności

Kreator raportów wydajności służy zarówno do tworzenia nowych własnych szablonów raportów jak i do generowania w oparciu o takie szablony personalizowanych raportów trendów. Definiowanie szablonów raportów polega na formułowaniu definicji wykresów, które mają pojawić się w raporcie oraz ustawianiu różnorakich właściwości tychże wykresów. Korzyścią stosowania szablonów raportów jest fakt, iż bazując na starannie zaplanowanych, uprzednio zapisanych definicjach raportu można łatwo i szybko tworzyć własne raporty trendów wydajności, które obrazują określone dane z wybranych przedziałów czasu.

Sam **Kreator raportów wydajności** działa niezależnie od głównego programu NetCrunch. Jednakże, aby móc generować personalizowane raporty trendów (oparte na utworzonych uprzednio szablonach raportów) należy z reguły włączyć dany raport w NetCrunchu (dla węzła, mapy lub całego atlasu) i przeczekać określoną ilość czasu niezbędną do uzyskania odpowiedniej ilości danych trendów. Por. sekcję *Włączanie raportów* na stronie 95 w celu uzyskania dodatkowych informacji nt. tej procedury.

Uruchamianie programu

Aby uruchomić **Kreatora raportów wydajności**, należy w menu **Narzędzia** NetCruncha wybrać opcję **Raporty**, a następnie opcję **Własne raporty trendów**; alternatywą jest kliknięcie 

ikony ***Raporty*** i wybranie opcji **Własne raporty trendów**. Natomiast, aby włączyć narzędzie **Kreator raportów wydajności** bezpośrednio dla konkretnego węzła, należy w jego podręcznym menu wybrać opcję **Raporty**, a następnie pozycję **Zobacz własne raporty trendów**.

Używanie kreatora raportów

Przy uruchomieniu programu w pierwszej kolejności domyślnie otwiera się okno **Kreator raportów** służące do wykonywania powszechnie stosowanych funkcji. Możliwe jest wykonywanie takich czynności jak:

- **Otwórz raport** – umożliwia przeglądanie uprzednio wygenerowanego i zapisanego personalizowanego raportu trendów.
- **Utwórz raport**– generuje personalizowany raport trendów w oparciu o wybrany uprzednio zdefiniowany szablon raportu.
- **Zarządzaj szablonami raportów** – pozwala na tworzenie od podstaw nowych szablonów raportów lub modyfikowanie szablonów już istniejących programie.

Uwagi

- *Aby pominąć początkowe okno **Kreator raportów** podczas kolejnego uruchomienia programu, należy odznaczyć pole wyboru **Wyświetlaj to okno przy rozpoczęciu pracy** umieszczone na ekranie kreatora.*
- *Aby kreator pokazał się przy następnym uruchomieniu programu, w menu **Widok** zaznacz pozycję **Wyświetlaj kreatora raportów przy starcie**.*

Zarządzanie szablonami raportów

Szablony raportów zawierają wszystkie informacje określające, co ma być wyświetlane w generowanych raportach. Poniższa lista pokazuje elementy definiowane w szablonie raportu:

- **Nazwa** – określa nazwę, pod jaką będzie figurował raport w programie NetCrunch.
- **Pozycja** – definiuje, czy dane raportu (wykresy) mają być pokazywane na każdej stronie w formacie pionowym czy poziomym.
- **Układ** – określa układ graficzny wykresów na każdej stronie raportu.
- **Styl domyślny** – określa domyślny styl wykresu, jaki jest stosowany w danych raporcie.
- **Tytuł** – precyzuje główny tytuł, jaki jest prezentowany na pierwszej stronie raportu; możliwe jest modyfikowanie rodzaju czcionki tytułu, a także jej krój, rozmiar i kolor.
- **Opis** – zawiera krótką charakterystykę danego szablonu raportu.
- **Wykresy** – najważniejszy aspekt szablonów raportów: określa dowolną liczbę wykresów, które mają być prezentowane na raporcie; z reguły wykresy te są dodawane z definicji wykresów predefiniowanych.

Tworzenie szablonu raportu

Szablon raportu można utworzyć albo w pierwszym oknie **Kreatora raportów** otwierającym się przy starcie programu, albo używając bezpośrednio polecenia z menu głównego. W obu wypadkach w programie zostanie wywołane okno z kartami prezentujące wszystkie informacje związane z nowym szablonem raportu. Można w nim dokonywać dowolnych modyfikacji szablonów raportów. Jednakże należy pamiętać o kliknięciu ikony ***Zapisz*** w pasku narzędzi po zakończeniu wprowadzania zmian we właściwościach szablonu raportu.

Aby utworzyć nowy szablon raportu w pierwszym oknie Kreatora raportów

1. W początkowym oknie **Kreatora raportów** wybierz przycisk opcji **Zarządzaj szablonami** raportów, a następnie kliknij **Dalej**.
   Pojawi się ekran **Edytuj lub utwórz nowy szablon raportu**.
2. Wybierz przycisk opcji **Utwórz nowy**.
3. Z rozwijanej listy **Zastosowanie** określ obszar zastosowania nowego szablonu raportu.
4. W polu **Nazwa** wpisz nazwę tworzonego szablonu raportu i kliknij **OK**.
5. Pojawi się pusty szablon raportu w postaci okna z kartami.
6. Z menu **Szablon** wybierz opcję **Właściwości**.
   Otworzy się okno **Właściwości raportu**.
7. Określ właściwości szablonu raportu i kliknij **OK**, aby zamknąć okno **Właściwości raportów**.
8. Następnie dodaj do szablonu raportu wykresy (bądź całkiem nowe bądź wykresy wybrane z zapisanych definicji wykresów). Por. sekcję *Dodawanie wykresu do szablonu raportu* na stronie 108 w celu uzyskania szczegółowych informacji.

9. Kliknij ikonę ***Zapisz*** w pasku narzędzi, aby zapisać właściwości nowego szablonu raportu.

Aby utworzyć nowy szablon raportu przy użyciu polecenia z menu

1. Z menu **Plik** wybierz pozycję **Nowy szablon**.
   Pojawi się okno dialogowe **Nowy szablon raportu**.
2. Z rozwijanej listy **Zastosowanie** wybierz odpowiedni obszar zastosowania tworzonego właśnie szablonu raportu.
3. W polu **Nazwa** wpisz nazwę nowego szablonu raportu i kliknij **OK**.
   Pojawi się pusty szablon raportu w postaci okna z kartami.
4. Z menu **Szablon** wybierz pozycję **Właściwości**.
   Otworzy się okno **Właściwości szablonu raportu**.
5. Określ właściwości szablonu raportu i kliknij **OK.**
   Okno **Właściwości szablonu raportu** zostanie zamknięte.
6. Następnie dodaj do szablonu raportu wykresy (bądź całkiem nowe bądź wykresy wybrane z zapisanych definicji wykresów). Por. sekcję *Dodawanie wykresu do szablonu raportu* na stronie 108 w celu uzyskania szczegółowych informacji.

7. W pasku narzędzi kliknij ikonę ***Zapisz***, aby zapisać właściwości nowego szablonu raportu.

Uwagi

- *Informacje związane z aktualnie widocznym szablonem znajdują się w panelu po lewej stronie (zawiera on właściwości i wykresy uprzednio użyte w szablonie). Informacje wyświetlane w panelu po prawej stronie bezpośrednio odnoszą się do wybranego wykresu należącego do właśnie wyświetlanego szablonu raportu.*



- *Szablon raportu zawsze zawiera w swojej karcie ikonę pokazaną w lewym marginesie niniejszego akapitu, z kolei raport wygenerowany zawiera w swojej karcie ikonę znajdującą się poniżej wspomnianej ikony.*
- *Po utworzeniu nowego szablonu raportu można wygenerować właściwy raport. W tym celu w pasku narzędzi kliknij ikonę* **Utwórz raport**.
- *Aby zamknąć aktualnie wyświetlany szablon raportu, kliknij standardową ikonę systemu Windows* ***Zamknij*** *widoczną w prawym górnym rogu obszaru wyświetlania okna z kartami.*
- *Aby powiększyć lub pomniejszyć zawartość szablonu raportu należy użyć odpowiednich ikony powiększania w pasku narzędzi. Można także posłużyć się rozwijaną listą* ***Powiększenie*** *w tym samym pasku narzędzi, aby sprecyzować rząd powiększania/pomniejszania bądź kliknąć bezpośrednio ikony* **Dopasuj szerokość** *i* **Dopasuj stronę**, *aby dostosować szablon do szerokości lub rozmiaru strony.*


Edytowanie szablonu raportu

Modyfikowanie właściwości szablonu raportu odbywa się podobnie jak w przypadku tworzenia nowego raportu. Można w tym celu albo posłużyć się oknem **Kreator raportów** pojawiającym się przy starcie programu, albo wybrać odpowiednie polecenie z głównego menu.

Aby dokonać edycji szablonu raportu w początkowym oknie Kreatora raportów

1. Na pierwszym ekranie okna **Kreatora raportów** zaznacz przycisk opcji **Zarządzaj szablonami raportów** i kliknij **Dalej**.
   Pojawi się ekran **Edytuj lub utwórz nowy szablon raportu**.
2. Zaznacz pole wyboru **Edytuj istniejące**.
3. Z zamieszczonej poniżej listy wybierz szablon raportu do edycji, a następnie kliknij **OK**.
   Szablon raportu pojawi się w programie w postaci okna z kartami.
4. W menu **Szablon** wybierz pozycję **Właściwości**.
   Otworzy się okno **Właściwości szablonu raportu**.
5. Zmień właściwości związane z aktualnie wyświetlanym szablonem raportu i kliknij **OK**.
6. Następnie albo dodaj do szablonu nowe wykresy albo usuń z niego już istniejące wykresy. Możesz także edytować określone właściwości wykresów.

7. W pasku narzędzi kliknij ikonę ***Zapisz***, aby zapisać zmiany dokonane w otwartym szablonie raportu.

Aby edytować szablon raportu przy użyciu polecenia z menu

1. W menu **Plik** wybierz pozycję **Otwórz szablon**.
   Otworzy się okno **Otwórz szablon**.
2. Z listy szablonów wybierz szablon raportu, który ma zostać zmodyfikowany, a następnie kliknij **OK**.
   Wybrany szablon raportu pojawi się w programie w postaci okna z kartami.
3. W menu **Szablon** wybierz opcję **Właściwości**.
   Otworzy się okno **Właściwości szablonu raportu**.
4. Zmień właściwości opisujące wyświetlany szablon raportu, po czym kliknij **OK**.

5. Następnie albo dodaj nowe wykresy, albo usuń już istniejące wykresy z szablonu raportu. Możesz także dokonać edycji określonych właściwości wykresów.

6. W pasku narzędzi kliknij ikonę ***Zapisz***, aby zapisać zmiany wprowadzone do otwartego szablonu raportu.

Uwagi

- *Jeżeli w punkcie 2 nie pojawi się w liście żaden szablon, oznacza to, że programie nie zawiera żadnych szablonów raportu. W pierwszej kolejności należy utworzyć szablon raportu – dopiero potem będzie możliwe edytowanie jego właściwości.*
- *Aby zamknąć aktualnie wyświetlany szablon raportu, kliknij standardową ikonę* ***Zamknij*** *systemu Windows widoczną w prawym górnym rogu obszaru wyświetlania w oknie z kartami.*

Usuwanie szablonu raportu

Kreator raportów wydajności umożliwia także usuwanie szablonów raportu. Jednakże usunięcie szablonu raportu powoduje także automatyczne usunięcie wszystkich własnych szablonów raportu opartych na usuwanym szablonie.

Aby usunąć szablon raportu

1. W menu **Plik** wybierz pozycję **Otwórz szablon**.
   Wyświetli się okno **Otwórz szablon**.
2. Z wyświetlanej w nim listy szablonów raportów kliknij prawym przyciskiem myszy szablon do usunięcia, a następnie w jego podręcznym menu wybierz polecenie **Usuń**.
   Pojawi się okno dialogowe potwierdzenia.
3. Kliknij **Tak**.
   Wybrany szablon raportu zostanie usunięty z dysku lokalnego wraz z wszystkimi związanymi z nim raportami, które zostały dotychczas wygenerowane.

Uwagi

- *Należy pamiętać, że usunięcie określonego szablonu raportu oznacza, że odpowiedni plik związany z tym szablonem zostanie usunięty z następującego katalogu, w którym został zainstalowany NetCrunch 4.x:* `/Data/NTView/ReportTemplates`.
- *Aby usunąć tylko jeden wygenerowany raport, a nie cały szablon raportu, należy wykonać to odrębną czynność. Por. sekcję* Usuwanie własnego raportu trendów *na stronie 119 w celu uzyskania szczegółowych informacji.*

Zarządzanie wykresami

Wykresy są najważniejszą składową personalizowanych szablonów raportów. Podstawową czynnością przy tworzeniu szablonu raportu jest bowiem wybranie wykresów, które mają tworzyć szablon i prezentować się w wygenerowanym raporcie. **Kreator raportów wydajności** ułatwia tę procedurę udostępniając definicje wykresów. Pozwalają one na wielokrotne stosowanie wykresów o identycznych właściwościach na różnych raportach zamiast tworzenia za każdym razem nowego wykresu. Oczywiście jeśli zachodzi taka potrzeba, możliwe jest również tworzenie nowych wykresów bez zapisywania ich jako definicji w celu ponownego użycia w przyszłości.

Definicje wykresów są zawsze zapisywane w podkatalogu `/NTView/ChartTemplates`, w którym jest instalowany NetCrunch 4.x. Można je zapisać dla określonej kategorii – zostaną one umieszczone w odpowiednim podkatalogu o tej samej nazwie.

Właściwości wykresu można podzielić na opisane poniżej cztery główne obszary:

- **Właściwości wykresu** – obszar ten określa treść i wygląd (krój, rozmiar, styl i kolor czcionki) dodatkowych tekstów widniejących na wykresie, takich jak nagłówek, stopka czy opis osi y; umożliwia również wybór jednego spośród predefiniowanych stylów wykresu. Por. sekcję *Modyfikowanie właściwości wykresów* na stronie 112 w celu uzyskania szczegółowych informacji.
- **Serie danych** – opisuje serie danych licznika wydajności węzła, jakie zostaną wyświetlone na wykresie, a także właściwości takie jak kolor każdej serii szeregu danych i rodzaj wykresu (tzn. wykres kołowy, wykres słupkowy i wskaźnik wychyłowy). Por. sekcję *Modyfikowanie serii danych* na stronie 113 w celu uzyskania szczegółowych informacji.
- **Rodzaj analizy** – określa zakres czasowy (szczegółową datę lub okres) serii danych wybranych liczników. Można również określić rodzaj analizy (trendy, rozkład lub analiza sumaryczna) i ustawić dzienną/godzinną maskę czasową, dzięki której na wykresie zostaną zaprezentowane przykładowo dane jedynie z określonych godzin. Por. sekcję *Modyfikowanie rodzaju analizy* na stronie 114 w celu uzyskania dodatkowych informacji.
- **Układ strony** – określa, czy dane różnych węzłów powinny zostać umieszczone na osobnych pojedynczych wykresach, czy też na jednym wykresie. Ponadto pozwala określać układ wykresów na stronie np. umieszczać odwrócone wykresy lub kilka wykresów na stronie. Por. sekcję *Modyfikowanie układu strony* na stronie 115 w celu uzyskania szczegółowych informacji.

Dodawanie wykresu do szablonu raportu

Możliwe jest umieszczanie dowolnej liczby wykresów w szablonie raportu, który jest aktualnie otwarty w oknie z kartami. Do dodawania wykresów służy okno **Dodaj wykres**. Istnieje możliwość utworzenia nowego wykresu lub dodanie wykresu już istniejącego, tzn. takiego, który został wcześniej ustawiony jako definicja wykresu. W pierwszym wypadku istnieje także opcja zapisu nowo utworzonego wykresu jako definicji, która w przyszłości może wielokrotnie posłużyć do dodawania wykresów do innych szablonów raportów.

Dodawanie nowego wykresu

Aby dodać nowy wykres do szablonu raportu

1. Otwórz szablon raportu, do którego ma zostać dodany wykres.

2. W pasku narzędzi kliknij ikonę ***Nowy wykres*** lub z menu **Szablon** wybierz polecenie **Nowy wykres**.
   Otworzy się okno **Dodaj wykres**.
3. Zaznacz przycisk opcji **Utwórz nowy** i kliknij **Dalej**.
   Otworzy się ekran **Serie danych** w oknie **Dodaj wykres**.
4. Wpisz nazwę opisującą wykres.

5. Wybierz zakres danych wykresu używając ikony ***Dodaj szereg***, a następnie kliknij **Dalej**.

6. Wybierz okres analizy, datę lub przedział czasowy, rodzaj analizy a także maskę dzienną/godzinną i kliknij **Dalej**.
7. Określ nagłówek, stopkę, tytuł osi y (krój czcionki, styl, rozmiar i kolor) oraz rodzaj wykresu, a następnie kliknij **Dalej**.
8. Wybierz odpowiedni przycisk opcji opisujący metodę rozmieszczania danych; dane mogą zostać umieszczone na osobnym wykresie dla każdego węzła bądź na jednym wykresie dla wszystkich węzłów; kliknij **Dalej**.
9. Wybierając odpowiedni przycisk opcji zdecyduj, czy ma zostać użyty domyślny styl szablonu raportu czy też styl własny; kliknij **Dalej**.
10. Zaznacz pole wyboru **Umieść na nowej stronie**, jeśli chcesz, by każdy wykres znajdował się na osobnej stronie.
    W tej sytuacji należy również określić dodatkowe właściwości układu strony.
11. Kliknij **OK**.
    Nowy wykres zostanie dodany do aktualnego szablonu raportu.

Uwagi

- *W punkcie 5 można wybrać więcej niż jeden zestaw serii danych dla określonego lub innego zestawu liczników wydajności.*
- *W punkcie 5 po kliknięciu ikony* **Dodaj szereg** *pojawi się okno* ***Wybierz liczniki****. Należy wybrać w nim rodzaj licznika, węzeł źródłowy, obiekt, rzeczywisty licznik i wystąpienie (w stosownych przypadkach). Należy zwrócić uwagę, że lista liczników wydajności węzła źródłowego jest odczytywana bezpośrednio przy użyciu NetCruncha. Jednakże węzeł źródłowy* ***n i e b ę d z i e*** *używany w celu zbierania danych wydajnościowych raportu (węzeł tego rodzaju jest wybierany później przy okazji włączania własnego raportu trendów w oknie Konfiguracja raportów lub podczas generowania własnego raportu trendów). Węzeł źródłowy jest używany w oknie* ***Wybierz liczniki*** *jedynie w charakterze przykładu, umożliwiając tym samym wybór poprawnego licznika wydajności i wystąpienia.*
- *W punkcie 6 w rozwijanej liście* ***Data*** *zalecane jest wybieranie domyślnej opcji „****Raportuj aktualny okres****”. Oznacza to, że przy generowaniu własnego raportu trendów NetCrunch będzie bazował na uzyskanych danych licznika dla aktualnie wybranego okresu. Wybór pozostałych opcji, czyli „****Wybrany****” oraz „****Raportuj poprzedni okres****”, oznacza, że raport będzie z a w s z e generowany przy użyciu danych licznika dla wybranego w tym miejscu okresu.*
- *Po wykonaniu punktu 10 można dodatkowo zapisać aktualny wykres jako definicję, dzięki czemu będzie można go wielokrotnie używać w innych szablonach raportów. W tym celu kliknij przycisk* ***Zapisz*** *znajdujący się w lewym górnym rogu okna, a następnie w otwartym oknie dialogowym* ***Zapisz definicję wykresu*** *określ kategorię wykresu, do której powinien należeć, oraz jego nazwę.*
- *W celu uzyskania szczegółowych informacji o tym, jakie właściwości wykresu można definiować, por. sekcję* Zmienianie właściwości wykresu *na stronie 112.*
- *Umiejscowienie wykresu w szablonie raportu – zarówno na górze, jak i pod innymi wyszczególnionymi na liście wykresami – może być modyfikowane. Aby zmienić położenie dowolnego wykresu prezentowanego w szablonie raportów, należy z panelu* ***Wykresy*** *przeciągnąć nazwę wykresu na początek listy wykresów lub na pozycję pod nazwami innych wykresów.*
- *Dodawanie wykresów kołowych zostało opisane w sekcji* Dodawanie wykresu kołowego *na stronie 110.*

Dodawanie wykresu z istniejącej definicji

Aby dodać do szablonu raportu wykres, którego definicja już istnieje

1. Otwórz szablon raportu, na którym ma zostać umieszczony dany wykres.
2.  W pasku narzędzi kliknij ikonę ***Nowy wykres*** lub wybierz polecenie **Nowy wykres** z menu **Szablon**.
   Otworzy się okno **Dodaj wykres**.
3. Zaznacz przycisk opcji **Dodaj wykres predefiniowany** i kliknij **Dalej**.
4. Z rozwijanej liście **Kategoria wykresu** wybierz kategorię, do jakiej należy wykres.
5. W rozwijanej liście **Definicja** wybierz predefiniowaną definicję wykresu, którą chcesz dodać do szablonu raportu, a następnie kliknij **Dalej**.
6. Określ sposób rozmieszczania danych zaznaczając odpowiedni przycisk opcji. Dane mogą być prezentowane na osobnym wykresie dla każdego węzła lub na jednym wykresie dla wszystkich węzłów. Kliknij **Dalej**.
7. Zaznaczając odpowiedni przycisk opcji zdecyduj, czy na wykresie ma zostać użyty domyślny styl szablonu raportu, czy też styl własny. Kliknij **Dalej**.
8. Zaznacz pole wyboru **Umieść na nowej stronie**, jeśli chcesz, by każdy wykres był umieszczany na osobnej stronie.
   W takim przypadku określ dodatkowe właściwości układu strony.
9. Kliknij **OK**.
   Predefiniowany wykres zostanie dodany do szablonu raportu uwzględniając opcje określone w punktach 6-8 – pojawi się on w oknie wyświetlania, a jego nazwa będzie wyszczególniana w panelu **Wykresy** po lewej stronie.

Uwagi

- *W punkcie 2 można ewentualnie kliknąć odsyłacz **Dodaj wykres** znajdujący się w panelu **Zadania** po lewej stronie.*
- *Umiejscowienie wykresu w szablonie raportu – zarówno na górze, jak i pod innymi wyszczególnionymi na liście wykresami – może być modyfikowane. Aby zmienić położenie dowolnego wykresu prezentowanego w szablonie raportów, należy z panelu **Wykresy** przeciągnąć nazwę wykresu na początek listy wykresów lub na pozycję pod nazwami innych wykresów.*

Dodawanie wykresu kołowego

Na procedurę definiowania wykresu kołowego i dodawania go do szablonu raportu składa się kilku istotnych czynności, takich jak:

- Wybranie przynajmniej dwóch zestawów serii danych związanych z pokrewnymi (uzupełniającymi się) rodzajami wielkości statystycznych (np. procent wykorzystania pamięci i procent dostępnej pamięci dla węzła), których łączna wartość wynosi 100%.
- Wybranie porównania sumarycznego jako rodzaj analizy – oznacza to, że przy porównaniu statystyk komplementarnych serii danych zostanie użyta suma wartości danych zmierzonych we wskazanym okresie.

- Zdefiniowanie rodzaju wykresu jako „kołowy”.

Aby dodać wykres kołowy do szablonu raportu

1. Otwórz szablon raportu, do którego ma zostać dodany wykres kołowy.
2. W panelu **Zadania** po lewej stronie kliknij odnośnik **Dodaj wykres**.
3. Zaznacz przycisk opcji **Utwórz nowy** i kliknij **Dalej**.
4. Dodaj co najmniej dwa zestawy szeregów danych i kliknij **Dalej**.
5. Z rozwijanej listy **Okres** wybierz zakres czasowy dla wszystkich szeregów danych (dzień, tydzień, miesiąc, kwartał lub rok) oraz odpowiednią datę, do której powinien on się odnosić (domyślne ustawienie ma wartość „Raportuj aktualny okres”).
6. Z rozwijanej listy **Rodzaj analizy** wybierz element **Porównanie sumaryczne** i kliknij **Dalej**.
7. Z rozwijanej listy **Rodzaj wykresu** wybierz element **Wykres kołowy** i kliknij **Dalej**.
8. Określ sposób rozmieszczania danych lub dane (na osobnym wykresie dla każdego węzła lub na pojedynczym wykresie). Kliknij **Dalej**.
9. Wybierz styl wykresu i kliknij **Dalej**.
10. Określ układ strony i kliknij **OK**.
    Wykres w postaci kołowej zostanie dodany do aktualnego szablonu raportu.

Uwagi

- *Data i przedział dat zdefiniowany w kroku 5 będzie stosowany w całości, aby uzyskać część wykresu kołowego. Przykładowo przy wybraniu dnia, dane zebrane w przeciągu całego okresu 24 godzin posłużą do obliczenia fragmentów wykresu kołowego wszystkich statystyk serii danych licznika wydajności.*
- *Po wykonaniu czynności opisanej w punkcie 10 można generować raport w postaci wykresu kołowego zawierającego określone statystyki.*

Usuwanie wykresu z szablonu raportu

Usuwanie wykresu z szablonu raportu odbywa się poprzez wybór stosownego polecenia z menu lub kliknięcie ikony na pasku narzędzi.

Aby usunąć wykres z szablonu raportu

1. Otwórz szablon raportu, z którego chcesz usunąć wykres.
2. W widocznym po lewej stronie panelu **Wykresy** wybierz nazwę wykresu.
3.  W pasku narzędzi kliknij ikonę ***Usuń wykres*****,** ewentualnie z menu **Szablon** wybierz polecenie **Usuń wykres**.
   Pojawi się okno dialogowe z potwierdzeniem.
4. Kliknij **Tak**.
   Wykres zostanie usunięty z otwartego szablonu raportu.

Uwaga

*W punkcie 3 możesz także wybrać odnośnik **Usuń wykres** w panelu **Zadania** znajdującym się po lewej stronie.*

Zmienianie właściwości wykresu

Po otworzeniu określonego szablonu raportów można łatwo modyfikować dowolne właściwości wykresów, które składają się na dany szablon. W tym celu wystarczy wybrać wykres w oknie z zakładkami szablonu raportu i wprowadzić zmiany w panelach po prawej stronie: **Właściwości wykresu**, **Szereg danych**, **Rodzaj analizy** oraz **Układ strony**.

Aby zmienić właściwości wykresu

1. Otwórz szablon raportu.
2. Z listy wykresów w panelu **Wykresy** wybierz określony wykres szablonu raportu.
3. Wprowadź zmiany.

Uwaga

Dodatkowe kwestie związane z modyfikowalnymi właściwościami wykresów zostały opisane w czterech zamieszczonych poniżej sekcjach.

Modyfikowanie właściwości wykresów

Właściwości wykresów są modyfikowane w panelu **Właściwości wykresu** znajdującym się po prawej stronie, gdy w programie otwarty jest szablon raportów w postaci strony z zakładkami. Dla wybranego wykresu możliwe jest modyfikowanie następujących informacji:

Nagłówek	Określa tekst nagłówka oraz jego poziome wyrównanie, krój czcionki, styl, rozmiar i kolor.
Stopka	Określa tekst stopki oraz jego poziome wyrównanie, krój czcionki, styl, rozmiar i kolor.
Opis osi Y	Definiuje tekst, który ma pojawiać się przy osi y wykresu, a także jego krój czcionki, styl, rozmiar i kolor.
Styl wykresu	Określa jeden z predefiniowanych styli wykresów, które są wyszczególnione w pozycji `/NTView/Styles` w podkatalogu, w którym został zainstalowany program NetCrunch 4.x.

Uwagi

- *W polach **Nagłówek** i **Stopka** można wpisać specjalne parametry (**$AnalyzeType**, **$DateRange**, **$DateFrom**, **$DateTo**, **$MonthFrom**, **$MonthTo**, **$DayFrom**, i **$DayTo**) – w tym celu należy prawym przyciskiem myszy kliknąć jedno z tych dwóch pól, a następnie dokonać wyboru w menu podręcznym. Podczas generowania raportów zostaną one automatycznie wypełnione odpowiednimi danymi, które opisują.*
- *Aby modyfikować bardziej szczegółowe właściwości wykresu dla dowolnego wykresu, należy prawym przyciskiem myszy kliknąć na niego w otwartym szablonie raportu i w podręcznym menu wybrać opcję*

***Właściwości wykresu**. Otworzy się okno **Właściwości wykresu**, w którym można modyfikować właściwości wykresu związane z tłem, formatem 3D, osią, ściankami i ogólnymi właściwościami.*

Modyfikowanie serii danych

Właściwości szeregu danych modyfikowane są w panelu **Szereg danych** widocznym po prawej stronie po otworzeniu w programie szablonu raportu w postaci okna z zakładkami. Zawierają one następujące informacje o wybranym wykresie w szablonie raportów:

Statystyki szeregu danych	Określa rodzaj danych statystycznych (licznik wydajności węzła) zebranych trendów, jaki ma być prezentowany w postaci serii danych na wykresie.
Funkcja szeregu	Określa, czy dane trendu szeregu mają mieć wartość uśrednioną, maksymalną czy minimalną.
Skala szeregu	Określa jaki rodzaj skali dla serii danych ma być użyty na wykresie (tj. 0.001, 0.01, 0.1, 1, KB, MB lub GB).
Kolor szeregu	Uściśla kolor wskazanej serii danych na wykresie.
Szerokość linii szeregu	Precyzuje szerokość linii serii danych na wykresie.
Styl linii szeregu	Określa styl linii (ciągła, przerywana) serii danych na wykresie
Rodzaj wykresu	Określa, czy seria danych ma być prezentowana w postaci linii, pionowych lub poziomych słupków, wykresu kołowego czy też obszaru.

Uwagi

- *Możliwe jest dodawanie w postaci serii danych kilku rodzajów statystyk (czyli kilku różnych liczników wydajności węzła) na jednym wykresie, którego właściwości są modyfikowane. W tym calu należy – dla statystyk każdej serii danych z osobna – kliknąć ikonę* **Dodaj szereg** *znajdującą się na panelu **Szereg danych**, a następnie w nowo otwartym oknie **Wybierz liczniki** określić rodzaj licznika, przykładowy węzeł źródłowy, obiekt, licznik wydajności oraz wystąpienie (w stosownych przypadkach). Należy jednak pamiętać, że w praktyce dane licznika wydajności węzła źródłowego **nie będą** zbierane. Węzeł źródłowy jest używany jedynie w celach opisowych, aby umożliwić wybór poprawnego licznika wydajności (i ewentualnie wystąpienia) w charakterze analizowanych danych.*
- *Aby usunąć serię danych dla wielkości statystycznej (licznika wydajności), należy zaznaczyć do w panelu **Szereg danych** i kliknąć ikonę* **Usuń szereg danych**.
- *W przypadku wybrania wykresu w postaci poziomych lub pionowych słupków należy zdefiniować dodatkowy element – ich kształt. Prezentowane na wykresie słupki można zdefiniować jako prostokąty (ustawienie domyślne), prostokąty gradientowe, ostrosłupy, obrócone ostrosłupy, walce, elipsy lub strzałki.*
- *Możliwe jest modyfikowanie tytułu każdego szeregu danych, jaki pojawia się w legendzie wykresu. W tym celu należy prawym przyciskiem myszy kliknąć serię danych w panelu **Szereg danych** i z podręcznego menu wybrać element **Właściwości szeregu**. Wówczas zostanie wywołane okno dialogowe **Właściwości szeregu**, w którym należy wpisać nowy tytuł dla serii danych w polu **Tytuł**.*

Modyfikowanie rodzaju analizy

Wybór rodzaju analizy dokonywany jest w panelu **Rodzaj analizy** widocznym po prawej stronie po otwarciu w programie szablonu raportu w postaci okna z zakładkami. W panelu tym definiuje się następujące informacje dotyczące wskazanego wykresu w otwartym szablonie raportów:

Jednostka czasu	Określa, czy informacje prezentowane na wykresie mają dotyczyć dnia, tygodnia, miesiąca, kwartału czy też roku.
Okres	Określa, czy informacje prezentowane na wykresie mają pochodzić z okresu aktualnego (wybranego w momencie generowania), poprzedniego (w stosunku do okresu zdefiniowanego w momencie generowania) czy też osobiście wskazanego okresu (bez względu na to, co zostało zdefiniowane w momencie generowania).
Data	Określa dokładną datę czy też zakres dat po wybraniu pojedynczego okresu.
Rodzaj analizy	Określa rodzaj analizy, jak ma być prezentowany na wykresie: trendy standardowe, podstawowy rozkład (godzinny, dzienny rozkład tygodnia oraz dzienny rozkład miesiąca) a także ogólna analiza porównawcza (dla wykresów kołowych).
Podzakres	Określa maskę dni/godzin, czyli dni tygodnia i godzin dnia, dla których prezentowane będą dane na wykresie.

Uwagi

- *Niezwykle ważnym krokiem jest wybór odpowiedniej **Jednostki czasu**. Jeśli jest nią rok, a następnie zachodzi potrzeba utworzenia raportu dziennego przy użyciu tego samego wykresu, wówczas na wykresie raportu zostaną wygenerowane i zaprezentowane nieodpowiednie dane.*
- *Zalecanym ustawieniem wielkości **Okres** jest **Raportuj aktualny okres**, dzięki czemu podczas generowania własnego raportu trendów wartość ta zostanie zastosowana dla daty wybranego raportu bazowego.*
- *Podczas użycia opcji **Raportuj poprzedni okres** przy generowaniu własnego raportu trendów program zawsze będzie używał okresu bezpośrednio poprzedzającego okres wybrany jako data raportu bazowego.*
- *Aby wygenerować raport dla identycznego zapisanego okresu, należy dla opcji **Okres** użyć ustawienia **Wybrany**. W takich wypadkach w polu poniżej należy wybrać odpowiednią datę, natomiast dokonany w późniejszym czasie wybór daty raportu bazowego nie będzie miał wpływu na generowany raport.*
- *Aby włączyć maskę analizy, należy zaznaczyć pole wyboru **Włącz maskę dzienną/godzinną** w panelu **Rodzaj analizy**. Aby ją wyłączyć, wystarczy odznaczyć powyższe pole wyboru.*
- *Aby zmodyfikować maskę dzienną/godzinną, kliknij przycisk **Zmień maskę** w panelu **Rodzaj analizy**, a następnie w oknie dialogowym **Maska dzienna/czasowa** za pomocą lewego i prawego przycisku myszy zaznacz bądź odznacz wybrane fragmenty tygodnia i dnia. Przykładowo, maska*

dzienna/godzinna może prezentować wyłącznie dane dla dni powszednich, od poniedziałku do piątku między 7 a 19, co pokazuje przedstawiony poniżej rysunek 1.

Modyfikowanie układu strony

Właściwości układu strony można modyfikować w panelu **Układ strony** widocznym po prawej stronie, gdy w programie otwarty jest szablon raportu w postaci okna z zakładkami. Zawierają one następujące informacje dla wybranego wykresu w aktualnie otwartym szablonie raportu:

Położenie danych	Określa, czy zostanie utworzony jeden wykres, na którym zostaną umieszczone wszystkie szeregi danych, czy też dla każdej serii danych węzła zostanie utworzony osobny wykres.
Układ	Określa, czy pod wykresem ma znajdować się łamanie strony, oraz definiuje układ wykresów na stronie (jeśli występuje więcej niż jeden wykres): - **Domyślna raportu**– oznacza, że będą używane ustawienia globalne określone we właściwościach szablony raportu. - **Jeden wykres na stronie** – oznacza, że tylko jeden wykres zostanie umieszczony na każdej stronie. - **Jeden obrócony wykres** – oznacza, że zostanie zaprezentowany tylko jeden wykres obrócony o 90 stopni w prawą stronę z stosunku do jego normalnej pozycji. - **1 x 2** – oznacza, że na jednej stronie zostaną umieszczone co najwyżej dwa wykresy, każdy w osobnym rzędzie. - **2 x 1** – oznacza, że na jednej stronie zostaną umieszczone co najwyżej dwa wykresy, każdy w osobnej kolumnie. - **2 x 2** – oznacza, że na jednej stronie zostaną umieszczone co najwyżej cztery wykresy, po dwa w każdym rzędzie. - **2 x 3** – oznacza, że na jednej stronie zostanie umieszczonych maksymalnie sześć wykresów, po dwa w każdym w trzech rzędów.
Wysokość wykresu	Określa dokładną wysokość wykresu na stronie.
Tytuł	Określa tekst tytułowy umieszczony na górze strony razem z wykresem, a także wyrównanie poziome, krój czcionki, styl, rozmiar i kolor.

Uwaga

Należy pamiętać, że właściwości układu strony są również definiowane we właściwościach szablonu raportu. Są one używane globalnie dla wszystkich wykresów, które są częścią szablonu raportu. Z drugiej strony właściwości układu strony dla pojedynczych wykresów są nadrzędne w stosunku do właściwości szablonu raportu; oznacza to, że mają one pierwszeństwo, jeśli są definiowane dla dowolnego pojedynczego wykresu.

Tworzenie własnych raportów trendów

Do wygenerowania własnego raportu trendów służy szablon raportu, na którym ma on bazować. W ten sposób możliwe jest sprawne tworzenie raportów w oparciu o zebrane trendy – szablon zawiera bowiem gotowe definicje sposobu prezentowania informacji. Należy mieć na względzie, że dane trendów są oparte na określonych licznikach wydajności – są one ustawiane w także w **Kreatorze raportów wydajności**.

Aby wygenerować własny raport trendów, należy określić:

- **szablon raportu** – sposób, w jaki będą prezentowane informacje wchodzące w skład raportu,
- **bazową datę raportu** – dokładny okres, dla którego zostaną pokazane trendy wydajności w raporcie;
- **węzeł lub kilka węzłów** – węzeł/węzły, których będą dotyczyć prezentowane informacje.

Raport można utworzyć bądź z poziomu okna **Kreatora raportów**, które pojawia się przy starcie programu, lub poprzez wybór odpowiedniego polecenia z głównego menu, gdy otwarty jest program i odpowiedni szablon.

Uwagi

- *Bazowa data raportu powinna pokrywać się z okresem, podczas którego były zbierane odpowiednie dane trendów dla wybranych węzłów. W przeciwnym razie przy tworzeniu własnego raportu trendów dla okresu, dla którego nie zostały uprzednio zgromadzone żadne dane, finalny raport dla węzła lub węzłów będzie zawierał puste wykresy pozbawione danych.*
- *Dane trendów w NetCrunchu są gromadzone na kilka sposobów. Najbardziej podstawowym jest włączenie określonego raportu dla węzła (mapy lub atlasu) w oknie* ***Konfiguracja raportów*** *(por. sekcję* Włączanie generowania raportów *na stronie 96 w celu uzyskania szczegółowych informacji). Innym sposobem jest utworzenie widoku wydajności w postaci wykresów określonego licznika wydajności dla węzła lub węzłów (por. sekcję* Widoki wydajności *na stronie 53 w celu uzyskania szczegółowych informacji). Ponadto można ustawić w NetCrunchu wszczęcie procedury zbierania trendów dla licznika wydajności z poziomu* ***Przeglądarki raportów*** *poprzez włączenie w tymże programie dowolnego z predefiniowanych raportów dla określonego węzła lub mapy (por. sekcję* Przeglądarka raportów *na stronie 100 w celu uzyskania szczegółowych informacji).*

Aby wygenerować raport z pierwszego ekranu Kreatora raportów

1. W pierwszym ekranie **Kreatora raportów** wybierz przycisk opcji **Utwórz raport z szablonu**, a następnie kliknij **Dalej**.
   Pojawi się ekran **Szablony raportów**.
2. Z dostępnej listy wybierz szablon raportu, na którym ma bazować raport, po czym kliknij **Dalej**.
   Otworzy się ekran **Utwórz raport**.
3. Z rozwijanej listy **Bazowa data raportu** wybierz datę określającą generowany raport – trendy wydajności pojawiające się na dowolnych wykresach będą mieścić się w powyższej dacie bazowej.
4.  Za pomocą ikony ***Dodaj węzeł*** wybierz węzły, dla których zostaną zaprezentowane trendy na wykresach (wskazane w wybranym szablonie raportu).

5. Kliknij **OK**.
   Raport oparty na wybranym szablonie zostanie natychmiast wygenerowany, zapisany na dysku lokalnym oraz wyświetlony w **Kreatorze raportów wydajności** w postaci osobnego okna z zakładkami.

Aby wygenerować raport przy użyciu polecenia menu

1. Z menu **Plik** wybierz opcję **Otwórz szablon**.
   Wyświetli się okno dialogowe **Otwórz szablon**.
2. Z listy **Nazwa szablonu** wybierz szablon raportu, na bazie którego zostanie wygenerowany raport, a następnie kliknij **OK**.
   W programie otworzy się wybrany szablon raportu w postaci osobnego okna z zakładkami.
3. Z menu **Szablon** wybierz opcję **Wygeneruj raport** bądź w głównym pasku narzędzi kliknij bezpośrednio ikonę ***Wygeneruj raport***.
   Otworzy się okno dialogowe **Wygeneruj raport**.
4. Z rozwijanej listy **Bazowa data raportu** wybierz datę stanowiącą punkt odniesienia raportu.
5. Za pomocą ikony ***Dodaj węzeł*** wybierz węzeł lub węzły, których dane trendów mają znaleźć się w raporcie.
6. Kliknij **OK**.
   Raport oparty na otwartym szablonie zostanie natychmiast wygenerowany, zapisany na dysku lokalnym oraz wyświetlony w programie w postaci osobnego okna z zakładkami.

Uwagi

- *Po punkcie 2, gdy informacje szablonu raportu pojawią się na ekranie w postaci osobnego okna z zakładkami, można przed samym wygenerowaniem raportu zmodyfikować jego ustawienia. Por. sekcję* Edytowanie szablonu raportu *na stronie 106.*
- *Sam wygenerowany raport jest zapisywany na dysku lokalnym w katalogu, w którym został zainstalowany NetCrunch 4.x, czyli w podkatalogu* `/Data/<ATLAS_NUMBER> /NTVReports`*. Plik zawierający wygenerowany raport zawsze posiada rozszerzenie* `.NTR`*.*
- *W swojej zakładce szablon raportu zawsze zawiera ikonę przedstawioną na lewym marginesie, natomiast wygenerowany raport zawiera tę ikonę w swojej zakładce.*
- *Aby powiększyć lun pomniejszyć treść wygenerowanego raportu, należy użyć odpowiednich ikon w pasku narzędzi. Można również posłużyć się odpowiednią rozwijaną listą* **Powiększenie** *w tymże pasku narzędzi w celu określenia żądanej wielkości przybliżenia/oddalenia bądź kliknąć ikony* **Dopasuj szerokość** *i* **Dopasuj stronę** *w celu dostosowania treści raportu odpowiednio do szerokości bądź długości strony.*
- *Możliwe jest również przystosowanie obszaru dowolnego wykresu należącego do wygenerowanego raportu. Por. sekcję* Dostosowywanie obszaru wyświetlania *na stronie 118 w celu uzyskania szczegółowych informacji.*

Przeglądanie zapisanych raportów

Aby otworzyć własny raport trendów, dany raport powinien być uprzednio utworzony przez program na bazie określonego szablonu raportów. W trakcie generowania raport jest także automatycznie zapisywany na dysku lokalnym. W efekcie można oglądać tylko raporty, które zostały uprzednio zapisane. Ponadto statystyki wybranych liczników wydajności, jakie mają pojawić się w raporcie (zdefiniowane w szablonie raportów) powinny zawierać dane, które zostały wcześniej zebrane w NetCrunchu. W przeciwnym wypadku, jeśli wcześniej nie zostały zebrane żadne stosowne trendy, wygenerowany raport nie będzie zawierał żadnych danych na wchodzących w jego skład wykresach.

Aby otworzyć zapisany raport

1. Otwórz **Kreatora raportów wydajności**.
2. W menu **Plik** wybierz opcję **Otwórz raport** bądź z okna **Kreatora raportów** (jeśli pojawia się automatycznie przy starcie) zaznacz przycisk opcji **Otwórz zapisany raport** i kliknij **Dalej**.
   Otworzy się ekran **Otwórz raport**.
3. Z zaprezentowanej listy wybierz raport, który ma zostać otwarty (za pomocą kart **Wg szablonów** lub **Wg daty** pogrupuj informacje według nazwy szablonu lub daty raportu).

Uwagi

- *Przy wyborze określonego raportu w punkcie 3 obok samej listy pojawią się stosowne związane z nim informacje (dotyczące związanego z nim węzła i daty jego utworzenia).*
- *Po otworzeniu raportu pojawia się on w programie jako nowe okno z zakładkami, natomiast nazwa raportu ukaże się u góry.*
- *Aby szybko przeglądać kilka stron raportów, wybierz określoną stronę lub wykres z położonej po lewej stronie listy stron, jeśli na dowolnej stronie znajduje się więcej niż jeden wykres.*
- *Możliwe jest dostosowywanie obszaru dowolnego wykresu należącego do wygenerowanego raportu. Por. poniższą sekcję* Dostosowywanie obszaru wyświetlania *w celu uzyskania szczegółowych informacji.*

Dostosowywanie obszaru wyświetlania raportu

Po wygenerowaniu raportu – gdy wyświetla się on jako okno z zakładkami – można szczegółowo określić, która jego część ma być prezentowana na dowolnym z jego wykresów. W tym celu należy klikać i przeciągać oba przyciski myszy na aktualnie wyświetlanym obszarze wykresu.

Aby dostosować (przybliżyć) obszar wyświetlania wykresu w celu szczegółowej prezentacji wybranego fragmentu widoku wykresu

1. Umieść kursor myszy w lewym górnym rogu obszaru, jaki ma być wyświetlany.
2. Przeciągaj kursor myszy (przytrzymując wciśnięty lewy przycisk myszy) w kierunku prawego dolnego rogu aż w prostokątnym obszarze pojawi się fragment, do którego ma zostać dostosowany obszar wyświetlania.
3. Zwolnij przycisk myszy.
   Obszar w prostokącie stanie się nowym obszarem wykresu – wykres powiększy się obejmując cały wybrany fragment obszaru wyświetlania.

Aby dostosować (oddalić) obszar wyświetlania wykresu do domyślnego obszaru widoku

1. Przeciągnij przycisk myszy (przytrzymując wciśnięty lewy przycisk myszy) z pozycji na wykresie w kierunku lewego górnego rogu.
2. Zwolnij przycisk myszy.
   Wykres powróci do domyślnego obszaru wyświetlania.

Aby przesunąć aktualny obszar wyświetlania wykresu w górę lub w dół osi x i y

1. Przeciągaj kursor myszy (przytrzymując wciśnięty prawy przycisk myszy) w górę lub w dół (dotyczy osi y) bądź w prawo lub lewo (dotyczy osi x).
2. Zwolnij przycisk myszy.
   Widok wykresu zaprezentuje wówczas nowy obszar wyświetlania.

Uwagi

- *Po dostosowaniu obszaru wyświetlania dowolnego wykresu raportu można wydrukować go w postaci, w jakiej jest on prezentowany na ekranie.*
- *Opisana wyżej opcja jest niezwykle przydatna, gdyż umożliwia personalizowanie ważnego obszaru wykresu przy jednoczesnym pominięciu innych danych wykresu. Przykładowo dla celów analizy porównawczej można wyświetlić wartości ujemne osi y wykresu.*

Drukowanie własnego raportu trendów

Gdy otworzony został w celu przeglądania uprzednio wygenerowany raport, można wydrukować jego zawartość. W tym celu należy kliknąć ikonę ***Wydrukuj*** znajdującą się w pasku narzędzi.

Aby wydrukować raport

1. Otwórz raport do przeglądania tak, by pojawił się w postaci okna z zakładkami w panelu wyświetlania.

2. W pasku narzędzi kliknij ikonę ***Drukuj***.
   Otworzy się okno **Podgląd wydruku**.
3. Wprowadź zmiany związane z formatem układu strony.

4. W pasku narzędzi **Podgląd wydruku** kliknij ikonę ***Drukuj***, aby rozpocząć drukowanie wskazanego raportu.

Uwaga

W punkcie 3 można dodatkowo kliknąć ikonę **Okno dialogowe drukowania***, aby otworzyć standardowe okno dialogowe* ***Drukuj*** *systemu Windows, w którym można wybrać inną drukarkę niż domyślna, a także zmienić ustawienia związane z wybraną drukarką.*

Usuwanie własnego raportu trendów

Możliwe jest szybkie usuwanie dowolnego z uprzednio utworzonych i zapisanych własnych raportów trendów – odbywa się to w **Kreatorze raportów**.

Aby usunąć wygenerowany raport

1. Otwórz **Kreatora raportów wydajności**.
2. Z menu **Plik** wybierz opcję **Otwórz raport**, ewentualnie w oknie **Kreator raportów** (jeśli pojawi się automatycznie przy starcie programu) zaznacz przycisk wyboru **Otwórz zapisany raport** i kliknij **Dalej**.
   Otworzy się ekran **Otwórz raport**.
3. W wyświetlanej liście wybierz raport do usunięcia (za pomocą kart **Wg szablonów** lub **Wg daty** pogrupuj informacje według nazwy szablonu lub daty raportu).
4.  Kliknij ikonę ***Usuń raport***.
   Pojawi się okno z potwierdzeniem.
5. Kliknij przycisk **Tak**.

Uwagi

- *Przy wyborze określonego raportu w punkcie 3 związane z nim informacje (dotyczące związanych z nim węzłów oraz data jego utworzenia) pojawiają się obok samej listy.*

6. Możliwe jest również usuwanie wygenerowanego własnego raportu trendów ręcznie poprzez kasowanie go z odpowiedniego pliku o rozszerzeniu `.NTR` znajdującym się w podkatalogu `/Data/<ATLAS_NUMBER> /NTVReports`, w którym NetCrunch 4.x został pierwotnie zainstalowany.

Format zapisu trendów

NetCrunch automatycznie zbiera trendy dotyczących monitorowanych węzłów – są to w zasadzie wyniki pomiaru wskazań liczników wydajności, czasu odpowiedzi (w milisekundach), dostępności oraz procentowego udziału utraconych pakietów dla każdej usługi sieciowej odpytywanej w danym węźle. Chcąc przeanalizować historyczną zmienność trendów związanych z usługami sieciowymi w danym węźle, należy otworzyć okno **Stan** lub obejrzeć widoki map dotyczące Windows NT, NetWare czy SNMP.

Wszystkie dane o trendach zapisywane są w następującym katalogu:

`<ŚCIEŻKA_KATALOGU_INSTALACJI_NETCRUNCH>/data/<NUMER_ATLASU>/trends`

gdzie <NUMER_ATLASU> to numer identyfikujący dany atlas. Jeżeli na przykład utworzone zostały trzy oddzielne atlasy, to każdemu takiemu atlasowi przydzielony został osobny katalog, oznaczony unikatowym numerem: *1*, *2* lub *3*. Co więcej, w katalogu takim każdy węzeł należący do danego atlasu będzie miał własny podkatalog, w którym będą zapisywane wszystkie dane o trendach dotyczących tego węzła. Każda nazwa takiego podkatalogu będzie oznaczana czterocyfrową unikatową liczbą, np. 1001, 1002, itd.

W przypadku każdego węzła wszystkie związane z nim dane o trendach zapisywane są w takim katalogu jako pojedynczy plik, zawierający wszelkie dane o trendach zebrane w ciągu bieżącego dnia. Plik ten ma rozszerzenie `.TRD`, a jego nazwa składa się z roku, miesiąca i dnia, w którym dane te zostały zebrane. Przykładowo plik o nazwie `2004 114.TRD` zawiera dane zebrane 14 stycznia 2004 roku. Oprócz pliku `.TRD` z każdym węzłem związany jest jeszcze inny plik, o rozszerzeniu `.ARC`. Zawiera on, w skompresowanej postaci, wszystkie

dane o trendach zebrane w tych dniach w przeszłości, w których uruchomiony był NetCrunch. W przypadku gdy węzeł atlasu monitorowany jest przez dłuższy okres czasu, plik ten można nabrać całkiem sporych rozmiarów. W chwili obecnej program NetCrunch nie jest wyposażony w mechanizm umożliwiający kasowanie najstarszych danych historycznych.

Zarządzanie atlasem sieci

Dodawanie sieci

W programie NetCrunch dodawanie nowej sieci do atlasu jest czynnością niemal intuicyjną, przy czym może odbywać się w sposób bezpośredni albo pośredni. Można albo dodać nową sieć, o ile znany jest jej adres IP, albo po prostu do *Wykazu węzłów* dodać nowy węzeł (należący do nieznanej sieci). W tym ostatnim przypadku taka nowa sieć zostanie dodana automatycznie i będzie widoczna w sekcji *Sieci IP* w oknie **Atlas sieci**.

Dodawanie nowej sieci

Aby dodać nową sieć, należy wybrać odpowiednie polecenie z menu podręcznego w drzewie *Atlas sieci*.

Aby dodać nową sieć

1. W oknie **Atlas sieci** zaznacz folder *Zdalne*, a następnie w menu podręcznym wskaż pozycję **Nowy** i wybierz polecenie **Sieć TCP/IP**.
2. W nowo otwartym oknie wpisz adres i (opcjonalnie) maskę sieci, którą chcesz dodać do atlasu.
3. Postępuj zgodnie z poleceniami wyświetlanymi przez *Kreatora wykrywania sieci*. Na podstawie wybranych opcji kreator automatycznie wykryje wszystkie węzły należące do nowej sieci.

Uwagi

- *Nową sieć można również dodać przez wskazanie w menu **Narzędzia** pozycji **Zadania**, a następnie wybranie polecenia **Dodaj sieć do monitorowania**.*
- *Aby dodać nową sieć w sposób pośredni, należy w menu **Narzędzia** wskazać pozycję **Zadania**, a następnie wybrać polecenie **Dodaj węzeł do monitorowania**. Następnie należy wpisać adres IP lub nazwę DNS dowolnego węzła nowej sieci, który chcemy monitorować. Więcej informacji na ten temat zawiera rozdział* Dodawanie i usuwanie węzłów *na stronie 130.*

Operacje na atlasie

Tworzenie map

Dodawanie nowych map jest możliwe wyłącznie w sekcji atlasu *Widoki własne*. Aby dodać mapę sieci w sekcji *Sieci IP*, przejdź do znajdującego się powyżej rozdziału pt. *Dodawanie sieci*. Program umożliwia tworzenie map własnych poprzez ręczne dodawanie i rozmieszczanie węzłów oraz tworzenie map filtrowanych aktualizowanych dynamicznie (w oparciu o wybrane przez użytkownika reguły filtrowania). Każda z takich map może być

umieszczona w jednym ze wstępnie zdefiniowanych folderów map (eDirectory lub Domeny Windows) albo w dowolnym folderze utworzonym wcześniej przez użytkownika.

Mapa własna

Pustą mapę własną można dodać do dowolnego folderu w sekcji atlasu *Widoki własne*.

Aby dodać nową pustą mapę własną

1. W oknie **Atlas sieci**, w sekcji *Widoki własne*, zaznacz folder, w którym ma się znaleźć dodawana mapa (mapa ta będzie statyczna).
2. Kliknij prawym przyciskiem myszy nazwę tego folderu, w menu podręcznym wskaż pozycję **Nowy**, a następnie wybierz polecenie **Pusta mapa**.
3. Nowa mapa zostanie utworzona w ramach grupy wybranej w sekcji *Widoki własne* w oknie **Atlas sieci**.

Uwaga

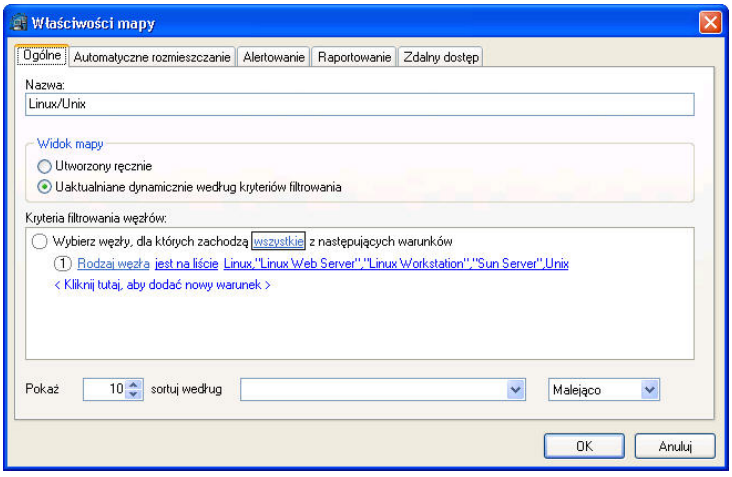
- *Nazwę nowo utworzonej mapy można łatwo zmienić. Więcej informacji na ten temat zawiera rozdział* Zmiana nazwy mapy *na stronie 128.*
- *Po utworzeniu pustej mapy można przystąpić do nanoszenia na nią węzłów. Więcej informacji na ten temat udostępnia rozdział* Wstawianie węzła na mapę w sekcji Widoki własne *na stronie 178.*
- *Utworzona ręcznie w sekcji* Widoki własne *(statyczna) mapa może zostać później w prosty sposób zmieniona w dynamiczny widok filtrowany (czyli aktualizowany na bieżąco). W tym celu w drzewie* ***Atlas sieci*** *wystarczy kliknąć daną mapę prawym przyciskiem myszy, a następnie z menu podręcznego wybrać opcję polecenie* ***Właściwości****. W nowo otwartym oknie, w obszarze* ***Widok mapy****, należy wybrać przycisk opcji* ***Uaktualniany dynamicznie wg kryteriów filtrowania****, określić wszelkie kryteria filtrowania i kliknąć przycisk* ***OK****, aby zapisać wprowadzone zmiany.*

Mapa widoku filtrowanego

Mapa widoku filtrowanego (dynamiczna) może być dodawana do dowolnego folderu w sekcji *Widoki własne*.

Aby dodać nowy widok filtrowany

1. W oknie **Atlas sieci**, w sekcji *Widoki własne*, zaznacz folder, w którym ma się znaleźć nowa mapa.
2. Kliknij prawym przyciskiem myszy nazwę tej grupy, w menu podręcznym wskaż pozycję **Nowy**, a następnie wybierz polecenie **Widok filtrowany**.
   Spowoduje to otwarcie okna **Właściwości mapy** (przedstawionego na rysunku poniżej). Upewnij się, że w obszarze **Widok mapy** został wybrany przycisk opcji **Uaktualniany dynamicznie wg kryteriów filtrowania**.



3. Określ kryteria filtrowania dla nowo utworzonej mapy. Możesz w tym celu zastosować dowolną ilość nawiasów i warunków. Szczegółowy opis procedury określania kryteriów filtrowania podany został w rozdziale *Określanie kryteriów filtrowania* na stronie 125.

Uwagi

- *Możliwe jest, że utworzona nowa mapa widoku filtrowanego (dynamiczna) będzie początkowo pusta, czyli nie będzie zawierać żadnych węzłów. Może się tak zdarzyć w przypadku, gdy żaden węzeł w sieci nie spełnia kryteriów wyboru, na podstawie których węzły umieszczane są na nowej mapie. Aby taką mapę zapełnić węzłami, należy odpowiednio zmienić kryteria filtrowania.*
- *Mapa widoku filtrowanego (dynamiczna) należąca do sekcji* Widoki własne *może zostać później w prosty sposób zmieniona w mapę pustą (statyczną). W tym celu wystarczy w oknie* ***Atlas sieci*** *kliknąć daną mapę prawym przyciskiem myszy, a następnie z menu podręcznego wybrać polecenie* ***Właściwości****. W nowo otwartym oknie, w obszarze* ***Widok mapy****, należy wybrać przycisk opcji* ***Utworzony ręcznie****, a następnie kliknąć przycisk* ***OK****, aby zapisać wprowadzone zmiany.*

Określanie kryteriów filtrowania

W programie NetCrunch określanie kryteriów filtrowania dla nowej mapy lub zmienianie ich dla już utworzonej mapy przeprowadzane jest w sposób niezwykle intuicyjny. Odbywa się to poprzez otwarcie okna **Właściwości mapy** i wybranie karty **Ogólne** (musi przy tym być wybrana opcja **Uaktualniany dynamicznie wg kryteriów filtrowania**). W polu **Kryteria filtrowania węzłów** można określić dowolne kryteria filtrowania.

We wszelkich kryteriach filtrowania wykorzystywane są jedynie wyrażenia powszechnie używane w języku polskim, a zatem nie jest konieczne wcześniejsze dysponowanie jakąś specjalistyczną wiedzą na temat ich definiowania. Użytkownik ma możliwość dodania dowolnej ilości następujących dwóch rodzajów wyrażeń:

Warunek	Wyraża regułę filtrowania; np. „Rodzaj węzła jest równe Ruter".
Nawias	Jest wykorzystywany do łączenia w jedną grupę dowolnej ilości warunków filtrowania, np. „Zachodzą dowolne z następujących warunków". Po dodaniu nowego nawiasu zostaje pod nim również dodany nowy warunek filtrowania.

Kliknięcie dowolnego numeru wyrażenia, który to numer znajduje się na lewo od treści takiego wyrażenia, powoduje wywołanie podręcznego menu ze wszystkimi akcjami, jakie mogą być przeprowadzone na danym wyrażeniu. Należą do nich następujące operacje:

Dodaj warunek	Dodaje pod zaznaczonym wyrażeniem nowy warunek.
Dodaj nawias	Dodaje, bezpośrednio pod zaznaczonym wyrażeniem, nowy nawias z umieszczonym pod nim nowym warunkiem.
Usuń aktualny wiersz	Usuwa zaznaczone wyrażenie oraz wszelkie inne zdefiniowane pod nim warunki lub nawiasy.

W każdym wyrażeniu niektóre jego elementy mogą być zmieniane – albo przez kliknięcie określonej części danego wyrażenia i wybranie odpowiedniej opcji z listy rozwijanej, albo przez bezpośrednie wpisanie w to miejsce właściwej wartości. W szczególności, dla pierwszej części wyrażenia określającego warunek, użytkownik ma możliwość wyboru jednego spośród następujących elementów:

Nazwa DNS	Umożliwia wybór węzłów na podstawie nazwy DNS.
Domena, eDirectory	Umożliwia wybór węzłów na podstawie domen Windows lub katalogów Novell eDirectory, do których należą.
Info1	Umożliwia wybór węzłów na podstawie informacji umieszczonych w specjalnym polu *Info1*, które to informacje, mogą być określane w opcjach każdego z węzłów.
Info2	Umożliwia wybór węzłów na podstawie informacji umieszczonych w specjalnym polu *Info2*, które to informacje, mogą być określane w opcjach każdego z węzłów.
Moment wstawienia węzła	Umożliwia wybór węzłów według momentu, w którym węzeł został umieszczony na mapie.
Adres IP	Umożliwia wybór węzłów na podstawie zakresu adresów IP, do którego należą.

Moment ostatniego alertu	Umożliwia wybór węzłów na podstawie czasu wystąpienia ostatniego zdarzenia związanego z węzłem.
Lokalizacja	Umożliwia wybór węzłów na podstawie lokalizacji sieci, do której należą.
Liczba minut od momentu wstawienia węzła	Umożliwia wybór węzłów na podstawie liczby minut, jakie upłynęły od momentu umieszczenia węzła w atlasie.
Liczba minut od ostatniego alertu	Umożliwia wybór węzłów na podstawie liczby minut, jakie upłynęły od momentu wystąpienia zdarzenia na węźle.
Liczba minut od zmiany stanu	Umożliwia wybór węzłów na podstawie liczby minut, jakie upłynęły od momentu wystąpienia zmiany stanu monitorowania węzła.
Lista usług sieciowych	Umożliwia wybór węzłów na podstawie monitorowanych w nich usług sieciowych.
Stan węzła	Umożliwia wybór węzłów na podstawie aktualnego stanu monitorowania węzła
Moment zmiany stanu węzła	Umożliwia wybór węzłów na podstawie daty i czasu ostatniej zmiany stanu monitorowania węzła.
Rodzaj węzła	Umożliwia wybór węzłów na podstawie ich rodzaju, czyli np. tego, czy jest to ruter, serwer NetWare itp.
Monitorowanie uproszczone	Umożliwia wybór węzłów na podstawie tego, czy jest na nich włączone lub wyłączone monitorowanie uproszczone.
Liczba niepotwierdzonych alertów	Umożliwia wybór węzłów na podstawie liczby niepotwierdzonych alertów.

Wyświetlanie wyłącznie czołowych węzłów

W przypadku map dynamicznie uaktualnianych można skonfigurować program, aby pokazywał wyłącznie wybraną liczbę węzłów posortowanych według wskazanej właściwości lub funkcji węzła w szyku rosnącym lub malejącym.

Aby wyświetlać wyłącznie czołowe węzły posortowane w porządku rosnącym/malejącym

1. Otwórz okno **Właściwości mapy** dotyczące uaktualnianej dynamicznie mapy.
2. W dolnej części pola określ, ile posortowanych czołowych węzłów ma być prezentowanych na mapie.
3. W położonej na prawo od powyższego pola rozwijanej liście wskaż właściwość lub funkcję węzła, według których mają zostać posortowane węzły.

4. Określ, czy węzły na mapie dynamicznej powinny być sortowane w porządku rosnącym czy malejącym w oparciu o właściwość wybraną w punkcie 3.

Uwagi

- *Opcja wyświetlania wyłącznie określonej liczby czołowych węzłów nie powoduje automatycznego rozmieszczania węzłów na mapie. Aby je rozmieścić, należy użyć polecenia* ***Rozmieść węzły*** *z menu* ***Mapa*** *lub wypełnić pola w karcie* ***Automatyczne rozmieszczanie*** *okna* ***Właściwości mapy****.*
- *Aby wyłączyć tę funkcję, wybierz opcję z pustym polem w rozwijanej liście w punkcie 3.*

Usuwanie mapy

Program umożliwia usunięcie dowolnej mapy należącej do określonej grupy. Jednakże zalecane jest usuwanie map tylko w tych grupach drzewa atlasu, które należą do sekcji *Widoki własne*. Należy przy tym pamiętać, że mapy utworzone w sekcji *Widoki własne* są jedynie częściowymi widokami skanowanej sieci – jej pełny obraz daje dopiero widok *Sieci IP*. Mapy należące do sekcji *Topologia fizyczna* nie mogą być ani zmieniane, ani usuwane.

Podczas usuwania map z sekcji *Sieci IP* należy zachować szczególną ostrożność. Usunięcie takiej mapy spowoduje równoczesne usunięcie wszystkich należących do niej węzłów. Jeśli usuwane w ten sposób węzły należałyby do jakichkolwiek innych map w sekcji *Widoki własne*, zostaną one z tych map również usunięte.

Aby usunąć mapę

1. W oknie **Atlas sieci** zaznacz mapę, którą chcesz usunąć.
2. Kliknij prawym przyciskiem myszy tę mapę i z menu podręcznego wybierz polecenie **Usuń**.
   Na ekranie pojawi się okno potwierdzenia.
3. Kliknij przycisk **Tak**.

Zmiana nazwy mapy

W programie istnieje możliwość zmiany nazwy dowolnej mapy utworzonej przez użytkownika lub program i należącej do sekcji *Sieci IP*, *Widoki własne*, lub *Topologia fizyczna*.

Aby zmienić nazwę mapy

1. W oknie **Atlas sieci** zaznacz mapę, której nazwę chcesz zmienić.
2. Kliknij nazwę mapy lub naciśnij klawisz **F2**.
3. Wpisz nową nazwę mapy i naciśnij klawisz **Enter**.

Uwaga

Nazwę mapy można również zmienić w inny sposób – wybierając z menu ***Mapa*** *polecenie* ***Właściwości****.*

Przenoszenie mapy

Wszelkie mapy, z wyjątkiem map, które w oknie atlasu sieci należą do sekcji *Topologia fizyczna*, mogą być przenoszone do dowolnego innego miejsca w drzewie atlasu. W tym celu wystarczy przeciągnąć mapę do nowego miejsca w atlasie i upuścić ją tam.

Aby przenieść mapę do innego miejsca w drzewie atlasu sieci

1. W oknie **Atlas sieci** przeciągnij mapę, którą chcesz przenieść, i upuść ją w nowym miejscu.

Uwaga

Jeżeli podczas przeciągania mapy zmieni się wygląd kursora i pojawi się symbol przekreślenia, oznacza to, że mapa ta nie może zostać umieszczona w danym miejscu.

Foldery atlasu

Foldery atlasu służą do grupowania zestawów map, które z pewnych względów powinny zostać umieszczone razem, w jednym miejscu – pełnią one funkcję analogiczną do katalogów w systemie plików lub rozdziałów w książce.

Uwaga

Dodawanie, przenoszenie, usuwanie i zmienianie nazw folderów jest możliwe tylko w sekcji Widoki własne *okna* ***Atlas sieci****.*

Dodawanie nowego folderu

Aby utworzyć nowy folder w sekcji *Widoki własne* okna **Atlas sieci**, należy wybrać miejsce, w którym taki folder ma zostać dodany, a następnie skorzystać z odpowiedniego polecenia w menu podręcznym.

Aby dodać nowy folder do sekcji Widoki własne

1. W oknie **Atlas sieci** wybierz pozycję w sekcji *Widoki własne*, w której chcesz dodać nowy folder.
2. Kliknij tę pozycję prawym przyciskiem myszy, w menu podręcznym wskaż polecenie **Nowy**, a następnie wybierz polecenie **Folder mapy**.
3. Wpisz nazwę nowo tworzonej grupy.

Przenoszenie folderu

Przeniesienia folderu dokonuje się poprzez jego przeciągnięcie i upuszczenie w żądanym miejscu.

Aby przenieść folder do innego miejsca w sekcji Widoki własne

1. W oknie **Atlas sieci** przeciągnij nazwę folderu, którego położenie chcesz zmienić, i upuść ją w wybranym nowym miejscu.

Usuwanie folderu

Chcąc usunąć folder z sekcji *Widoki własne*, należy kliknąć prawym przyciskiem myszy jego nazwę, a następnie wybrać odpowiednie polecenie z menu podręcznego.

Aby usunąć folder z sekcji Widoki własne

1. W oknie **Atlas sieci** wybierz folder, który chcesz usunąć.
2. Kliknij prawym przyciskiem myszy jego nazwę, a następnie z menu podręcznego wybierz polecenie **Usuń**.
3. Wyświetlone zostanie teraz okno potwierdzenia, ostrzegające, że dany folder i wszystkie należące do niego mapy zostaną usunięte. Kliknij przycisk **Tak**, aby przejść dalej.

Zmiana nazwy folderu

W sekcji *Widoki własne*, oprócz dodawania, przenoszenia i usuwania folderu, możliwa jest także zmiana jego nazwy.

Aby zmienić nazwę folderu w sekcji Widoki własne

1. W oknie **Atlas sieci** wybierz folder, którego nazwę chcesz zmienić.
2. Kliknij go prawym przyciskiem myszy, a następnie z menu podręcznego wybierz polecenie **Zmień nazwę**.
3. Wpisz nową nazwę folderu.

Dodawanie i usuwanie węzłów

Aby objąć dany węzeł monitorowaniem (dodać go do zbioru węzłów monitorowanych) lub zaprzestać jego monitorowania (usunąć go z tego zbioru), należy wybrać odpowiednie polecenie z menu. Podczas dodawania nowego węzła do zbioru węzłów monitorowanych będzie on zawsze dołączany do tabeli *Wykaz węzłów*, zawierającej listę wszystkich monitorowanych węzłów atlasu.

Aby objąć dany węzeł monitorowaniem

1. W menu **Narzędzia** wskaż pozycję **Zadania**, a następnie wybierz polecenie **Dodaj węzeł do monitorowania**.
2. Wpisz adres IP lub nazwę DNS węzła, który chcesz monitorować.

Uwagi

- *Jeżeli dany węzeł należy do sieci, która już jest monitorowana, zostanie on automatycznie wstawiony na mapę w sekcji* Sieci IP.
- *Jeżeli dany węzeł należy do sieci, która jest programowi nieznana, wówczas do sekcji* Sieci IP *zostanie dodana nowa mapa sieci. Będzie ona zawierać tylko ten nowo dodany węzeł.*

Aby zaprzestać monitorowania danego węzła

1. Na mapie w sekcji *Sieci IP* lub na widoku *Wykaz węzłów* wybierz węzeł, który chcesz usunąć.

2. Kliknij ten węzeł prawym przyciskiem myszy, a następnie z menu podręcznego wybierz polecenie **Usuń**.
3. Kliknij przycisk **Tak**, aby potwierdzić usunięcie.

Uwaga

Usuwany węzeł zostanie także automatycznie usunięty ze wszystkich pozostałych map (tzn. z map w sekcji Widoki własne*, do których węzeł ten należał).*

Włączanie i wyłączanie monitorowania atlasu

Włączanie lub wyłączanie monitorowania atlasu odbywa się w sposób prosty i natychmiastowy. Wyłączenie monitorowania atlasu oznacza, że program nie będzie przeprowadzał w danym atlasie jakiegokolwiek rodzaju monitorowania, nie będzie sprawdzał włączonych zdarzeń, ani nie będzie gromadził żadnych zapisów trendów bądź danych na potrzeby aktualnie włączonych raportów. Włączenie monitorowania atlasu powoduje wznowienie wszystkich wyżej wymienionych funkcji.

Aby włączyć lub wyłączyć monitorowanie atlasu

1. Aby wyłączyć monitorowanie atlasu, wybierz z menu **Atlas** polecenie **Wyłącz monitorowanie**.
   Aby włączyć monitorowanie atlasu, wybierz z menu **Atlas** polecenie **Włącz monitorowanie**.

Operacje pomocnicze

Eksport atlasu

Możliwe jest eksportowanie zarówno atlasu aktualnie otwartego, jak i takiego, który został już wcześniej zapisany. W ten sposób wszystkie informacje związane z określonym atlasem (dotyczące m.in. wszystkich jego map i węzłów) zostaną natychmiast wyeksportowane do pliku z rozszerzeniem `.NCB`. Możliwe jest również zadecydowanie, czy do eksportowanego pliku ma zostać włączony zapis trendów wydajności a także baza danych zdarzeń i baza danych haseł.

Aby wyeksportować atlas

1. W menu **Plik** wskaż polecenie **Eksportuj**, a następnie wybierz polecenie **Atlas**. Spowoduje to wyświetlenie okna **Eksportuj atlas**.
2. Na wyświetlanej liście zaznacz atlas, który chcesz wyeksportować.
3. Jeżeli chcesz, aby w eksportowanym pliku `.NCB` znalazły się zebrane dane dotyczące trendów wydajności, zaznacz pole wyboru **Zapis trendów wydajności**.

4. Jeżeli chcesz, aby w eksportowanym pliku `.NCB` znalazły się informacje o wszystkich wygenerowanych zdarzeniach, które do chwili uruchomienia eksportu zostały zapisane w bazie danych, zaznacz pole wyboru **Baza danych zdarzeń**.
5. Jeżeli chcesz, aby w eksportowanym pliku `.NCB` znalazła się baza danych haseł, zaznacz pole wyboru **Baza danych haseł**.
6. W polu **Nazwa pliku** wpisz wybraną przez siebie nazwę docelowego pliku `.NCB`, który zostanie zapisany przez program.
   Zamiast tego możesz kliknąć ikonę ***Przeglądaj***, aby wskazać ścieżkę i nazwę już istniejącego, wyeksportowanego pliku atlasu. W takim przypadku w standardowym oknie dialogowym **Otwórz** wpisz nazwę pliku w polu **Nazwa pliku**, a następnie kliknij przycisk **Otwórz**. Spowoduje to zamknięcie okna dialogowego.
7. Kliknij przycisk **Eksportuj**. Program NetCrunch rozpocznie eksport atlasu do tak określonego pliku. Po zakończeniu operacji eksportowania wyświetlone zostanie odpowiednie okno informacyjne.

Uwagi

- *Zbierane przez program dane o trendach zapisywane są dla każdego monitorowanego węzła należącego do aktualnie wybranego atlasu. Dla każdej usługi sieciowej, która jest monitorowana w jakimkolwiek węźle atlasu, gromadzone są dane o trendach pochodzące z trzech oddzielnych liczników: czas odpowiedzi (RTT) dla pakietów wysłanych, % pakietów utraconych oraz % pakietów odebranych.*
- *Po pomyślnym wyeksportowaniu atlasu do pliku `.NCB` można go w późniejszym czasie zaimportować z powrotem do programu. Więcej informacji na ten temat znajduje się poniżej, w rozdziale* Import atlasu.
- *Eksportowanie atlasu i tworzenie jego kopii zapasowej są niemal identyczne – w obu przypadkach tworzony jest plik z kopią zapasową atlasu, o rozszerzeniu `.NCB`. Jednakże eksport atlasu umożliwia zapisanie docelowego pliku w dowolnym katalogu w sieci. Natomiast podczas sporządzania kopii zapasowej atlasu plik `.NCB` jest zapisywany automatycznie w domyślnym katalogu kopii zapasowych NetCruncha określonym w opcjach programu (na stronie **Konserwacja**). Po zainstalowaniu programu, do tego domyślnego katalogu prowadzi ścieżka `..\DATA\BACKUP`, wiodąca z katalogu, w którym zainstalowany został sam program.*

Import atlasu

Wszelkie informacje o atlasie, które zostały wcześniej wyeksportowane, mogą w każdej chwili zostać z powrotem zaimportowane do programu. W tym celu wystarczy wskazać ścieżkę katalogu i nazwę zapisanego pliku z kopią zapasową atlasu (pliku o rozszerzeniu `.NCB`).

Aby zaimportować atlas

1. Z menu **Plik** wybierz polecenie **Importuj**. Spowoduje to otwarcie okna **Wybierz plik kopii zapasowej**.
2. Zaznacz plik z kopią zapasową atlasu (o rozszerzeniu `.NCB`) lub wpisz nazwę pliku bezpośrednio w polu **Nazwa pliku**.

3. Kliknij przycisk **Otwórz**.
   Okno **Wybierz plik kopii zapasowe** zostanie zamknięte, natomiast pojawi się okno **Importuj atlas z pliku kopii zapasowej**.
4. Jeżeli chcesz zaimportować wszystkie zdarzenia z bazy danych, zaznacz pole wyboru **Baza danych zdarzeń**.
5. Jeżeli chcesz również zaimportować z danego pliku wszystkie znajdujące się w nim zapisy trendów wydajności, zaznacz pole wyboru **Zapis trendów wydajności**.
6. Jeżeli chcesz również zaimportować z danego pliku bazę danych haseł, zaznacz pole wyboru **Baza danych haseł**.
7. Klinknij przycisk **Importuj**.
   Spowoduje to otwarcie okna potwierdzenia, informującego, że aby kontynuować, należy zamknąć aktualnie otwarty atlas.
8. Kliknij przycisk **Tak**.
   Wybrany plik zostanie zaimportowany. Po ukończeniu tej operacji wyświetlone zostanie niewielkie okno informujące, że przywracanie atlasu zostało zakończone.

Uwagi

- *Import atlasu i przywracanie go to dwie różne operacje, pomimo że obie wykorzystują wcześniej zapisany plik kopii zapasowej o rozszerzeniu* `.NCB`*. Operacja przywracania atlasu zastępuje (nadpisuje) aktualnie otwarty atlas (z wyjątkiem sytuacji, gdy przywracany jest atlas, który został wcześniej usunięty). Natomiast operacja importowania jedynie zamyka aktualnie otwarty atlas i tworzy całkowicie nowy atlas, zawierający dane z importowanego pliku.*
- *Atlas może zostać zaimportowany z dowolnego pliku* `.NCB` *zapisanego w katalogu sieciowym. Natomiast plik* `.NCB` *wykorzystywany podczas przywracania atlasu musi znajdować się w przeznaczonym do tego celu domyślnym katalogu kopii zapasowych programu NetCrunch. Po zainstalowaniu programu, do tego domyślnego katalogu prowadzi ścieżka* `..\DATA\BACKUP`*, wiodąca z katalogu, w którym zainstalowany został sam program. Ścieżka ta może zostać dowolnie zmieniona w opcjach programu (na stronie* ***Konserwacja****).*
- *Do programu NetCrunch można również zaimportować mapy sporządzone za pomocą narzędzia Ipswitch WhatsUp (poprzednio noszącego nazwę WhatsUp Gold) – program utworzy wówczas automatycznie nowy atlas. W tym celu w menu* ***Plik*** *należy wskazać polecenie* ***Importuj****, a następnie wybrać polecenie* ***Mapy z programu WhatsUp****.*

Sporządzanie kopii zapasowej atlasu

Wszelkie informacje wyświetlane w otwartym atlasie mogą być zapisywane w kopii zapasowej – sporządzanej na żądanie lub w określonych odstępach czasu. Kopia zapasowa sporządzana za pomocą programu NetCrunch zawiera takie istotne informacje, jak wykaz wszystkich map i węzłów, ich charakterystyki związane z monitorowaniem, w tym m.in. informacje o trendach, a także informacje o zdarzeniach zbierane dla potrzeb alertowania i raportowania. Podczas tworzenia kopii zapasowej użytkownik ma oczywiście możliwość zadecydowania o niewłączaniu do niej generowanych przez program zdarzeń lub zapisu trendów. Sporządzanie kopii zapasowej atlasu bardzo przypomina jego eksportowanie – w obu

metodach informacje o atlasie zapisywane są w tworzonym przez NetCruncha specjalnym pliku kopii zapasowej o rozszerzeniu `.NCB`.

Każda kopia zapasowa zapisana przez program może oczywiście zostać później przywrócona. Więcej informacji na ten temat można znaleźć w rozdziale *Przywracanie atlasu* na stronie 135.

Uwaga

Podczas tworzenia kopii zapasowej zawartość atlasu jest automatycznie zapisywana w domyślnym katalogu, do którego prowadzi ścieżka `..\DATA\BACKUP`*, wiodąca z katalogu, w którym zainstalowany został sam program. Jednak tą ścieżkę można dowolnie zmienić w opcjach programu (na stronie* ***Konserwacja*****).**

Aby sporządzić „na żądanie" kopię zapasową atlasu

1. W lewej części okna programu kliknij prawym przyciskiem myszy nazwę atlasu, stanowiącą korzeń drzewa atlasu (znajdującą się na samej górze widoku tego drzewa), a następnie z menu podręcznego wybierz polecenie **Właściwości**. Spowoduje to wyświetlenie okna **Właściwości atlasu**.
2. W górnej części okna kliknij kartę **Kopie zapasowe**. Wyświetlone zostaną na niej informacje związane z tworzeniem kopii zapasowej atlasu.
3. Aby do pliku kopii zapasowej dołączyć wszelkie zapisy trendów wydajności związane z danym atlasem, zaznacz pole wyboru **Zapis trendów wydajności**.
4. Aby do pliku kopii zapasowej dołączyć informacje o wszystkich wygenerowanych zdarzeniach, które zostały zapisane w bazie danych, zaznacz pole wyboru **Baza danych zdarzeń**.
5. Aby do pliku kopii zapasowej dołączyć hasła zapisane w obecnym atlasie, zaznacz pole wyboru **Baza danych haseł**.
6. Kliknij przycisk **Wykonaj teraz**, aby natychmiast rozpocząć operację tworzenia kopii zapasowej aktualnie otwartego atlasu. Po jej zakończeniu wyświetlone zostanie okno ze stosowną informacją.

Uwaga

Innym sposobem natychmiastowego utworzenia kopii zapasowej aktualnie otwartego atlasu jest wybranie z menu ***Plik*** *polecenia* ***Utwórz kopię zapasową****.*

Aby zaplanować harmonogram tworzenia kopii zapasowej atlasu w regularnych odstępach czasu

1. W lewej części okna kliknij prawym przyciskiem myszy nazwę atlasu, stanowiącą korzeń drzewa atlasu sieci (znajdującą się na samej górze widoku tego drzewa), a następnie z menu podręcznego wybierz polecenie **Właściwości**. Spowoduje to wyświetlenie okna **Właściwości atlasu**.
2. W górnej części okna kliknij kartę **Kopie zapasowe**.
3. Aby umożliwić programowi automatyczne sporządzanie kopii zapasowej, zaznacz pole wyboru **Włącz automatyczne tworzenie kopii zapasowej atlasu**.

4. W obszarze **Uruchom** określ częstotliwość, z jaką sporządzana ma być kopia zapasowa – wykorzystując do tego celu pole **Co** oraz związaną z nim listę rozwijaną. Można wybrać opcję tworzenia kopii zapasowej w godzinnych, dziennych lub tygodniowych odstępach czasu.
5. W polu **Początek** określ termin początku cyklu tworzenia kopii zapasowych. Tam gdzie jest to możliwe, z listy rozwijanej wybierz dzień tygodnia, od którego ma się rozpocząć tworzenie kopii zapasowych.
6. Aby do pliku kopii zapasowej dołączyć wszelkie dane dotyczące trendów wydajności, zaznacz pole wyboru **Zapis trendów wydajności**.
7. Jeżeli chcesz, aby do pliku kopii zapasowej dołączone zostały informacje o wszystkich wygenerowanych zdarzeniach, które zostały zapisane w bazie danych, zaznacz pole wyboru **Baza danych zdarzeń**.
8. Aby do pliku kopii zapasowej dołączyć hasła zapisane w obecnym atlasie, zaznacz pole wyboru **Baza danych haseł**.
9. W polu **Ilość kopii zapasowych do przechowywania** określ maksymalną liczbę kopii, które mają być przechowywane na dysku. Na przykład wpisanie liczby 3 oznacza, że na dysku przechowywane będą tylko trzy ostatnio utworzone kopie zapasowe. Jeśli sporządzisz następnie kolejną kopię zapasową, najstarszy istniejący plik z kopią zapasową zostanie automatycznie usunięty.

Uwaga

*Maksymalna liczba kopii zapasowych przechowywanych na dysku (określona w punkcie 9.) ma zastosowanie również w sytuacji, gdy użytkownik klika bezpośrednio przycisk **Wykonaj teraz**.*

Przywracanie atlasu

Dowolna kopia zapasowa atlasu, czy to utworzona automatycznie (zgodnie z harmonogramem), czy „na żądanie", może w późniejszym czasie zostać przez użytkownika przywrócona.

W celu przywrócenia określonego atlasu należy otworzyć okno **Przywróć atlas**. Zapisane kopie zapasowe atlasów pogrupowane są na liście według nazw atlasów. Pod każdą nazwą atlasu wyszczególnione są wszystkie sporządzone kopie zapasowe tego atlasu, uporządkowane według daty ich utworzenia. Ponadto w oddzielnej sekcji zebrane zostały wszystkie kopie zapasowe atlasów, które zostały usunięte.

Aby przywrócić kopię zapasową atlasu

1. Z menu **Plik** wybierz plecenie **Przywróć**.
   Spowoduje to wyświetlenie okna **Przywróć atlas**.
2. Pojawi się w nim, pod nazwą wybranego atlasu, lista sporządzonych i zapisanych kopii zapasowych tego atlasu, posortowana według daty ich utworzenia.
3. Zaznacz datę utworzenia tej kopii zapasowej atlasu, którą zamierzasz przywrócić. Dodatkowe informacje dotyczące zaznaczonego pliku kopii zapasowej atlasu podawane

są w obszarze **Szczegóły** (w tym m.in. dokładna data jego utworzenia oraz skrócony opis samego atlasu).

4. Jeżeli chcesz przywrócić zdarzenia z bazy danych zapisanej w kopii zapasowej atlasu, zaznacz w obszarze **Przywróć** pole wyboru **Baza danych zdarzeń**.
5. Jeżeli chcesz z kopii zapasowej atlasu przywrócić dane o trendach, zaznacz w obszarze **Przywróć** pole wyboru **Zapis trendów wydajności**.
6. Jeżeli chcesz z kopii zapasowej atlasu przywrócić dane o hasłach, zaznacz w obszarze **Przywróć** pole wyboru **Baza danych haseł**.
7. Kliknij przycisk **Przywróć**, aby rozpocząć operację przywracania wybranego atlasu z pliku kopii zapasowej.
   Pojawi się okno potwierdzenia, informujące, że aktualnie otwarty atlas zostanie zamknięty.

Uwagi

- *Wszystkie pliki kopii zapasowej utworzone w programie NetCrunch mają rozszerzenie* `.NCB`. *Przywracanie plików kopii zapasowych może odbywać się tylko z domyślnego katalogu programu, do którego prowadzi ścieżka* `..\DATA\BACKUP`, *wiodąca z katalogu, w którym zainstalowany został sam program NetCrunch. Jednak tą ścieżkę można dowolnie zmienić w opcjach programu (na stronie* ***Konserwacja****).*

Reguły atlasu

Alertowanie

Program NetCrunch umożliwia konfigurowanie alertowania na trzech poziomach – węzła, mapy oraz całego atlasu. Jeżeli włączanie alertów odbywa się na poziomie mapy lub atlasu, czynność ta określana jest jako tworzenie reguł alertowania. Niemniej jednak procedura definiowania zdarzeń, ich włączania albo wyłączania lub kojarzenia ze zdarzeniem określonego zestawu akcji, przeprowadzana jest zawsze w taki sam sposób – bez względu na to, czy odbywa się to na poziomie atlasu, mapy czy węzła.

Aby ułatwić procedurę konfiguracji alertów, program został wyposażony w gotowy, wstępnie zdefiniowany zestaw najważniejszych rodzajów zdarzeń, takich jak URZĄDZENIE NIE ODPOWIADA, HTTP NIE ODPOWIADA itp. Natomiast o tym, jak utworzyć nowy rodzaj zdarzenia, traktuje rozdział *Definiowanie nowych zdarzeń* na stronie 34.

Jeżeli określone zostały reguły alertowania dla danego atlasu, oznacza to, że dane dotyczące włączonych zdarzeń będą zbierane dla wszystkich węzłów należących do tego atlasu. Oznacza to również, że gdy w którymkolwiek z węzłów atlasu wystąpią tego rodzaju zdarzenia, podjęte zostaną odpowiednie skojarzone z nimi akcje (o ile takowe zostały zdefiniowane).

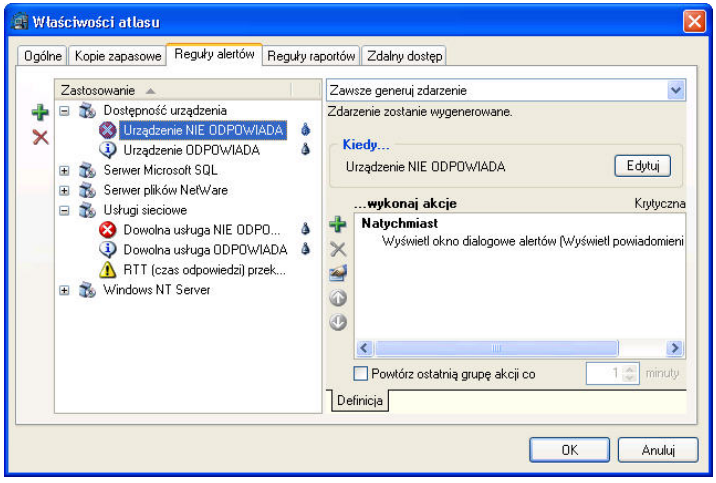
Aby określić lub zmienić reguły alertowania dla atlasu

1. Z menu **Atlas** wybierz polecenie **Reguły alertów**.

2. W oknie **Konfiguracja alertów** wykonaj czynności związane z alertowaniem.
   W lewym panelu możesz wybrać lub dodać nowe zdarzenia.
   W górnej części prawego panelu możesz włączyć lub wyłączyć generowanie aktualnie wybranego zdarzenia. W prawym panelu możesz również zdefiniować i skojarzyć z aktualnie wybranym zdarzeniem odpowiednie akcje.

Uwaga

Więcej informacji na temat alertowania zawiera rozdział Alertowanie *na stronie 19.*



Rys. 12 Okno Właściwości atlasu – karta Reguły alertów

Raportowanie

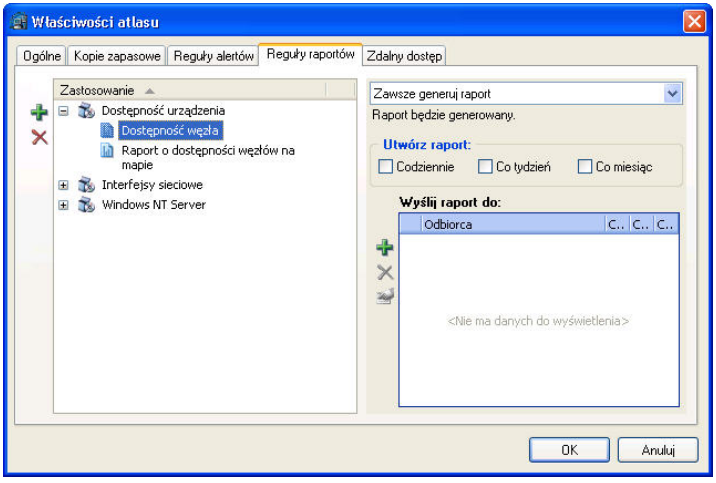
Funkcja raportowania obejmuje zbieranie odpowiednich danych i późniejsze ich prezentowanie w przejrzystej postaci, np. w formie tabeli lub wykresu. NetCrunch umożliwia konfigurowanie raportowania na trzech poziomach – dla całego atlasu, dla wybranej mapy lub dla wybranego węzła. Jeżeli włączanie raportu odbywa się na poziomie mapy lub atlasu, oznacza to, że w ten sposób dla takiego obiektu tworzone są reguły raportów. Włączenie danego raportu dla atlasu oznacza, że w ramach tego atlasu zbierane będą wszelkie niezbędne dane (uzależnione od wybranego rodzaju raportu).

Ogólne procedury stosowane na wszystkich trzech poziomach wyglądają tak samo. Użytkownik może włączyć lub wyłączyć określony raport (w przypadku atlasu, mapy lub węzła) lub zdecydować o dziedziczeniu odpowiednich ustawień (tylko w przypadku mapy lub węzła). W tym ostatnim przypadku to czy dany raport jest włączony, czy też nie, będzie wyznaczone przez ustawienia określone dla obiektu na wyższym poziomie w hierarchii obiektów programu (czyli dla atlasu lub mapy). Włączenie danego rodzaju raportu oznacza, że NetCrunch zacznie zbierać wszelkie niezbędne dane, na podstawie których później utworzy w przeglądarce raportów odpowiednią tabelę lub wykres.

Aby ułatwić tworzenie raportów, NetCrunch został wyposażony w zestaw gotowych, wstępnie zdefiniowanych rodzajów raportów. Włączenie i wyłączanie raportów dla całego atlasu odbywa się w oknie **Właściwości atlasu** (znanym także pod nazwą **Konfiguracja raportów**). Ponadto program umożliwia określenie częstotliwości generowania raportu dla danego atlasu oraz zdecydowanie, do kogo i jak często ma on być przesyłany.

Aby ustanowić reguły raportowania dla atlasu

1. Z menu **Atlas** wybierz polecenie **Reguły raportów**.
2. W oknie **Właściwości atlasu** wykonaj odpowiednie czynności związane z raportowaniem.
   W lewej części okna możesz wybierać lub dodawać raporty. W prawej górnej części okna możesz skorzystać z listy rozwijanej, aby włączyć lub wyłączyć generowanie aktualnie wybranego raportu. W prawej części okna możesz określić, jak często ma on być generowany oraz do kogo ma być przesyłany po jego wygenerowaniu.



Rys. 13 Okno Właściwości atlasu – karta Reguły raportów

Uwagi

- *Więcej informacji na temat okna **Konfiguracja raportów**, włączania raportu, dodawania i usuwania odbiorców oraz zmiany ich parametrów zawiera rozdział* Przydzielanie raportów *na stronie 96.*
- *Po ustanowieniu reguł raportowania dla atlasu program rozpocznie zbieranie w tle wszelkich niezbędnych danych. Informacje te można później przeglądać i analizować w oknie **Przeglądarka raportów**, w postaci odpowiednich tabel lub wykresów (w tym celu należy kliknąć ikonę* **Raporty**, *znajdującą się na głównym pasku narzędzi).*

Właściwości zdalnego dostępu

Profile zdalnego dostępu służą do przechowywania odpowiednich praw dostępu do różnorodnych obiektów programu przy użyciu przeglądarki internetowej. Dzięki nim można

po prostu powiązać dany profil zdalnego dostępu ze zdefiniowanym użytkownikiem, przyznając mu tym samym ściśle sprecyzowane prawa dostępu do funkcji programu w zakresie niezbędnym do wykonywania określonych czynności administracyjnych.

W przypadku zdefiniowanego już profilu zdalnego dostępu możliwe jest sprawne edytowanie różnorodnych praw dostępu związanych z obiektem atlasu. Odbywa się to w oknie **Właściwości atlasu** związanym z mapą poprzez wybór karty **Zdalny dostęp**.

Aby zmodyfikować uprawnienia zdefiniowane w profilu zdalnego dostępu dla atlasu

1. W menu **Atlas** wskaż pozycję **Właściwości**.
   Otworzy się okno **Właściwości atlasu**.
2. Kliknij kartę **Zdalny dostęp**.
3. Z listy **Dostępne profile zdalnego dostępu** wybierz zdalny profil, który ma zostać zmodyfikowany.
   Poniżej zostaną wyświetlone aktualnie obowiązujące prawa dostępu do obiektów atlasu (należące do zaznaczonego profilu zdalnego dostępu).
4. Aby dodać nowe prawo, kliknij ikonę ***Dodaj uprawienie*** a następnie w nowo otwartym oknie **Właściwości praw dostępu** określ docelowe prawa dostępu do obiektu atlasu.
   Aby zmodyfikować właściwości istniejącego prawa dostępu, wskaż go na liście i kliknij ikonę ***Edytuj uprawnienie***. W oknie **Właściwości praw dostępu** dokonaj stosownych zmian.
   Aby usunąć istniejące prawo dostępu, wskaż je na liście i kliknij ikonę ***Usuń uprawnienie***.

Uwagi

- *Możliwe jest zmienianie praw dostępu dla dowolnej ilości węzłów zdefiniowanych w profilu zdalnego dostępu – służy do tego funkcja wielokrotnego wyboru. W tym celu należy przed podjęciem kroków opisanych w punkcie 1 wybrać wszystkie docelowe węzły na mapie.*
- *Należy pamiętać, że zmiany dokonywane w prawach dostępu – i zapisywaniu ich w profilu zdalnego dostępu – obejmują swym zasięgiem wszystkich zdalnych użytkowników skojarzonych z danym profilem.*
- *W celu uzyskania dodatkowych informacji związanych z profilach zdalnego dostępu, por. sekcję* Zarządzanie profilami zdalnego dostępu *na stronie 196, a także wszystkie kolejne sekcje.*

Zarządzanie węzłem

Właściwości

NetCrunch umożliwia zmianę kilku ogólnych właściwości związanych z określonym węzłem. W tym celu należy otworzyć okno **Właściwości węzła** i kliknąć kartę **Ogólne**. Na karcie tej udostępnione są następujące właściwości:

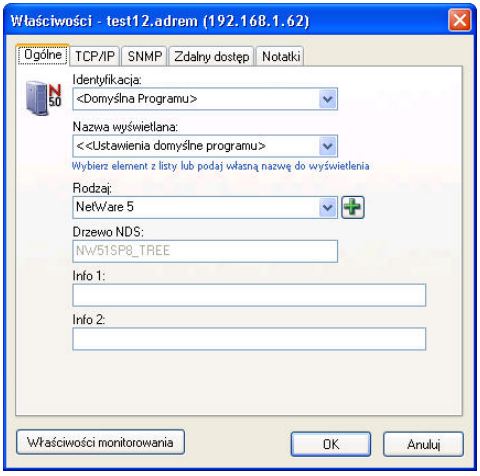
Identyfikacja	Węzeł może być identyfikowany albo poprzez jego nazwę, albo poprzez adres IP – w zależności od tego, czy wykorzystuje on adresowanie dynamiczne, czy statyczne. Jeżeli w polu identyfikacji wpisany zostanie adres IP, wówczas program przeprowadzi rozpoznanie nazwy węzła. Natomiast w innych przypadkach dokona rozpoznania adresu IP. Jeżeli wpisany adres IP dla danej nazwy urządzenia nie będzie mógł być rozpoznany za pomocą usługi DNS, wówczas stan węzła ulegnie zmianie na NIE ODPOWIADA
Nazwa wyświetlana	Nazwa wpisana w tym polu będzie zawsze wyświetlana przy danym węźle na mapie. Jeżeli pole to pozostanie puste, wówczas stosowana będzie domyślna, konwencjonalna nazwa urządzenia.
Rodzaj	Pole to określa rodzaj monitorowanego węzła i umożliwia użytkownikowi przypisanie do niego ikony, za pomocą której węzeł ten będzie przedstawiany na mapie.
Domena/Drzewo NDS	W polu tym, o właściwościach „tylko do odczytu", podawany jest nazwa domeny Windows lub nazwa drzewa NDS, do której należy węzeł.
Info1	Dodatkowe pole do wykorzystania przez użytkownika – może być do niego wpisana dowolna informacja. Wpisanie w tym polu dodatkowej, określonej przez użytkownika informacji umożliwia na mapie widoku filtrowanego pogrupowanie węzłów o zbliżonych cechach (o takiej samej zawartości pola Info1).
Info2	Dodatkowe pole do wykorzystania przez użytkownika – może być do niego wpisana dowolna informacja. Wpisanie w tym polu dodatkowej, określonej przez użytkownika informacji umożliwia na mapie widoku filtrowanego pogrupowanie węzłów o zbliżonych cechach (o takiej samej zawartości pola Info2).

Uwaga

Możliwe jest również zaznaczenie wielu węzłów i równoczesne wprowadzenie zmian w ich właściwościach.

Aby zmienić ogólne właściwości węzła

1. Zaznacz wybrany węzeł.
2. Kliknij ten węzeł prawym przyciskiem myszy, a następnie z menu podręcznego wybierz polecenie **Właściwości**.
3. Jeżeli chcesz, aby program identyfikował węzeł według nazwy, w polu **Identyfikacja** wpisz nazwę DNS.
4. W polu **Nazwa wyświetlana** wpisz nazwę, która ma być wyświetlana wraz z danym węzłem, lub pozostaw to pole puste.
5. Wybierz ikonę węzła, korzystając z listy rozwijanej **Rodzaj**.
6. W polach **Info1** i **Info2** wpisz dodatkowe informacje.



Aby równocześnie zmienić właściwości ogólne wielu węzłów

1. Zaznacz wybrane węzły. (Możesz tego dokonać klikając poszczególne węzły przy wciśniętym klawiszu **Ctrl**.)
2. Kliknij prawym przyciskiem myszy dowolny z zaznaczonych węzłów, a następnie z menu podręcznego wybierz polecenie **Właściwości**.
3. W odpowiednich polach wprowadź zmiany, które uznasz za stosowne.

Uwagi

- *Dla wybranych w ten sposób węzłów te pola, które oznaczone są ikoną* **Kłódka**, *nie zostanie zmienione.*
- *Jeżeli w danym polu wprowadzone już zostały pewne zmiany, a chcemy z nich zrezygnować i pozostawić to pole w stanie niezmienionym, należy kliknąć ikonę* **Zaznaczenie**, *znajdującą się na lewo od takiego pola. Ikona* **Zaznaczenie** *zmieni się na ikonę* **Kłódka**, *wskazując, że dla wszystkich wybranych węzłów dane pole zostanie pozostawione w stanie niezmienionym.*
- *Informacja we wszystkich tych polach, które zostały zmienione, wyświetlana będzie czcionką pogrubioną, aby wyróżnić w ten sposób wprowadzone zmiany.*
- *Aby dodać definicję nowego urządzenia na podstawie rodzaju wybranego węzła, należy kliknąć ikonę* ***Dodaj****, znajdującą się na prawo od listy rozwijanej* ***Rodzaj****, a następnie postępować zgodnie z wyświetlanymi wskazówkami. Więcej informacji na ten temat zawiera rozdział Dodawanie nowej definicji urządzenia na stronie 246.*

Właściwości TCP/IP

Otwarcie okna **Właściwości** i kliknięcie karty **TCP/IP** wyświetla informacje na temat węzła jak również sieci, do której należy. Uściślając, prezentowane są wówczas następujące informacje:

Adres IP	Pole określa adres IP węzła w sieci.
Maska sieciowa	Pole określa maskę sieciową sieci IP, do której należy dany węzeł.
Nazwa	Pole określa nazwę węzła w sieci.
Adres sprzętowy	Pole o właściwościach „tylko do odczytu", określające adres sprzętowy (MAC) węzła. Adres fizyczny jest dostępny wyłącznie w przypadku segmentów sieci lokalnej.

Uwagi

- *Dostępne na węźle pola **Adres IP** i **Nazwa** można modyfikować – w takim wypadku zmieniane są wszystkie zawarte w NetCrunchu odniesienia do tego węzła.*
- *Możliwe jest zmienianie maski sieciowej węzła poprzez bezpośrednie wpisanie jej w odpowiednim polu na tej karcie. Jeśli taka nowa sieć IP, w której znajduje się dany węzeł, nie jest wyświetlana na liście, to wówczas zostanie automatycznie dodana do sekcji **Sieci IP** okna **Atlas sieci**.*

Właściwości zarządzania poprzez agenta SNMP

Program NetCrunch umożliwia użytkownikowi łatwe włączanie w węźle zarządzania za pomocą agenta SNMP. Możliwe jest również dla takiego węzła określenie wspólnoty odczytu i zapisu SNMP. Oba te ustawienia dają użytkownikom uprawnienia do przeglądania lub zmiany niektórych informacji za pomocą usługi SNMP.

Jeżeli włączone jest zarządzanie węzłem za pomocą agenta SNMP, wówczas taki węzeł pojawi się na widoku SNMP dowolnej mapy (po kliknięciu karty **SNMP**, znajdującej się u dołu obszaru podglądu). Jeżeli oprócz tego określona została prawidłowa wspólnota odczytu, to otwarcie okna widoku SNMP umożliwi przeglądanie wszystkich informacji SNMP na temat danego węzła. Jeżeli natomiast określona została również prawidłowa wspólnota zapisu, to użytkownik będzie miał możliwość zmiany niektórych informacji SNMP dotyczących danego węzła.

Uwagi

- *Szybszym sposobem na zmianę określonych właściwości węzłów na mapie jest zaznaczenie na dowolnej mapie kilku węzłów i za pomocą jednego okna wprowadzenie zmiany właściwości SNMP we wszystkich zaznaczonych węzłach.*
- *Gdy na mapie zostają umieszczone nowe węzły z agentami SNMP – na skutek ich wykrycia lub gdy umieszcza je ręcznie użytkownik – mogą one mieć automatycznie przypisywane domyślne właściwości zarządzania przy użyciu SNMP (czyli numer portu SNMP i profil SNMP). Funkcję tą należy uprzednio zdefiniować w opcjach programu. Por. sekcję* Ustawianie domyślnych właściwości monitorowania oraz zarządzania przez SNMP *na stronie 203 w celu uzyskania dodatkowych informacji.*
- *W oknie **Właściwości** dla węzła (przy wybranej karcie **SNMP**) można dodatkowo kliknąć ikonę* **Właściwości** *znajdującą się obok rozwijanej listy **Profil SNMP**, aby szybko utworzyć nowy profil SNMP bądź zmodyfikować lub usunąć już istniejący. Por. sekcję* Zarządzanie profilami SNMP *na stronie 238 w celu uzyskania dodatkowych informacji.*
  Aby przeglądać informacje o węźle za pośrednictwem protokołu SNMP na węźle powinien być zainstalowany agent SNMP. W przypadku braku takiego agenta, Nawet gdy zaznaczone jest pole

*wyboru **Urządzenie zarządzane przez SNMP** dla węzła, NetCrunch nie będzie w stanie pobrać tym sposobem żadnych danych o węźle.*

Właściwości zdalnego dostępu

Profile zdalnego dostępu służą do przechowywania odpowiednich praw dostępu w różnorodnych obiektów programu przy użyciu przeglądarki internetowej. Na kolejnym etapie można po prostu powiązać dany profil zdalnego dostępu zdefiniowanym użytkownikiem, przyznając mu tym samym ściśle sprecyzowane prawa dostępu do funkcji programu w zakresie niezbędnym do wykonywania określonych czynności administracyjnych.

W przypadku zdefiniowanego już profilu zdalnego dostępu możliwe jest sprawne edytowanie różnorodnych praw dostępu związanych z obiektem atlasu. Odbywa się to w oknie **Właściwości atlasu** związanym z mapą poprzez wybór karty **Zdalny dostęp**.

Aby zmodyfikować uprawnienia zdefiniowane w profilu zdalnego dostępu dla atlasu

1. Kliknij prawym przyciskiem myszy węzeł na mapie i w podręcznym menu wskaż pozycję **Właściwości**.
   Otworzy się okno **Właściwości** dla wybranego węzła.
2. Kliknij kartę **Zdalny dostęp**.
3. Z listy **Dostępne profile zdalnego dostępu** wybierz zdalny profil, który ma zostać zmodyfikowany.
   Poniżej zostaną wyświetlone aktualnie obowiązujące prawa dostępu do obiektów atlasu (należące do zaznaczonego profilu zdalnego dostępu).
4. Aby dodać nowe prawo, kliknij ikonę ***Dodaj uprawnienie*** a następnie w nowo otwartym oknie **Właściwości praw dostępu** określ docelowe prawa dostępu do obiektu atlasu.
   Aby zmodyfikować właściwości istniejącego prawa dostępu, wskaż go na liście i kliknij ikonę ***Edytuj uprawnienie***. W oknie **Właściwości praw dostępu** dokonaj stosownych zmian.
   Aby usunąć istniejące prawo dostępu, wskaż je na liście i kliknij ikonę ***Usuń uprawnienie***.

Uwagi

- *Możliwe jest zmienianie praw dostępu dla dowolnej ilości węzłów zdefiniowanych w profilu zdalnego dostępu – służy do tego funkcja wielokrotnego wyboru. W tym celu należy przed podjęciem kroków opisanych w punkcie 1 wybrać wszystkie docelowe węzły na mapie.*
- *Należy pamiętać, że zmiany dokonywane w prawach dostępu – i zapisywaniu ich w profilu zdalnego dostępu – obejmują swym zasięgiem wszystkich zdalnych użytkowników skojarzonych z danym profilem.*
- *W celu uzyskania dodatkowych informacji związanych z profilach zdalnego dostępu, por. sekcję* Zarządzanie profilami zdalnego dostępu *na stronie 196 a także wszystkie kolejne sekcje.*

Notatki węzła

Funkcja **Notatki węzła** umożliwia użytkownikom szybkie zapisywanie ważnych informacji o węźle i przechowywanie ich w postaci listy z zamiarem późniejszego zastosowania. Bezpośrednie dotarcie do notatek węzła jest możliwe w oknie właściwości danego węzła. W oknie tym (w karcie **Notatki**) można dodawać, zmieniać właściwości lub usuwać istniejące notatki węzła. Notatnik węzła składa się z tematu, daty utworzenia, kategorii i właściwych zapisków.

Aby zarządzać notatkami pojedynczego węzła

1. Kliknij prawym przyciskiem myszy węzeł na mapie i w jego podręcznym menu wybierz opcję **Właściwości**.
   Wyświetli się okno **Właściwości** wybranego węzła.
2. Kliknij kartę **Notatki**.
3. Aby dodać nową notatkę, kliknij ikonę ***Dodaj notatkę***, a następnie w oknie **Nowa notatka** wpisz informacje (temat, kategorię i zapiski).
   Aby edytować notatkę, wskaż ją na liście i kliknij ikonę ***Właściwości notatki***.
   Aby usunąć notatkę, wskaż ją na liście i kliknij ikonę ***Usuń***.

Uwaga

*Zarządzanie notatkami węzła (należącego do określonej mapy) może również odbywać się w oknie **Notatki węzła**. Por. sekcję Zarządzanie Notatnikiem węzła na stronie 184 w celu uzyskania szczegółowych informacji.*

Monitorowanie węzła

Właściwości monitorowania węzła mogą być w łatwy sposób zmieniane w specjalnym oknie **Monitorowanie**. Wszystkie dopuszczające modyfikację parametry zostały podzielone na kilka grup tematycznych, które mogą być wyświetlane po kliknięciu odpowiedniej karty w górnej części okna:

Ogólne	Ta karta umożliwia użytkownikowi całkowite włączenie lub wyłączenie monitorowania danego węzła. Użytkownik określa na niej także częstotliwość odpytywania monitorowanego węzła, a także dokładny okres czasu, w którym powinno ono następować. Możliwe jest także podanie informacji o tym, że dany węzeł jest zależny od innego węzła (i będzie w związku z tym monitorowany jedynie wówczas, gdy ten ostatni będzie działał prawidłowo).
Usługi sieciowe	Karta pozwala użytkownikowi określić, które z usług sieciowych mają być monitorowane w danym węźle. Usługi sieciowe przewidziane do monitorowania mogą być dodawane, usuwane, jak również mogą być zmieniane ich właściwości. Na karcie tej możliwe jest także automatyczne wykrywanie, jakie usługi sieciowe uruchomione są w poszczególnych węzłach, a następnie zapoczątkowanie ich monitorowania.

Wydajność Windows	Ta karta pozwala użytkownikowi włączać lub wyłączać monitorowanie związane z licznikami wydajności systemu Windows. Innymi słowy, jeżeli monitorowanie wydajności systemu Windows zostanie wyłączone, wówczas żadne tego rodzaju informacje nie będą przez NetCruncha zbierane, a liczniki związane z systemem Windows, dostępne na widoku Windows NT danej mapy, nie będą w ogóle uaktualnianie.
Wydajność SNMP	Ta karta pozwala użytkownikowi włączać lub wyłączać monitorowanie związane z informacjami o węźle uzyskiwanymi za pośrednictwem agenta SNMP. Jeżeli monitorowanie wydajności usługi SNMP jest wyłączone, oznacza to, że na widoku SNMP danej mapy nie będą uaktualniane żadne informacje SNMP.
Wydajność NetWare	Ta karta pozwala użytkownikowi włączać lub wyłączać monitorowanie związane z systemem NetWare. Jeżeli monitorowanie wydajności systemu NetWare jest wyłączone, wówczas na widoku NetWare danej mapy nie będą uaktualniane żadne informacje, które dotyczą danego węzła i związane są z systemem NetWare.
Linux/Unix	Ta karta umożliwia określenie nazwy użytkownika, hasła oraz hasła administratora systemu, służących do logowania do komputera pracującego pod kontrolą systemu Linux lub Unix, aby możliwe było podejmowanie na nim różnego rodzaju akcji, takich jak na przykład wykonywanie skryptów.
Zaawansowane	Wybór tej karty umożliwia określanie priorytetu monitorowania usług sieciowych oraz strategii wstrzymywania zdarzeń wywołanych zmianą stanu usługi sieciowej w momencie, gdy węzeł przestaje lub zaczyna odpowiadać. Ponadto pozwala na włączenie wstrzymywania zdarzeń związanych z usługą lub węzłem na wszystkich węzłach zależnych od wybranego węzła. W powyższej karcie można także określić wyjątek od reguły wstrzymywania zdarzeń na węźle. Por. sekcję *Opcje zaawansowane* na stronie 160 w celu uzyskania dodatkowych informacji.

W oknie **Monitorowanie** karty o nazwach **Ogólne** oraz **Usługi sieciowe** są w przypadku wszystkich węzłów zawsze dostępne. Natomiast karty **Wydajność Windows**, **Wydajność SNMP** oraz **Wydajność NetWare** mogą dla niektórych węzłów nie być dostępne. I tak na przykład dla węzła, w którym uruchomiony jest system operacyjny Windows oraz agent SNMP, dostępne będą tylko karty **Wydajność Windows** oraz **Wydajność SNMP**. Karta **Linux** pojawiać się będzie jedynie w przypadku, gdy dany węzeł pracuje pod kontrolą systemu operacyjnego Linux.

Opcje ogólne

Zmiana ogólnych opcji monitorowania dla danego węzła przeprowadzana jest w oknie **Monitorowanie**, na karcie **Ogólne**. W szczególności zmieniane mogą być następujące opcje:

- całkowite włączenie lub wyłączenie monitorowania w węźle,

- określenie częstotliwości monitorowania (jak często dany węzeł powinien być sprawdzany),
- podanie zakresu czasu, w którym program powinien monitorować dany węzeł,
- określenie danego węzła jako zależnego od innego monitorowanego węzła,
- włączenie lub wyłączenie uproszczonego monitorowania.

Uwaga

Użytkownik może na dowolnej mapie zaznaczyć wiele węzłów, aby w szybki sposób zmienić równocześnie niektóre spośród ich właściwości. Innymi słowy użytkownik może zaznaczyć na mapie więcej niż jeden węzeł i za pomocą jednego okna zmienić ogólne właściwości monitorowania we wszystkich zaznaczonych węzłach. Jest to na przykład wygodne w sytuacji, gdy chcemy w tym samym czasie szybko włączyć lub wyłączyć monitorowanie wszystkich wybranych węzłów.

Wyłączanie monitorowania węzła

Po wyłączeniu monitorowania sieci w danym węźle stan wszystkich określonych dla tego węzła usług sieciowych przestanie być sprawdzany. Nie będzie także monitorowana wydajność systemu Windows (w przypadku gdy węzeł pracuje pod kontrolą systemu operacyjnego Windows), wydajność systemu NetWare (w przypadku gdy w węźle uruchomiony jest system NetWare) ani wydajność mierzona za pomocą agentów SNMP. Jeżeli dany węzeł wyposażony jest w interfejsy sieciowe, one również nie będą monitorowane.

Czas monitorowania

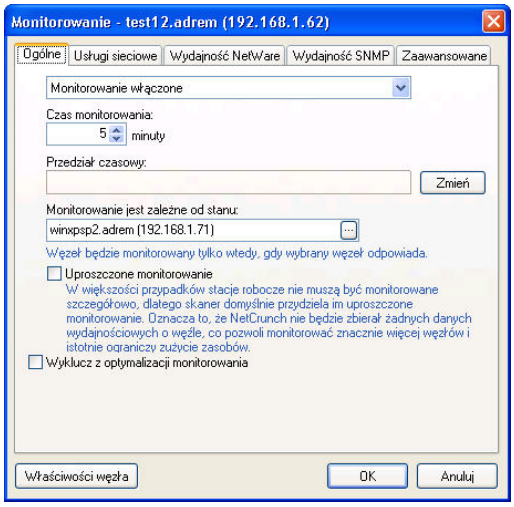
Czas monitorowania jest parametrem określającym, z jaką częstotliwością sprawdzany jest dany węzeł. Może on być w programie w łatwy sposób zmieniany. Należy przy tym pamiętać, że ze względu na to, iż program stosuje monitorowanie inteligentne, dokładny czas, po którym dany węzeł jest sprawdzany ulega wahaniom i w rzeczywistości jest wielkością zmienną. Ogólnie jednak dokładna wartość czasu monitorowania jest zbliżona do wartości zadanej.

Ponadto podany dokładny czas monitorowania wykorzystywany jest przez wszystkie rodzaje monitorowania danego węzła, w tym monitorowanie usług sieciowych, liczników wydajności Windows, liczników wydajności SNMP oraz liczników wydajności NetWare w tym węźle. Określa on, z jaką częstotliwością sprawdzany jest dany węzeł. Oczywiście, jeżeli tylko zachodzi taka potrzeba, istnieje możliwość określenia odrębnych czasów monitorowania dla liczników wydajności Windows, SNMP i NetWare. Możliwe jest również podanie zupełnie niezależnego czasu monitorowania dla określonej usługi sieciowej, która ma być monitorowana w danym węźle. Więcej informacji na ten temat zawiera rozdział *Monitorowanie usług sieciowych* na stronie 132.

Oprócz możliwości określenia częstotliwości monitorowania danego węzła, program NetCrunch pozwala również określić czas, w którym monitorowanie takiego węzła powinno być włączone. W szczególności użytkownik może wskazać dni tygodnia oraz dokładne pory dnia, w których program NetCrunch powinien przeprowadzać monitorowanie węzła.

Aby zmienić czas monitorowania węzła

1. Kliknij dany węzeł prawym przyciskiem myszy, w menu podręcznym wskaż pozycję **Monitorowanie**, a następnie wybierz polecenie **Właściwości**.
2. W polu **Czas monitorowania** wpisz, jak często dany węzeł powinien być sprawdzany.
3. Jeżeli chcesz sprecyzować porę dnia czy dni tygodnia, w których przeprowadzane powinno być monitorowanie, kliknij przycisk **Zmień**.
   Spowoduje to otwarcie okna **Zakres czasu**, w którym możesz uściślić okres monitorowania lub wprowadzić odpowiednie zakresy czasowe.



Aby równocześnie zmienić czas monitorowania kilku węzłów

1. W oknie **Widok sieci** zaznacz wszystkie te węzły, którym chcesz zmienić czas monitorowania.
2. Kliknij prawym przyciskiem myszy dowolny z zaznaczonych węzłów, w menu podręcznym wskaż pozycję **Monitorowanie**, a następnie wybierz polecenie **Właściwości**.
3. W polu **Czas monitorowania** wpisz, jak często (w minutach) wybrane węzły powinny być sprawdzane.
4. Jeżeli chcesz sprecyzować porę dnia czy dni tygodnia, w których przeprowadzane powinno być monitorowanie tych węzłów, kliknij przycisk **Zmień**.
   Spowoduje to otwarcie okna **Zakres czasu**, w którym możesz uściślić okres monitorowania lub wprowadzić odpowiednie zakresy czasowe.

Uwagi

- *Jeżeli po lewej stronie pola **Czas monitorowania** lub pola **Przedział czasowy** wyświetlana jest ikona **Kłódka**, oznacza to, że dla wybranych węzłów odpowiednie pole nie zostanie zmienione. Jeżeli natomiast po lewej stronie któregokolwiek z tych pól wyświetlana jest ikona **Zaznaczenie**, oznacza to, że dla wybranych węzłów odpowiednie pole zostanie zmienione.*
- *Jeżeli w danym polu wprowadzone już zostały pewne zmiany, a chcemy z nich zrezygnować i pozostawić to pole w stanie niezmienionym, wystarczy kliknąć ikonę **Zaznaczenie**, znajdującą się na lewo od takiego pola. Zmieni się ona wówczas z powrotem w ikonę **Kłódka**, wskazując, że dla wszystkich wybranych węzłów dane pole zostanie pozostawione w stanie niezmienionym.*
- *Informacje we wszystkich tych polach, które zostały zmienione, wyświetlane będą czcionką pogrubioną, aby odróżnić je od pól, w których nie zostały wprowadzone żadne zmiany.*

Określanie zależności pomiędzy węzłami

Niezwykle przydatną funkcją w programie jest opcja przypisywania określonemu monitorowanemu węzłowi zależności od innego węzła w aktualnie otwartym atlasie. W takim przypadku węzeł zależny będzie monitorowany jedynie wówczas, gdy węzeł, od którego jest on zależny, odpowiada (to znaczy znajduje się w stanie OK lub OSTRZEŻENIE). Gdy natomiast węzeł nadrzędny będzie znajdować się będzie w stanie NIE ODPOWIADA, węzeł zależny nie będzie monitorowany. W takim przypadku stan owego węzła zależnego zostanie zmieniony na NIEZNANY, a jego ikona zmieni kolor na szary. Ponadto możliwe jest zarządzanie wszelkimi zależnościami sieciowymi w atlasie – odbywa się to w oknie **Zależności sieciowe**. Więcej informacji na ten temat zawiera rozdział *Koncepcje zaawansowanego monitorowania węzłów* na stronie 217.

Aby przypisać węzłowi zależność od innego węzła

1. Kliknij dany węzeł prawym przyciskiem myszy, w menu podręcznym wskaż pozycję **Monitorowanie**, a następnie wybierz opcję **Właściwości**.
2. Korzystając z listy rozwijanej **Monitorowanie jest zależne od stanu:**, wybierz inny węzeł, od którego dany węzeł ma być zależny.

Uwaga

Węzły na liście rozwijanej uporządkowane są w kolejności alfabetycznej według nazw DNS.

Monitorowanie uproszczone

Jeżeli w danym węźle włączone zostało pełne monitorowanie, wówczas oprócz wszelkich usług sieciowych wykrytych w tym węźle, sprawdzane mogą być również różnego rodzaju liczniki wydajności, w które węzeł ten jest wyposażony. Liczniki wydajności uzależnione będą od rodzaju systemu operacyjnego uruchomionego w danym węźle oraz od tego, czy węzeł może być zarządzany za pomocą agenta SNMP. Liczniki takie wyświetlane są w oknie **Widok sieci**, po kliknięciu odpowiedniej karty (**Windows NT**, **SNMP** lub **NetWare**).

Aby umożliwić programowi monitorowanie większej ilości węzłów przy zmniejszonym wykorzystaniu zasobów, dla dowolnego węzła istnieje możliwość włączenia trybu monitorowania uproszczonego. Wybranie tej opcji dla danego węzła sprawia, że program nie zbiera żadnych danych nt. wydajności (związanych z system Windows, NetWare lub usługą SNMP). Monitorowane będą jedynie te usługi, które zostały już wcześniej wykryte w danym węźle (na przykład PING, HTTP lub FTP), jak również gromadzone będą w sposób ciągły związane z nimi dane o trendach, takie jak Czas odpowiedzi (RTT), % Dostępności czy % Utraconych pakietów.

Aby włączyć lub wyłączyć w węźle monitorowanie uproszczone

1. Kliknij dany węzeł prawym przyciskiem myszy, w menu podręcznym wskaż pozycję **Monitorowanie**, a następnie wybierz polecenie **Właściwości**.
2. Aby w danym węźle włączyć monitorowanie uproszczone, zaznacz pole wyboru **Monitorowanie uproszczone**.
   Aby w danym węźle wyłączyć uproszczone monitorowanie, usuń zaznaczenie w polu wyboru **Uproszczone monitorowanie**.

Uwagi

- *Domyślnie opcja uproszczonego monitorowania węzłów jest wyłączona (chyba że użytkownik przed przeprowadzeniem pierwotnego skanowania sieci za pomocą* Kreatora wykrywania sieci *określi inne jej ustawienia).*
- *W węźle, w którym włączone zostało uproszczone monitorowanie,* ***n i e b ę d ą*** *zbierane żadne dane o zdarzeniach na potrzeby alertowania lub raportowania. Aby skonfigurować dla danego węzła funkcję alertowania lub raportowania, konieczne jest wcześniejsze wyłączenie monitorowania uproszczonego dla takiego węzła.*
- *Aby za jednym razem włączyć lub wyłączyć uproszczone monitorowanie wielu węzłów, należy w oknie* ***Widok sieci*** *zaznaczyć wszystkie wybrane węzły, korzystając z klawisza* ***Ctrl****, a następnie przejść do wykonania czynności opisanych w punktach 1-2.*

Wykluczanie z optymalizacji monitorowania

Przed planowanym uruchomieniem kreatora *Optymalizacja monitorowania* możliwe jest indywidualne wyłączenie z takiej optymalizacji określonego węzła lub grupy węzłów. Czynność tę przeprowadza się w odpowiadającym danemu węzłowi oknie **Monitorowanie**, po wybraniu karty **Ogólne**.

Aby wykluczyć węzeł (węzły) z optymalizacji monitorowania

1. Zaznacz węzeł lub zaznacz równocześnie wiele węzłów, które chcesz wyłączyć z optymalizacji monitorowania.
2. Kliknij wybrany węzeł prawym przyciskiem myszy, w menu podręcznym wskaż pozycję **Monitorowanie**, a następnie wybierz polecenie **Właściwości**.
3. Zaznacz pole wyboru **Wyklucz z optymalizacji monitorowania**.

Uwagi

- *Aby włączyć optymalizację monitorowania dla danego węzła lub węzłów, wystarczy odznaczyć pole wyboru* ***Wyklucz z optymalizacji monitorowania****.*
- *Więcej informacji na temat korzystania z kreatora* Optymalizacja monitorowania *zawiera rozdział* Optymalizacja monitorowania *na stronie 52.*

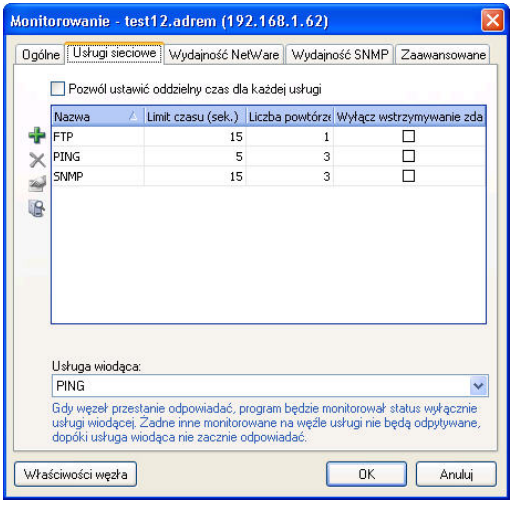
Monitorowanie usług sieciowych

Monitorowanie dowolnych usług sieciowych w danym węźle jest najbardziej podstawową metodą uzyskiwania informacji o jego aktualnym stanie. Oprogramowanie NetCrunch pozwala użytkownikowi na dodanie dowolnej liczby usług sieciowych (takich jak na przykład usługa PING, HTTP, FTP itp.) do listy monitorowanych usług. W łatwy sposób można również usługi sieciowe z takiej listy usunąć lub zmienić ich odpowiednie parametry monitorowania. Ponadto użytkownik ma możliwość szybkiego przeskanowania węzła w poszukiwaniu nowych usług sieciowych, które są w nim udostępniane (tak, aby mogły one zostać natychmiast dodane do aktualnej listy usług monitorowanych). Wreszcie możliwe jest – przy użyciu jednego polecenia menu – natychmiastowe sprawdzenie aktualnego stanu wszystkich usług sieciowych związanych z danym węzłem (znajdujących się na liście usług monitorowanych).

Przeglądanie aktualnie monitorowanych usług sieciowych w danym węźle

Jakikolwiek węzeł odpytywany przez NetCruncha pod kątem jego stanu musi z definicji udostępniać przynajmniej jedną usługę sieciową, która jest monitorowana (będzie się ona znajdować na liście usług monitorowanych w tym węźle). Oczywiście do takiej listy może zostać dodana lub z niej usunięta dowolna liczba innych usług sieciowych.

W celu ustalenia strategii monitorowania NetCrunch stosuje koncepcję wiodącej usługi sieciowej. Domyślnie wiodącą usługą sieciową wykorzystywaną przez program jest Ping. Jeżeli nie jest ona dostępna na danym węźle, program użyje w charakterze usługi wiodącej pierwszą usługę sieciową na liście usług monitorowanych na danym węźle. Możliwe jest jednakże przyznanie statusu usługi wiodącej dowolnej usłudze sieciowej dostępnej na liście monitorowanych usług – należy wówczas użyć rozwijanej listy **Usługa wiodąca** w oknie **Monitorowanie** węzła. W momencie kiedy wiodąca usługa sieciowa – oraz wszystkie inne monitorowane dotychczas usługi – staną się niedostępne (ich stan zmieni się na NIE ODPOWIADA), monitorowanie tych wszystkich pozostałych usług zostanie okresowo wstrzymane. Wyłączone zostanie również monitorowanie liczników wydajności na tym węźle. Ta ograniczona metoda monitorowania będzie kontynuowana – w celu zminimalizowania wykorzystania zasobów – do momentu, kiedy wiodąca usługa sieciowa znowu zacznie odpowiadać poprawnie. Wówczas monitorowanie pozostałych usług sieciowych i liczników wydajności powróci do poprzedniego stanu – będą one znowu monitorowane w normalnym trybie.



Aby zobaczyć, jakie usługi sieciowe są aktualnie monitorowane w danym węźle

1. Kliknij dany węzeł prawym przyciskiem myszy, w menu podręcznym wskaż pozycję **Monitorowanie**, następnie wskaż pozycję **Usługi sieciowe** i wybierz polecenie **Właściwości**.
   Spowoduje to wyświetlenie listy usług sieciowych aktualnie monitorowanych w tym węźle.

Uwagi

- *Gdy dla określonej usługi sieciowej na liście usług monitorowanych zaznaczone jest pole wyboru **Dodaj do wszystkich**, oznacza to, że dana usługa sieciowa jest lub będzie (jeżeli opcja ta właśnie została wybrana) monitorowana we wszystkich aktualnie wybranych węzłach sieci.*
- *Gdy dla określonej usługi sieciowej, znajdującej się na liście usług monitorowanych, pole wyboru **Dodaj do wszystkich** nie jest zaznaczone, oznacza to, że dana usługa sieciowa jest monitorowana jedynie na niektórych spośród aktualnie wybranych węzłów sieci (nie na wszystkich).*

- *Jeżeli na liście usług monitorowanych nazwa usługi sieciowej oraz którakolwiek ze związanych z nią właściwości wyświetlane są w kolorze szarym, zamiast (domyślnie) w czarnym, oznacza to, że dana właściwość monitorowania (limit czasu odpowiedzi [timeout], liczba powtórzeń czy czas monitorowania) jest w poszczególnych aktualnie wybranych węzłach zróżnicowana. Innymi słowy, takie właściwości jak timeout, liczba powtórzeń czy czas monitorowania, mają wśród aktualnie wybranych węzłów różne wartości.*

Dodawanie usług sieciowych do listy monitorowanych usług

Do listy usług monitorowanych w danym węźle dodawane mogą być różnego rodzaju usługi sieciowe. Jedynym wymogiem, który powinien być spełniony, jest to, aby dana usługa była zdefiniowana w programie. NetCrunch wyposażony został w rozbudowaną listę najczęściej wykorzystywanych usług sieciowych.

Podczas dodawania nowej usługi sieciowej do listy usług monitorowanych w danym węźle konieczne jest określenie kilku parametrów (pierwsze dwa spośród nich są zawsze dostępne, trzeci pojawia się jedynie wówczas, gdy wybrana została opcja różnych czasów monitorowania dla poszczególnych usług). W tabeli poniżej omówione zostały te trzy parametry.

Limit czasu odpowiedzi (Timeout)	Parametr ten określa maksymalny czas (w sekundach), przez jaki NetCrunch powinien czekać na odpowiedź od monitorowanej usługi sieciowej, zanim podejmie działania związane z przekroczeniem limitu czasu.
Liczba powtórzeń	Parametr ten określa ile pakietów powinno zostać wysłanych za każdym razem, gdy dana usług sieciowa w węźle jest sprawdzana.
Dodatkowa liczba powtórzeń	Parametr ten określa, ile pakietów powinno zostać wysłanych w przypadku, gdyby wszystkie dotychczas wysłane pakiety (zdefiniowane w polu **Liczba powtórzeń**) nie przyniosły odpowiedzi w trakcie sprawdzania usługi sieciowej.
Wyłącz wstrzymywanie zdarzeń na usługach sieciowych	Opcja zaawansowana – zaznaczenie tego pola wyboru umożliwia utworzenie wyjątku od reguły wstrzymywania zdarzeń związanych ze stanem usług sieciowych zdefiniowanej dla węzła. Por. sekcję *Tworzenie wyjątków od reguły wstrzymywania zdarzeń związanych ze stanem usługi* na stronie 159 w celu uzyskania dodatkowych informacji.
Czas monitorowania	Parametr ten umożliwia wybranie dokładnej częstotliwości monitorowania danej usługi sieciowej. Jeżeli opcja ta nie jest dostępna, oznacza to, że w przypadku określonej usługi sieciowej zastosowany zostanie domyślny czas monitorowania, określony na karcie **Ogólne** w oknie **Monitorowanie**, odnoszącym się do danego węzła.

Aby dodać usługę sieciową do listy usług monitorowanych na danym węźle

1. Kliknij dany węzeł prawym przyciskiem myszy, w menu podręcznym wybierz opcję **Monitorowanie**, następnie wskaż pozycję **Usługi sieciowe** i wybierz opcję **Właściwości**.
2. Jeżeli chcesz, aby w programie dla każdej usługi sieciowej ustawiony był indywidualny czas monitorowania, zaznacz pole wyboru **Chcę ustawić oddzielny czas dla każdej usługi**.
3. Kliknij znajdującą się po lewej stronie ikonę ***Dodaj***.
4. W oknie **Dodaj nową usługę** z listy rozwijanej **Nazwa** wybierz usługę sieciową, którą chcesz monitorować.
5. W polu **Timeout** wpisz wartość limitu czasu odpowiedzi (w sekundach), która będzie obowiązywać podczas każdorazowego odpytania monitorującego.
6. W polu **Liczba powtórzeń** określ dokładną liczbę pakietów, jaka ma być wysyłana podczas każdorazowego odpytania usługi sieciowej.
7. W polu **Dodatkowa liczba powtórzeń** określ liczbę dodatkowych pakietów, jakie będą wysyłane, gdy pakiety określone w polu **Liczba powtórzeń** nie przyniosą rezultatu.
8. Jeżeli w punkcie 2. wybrana została opcja różnych czasów monitorowania dla poszczególnych usług sieciowych, określ w polu **Czas monitorowania** częstotliwość, z jaką ta nowo dodawana usługa ma być sprawdzana. Jeżeli pole to nie jest dostępne, zamiast podawanej w nim wartości program NetCrunch zastosuje czas monitorowania określony na karcie **Ogólne** w oknie **Monitorowanie**.

Uwagi

- *Możliwe jest również równoczesne wybranie kilku węzłów i dodanie – za pomocą jednorazowych czynności podejmowanych w pojedynczym oknie – nowych usług sieciowych do list usług monitorowanych w tych węzłach. W tym celu w oknie **Widok sieci** należy zaznaczyć wybrane węzły, korzystając z klawisza **Ctrl**. Następnie należy przejść do wykonania opisanych powyżej czynności.*
- *Nowo dodana usługa sieciowa wyświetlana jest na liście pogrubioną czcionką, tak aby była ona łatwo zauważalna.*
- *Ze względu na specyfikę protokołów usług sieciowych opartych na protokole UDP sugeruje się wysyłanie za jednym razem co najmniej trzech pakietów (w polu **Liczba powtórzeń** należy wpisać wartość co najmniej 3).*
- *W protokołach opartych na protokole TCP przewidziany może być dłuższy czas połączenia, zatem zalecane jest ustawienie limitu czasu odpowiedzi (w polu **Timeout**) na wartość co najmniej 15 sekund.*
- *Wszelkie właściwości monitorowania usługi sieciowej mogą zostać przez użytkownika w późniejszym czasie zmienione. Więcej informacji na ten temat zawiera rozdział* Zmiana właściwości monitorowanych usług sieciowych *na stronie 154.*
- *Jeżeli usługa sieciowa, która ma być monitorowana, nie jest wymieniona na liście rozwijanej **Nazwa** w oknie **Dodaj nową usługę**, wówczas konieczne jest jej wcześniejsze zdefiniowanie w programie. Odbywa się to w ramach opcji programu. Więcej informacji na ten temat można znaleźć w rozdziale* Zmiana definicji usług sieciowych *na stronie 205.*

Usuwanie usług sieciowych z listy usług monitorowanych

Procedura usuwania usług sieciowych z listy usług monitorowanych jest niezwykle prosta. Najpierw dla danego węzła należy wyświetlić listę aktualnie monitorowanych usług sieciowych, potem wybrać usługę sieciową, której nie chcemy monitorować, a następnie kliknąć ikonę ***Usuń***.

Aby usunąć usługę sieciową z listy usług monitorowanych w danym węźle

1. Kliknij dany węzeł prawym przyciskiem myszy, w menu podręcznym wskaż pozycję **Monitorowanie**, następnie wskaż pozycję **Usługi sieciowe** i wybierz polecenie **Właściwości**.
2. Na wyświetlanej liście usług monitorowanych w danym węźle zaznacz tę usługę sieciową, którą chcesz usunąć.

3. Kliknij ikonę ***Usuń***.
4. W oknie **Potwierdź** kliknij przycisk **Tak**.

Uwagi

- *Możliwe jest wybranie kilku węzłów i jednoczesne usunięcie – w tym samym oknie – wybranych usług sieciowych z list usług monitorowanych w tych węzłach. W oknie **Widok sieci** należy zaznaczyć wszystkie wybrane węzły, korzystając z klawisza **Ctrl**, a następnie przejść do wykonania czynności opisanych w punktach 1-4.*
- *Jeżeli z listy usług monitorowanych w jakimkolwiek węźle zostanie usunięta usługa sieciowa PING, a na liście takiej nie pozostaną żadne inne usługi, to w takim przypadku program NetCrunch utraci możliwość sprawdzania stanu takiego węzła (a więc określania czy jest on w stanie OK, OSTRZEŻENIE czy NIE ODPOWIADA), w związku z czym jego stan będzie zawsze sygnalizowany jako NIEZNANY. Ikona reprezentująca taki węzeł na mapie będzie domyślnie wyświetlana w kolorze szarym. Zaleca się, aby usługa sieciowa PING w danym węźle była monitorowana zawsze (powinna pojawiać się na liście usług monitorowanych w danym węźle), tak aby nawet w przypadku usunięcia z listy wszystkich pozostałych usług sieciowych możliwe było wyznaczenie aktualnego stanu takiego węzła.*

Zmiana właściwości monitorowanych usług sieciowych

W dowolnym węźle, dla każdej z usług sieciowych aktualnie w nim monitorowanych, istnieje możliwość wprowadzania zmian we właściwościach monitorowania danej usługi. W ten sposób można modyfikować właściwości identyczne z tymi, które zostały omówione w rozdziale *Dodawanie usług sieciowych do listy monitorowanych usług* na stronie 152.

Na przykład podczas odpytywania może się zdarzyć, że NetCrunch nie będzie czekał wystarczająco długo na odpowiedź od monitorowanej usługi sieciowej w danym węźle. Usługi sieciowe, które wykorzystują protokoły oparte na protokole TCP, mogą wymagać dłuższych czasów połączenia. W takim przypadku program uzna, że dana usługa sieciowa znajduje się w stanie NIE ODPOWIADA, pomimo że być może działa ona w tym węźle prawidłowo. W celu rozwiązania tego problemu należy zwiększyć czas oczekiwania programu NetCrunch na odpowiedź (zmieniona musi zostać jedna z właściwości monitorowania tej usługi sieciowej, a mianowicie limit czasu odpowiedzi [timeout]).

Podczas odpytywania określonej usługi sieciowej na węźle NetCrunch wysyła ustaloną liczbę pakietów, na przykład jeden lub trzy. Wartość ta określona jest w dwóch polach we właściwościach monitorowania usługi sieciowej pod nazwą **Liczba powtórzeń** i **Dodatkowa liczba powtórzeń**. Pole **Liczba powtórzeń** określa dokładną liczbą pakietów, które będą zawsze wysyłane w celu sprawdzenia, czy węzeł odpowiada poprawnie. Z kolei pole **Dodatkowa liczba powtórzeń** definiuje dodatkowa liczbę pakietów wysyłanych tylko wówczas, gdy wszystkie wysłane uprzednio pakiety (określone w polu **Liczba powtórzeń**) nie przyniosły odpowiedzi. Definiowanie dwóch osobnych pól zamiast jednego umożliwia programowi na oszczędne rozporządzanie dostępnymi zasobami, bowiem dodatkowe sprawdzanie usługi sieciowej odbywa się wówczas wyłącznie, gdy zdefiniowane w polu **Liczba powtórzeń** pakiety nie przynoszą rezultatu. Przykładowo można w polu usługi sieciowej **Liczba powtórzeń** ustawić wartość 2, a w polu **Dodatkowa liczba powtórzeń** – 3. Wówczas w celu sprawdzenia stanu usługi sieciowej zawsze będą wysyłane dwa pakiety, a jeśli nie przyniosą odpowiedzi, zostaną wysłane 3 dodatkowe pakiety.

Monitorowanie usług sieciowych wykorzystujących protokoły oparte na protokole UDP może okazać się mało miarodajne (niektóre pakiety mogą być w takim przypadku tracone). Wówczas zaleca się zwiększenie liczby pakietów wysyłanych podczas każdorazowego odpytania (czyli zwiększenie wartości podawanej w polu właściwości o nazwie **Dodatkowa liczba powtórzeń**).

Aby zmienić właściwości monitorowania usługi sieciowej w danym węźle

1. Kliknij dany węzeł prawym przyciskiem myszy, w menu podręcznym wybierz opcję **Monitorowanie**, następnie wskaż pozycję **Usługi sieciowe** i wybierz polecenie **Właściwości**.
2. Na wyświetlanej liście usług monitorowanych w danym węźle zaznacz tę usługę sieciową, której właściwości chcesz zmienić.
3. Kliknij ikonę ***Właściwości***.
4. W oknie **Właściwości usługi** zmień wartość limitu czasu odpowiedzi określoną (w sekundach) w polu **Timeout**. Jest to maksymalny okres, w którym program będzie odczekiwał – podczas każdorazowego sprawdzania stanu usługi sieciowej w danym węźle – zanim uzna wysłane pakiety za utracone.
5. Zmień liczbę pakietów, jaka ma być wysyłana podczas sprawdzania stanu usługi sieciowej, wpisując inną wartość w polu **Liczba powtórzeń**.
6. W polu **Dodatkowa liczba powtórzeń** określ liczbę dodatkowych pakietów wysyłanych w momencie, gdy pakiety wysłane w ilości określonej w polu **Liczba powtórzeń** nie przynoszą odpowiedzi.
7. Jeżeli w oknie widoczne jest pole **Czas monitorowania**, możesz dodatkowo zmienić częstotliwość, z jaką sprawdzany będzie stan danej usługi sieciowej.

Uwagi

- *Możliwe jest równoczesne wybranie kilku węzłów i zmiana – za pomocą jednorazowych czynności podejmowanych w pojedynczym oknie – właściwości usług sieciowych monitorowanych w tych węzłach.*

*W tym celu w oknie **Widok sieci** należy, korzystając z klawisza **Ctrl**, zaznaczyć wybrane węzły, a następnie przejść do wykonania opisanych powyżej czynności.*

- *Usługa sieciowa, której właściwości monitorowania zostały zmienione, zostanie na liście usług monitorowanych w danym węźle wyświetlona pogrubioną czcionką.*
- *W polu **Dodatkowa liczba powtórzeń** można wpisać wartość 0 – wówczas program zawsze będzie wysyłał niezmienną liczbę pakietów, w celu sprawdzenia określonej usługi sieciowej.*
- *W oknie **Właściwości usługi** znajduje się dodatkowa właściwość związana z usługą sieciową – jest oto pole wyboru **Wyklucz ze wstrzymywania zdarzeń wywołanych przez usługi sieciowe**. Por. sekcję* Tworzenie wyjątków od reguły wstrzymywania zdarzeń związanych ze stanem usługi *na stronie 159 w celu uzyskania dodatkowych informacji.*

Wykrywanie usług sieciowych

Za pomocą programu NetCrunch użytkownik ma możliwość szybkiego wykrycia wszelkich usług sieciowych dostępnych w danym węźle i automatycznego dodania ich do listy usług monitorowanych w tym węźle. Ściślej mówiąc, podczas tej czynności program sprawdzi obecność wyłącznie tych usług sieciowych, które są wymienione na specjalnej liście znajdującej się w opcjach programu (aby się do niej dostać, należy z menu **Narzędzia** wybrać polecenie **Opcje**, a następnie przejść do strony **Monitorowanie - Usługi**). Domyślnie w programie określony jest zestaw najczęściej spotykanych usług sieciowych, takich jak na przykład PING, HTTP, FTP itp. Aby zmienić listę usług sieciowych wykorzystywaną w przez funkcję wykrywania usług, należy zapoznać się z rozdziałem *Domyślne usługi sieciowe* na stronie 205.

Wykrywanie usług sieciowych w danym węźle może zostać przeprowadzone na trzy sposoby. Można zaznaczyć wybrany węzeł i kliknąć odpowiednią ikonę ***Wykryj usługi sieciowe***, znajdującą się na pasku narzędzi okna **Widok sieci**. Jeżeli dla danego węzła otwarte jest aktualnie okno **Monitorowanie**, a w nim wybrana jest karta **Usługi sieciowe**, można wówczas kliknąć ikonę ***Wykryj***, znajdującą się w lewej części okna. Można wreszcie bezpośrednio kliknąć dany węzeł prawym przyciskiem myszy, w menu podręcznym wskazać pozycję **Monitorowanie**, następnie wskazać pozycję **Usługi sieciowe** i wybrać polecenie **Wykryj**.

Aby wykryć usługi sieciowe, które mogą być monitorowane w danym węźle

1. W oknie **Widok sieci** zaznacz wybrany węzeł.
2. W oknie **Widok sieci** kliknij znajdują się na jego pasku narzędzi ikonę ***Wykryj usługi sieciowe*** lub kliknij dany węzeł prawym przyciskiem myszy, w menu podręcznym wskaż pozycję **Monitorowanie**, następnie wskaż pozycję **Usługi sieciowe** i wybierz polecenie **Wykryj**.

Uwagi

- *Na ikonie reprezentującej dany węzeł przez pewien krótki okres czasu (kilka sekund) pojawi się symbol lupy. W tym czasie program przeprowadzi w danym węźle poszukiwanie wszelkich uruchomionych w nim usług sieciowych. Jeżeli znalezione zostaną jakiekolwiek nowe usługi sieciowe, rozpocznie się ich monitorowanie w tym węźle (dołączone zostaną do listy monitorowanych usług sieciowych).*
- *Możliwe jest również równoczesne wybranie kilku węzłów i przeprowadzenie wykrywania w tych węzłach aktualnie dostępnych i uruchomionych usług sieciowych. W tym celu w oknie **Widok sieci***

*należy, korzystając z klawisza **Ctrl**, zaznaczyć wybrane węzły, a następnie przejść do wykonania czynności opisanych powyżej w punkcie 2.*

Sprawdzanie stanu usług sieciowych

Za pomocą programu NetCrunch możliwe jest natychmiastowe sprawdzenie w danym węźle stanu aktualnie monitorowanej usługi sieciowej. Można tego dokonać na dwa sposoby. Należy albo zaznaczyć wybrany węzeł i kliknąć ikonę ***Sprawdź węzeł teraz***, znajdującą się na pasku narzędzi w oknie **Widok sieci**, albo kliknąć ten węzeł prawym przyciskiem myszy i wybrać odpowiednie polecenie z menu podręcznego.

Aby natychmiast sprawdzić stan usług sieciowych w danym węźle

1. W oknie **Widok sieci** zaznacz wybrany węzeł.
2. Na pasku narzędzi w oknie **Widok sieci** kliknij ikonę ***Sprawdź węzeł teraz*** lub kliknij dany węzeł prawym przyciskiem myszy, w menu podręcznym wskaż pozycję **Monitorowanie**, następnie wskaż pozycję **Usługi sieciowe** i wybierz polecenie **Sprawdź teraz**.

Uwagi

- *Jeżeli w danym węźle lub zbiorze węzłów stan monitorowanych usług ulega zmianie, znajduje to natychmiast swoje odzwierciedlenie w programie. Domyślnie ikona reprezentująca taki węzeł odpowiednio zmieni swój kolor (chyba że domyślny sposób sygnalizowania za pomocą koloru ikon zostanie zmieniony na którąkolwiek z innych metod. Więcej informacji na ten temat zawiera rozdział* Sygnalizacja stanu węzła *na stronie 213.)*
- *Możliwe jest również równoczesne wybranie kilku węzłów i natychmiastowe sprawdzenie stanu wszelkich usług sieciowych monitorowanych w tych węzłach. W tym celu w oknie **Widok sieci** należy, korzystając z klawisza **Ctrl**, zaznaczyć wszystkie wybrane węzły, a następnie przejść do wykonania czynności opisanych powyżej w punkcie 2.*

Wybieranie wiodącej usługi sieciowej

W ustalaniu strategii monitorowania NetCrunch bazuje na koncepcji wiodącej usługi sieciowej. Domyślnie wiodącą usługą sieciową wykorzystywaną przesz program jest Ping. Jeżeli nie jest ona dostępna na danym węźle, program używa w charakterze usługi wiodącej pierwszą usługę sieciową na liście usług monitorowanych na danym węźle. Możliwe jest jednakże przyznanie statusu usługi wiodącej dowolnej usłudze sieciowej dostępnej na liście monitorowanych usług.

W momencie, kiedy wiodąca usługa sieciowa – oraz wszystkie inne monitorowane dotychczas usługi – stają się niedostępne (ich stan zmienia się na NIE ODPOWIADA), monitorowanie tych wszystkich pozostałych usług zostaje okresowo wstrzymane. Wyłączane jest również monitorowanie liczników wydajności na tym węźle. Ta metoda ograniczonego monitorowania będzie kontynuowana – w celu zminimalizowania wykorzystania zasobów – do momentu, kiedy wiodąca usługa sieciowa znowu zacznie odpowiadać poprawnie (czyli wraca do stanu ODPOWIADA. Wówczas monitorowanie pozostałych usług sieciowych i liczników wydajności powróci do poprzedniego stanu – będą one znowu monitorowane w normalnym trybie.

Aby wybrać wiodącą usługę sieciową dla węzła

1. W oknie **Widok sieci** wybierz węzeł, którego opcje monitorowania mają zostać zmienione.
2. W podręcznym menu węzła wskaż opcje **Monitorowanie> Usługi sieciowe> Właściwości**.
   Otworzy się okno **Monitorowanie** ze wskazaną kartą **Usługi sieciowe**.
3. Z rozwijanej listy **Usługa wiodąca** wybierz usługę sieciową, która ma mieć status wiodącej usługi sieciowej na danym węźle.

Uwagi

- *Ustawienie usługi sieciowej jako usługi wiodącej jest możliwe wówczas, gdy usługa ta jest aktualnie zdefiniowana w liście monitorowanych usług dla węzła.*
- *Procedura dodawania nowej usługi sieciowej do monitorowanych usług dla węzła została opisana w sekcji Dodawanie usług sieciowych do listy monitorowanych usług* *na stronie 151*.
- *W przypadku, gdy NetCrunch działa w oparciu o system operacyjny Windows XP Service Pack 2 i zachodzi potrzeba wybrania usługi sieciowej TCP w charakterze usługi wiodącej, zalecane jest zapoznanie się z zamieszczoną poniżej sekcją* Przypadki spowolnienia w monitorowaniu usług sieciowych opartych na protokole TCP .

Przypadki spowolnienia w monitorowaniu usług sieciowych opartych na protokole TCP

Gdy NetCrunch działa w oparciu o system operacyjny Windows XP Service Pack 2, może nastąpić spowolnienie w monitorowaniu usług sieciowych używających protokołu TCP (takich jak HTTP, POP3 lub SMTP). Zjawisko to ma związek z właściwościami systemu Windows XP Service Pack 2, w którym ograniczono liczbę równoczesnych niekompletnych przychodzących prób połączenia za pomocą protokołu TCP. W momencie gdy zostaje osiągnięta dopuszczalna liczba prób, kolejne próby połączenia (np. podejmowane przez NetCruncha usiłującego sprawdzić stan usług sieciowych TCP na nieodpowiadających węzłach) są kolejkowane. W takich wypadkach w systemowym dzienniku zdarzeń Windows pojawia się zdarzenie opatrzone numerem identyfikacyjnym 4226.

Uwagi

- *W celu uzyskania dodatkowych informacji warto zapoznać się z zamieszczonym na witrynie firmowej firmy Microsoft artykułem pt. Changes to Functionality in Microsoft Windows XP Service Pack 2 - TCP/IP.*
- *Z uwagi na opisany powyżej problem zalecane jest używanie protokołów ICMP lub UDP w charakterze usługi wiodącej (tj. PING lub SNMP). Dotyczy to sytuacji, gdy NetCrunch działa na komputerze funkcjonującym w oparciu o system operacyjny Windows XP Service Pack 2 i gdy zachodzi potrzeba monitorowania znacznej ilości węzłów.*
- *Aby uniknąć tego problemu, zalecane jest zainstalowanie NetCruncha na komputerze z systemem operacyjnym Windows Server 2003 (lub systemem operacyjnym wypuszczonym na rynek przed dodatkiem Windows XP Service Pack 2).*

Tworzenie wyjątków od reguły wstrzymywania zdarzeń związanych ze stanem usługi

Zdarzenia związane ze stanem usługi sieciowej to zdarzenia o treści „Usługa nie odpowiada" zachodzące na dowolnej usłudze sieciowej. Program potrafi wstrzymywać wszelkie zdarzenia związane ze stanem usługi sieciowej na węźle w momencie, gdy z jakiegoś powodu węzeł przestaje odpowiadać (także z powodu reguły zależności). W takich sytuacjach generowane jest wyłącznie zdarzenie o treści „Węzeł nie odpowiada", natomiast wszelkie inne zdarzenia związane ze stanem wszystkich monitorowanych na danym węźle usług nie zostaną wygenerowane (mimo, iż wówczas także i te usługi nie odpowiadają). Regułę tą można ustawić w zaawansowanych opcjach węzła. Por. sekcję *Wstrzymywanie zdarzeń związanych ze stanem usług sieciowych* na stronie 161 w celu uzyskania dodatkowych informacji.

W niektórych sytuacjach może jednakże zachodzić potrzeba wykluczenia określonej usługi sieciowej na węźle ze strategii wstrzymywania zdarzeń związanych z usługami, np. gdy jedna z monitorowanych na tym węźle usług sieciowych posiada zasadnicze znaczenie. Przykładowo, gdy węzeł jest serwerem webowym, niezwykle ważne może okazać się rygorystyczne kontrolowanie usługi sieciowej HTTP – oraz otrzymywanie powiadomień i podejmowanie akcji w momencie, gdy usługa ta przestaje odpowiadać – przy jednoczesnym wstrzymywaniu zdarzeń wywołanych zmianą stanu pozostałych usług sieciowych monitorowanych na węźle. Program umożliwia definiowane podobnych wyjątków od reguły wstrzymywania zdarzeń związanych ze zmianą stanu usług sieciowych dla dowolnej aktualnie monitorowanej usługi sieciowej na węźle.

Aby ustawić wyjątek od reguły wstrzymywania zdarzeń związanych ze zmianą stanu usługi sieciowej na węźle

1. Kliknij prawym przyciskiem myszy węzeł, a następnie w podręcznym menu wskaż pozycje **Monitorowanie> Usługi sieciowe> Właściwości**.
   Otworzy się okno **Monitorowanie** z wybraną kartą **Usługi sieciowe**.
2. Wybierz z listy usługę sieciową, która ma być pomijana w regule wstrzymywania zdarzeń związanych ze stanem usługi sieciowej.
3.  Kliknij ikonę ***Zmień właściwości***.
   Otworzy się okno **Właściwości usługi**.
4. Zaznacz pole wyboru **Wyłącz wstrzymywanie zdarzeń na usługach sieciowych**.

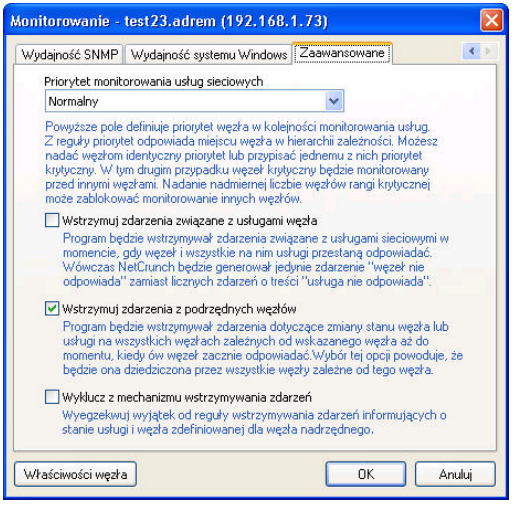
Uwagi

- *W dowolnej chwili można odznaczyć pole wyboru w punkcie 4, aby przywrócić wstrzymywanie zdarzeń związanych z usługami dla określonej usługi sieciowej.*
- *W punkcie 2 lista monitorowanych usług sieciowych zawiera kolumnę opisującą, czy program ma stosować regułę wstrzymywania zdarzeń na usługach dla danej usługi. Kolumna ta nosi nazwę* ***Wyklucz z reguły wstrzymywania****.*
- *Należy pamiętać, że ustawienie to obowiązuje w dla usługi sieciowej tylko wtedy, gdy związany z tą usługą węzeł posiada włączoną regułę wstrzymywania zdarzeń związanych z usługami.*
- *Mechanizm wstrzymywania zdarzeń jest dostępny jedynie w wersji Premium XE programu.*

Opcje zaawansowane

Ustawianie priorytetów monitorowania usług sieciowych

Zazwyczaj węzeł posiada priorytet monitorowania przydzielony na podstawie jego miejsca w hierarchii zależności. Jednakże dzięki zaawansowanym opcjom monitorowania można ustawić różne priorytety monitorowania usług sieciowych dla różnych węzłów. Funkcja ta jest szczególnie przydatna, gdy NetCrunch monitoruje sieć o stosunkowo dużej wielkości. W takim środowisku możliwość przydzielania pierwszeństwa w monitorowaniu wybranym węzłom oferuje niewątpliwe korzyści. Przykładowo, przy założeniu, że węzły typu serwery czy rutery mają znaczenie krytyczne dla ogólnego stanu sieci, możliwe jest przypisanie monitorowaniu ich węzłów sieciowych wyższego priorytetu niż w przypadku pozostałych węzłów. Wówczas NetCrunch będzie zawsze monitorował w pierwszej kolejności działające na nich usługi sieciowe, a dopiero potem usługi na innych węzłach.



Aby ustawić priorytet monitorowania usługi sieciowej

1. Kliknij węzeł prawym przyciskiem myszy i w podręcznym menu wskaż opcje **Monitorowanie** > **Właściwości**.
   Otworzy się okno **Monitorowanie**.
2. Kliknij kartę **Zaawansowane**.
3. Z rozwijanej listy **Priorytet monitorowania usług sieciowych** wybierz odpowiedni priorytet monitorowania dla węzła (niski, normalny, wysoki lub krytyczny).

Uwagi

- *Możliwe jest wybranie wielu węzłów i zmodyfikowanie priorytetu monitorowania usług sieciowych dla wszystkich wybranych węzłów jednocześnie. W tym celu należy w pierwsze kolejności wybrać wszystkie żądane węzły za pomocą klawisza **CTRL**, a następnie postępować zgodnie z procedurą opisaną powyżej.*
- *Z uwagi na złożony charakter priorytetów monitorowania usług sieciowych, należy zachować ostrożność przy ich modyfikacji. Ustawienie wartości krytycznej na zbyt wielu węzłach może spowodować zatrzymanie monitorowania usług sieciowych na innych, mniej ważnych węzłach. Dopuszczalna liczba węzłów, jakim można przypisać taki priorytet, jest uzależniona od różnych czynników, takich jak aktualny ruch sieciowy na każdym monitorowanym węźle oraz parametry komputera, na którym działa NetCrunch (np. szybkość procesora lub ilość dostępnej pamięci).*
- *Mechanizm priorytetów monitorowania jest dostępny wyłącznie w wersji Premium XE NetCruncha.*

Wstrzymywanie zdarzeń związanych ze stanem usług sieciowych i węzłów

Ta zaawansowana opcja monitorowania jest związana z możliwością wstrzymywania zdarzeń związanych ze stanem usługi (czyli zdarzeń o treści "Usługa nie odpowiada"). Włączenie tej opcji na węźle powoduje, że program wstrzymuje takie zdarzenia w momencie, gdy węzeł jest niesprawny i nie odpowiada żadna działająca na nim usługa. W takiej sytuacji program generuje tylko zdarzenie o treści "Węzeł nie odpowiada", zamiast generować dodatkowe zdarzenia o treści "usługa nie odpowiada" dla każdej monitorowanej usługi sieciowej na węźle, który w danym momencie także nie odpowiada. Opcja ta przydaje się w sytuacjach, gdy chcemy dowiadywać się o tym, że węzeł przestaje odpowiadać, a nie interesują nas zdarzenia związane z usługami sieciowymi; z kolei te ostatnie zdarzenia staja się istotne w momencie, gdy węzeł odpowiada poprawnie, lecz następuje awaria konkretnej usługi.

Aby włączyć/wyłączyć wstrzymywanie zdarzeń związanych z usługami sieciowymi na węźle

1. Kliknij prawym przyciskiem myszy węzeł, a następnie w podręcznym menu wskaż opcje **Monitorowanie** > **Właściwości**.
   Otworzy się okno **Monitorowanie**.
2. Kliknij zakładkę **Zaawansowane**.
3. Aby włączyć wstrzymywanie zdarzeń związanych z usługami sieciowymi, zaznacz pole wyboru **Wstrzymuj zdarzenia związane z usługami węzła**.
   Aby wyłączyć wstrzymywanie zdarzeń związanych z usługami sieciowymi, odznacz pole wyboru **Wstrzymuj zdarzenia związane z usługami węzła**.

Uwagi

- *Możliwe jest wybranie wielu węzłów w celu włączenia lub wyłączenia na nich wszystkich mechanizmu wstrzymywania zdarzeń. W tym celu należy zaznaczyć żądane węzły za pomocą klawisza **CTRL,** a następnie postępować zgodnie z procedurą opisaną powyżej.*
- *Możliwe jest tworzenie wyjątków od reguły wstrzymywania zdarzeń związanych z usługami sieciowymi na węźle. Por. sekcję* Tworzenie wyjątków od reguły wstrzymywania zdarzeń związanych ze stanem usługi *na stronie 159.*
- *W celu zarządzania mechanizmem wstrzymywania zdarzeń na węzłach z poziomu jednego okna, należy użyć Menedżera wstrzymywania zdarzeń. Por. sekcję* Menedżer wstrzymywania zdarzeń *na stronie 239 w celu uzyskania dodatkowych informacji.*
- *Należy mieć na uwadze, że zdarzenia komplementarne w stosunku do wstrzymywanych na węźle zdarzeń o treści "Usługa nie odpowiada" (czyli zdarzenia o treści "Usługa odpowiada"), zostaną automatycznie pominięte przez program i nie będą generowane.*
- *Mechanizm wstrzymywania zdarzeń jest dostępny wyłącznie w wersji Premium XE NetCruncha.*

Wstrzymywanie zdarzeń z węzłów podrzędnych

Kolejną zaawansowana opcją monitorowania jest mechanizm wstrzymywania zdarzeń (związanych ze stanem usługi sieciowej lub stanem węzła, innymi słowy zdarzeń o treści "Węzeł nie odpowiada" lub "Usługa nie odpowiada") na węzłach podrzędnych do momentu, gdy nadrzędny węzeł ponownie zaczyna poprawnie odpowiadać. Włączenie tej opcji powoduje, że zdarzenie jest generowane tylko raz dla węzła nadrzędnego (czyli zdarzenie o treści "Węzeł nie odpowiada" i ewentualnie "Usługa nie odpowiada"), natomiast wszystkie

podrzędne względem niego węzły (które na mocy reguły zależności posiadają status niesprawności) nie będą generować zbędnych zdarzeń związanych ze stanem usług lub węzłów sieciowych (czyli zdarzeń o treści "Węzeł nie odpowiada" i "Usługa nie odpowiada").

Przykładowo można przypisać kilku węzłom znajdującym się za ruterem status podrzędności w stosunku do węzła nadrzędnego (czyli rutera), a następnie w zaawansowanych opcjach monitorowania tego rutera ustawić wstrzymywanie zdarzeń związanych ze stanem usług lub węzłów sieciowych dla wszystkich węzłów podrzędnych. W momencie gdy ruter przestanie odpowiadać, zostanie wygenerowane jedynie zdarzenie o treści "Węzeł nie odpowiada". Wszystkie węzły podrzędne znajdujące się za tym ruterem (które na mocy reguły zależności posiadają status niesprawności), nie będą generować zdarzeń związanych ze stanem usług lub węzłów sieciowych.

Aby włączyć/wyłączyć wstrzymywanie zdarzeń z węzłów podrzędnych

1. Kliknij prawym przyciskiem myszy węzeł, a następnie w podręcznym menu wskaż opcje **Monitorowanie > Właściwości**.
   Pojawi się okno **Monitorowanie**.
2. Wybierz kartę **Zaawansowane**.
3. Aby włączyć wstrzymywanie zdarzeń z węzłów podrzędnych, zaznacz pole wyboru **Wstrzymuj zdarzenia z podrzędnych węzłów**. Aby wyłączyć wstrzymywanie zdarzeń z węzłów podrzędnych, odznacz pole wyboru **Wstrzymuj zdarzenia z podrzędnych węzłów**.

Uwagi

- *Możliwe jest wybranie wielu węzłów w celu włączenia lub wyłączenia na nich wszystkich mechanizmu wstrzymywania zdarzeń. W tym celu należy zaznaczyć żądane węzły za pomocą klawisza **CTRL**, a następnie postępować zgodnie z procedurą opisaną powyżej.*
- *Należy pamiętać, że włączenie tego ustawienia na węźle powoduje, że wszystkie zależne od niego węzły będą miały automatycznie włączone identyczne ustawienie. Jednakże wyłączenie tej opcji na węźle nie ma żadnego wpływu na zależne od niego węzły podrzędne. Omawiana opcja będzie w dalszym ciągu włączona na tychże węzłach – aby ją wyłączyć, należy to uczynić na każdym węźle z osobna albo przy użyciu funkcji wielokrotnego wyboru.*
- *W każdej chwili możliwe jest ustawienie wyjątku od reguły wstrzymywania zdarzeń związanych ze stanem węzła i usług sieciowych na węźle (zdefiniowanych na węźle nadrzędnym w stosunku do danego węzła). Por. poniższą sekcję* Tworzenie wyjątków od wstrzymywania zdarzeń *w celu uzyskania dodatkowych informacji.*
- *Jeśli zostanie włączone na węźle wstrzymywanie zdarzeń z węzłów podrzędnych w stosunku do niego, interwał monitorowania działającej na tym węźle usługi wiodącej zostanie automatycznie zmieniony do wartości około 30 sekund, aby umożliwić węzłom podrzędnym rozpoznanie jego stanu w stosunkowo krótkim czasie.*
- *W celu zarządzania mechanizmem wstrzymywania zdarzeń na węzłach z poziomu jednego okna, należy użyć Menedżera wstrzymywania zdarzeń. Por. sekcję* Menedżer wstrzymywania zdarzeń *na stronie 239 w celu uzyskania dodatkowych informacji.*
- *Należy mieć na uwadze, że zdarzenia komplementarne w stosunku do wstrzymywanych na węźle zdarzeń związanych ze stanem węzła lub usług (czyli mających treść "Węzeł odpowiada" i "Usługa odpowiada"), zostaną automatycznie pominięte przez program i będą generowane.*

- *Mechanizm wstrzymywania zdarzeń jest dostępny wyłącznie w wersji Premium XE NetCruncha.*

Tworzenie wyjątków od wstrzymywania zdarzeń

Możliwe jest narzucanie wyjątków od reguły wstrzymywania zdarzeń związanych ze stanem usługi lub węzła sieciowego zdefiniowanej na węźle nadrzędnym, od którego zależny jest dany węzeł. Włączenie tego ustawienia oznacza, że dany węzeł będzie generował zdarzenia o treści "Węzeł nie odpowiada" lub "Usługa nie odpowiada", mimo iż węzeł ten został wyłączony na mocy reguły zależności przez węzła nadrzędnego (który nie odpowiada).

Stosowanie powyższej opcji jest szczególnie przydatne w przypadku urządzeń sieciowych mających krytyczne znaczenie dla ogólnego stanu sieci; w takich przypadkach wskazane jest generowanie zdarzeń – a także uruchamianie akcji – w każdej sytuacji, gdy dany węzeł z jakiegoś powodu nie odpowiada.

Aby ustawić wyjątek od reguły wstrzymywania zdarzeń

1. Kliknij prawym przyciskiem myszy węzeł, a następnie w podręcznym menu wskaż opcje **Monitorowanie > Właściwości**.
   Pojawi się okno **Monitorowanie**.
2. Kliknij kartę **Zaawansowane**.
3. Zaznacz pole wyboru **Wyklucz z mechanizmu wstrzymywania zdarzeń**.

Uwagi

- *Aby anulować zdefiniowany wyjątek od reguły wstrzymywania zdarzeń na węźle, należy odznaczyć pole wyboru w punkcie 3.*
- *Należy pamiętać, że omawiana opcja ma zastosowanie na danym węźle tylko wtedy, gdy funkcja wstrzymywania zdarzeń z węzłów podrzędnych jest włączona na węźle nadrzędnym w stosunku do danego węzła.*
- *Włączanie wstrzymywania zdarzeń z węzłów podrzędnych zostało opisane w sekcji* Wstrzymywanie zdarzeń z węzłów podrzędnych *na stronie 161.*
- *Aby zarządzać z jednego okna mechanizmem wstrzymywania zdarzeń na węzłach, należy użyć Menedżera wstrzymywania zdarzeń. Por. sekcję* Menedżer wstrzymywania zdarzeń *na stronie 239 w celu uzyskania dodatkowych informacji.*
- *Mechanizm wstrzymywania zdarzeń jest dostępny wyłącznie w wersji Premium XE NetCruncha.*

Monitorowanie wydajności systemu Windows

W programie NetCrunch węzły Windows (czyli te, które działają pod kontrolą systemu operacyjnego Windows) mogą być monitorowane przy wykorzystaniu różnych liczników wydajności, w które wyposażone są tego rodzaju węzły. Możliwe jest przy tym włączanie lub wyłączanie monitorowania wydajności systemu Windows w węźle (węzłach) lub określenie czasu monitorowania odnoszącego się wyłącznie do liczników związanych z systemem Windows. Program umożliwia również podanie nazwy użytkownika i hasła, służących do logowania w systemie lub domenie, aby dzięki temu liczniki wydajności Windows mogły być poprawnie odczytywane z określonego węzła.

Włączanie monitorowania

W węzłach Windows, które zostały przez program prawidłowo rozpoznane podczas wykrywania sieci, monitorowanie liczników wydajności Windows może być albo włączone, albo wyłączone. Domyślnie w programie jest ono włączone.

Aby włączyć lub wyłączyć w węźle monitorowanie wydajności Windows

1. Kliknij dany węzeł prawym przyciskiem myszy, w menu podręcznym wskaż pozycję **Monitorowanie**, a następnie wybierz polecenie **Wydajność Windows**.
2. Aby w danym węźle włączyć monitorowanie wydajności Windows, zaznacz pole wyboru **Włącz**.
   Aby w danym węźle wyłączyć monitorowanie wydajności Windows, usuń zaznaczenie z pola wyboru **Włącz**.

Uwagi

- *Użytkownik może w oknie **Widok sieci** zaznaczyć wiele węzłów, a następnie zmienić równocześnie niektóre spośród właściwości wydajności Windows – w sposób szybszy i o wiele sprawniejszy. W tym celu należy, korzystając z klawisza **Ctrl**, zaznaczyć te węzły, dla których chcemy włączyć lub wyłączyć monitorowanie wydajności Windows, a następnie przejść do wykonania opisanych powyżej czynności.*
- *Jeżeli w oknie **Monitorowanie** karta **Wydajność Windows** nie jest dostępna, oznacza to, że w danym węźle nie został uruchomiony system operacyjny Windows, lub że program nie wykrył tego faktu w prawidłowy sposób. Wobec tego węzeł taki nie będzie udostępniał żadnych informacji dotyczących systemu Windows, a NetCrunch nie będzie mógł monitorować takich informacji.*
- *Aby włączyć/wyłączyć monitorowanie usług Windows NT w węźle, zaznacz lub odznacz pole wyboru **Monitoruj usługi Windows NT**.*

Zmiana czasu monitorowania

Domyślnie program stosuje taki czas monitorowania, jaki został dla danego węzła określony w oknie **Monitorowanie** na karcie **Ogólne**. Parametr ten jest wykorzystywany podczas monitorowania wszelkich istotnych informacji dotyczących danego węzła (usług sieciowych, liczników wydajności itp.). Jednakże dla liczników wydajności Windows istnieje możliwość oddzielnego określenia czasu monitorowania.

Aby zmienić czas monitorowania wydajności Windows dla danego węzła

1. Kliknij dany węzeł prawym przyciskiem myszy, w menu podręcznym wskaż pozycję **Monitorowanie**, a następnie wybierz polecenie **Wydajność Windows**.
2. W polu **Czas monitorowania** wpisz wybraną wartość czasu monitorowania (w minutach), która ma być stosowana dla potrzeb monitorowania wydajności systemu Windows.

Uwagi

- *Jeżeli pole **Czas monitorowania** zostanie pozostawione puste, wówczas dla potrzeb monitorowania wydajności systemu Windows wykorzystywany będzie podstawowy czas monitorowania (określony w oknie **Monitorowanie** na karcie **Ogólne**).*
- *Użytkownik może w oknie **Widok sieci** zaznaczyć wiele węzłów, a następnie zmienić czas monitorowania wydajności systemu Windows równocześnie we wszystkich wybranych węzłach. W tym*

*celu należy, korzystając z klawisza **Ctrl**, zaznaczyć odpowiednie węzły, a następnie przejść do wykonania opisanych powyżej czynności.*

- *Jeżeli po lewej stronie pola **Czas monitorowania** wyświetlana jest ikona **Kłódka**, oznacza to, że dla wybranych węzłów pole to nie zostanie zmienione. Jeżeli natomiast po lewej stronie tego pola wyświetlana jest ikona **Zaznaczenie**, oznacza to, że dla wybranych węzłów pole to zostanie zmienione (w polu tym wpisana zostanie nowa wartość).*

- *Jeżeli w danym polu wprowadzone już zostały pewne zmiany, a chcemy z nich zrezygnować i pozostawić to pole w stanie niezmienionym, wystarczy kliknąć ikonę **Zaznaczenie**, znajdującą się na lewo od takiego pola. Zmieni się ona wówczas z powrotem w ikonę **Kłódka**, wskazując, że dla wszystkich wybranych węzłów dane pole zostanie pozostawione w stanie niezmienionym.*

Określanie parametrów logowania

Aby móc monitorować w danym węźle liczniki wydajności Windows, konieczne jest zalogowanie się przez NetCrunch albo w tym właśnie węźle, albo w domenie, do której węzeł ten należy. Po wykonaniu tej operacji program będzie w stanie otrzymywać z danego węzła wszelkie informacje pochodzące z liczników wydajności Windows.

Aby dla danego węzła określić nazwę użytkownika i hasło w systemie Windows

1. Kliknij dany węzeł prawym przyciskiem myszy, w menu podręcznym wskaż pozycję **Monitorowanie**, a następnie wybierz polecenie **Wydajność Windows**.
2. W polu **Połącz się jako** wpisz nazwę użytkownika służącą do logowania w systemie Windows w danym węźle.
3. W polu **Hasło** wpisz hasło służące do logowania w systemie Windows.

Uwagi

- *Aby w punkcie 2. wybrać nazwę określonego użytkownika z dostępnej listy, należy kliknąć ikonę **Wybierz użytkownika**.*
- *Logowanie może zostać także przeprowadzone jako logowanie członka domeny Windows. Zamiast podawania w polu **Połącz się jako** nazwy użytkownika, należy wówczas wpisać nazwę domeny, bezpośrednio po niej ukośnik (znak „\"), a następnie nazwę użytkownika. Jeżeli na przykład zalogowany miałaby zostać użytkownik* krzysztof *należący do domeny* Przyklad*, w polu **Połącz się jako** należałoby wpisać:*

```
Przykład\krzysztof
```

- *Użytkownik może w oknie **Widok sieci** zaznaczyć wiele węzłów, a następnie określić nazwę użytkownika i hasło w systemie Windows równocześnie dla wszystkich wybranych węzłów. W tym celu należy, korzystając z klawisza **Ctrl**, zaznaczyć odpowiednie węzły, a następnie przejść do wykonania opisanych powyżej czynności.*

- *Jeżeli po lewej stronie pola **Połącz się jako** lub pola **Hasło** wyświetlana jest ikona **Kłódka**, oznacza to, że dla wybranych węzłów odpowiednie pole nie zostanie zmienione. Jeżeli natomiast po lewej stronie pola **Połącz się jako** lub pola **Hasło** wyświetlana jest ikona **Zaznaczenie**, oznacza to, że dla wybranych węzłów pole to zostanie zmienione (w polu tym wpisana zostanie nowa wartość).*

- *Jeżeli w danym polu wprowadzone już zostały pewne zmiany, a chcemy z nich zrezygnować i pozostawić to pole w stanie niezmienionym, wystarczy kliknąć ikonę **Zaznaczenie**, znajdującą się na lewo od takiego pola. Zmieni się ona wówczas z powrotem w ikonę **Kłódka**, wskazując, że dla wszystkich wybranych węzłów dane pole zostanie pozostawione w stanie niezmienionym.*

- *W opcjach programu możliwe jest określenie domyślnych parametrów logowania – nazwy użytkownika, hasła oraz domeny. NetCrunch będzie próbował zastosować te ustawienia w przypadku logowania się w jakimkolwiek węźle Windows, dla którego w opcjach monitorowania wydajności Windows nie zostały określone (w opisany powyżej sposób) oddzielne parametry logowania, czyli nazwa użytkownika, hasło i ewentualnie domena. Aby określić domyślne dane uwierzytelniające w systemie Windows, które mają być stosowane globalnie, dla wszystkich węzłów Windows, należy w menu* ***Narzędzia*** *wybrać polecenie* ***Opcje****, a następnie w otwartym w ten sposób oknie przejść do strony* ***Monitorowanie – Windows NT****.*

Monitorowanie wydajności systemu NetWare

Na węzłach z uruchomionym systemem operacyjnym NetWare (np. na serwerach NetWare) można za pomocą NetCruncha monitorować różne charakterystyczne dla tego systemu liczniki wydajności (takie jak na przykład *% Wykorzystania* lub *Liczba połączeń*). Możliwe jest przy tym – w stosunkowo łatwy sposób – włączanie lub wyłączanie monitorowania wydajności systemu NetWare w węźle (węzłach) lub określenie czasu monitorowania odnoszącego się wyłącznie do liczników wydajności systemu NetWare. Program umożliwia również określenie nazwy użytkownika i hasła w systemie NetWare, dzięki którym program będzie mógł poprawnie odczytywać informacje z liczników wydajności NetWare w określonym węźle (węzłach).

Włączanie monitorowania

Na węzłach działających pod kontrolą systemu operacyjnego NetWare i prawidłowo rozpoznanych przez program podczas wykrywania sieci, monitorowanie liczników wydajności NetWare może być albo włączone, albo wyłączone. Domyślnie w NetCrunchu jest ono włączone.

Aby włączyć lub wyłączyć w węźle monitorowanie wydajności NetWare

1. Kliknij dany węzeł prawym przyciskiem myszy, w menu podręcznym wskaż pozycję **Monitorowanie**, a następnie wybierz polecenie **Wydajność NetWare**.
2. Aby w danym węźle włączyć monitorowanie wydajności NetWare, zaznacz pole wyboru **Włącz**.
   Aby w danym węźle wyłączyć monitorowanie wydajności NetWare, usuń zaznaczenie z pola wyboru **Włącz**.

Uwagi

- *Użytkownik może na dowolnej mapie zaznaczyć wiele węzłów, a następnie zmienić równocześnie niektóre spośród związanych z tymi węzłami właściwości wydajności systemu NetWare – w sposób szybszy i o wiele sprawniejszy. W tym celu należy, korzystając z klawisza* ***Ctrl****, zaznaczyć te węzły, dla których chcemy włączyć lub wyłączyć monitorowanie wydajności systemu NetWare, a następnie przejść do wykonania opisanych powyżej czynności.*
- *Jeżeli w oknie* ***Monitorowanie*** *karta* ***Wydajność NetWare*** *nie jest dostępna, oznacza to, że w danym węźle nie został uruchomiony system operacyjny NetWare. W tej sytuacji węzeł taki nie udostępni żadnych informacji charakterystycznych dla systemu NetWare, a NetCrunch nie będzie mógł śledzić takich informacji.*

Zmiana czasu monitorowania

Domyślnie NetCrunch stosuje taki czas monitorowania, jaki został dla danego węzła określony w oknie **Monitorowanie**, na karcie **Ogólne**. Parametr ten jest wykorzystywany podczas monitorowania wszelkich istotnych informacji dotyczących danego węzła (usług sieciowych, liczników wydajności itp.). Jednakże dla liczników wydajności NetWare istnieje możliwość oddzielnego określenia czasu monitorowania.

Aby zmienić czas monitorowania wydajności NetWare dla danego węzła

1. Kliknij dany węzeł prawym przyciskiem myszy, w menu podręcznym wskaż pozycję **Monitorowanie**, a następnie wybierz polecenie **Wydajność NetWare**.
2. W polu **Czas monitorowania** wpisz wybraną wartość czasu monitorowania (w minutach), która ma być stosowana dla potrzeb monitorowania wydajności systemu NetWare.

Uwagi

- *Jeżeli pole **Czas monitorowania** zostanie pozostawione puste, wówczas dla potrzeb monitorowania wydajności systemu NetWare wykorzystywany będzie podstawowy czas monitorowania (określony w oknie **Monitorowanie** na karcie **Ogólne**).*
- *Użytkownik może w oknie **Widok sieci** zaznaczyć wiele węzłów, a następnie zmienić czas monitorowania wydajności systemu NetWare równocześnie we wszystkich wybranych węzłach. W tym celu należy, korzystając z klawisza **Ctrl**, zaznaczyć odpowiednie węzły, a następnie przejść do wykonania opisanych powyżej czynności.*

- *Jeżeli po lewej stronie pola **Czas monitorowania** wyświetlana jest ikona **Kłódka**, oznacza to, że dla wybranych węzłów pole to nie zostanie zmienione. Jeżeli natomiast po lewej stronie pola **Czas monitorowania** wyświetlana jest ikona **Zaznaczenie**, oznacza to, że dla wybranych węzłów pole to zostanie zmienione (w polu tym wpisana zostanie nowa wartość).*

- *Jeżeli w danym polu wprowadzone już zostały pewne zmiany, a chcemy z nich zrezygnować i pozostawić to pole w stanie niezmienionym, wystarczy kliknąć ikonę **Zaznaczenie**, znajdującą się na lewo od takiego pola. Zmieni się ona wówczas z powrotem w ikonę **Kłódka**, wskazując, że dla wszystkich wybranych węzłów dane pole zostanie pozostawione w stanie niezmienionym.*

Zarządzanie danymi uwierzytelnienia w drzewie eDirectory

Aby poprawnie monitorować moduły NLM oraz liczniki wydajności na serwerach działających w oparciu o system operacyjny NetWare, należy podać odpowiednie dane uwierzytelnienia w drzewie eDirectory. NetCrunch daje użytkownikom możliwość wpisywania takich informacji za pomocą karty **Wydajność NetWare** w oknie **Monitorowanie**. Domyślne dane logowania w katalogu eDirectory można także wskazać w opcjach programu. Należy mieć na uwadze, że wówczas NetCrunch automatycznie połączy się – i będzie monitorował – wszystkie serwery NetWare znajdujące się w drzewie NDS (eDirectory), dla którego określono dane uwierzytelnienia.

Aby zarządzać dane uwierzytelnienia w drzewie NDS

1. Kliknij prawym przyciskiem myszy węzeł NetWare, wskaż pozycję **Monitorowanie** w podręcznym menu, a następnie kliknij opcję **Wydajność NetWare**.

2. Kliknij przycisk **Zarządzaj hasłami drzewa eDirectory**.

3. Aby dodać dane uwierzytelnienia w drzewie eDirectory, kliknij ikonę ***Dodaj***.
W otwartym oknie dialogowym zdefiniuj odpowiednie informacje.
Aby zmienić właściwości przechowywanych danych uwierzytelnienia w drzewie NDS, wskaż je na liście i kliknij ikonę ***Zmień właściwości***. W otwartym oknie dialogowym dokonaj stosownych zmian.
Aby usunąć przechowywane dane uwierzytelnienia w drzewie NDS, wskaż je na liście i kliknij ikonę ***Usuń***.

Monitorowanie wydajności SNMP

NetCrunch umożliwia monitorowanie liczników wydajności SNMP w poszczególnych węzłach. Oczywiście w takim węźle musi być uruchomiony agent SNMP. Ponadto program musi rozpoznawać taki węzeł jako urządzenie zarządzane za pomocą agenta SNMP i wykorzystywać właściwą wspólnotę odczytu SNMP. Obie te opcje określane są bezpośrednio w odpowiadającym danemu węzłowi oknie **Właściwości** na karcie **SNMP**. Więcej informacji na ten temat zawiera rozdział *Właściwości zarządzania poprzez agenta SNMP* na stronie 143.

Dla dowolnych węzłów zarządzanych za pomocą agenta SNMP monitorowanie wydajności SNMP może być albo włączane, albo wyłączane. Użytkownik ma także możliwość oddzielnego określenia czasu monitorowania, który wykorzystywany jest przy odczytywaniu informacji pochodzących z liczników wydajności SNMP.

Włączanie monitorowania

Węzły, w których uruchomiony jest agent SNMP, mają domyślnie włączone monitorowanie wydajności usługi SNMP. Monitorowanie wydajności usługi SNMP może być włączane lub wyłączane bezpośrednio w oknie **Właściwości**.

Aby włączyć lub wyłączyć w węźle monitorowanie wydajności SNMP

1. Kliknij dany węzeł prawym przyciskiem myszy, w menu podręcznym wskaż pozycję **Monitorowanie**, a następnie wybierz polecenie **Wydajność SNMP**.

2. Aby w danym węźle włączyć monitorowanie wydajności usługi SNMP, zaznacz pole wyboru **Włącz**.
Aby w danym węźle wyłączyć monitorowanie wydajności usługi SNMP, usuń zaznaczenie z pola wyboru **Włącz**.

Uwagi

- *Jeżeli w otwartym dla danego węzła oknie **Monitorowanie** karta **Wydajność SNMP** nie jest dostępna, oznacza to, że w danym węźle nie został uruchomiony agent SNMP lub opcja zarządzania za pomocą agenta SNMP jest w programie dla tego węzła aktualnie wyłączona.*
- *Szybszym sposobem na zmianę określonej właściwości wydajności SNMP w kilku węzłach na raz jest zaznaczenie tychże węzłów. W tym celu należy, korzystając z klawisza **Ctrl**, zaznaczyć te węzły, dla których chcemy włączyć lub wyłączyć monitorowanie wydajności usługi SNMP, a następnie przejść do wykonania opisanych powyżej czynności.*

Zmiana czasu monitorowania

Podstawowy czas monitorowania wszystkich istotnych dla danego węzła informacji (związanych m.in. z usługami sieciowymi, licznikami wydajności itp.) może być zmieniany w oknie **Monitorowanie** na karcie **Ogólne**. Jednakże dla liczników wydajności SNMP istnieje w programie możliwość oddzielnego określenia czasu monitorowania.

Aby zmienić czas monitorowania wydajności usługi SNMP dla danego węzła

1. Kliknij dany węzeł prawym przyciskiem myszy, w menu podręcznym wskaż pozycję **Monitorowanie**, a następnie wybierz polecenie **Wydajność SNMP**.
2. W polu **Czas monitorowania** wpisz wybraną wartość czasu monitorowania (w minutach), która ma być stosowana podczas monitorowania wydajności SNMP.

Uwagi

- *Jeżeli pole **Czas monitorowania** zostanie pozostawione puste, wówczas dla potrzeb monitorowania wydajności usługi SNMP wykorzystywany będzie podstawowy czas monitorowania (określony na karcie **Ogólne**).*
- *Użytkownik może w oknie **Widok sieci** zaznaczyć wiele węzłów, a następnie zmienić czas monitorowania wydajności usługi SNMP równocześnie we wszystkich wybranych węzłach. W tym celu należy, korzystając z klawisza **Ctrl**, zaznaczyć odpowiednie węzły, a następnie przejść do wykonania opisanych powyżej czynności.*
- *Jeżeli po lewej stronie pola **Czas monitorowania** wyświetlana jest ikona **Kłódka**, oznacza to, że dla wybranych węzłów pole to nie zostanie zmienione. Jeżeli natomiast po lewej stronie tego pola wyświetlana jest ikona **Zaznaczenie**, oznacza to, że dla wybranych węzłów pole to zostanie zmienione (w polu tym wpisana zostanie nowa wartość).*
- *Jeżeli w danym polu wprowadzone już zostały pewne zmiany, a chcemy z nich zrezygnować i pozostawić to pole w stanie niezmienionym, wystarczy kliknąć ikonę **Zaznaczenie**, znajdującą się na lewo od takiego pola. Zmieni się ona wówczas z powrotem w ikonę **Kłódka**, wskazując, że dla wszystkich wybranych węzłów dane pole zostanie pozostawione w stanie niezmienionym.*

Opcje systemów Linux/Unix

Karta **Linux/Unix** pojawia się w oknie **Monitorowanie** jedynie w przypadku, gdy program rozpoznał, że w danym węźle została uruchomiona jedna z wersji systemu operacyjnego Linux lub system pochodny od platformy Unix. Na karcie tej możliwe jest określenie nazwy użytkownika i hasła, służących do logowania w węźle Linux/Unix, oraz hasła administratora systemu, dzięki czemu na węźle tym mogą być wykonywane wszelkie skrypty lub programy uruchamiane przez NetCruncha (o ile tylko tego rodzaju zdalne akcje zostały dla danego węzła zdefiniowane). W rzeczywistości program łączy się z węzłem Linux/Unix za pomocą usługi Telnet lub SSH, a następnie loguje się jako administrator systemu używając polecenia *su*.

Aby określić parametry logowania w systemie Linux

1. Kliknij dany węzeł Linux prawym przyciskiem myszy, w menu podręcznym wskaż pozycję **Monitorowanie**, a następnie wybierz polecenie **Właściwości**.
2. Kliknij kartę **Linux/Unix** znajdującą się w górnej części okna.

3. W polu **Zaloguj się jako** wpisz nazwę użytkownika, która ma być wykorzystywana podczas logowania do tego węzła.
4. W polu **Hasło** wpisz hasło użytkownika.
5. W polu **Hasło administratora systemu** wpisz hasło, które będzie wykorzystywane do logowania za pomocą polecenia *su*.

Alertowanie

NetCrunch umożliwia konfigurowanie alertowania na trzech poziomach – dla pojedynczego węzła, dla mapy lub dla całego atlasu. Jeżeli włączanie alertów odbywa się na poziomie mapy lub atlasu, wówczas mamy do czynienia z tworzeniem reguł alertowania. Niemniej jednak procedura definiowania zdarzeń, ich włączania, wyłączania lub kojarzenia ze zdarzeniem określonego zestawu akcji przeprowadzana jest zawsze w ten sam sposób – bez względu na to, czy odbywa się to na poziomie atlasu, mapy czy węzła.

Aby ułatwić procedurę konfiguracji alertów, program został wstępnie wyposażony w zestaw najczęściej wykorzystywanych rodzajów zdarzeń. Natomiast do tworzenia nowych rodzajów zdarzeń służy kreator *Warunki zdarzenia*. Chcąc utworzyć nowy rodzaj zdarzenia, należy zapoznać się z rozdziałem *Definiowanie nowych zdarzeń* na stronie 34.

Skonfigurowanie alertowania dla danego węzła oznacza, że w przypadku, gdy w węźle tym spełnione zostaną warunki wystąpienia określonych zdarzeń, wówczas te zdarzenia, które zostały wcześniej włączone, będą odpowiednio przetwarzane. Oznacza to również, że w przypadku gdy dla danego węzła zdarzenie takie zostanie wygenerowane, uruchomione zostaną odpowiednie skojarzone z nim akcje (o ile takowe zostały zdefiniowane). Do konfigurowania zdarzeń i akcji związanych z alertowaniem służy okno **Konfiguracja alertów**.

Aby dla danego węzła przeprowadzić czynności związane z alertowaniem

1. W oknie **Widok sieci** zaznacz wybrany węzeł.
2. W menu **Węzeł** wskaż pozycję **Alerty**, a następnie wybierz polecenie **Konfiguruj**.
3. W oknie **Konfiguracja alertów** wykonaj odpowiednie czynności związane z alertowaniem. W lewym panelu możesz wybrać lub dodać nowe zdarzenia. W górnej części prawego panelu możesz włączyć lub wyłączyć generowanie aktualnie wybranego zdarzenia, względnie wprowadzić dziedziczenie jego generowania. W prawym panelu możesz również zdefiniować i skojarzyć odpowiednie akcje z aktualnie wybranym zdarzeniem.

Uwaga

*Gdy wybrano opcję **Generuj zdarzenie, jeżeli istnieje definicja dziedziczona**, wówczas o tym, czy dane zdarzenie jest włączone czy wyłączone, decyduje definicja dziedziczona. Oznacza to, że o jego włączeniu lub wyłączeniu będą decydować ustawienia określone dla atlasu lub mapy, do której należy dany węzeł. Warto przy tym podkreślić, że gdy określony węzeł należy do dwóch lub większej liczby map (z których dla co najmniej jednej dane zdarzenie jest włączone, podczas gdy dla pozostałych jest ono wyłączone), wówczas w ramach dziedziczenia zdarzenie to będzie dla tego węzła automatycznie*

włączone – będzie ono generowane, gdy tylko w danym węźle spełnione zostaną wszystkie warunki jego wystąpienia.

Raportowanie

Funkcja raportowania obejmuje zbieranie odpowiednich informacji pochodzących z monitorowanej sieci i późniejsze ich prezentowanie w przystępnej postaci, na przykład w formie tabeli lub wykresu. Raportowanie definiuje się w programie na trzech poziomach – całego atlasu, wybranej mapy lub pojedynczego węzła. Włączenie określonego raportu dla danego węzła oznacza, że zbierane będą wszelkie informacje niezbędne do jego wygenerowania (uzależnione od wybranego rodzaju raportu).

Ogólne procedury stosowane na wszystkich trzech poziomach wyglądają tak samo. Użytkownik może włączyć lub wyłączyć określony raport lub zdecydować o dziedziczeniu odpowiednich ustawień od mapy lub atlasu, do których należy dany węzeł. Gdy określony raport zostaje włączony, NetCrunch rozpoczyna zbieranie wszelkich danych niezbędnych do tego, aby później na ich podstawie wygenerować za pomocą **Przeglądarki raportów** przejrzystą tabelę lub wykres z odpowiednimi informacjami.

Aby ułatwić tworzenie raportów, NetCrunch został wyposażony w zestaw gotowych, wstępnie zdefiniowanych rodzajów raportów. Włączanie, wyłączanie lub wprowadzanie dziedziczenia odpowiednich ustawień dla węzła odbywa się w oknie **Konfiguracja raportów**. Ponadto program umożliwia określenie częstotliwości generowania raportu oraz zdecydowanie o tym, do kogo i jak często ma on być przesyłany.

Aby skonfigurować raportowanie dla danego węzła

1. W oknie **Widok sieci** zaznacz wybrany węzeł.
2. W menu **Węzeł** wskaż pozycję **Raporty**, a następnie wybierz polecenie **Konfiguruj**.
3. W oknie **Konfiguracja raportów** wykonaj odpowiednie czynności związane z raportowaniem. W lewej części okna możesz wybierać lub dodawać raporty. W prawej górnej części okna w liście rozwijanej można włączyć lub wyłączyć generowanie aktualnie wybranego raportu, względnie wprowadzić dziedziczenie jego generowania. W prawej części okna możesz również określić jak często ma on być generowany oraz do kogo program NetCrunch powinien przesyłać gotowy raport.

Uwagi

- *Więcej informacji na temat okna **Konfiguracja raportów**, włączania raportu, dodawania i usuwania odbiorców oraz zmiany ich parametrów zawiera rozdział* Przydzielanie raportów *na stronie 96.*
- *Po włączeniu dla danego węzła określonego raportu program zacznie zbierać w tle wszelkie dane niezbędne do jego wygenerowania. Informacje te można później przeglądać i analizować w oknie **Przeglądarka raportów** w postaci odpowiednich tabel lub wykresów (w tym celu należy kliknąć ikonę **Raporty**, znajdującą się na głównym pasku narzędzi).*

Zarządzanie mapą

Właściwości

Aby zmienić właściwości wybranej mapy, należy albo z jej menu podręcznego w oknie **Atlas sieci** wybrać polecenie **Właściwości**, albo otworzyć menu podręczne w oknie **Widok sieci** i z niego wybrać polecenie **Właściwości**. Jeszcze innym sposobem jest bezpośrednie wybranie polecenia **Właściwości** z menu **Mapa**.

Właściwości mapy pogrupowane są na kilku kartach. W zależności od rodzaju mapy, niektóre z tych kart mogą nie być dostępne.

Karty z właściwościami mapy:

Ogólne	W przypadku map należących do widoków własnych karta ta pozwala nadać mapie nową nazwę oraz tak zmienić jej rodzaj, aby była ona w programie traktowana albo jak mapa utworzona ręcznie, albo jak mapa filtrowana, a także wprowadzić odpowiednie kryteria filtrowania. Natomiast w przypadku map należących do sekcji *Sieci IP* użytkownik może dla określonej sieci wprowadzić ograniczenie ruchu monitorowania.
Automatyczne wykrywanie (Sieci IP)	W przypadku sieci należącej do sekcji *Sieci IP* istnieje możliwość włączenia automatycznego skanowania sieci, która przedstawiona jest na danej mapie. Można również określić częstotliwość takiego skanowania oraz stosowane filtry.
Automatyczne rozmieszczanie	Karta ta umożliwia włączenie automatycznego rozmieszczania węzłów na mapie. Podczas każdorazowego dodawania do mapy nowego węzła lub usuwania z niej jakiegoś węzła, węzły na takiej mapie zostaną automatycznie rozmieszczone.
Reguły alertów	Karta ta pozwala określić dla danej mapy reguły alertowania.
Reguły raportów	Karta ta pozwala określić dla danej mapy reguły raportowania.
Zdalny dostęp	Karta ta pozwala zmienić prawa dostępu zdalnego do określonego obiektu mapy dla wszystkich profili zdalnego dostępu.

Ogólne

W zależności od rodzaju danej mapy, karta **Ogólne**, wyświetlana w oknie właściwości, może przybierać różny wygląd.

Mapy należące do sieci IP

W przypadku map należących do sekcji *Sieci IP* użytkownik może jedynie określić jedną ogólną właściwość, która w wybranej sieci pozwala ograniczyć ruch związany

z monitorowaniem. Jeżeli w danej sieci nałożone zostanie ograniczenie na ruch monitorowania, to tym samym automatycznie zwiększony zostanie odstęp czasu, w jakim monitorowane będą węzły należące do takiej sieci. Ta wyjątkowa cecha programu NetCrunch pomaga skutecznie monitorować nawet znaczną liczbę węzłów zdalnych.

Uwagi

- *Jeżeli dana sieć znajduje się za kilkoma bramami (sieciami), ruch monitorowania będzie ograniczany przez każde wprowadzone po drodze ograniczenie.*
- *Ponadto w oknie **Ruch monitorowania** użytkownik możne zmienić ograniczenie ruchu monitorowania dla dowolnej sieci logicznej.*

Mapy należące do sekcji Widoki własne

W przypadku map należących do sekcji *Widoki własne* użytkownik może zmienić kilka związanych z nimi właściwości ogólnych, takich jak:

- nazwa mapy,
- rodzaj mapy (filtrowana lub nie),
- kryteria filtrowania dla mapy filtrowanej.

Uwaga

*Nazwa mapy może zostać również w szybki sposób zmieniona bez konieczności otwierania okna **Właściwości mapy**. Wystarczy w tym celu w oknie **Atlas sieci** zaznaczyć daną mapę, a następnie z menu podręcznego wybrać polecenie **Zmień nazwę**.*

Zmiana rodzaju mapy

Zawartość map należących do sekcji *Widoki własne* może być zarządzana albo automatycznie przez program, albo ręcznie przez użytkownika. Uzależnione to jest od rodzaju mapy, która może być:

	**Utworzona ręcznie** *(statyczna)*	Wszystkie węzły muszą zostać ręcznie umieszczone na mapie przez użytkownika.
	**Filtrowana** *(dynamiczna)*	Na podstawie kryteriów filtrowania określonych przez użytkownika program przeprowadza automatyczną aktualizację węzłów mapy. Użytkownik może jedynie uzupełniać taką mapę o dodatkowe elementy graficzne oraz odsyłacze do innych map.

Uwaga

*Jedna z dwóch przedstawionych powyżej specjalnych ikon, wyświetlana w oknie **Atlas sieci** na lewo od nazwy każdej mapy, znacznie pomaga w szybkim zidentyfikowaniu rodzaju mapy.*

Zmiana kryteriów filtrowania

Kryteria filtrowania wykorzystywane przy tworzeniu mapy z widokiem filtrowanym mogą zostać przez użytkownika w dowolnej chwili zmienione. Cecha ta okazuje się szczególnie przydatna w sytuacji, gdy aktualny zakres sieci przedstawiony na mapie widoku filtrowanego

jest albo zbyt wąski, albo zbyt szeroki w stosunku do tego, co chcielibyśmy na takiej mapie przedstawić.

W odpowiednim oknie wyświetlane są wszystkie aktualne wyrażenia filtrujące. Mogą do nich zostać dodane nowe wyrażenia (nawiasy lub warunki), jak również mogą zostać usunięte lub zmienione dowolne z wyświetlanych wyrażeń. Szczegółowe omówienie kryteriów filtrowania można znaleźć w rozdziale *Określanie kryteriów filtrowania* na stronie 125.

Automatyczne wykrywanie sieci

Mapy przedstawiające sieci TCP/IP umożliwiają użytkownikowi zarządzanie opcjami automatycznego wykrywania sieci dla każdej wybranej sieci. Możliwe jest przy tym ustalenie odstępu czasu dla procesu wykrywania, a także określenie reguł filtrowania, jakie mają być stosowane podczas reskanowania sieci.

Uwaga

*W celu wykonania procedury automatycznego wykrywania sieci wywoływany jest oddzielny proces o nazwie **IScanner**.*

Automatyczne rozmieszczanie

W przypadku map, które mogą automatycznie zmieniać swoją zawartość, program pozwala określić, w jaki sposób mają być rozmieszczane węzły takiej mapy za każdym razem, gdy dodawany jest do niej nowy węzeł lub gdy jakiś węzeł jest z niej usuwany. Węzły mogą być grupowane według ich lokalizacji (zapisanej w odpowiednim polu SNMP w każdym węźle) oraz według ich sieci logicznych (jeżeli na aktualnej mapie wyświetlane są węzły pochodzące z więcej niż jednej mapy logicznej). Użytkownik może także określić styl ramki służącej do takiego grupowania.

Uwagi

- *Jeżeli dla danej mapy włączone zostało **Automatyczne rozmieszczanie**, a następnie użytkownik sam zmienił rozmieszczenie węzłów, wówczas zaznaczenie tej opcji zostanie automatycznie usunięte.*
- *Węzły można także rozmieścić w dowolnej chwili, po wybraniu z menu **Mapa** polecenia **Rozmieść węzły**. Więcej informacji na ten temat zawiera rozdział* Rozmieszczanie węzłów *na stronie 183.*

Reguły alertów

Konfigurowanie alertu w NetCrunchu można przeprowadzać na trzech poziomach – dla węzła, mapy lub całego atlasu. Jednakże, w ogólnym zarysie, procedura definiowania zdarzenia – włączania lub wyłączania go oraz przypisywania danemu zdarzeniu określonego zestawu akcji – jest we wszystkich tych przypadkach bardzo podobna. Konfigurowanie alertowania dla mapy oznacza ustanowienie dla niej pewnych reguł alertowania.

Jeśli określone zostały reguły alertowania dla mapy, oznacza to, że dla wszystkich węzłów należących do tej mapy zbierane będą dane dotyczące włączonych zdarzeń. Oznacza to również, że w przypadku gdy zdarzenia te wystąpią w którymkolwiek z węzłów mapy, podjęte zostaną odpowiednie skojarzone z nimi akcje (o ile takowe zostały zdefiniowane).

Uwagi

- *Obszerne omówienie zagadnienia alertowania wraz ze szczegółowym przedstawieniem wszystkich możliwości wykorzystania opisywanego tutaj okna zawiera rozdział* Alertowanie *na stronie 19.*
- *Zdarzenie dla danej mapy może być włączone, wyłączone lub jego stan może być dziedziczony od atlasu (ustawienia określone we właściwościach atlasu będą decydowały, czy dane zdarzenie będzie włączone, czy też nie).*

Reguły raportów

Reguły raportowania mogą zostać zdefiniowane albo dla całego atlasu, albo dla wybranej mapy. Raportowanie może także zostać włączone dla pojedynczego węzła. Włączenie danego raportu dla określonej mapy oznacza, że w ramach tej mapy zbierane będą wszelkie niezbędne dane (uzależnione od wybranego rodzaju raportu), w sposób umożliwiający ich późniejsze przedstawienie w postaci graficznej.

Ogólne procedury stosowane na wszystkich trzech poziomach (atlasu, mapy czy węzła) wyglądają tak samo. Użytkownik może dla danej mapy włączyć lub wyłączyć określony raport względnie ustanowić dziedziczenie odpowiednich ustawień od atlasu (co oznacza, że o tym czy będzie on włączony, czy też nie, decydować będą ustalone wcześniej reguły atlasu).

Aby ułatwić tworzenie raportów, NetCrunch został wyposażony w zestaw gotowych, wstępnie zdefiniowanych raportów, pogrupowanych według ich zastosowań. Raporty dla map różnią się od raportów dla węzłów tym, że te pierwsze uwzględniają informacje pochodzące z wielu różnych węzłów. Ponadto program umożliwia określenie częstotliwości generowania raportu dla danej mapy (odstępu czasu, w jakim ma się to odbywać) oraz zdecydowanie o tym, do kogo i jak często ma on być przesyłany.

Uwagi

- *Więcej informacji na temat okna* ***Konfiguracja raportów****, włączania raportu, dodawania i usuwania odbiorców oraz zmiany ich właściwości zawiera rozdział* Korzystanie z raportów *na stronie 95.*
- *Po włączeniu dla danej mapy określonego raportu program zacznie zbierać w tle wszelkie dane niezbędne do jego wygenerowania. Informacje te można później przeglądać i analizować w oknie* ***Przeglądarka raportów*** *w postaci odpowiednich tabel lub wykresów (w tym celu należy kliknąć ikonę* **Raporty***, znajdującą się na głównym pasku narzędzi).*

Właściwości zdalnego dostępu

Profile zdalnego dostępu służą do przechowywania odpowiednich praw dostępu do różnorodnych obiektów programu przy użyciu przeglądarki internetowej. Dzięki ich zastosowaniu można szybko powiązać dany profil zdalnego dostępu ze zdefiniowanym użytkownikiem, przyznając mu tym samym ściśle sprecyzowane prawa dostępu do funkcji programu w zakresie niezbędnym do wykonywania określonych czynności administracyjnych.

W przypadku zdefiniowanego już profilu zdalnego dostępu możliwe jest szybkie edytowanie różnorodnych praw dostępu związanych z obiektem atlasu. Odbywa się to w oknie **Właściwości mapy** związanym z mapą poprzez wybór karty **Zdalny dostęp**.

Aby zmodyfikować uprawnienia zdefiniowane w profilu zdalnego dostępu dla mapy

1. W oknie **Atlas sieci** wskaż pozycję **Właściwości**.
   Otworzy się okno **Właściwości mapy**.
2. Kliknij kartę **Zdalny dostęp**.
3. Z listy **Dostępne profile zdalnego dostępu** wybierz zdalny profil, który ma zostać zmodyfikowany.
   Poniżej zostaną wyświetlone aktualnie obowiązujące prawa dostępu do obiektów mapy (należące do zaznaczonego profilu zdalnego dostępu).
4.  Aby dodać nowe prawo, kliknij ikonę ***Dodaj uprawnienie***, a następnie w nowo otwartym oknie **Właściwości praw dostępu** określ docelowe prawa dostępu do obiektu atlasu.
    Aby zmodyfikować właściwości istniejącego prawa dostępu, wskaż go na liście i kliknij ikonę ***Edytuj uprawnienie***. W oknie **Właściwości praw dostępu** dokonaj stosownych zmian.
    Aby usunąć istniejące prawo dostępu, wskaż je na liście i kliknij ikonę ***Usuń uprawnienie***.

Uwagi

- *Możliwe jest zmienianie praw dostępu dla dowolnej ilości węzłów zdefiniowanych w profilu zdalnego dostępu – służy do tego funkcja wielokrotnego wyboru. W tym celu należy przed podjęciem kroków opisanych w punkcie 1 wybrać wszystkie docelowe węzły na mapie.*
- *Należy pamiętać, że zmiany dokonywane w prawach dostępu – oraz ich zapis w profilu zdalnego dostępu – obejmują swym zasięgiem wszystkich zdalnych użytkowników skojarzonych z danym profilem.*
- *W celu uzyskania dodatkowych informacji związanych z profilami zdalnego dostępu, por. sekcję* Zarządzanie profilami zdalnego dostępu *na stronie 196 a także wszystkie kolejne sekcje.*

Operacje na mapach

Wstawianie węzła

Węzeł może zostać wstawiony wyłącznie na mapę należącą do sekcji *Sieci IP*, *Widoki własne* lub do zbiorczej tabelarycznej listy *Wykaz węzłów*. Procedura ta w każdym z tych przypadków wygląda inaczej. Dodawanie węzłów do map należących do sekcji *Topologia fizyczna* nie jest możliwe. Mapy należące do tej sekcji są traktowane jako fizyczna reprezentacja danej sieci lokalnej.

Wstawianie węzła na mapę w sekcji Sieci IP

Do map logicznych należących do sekcji *Sieci IP* mogą być dodawane zupełnie nowe węzły (takie, z którymi program wcześniej nie miał do czynienia). Sekcja *Sieci IP* zawiera logiczną

reprezentację sieci lokalnych oraz sieci odległych. NetCrunch może oczywiście sam przeprowadzić automatyczne wykrywanie w monitorowanej sieci nowych węzłów i dodać je do odpowiedniej mapy logicznej w sekcji *Sieci IP* bez konieczności jakiejkolwiek ingerencji ze strony użytkownika. Więcej informacji na ten temat zawiera rozdział *Automatyczne wykrywanie sieci* na stronie 175.

Aby wstawić węzeł na mapę w sekcji Sieci IP

1. W oknie **Atlas sieci** zaznacz mapę należącą do sekcji *Sieci IP*, do której chcesz dodać nowy węzeł.
2. Z menu **Wstaw** wybierz polecenie **Węzeł**.
3. W polu **Adres IP węzła** wpisz adres IP nowo dodawanego węzła.

Uwagi

- *W punkcie 3. pierwsza część logicznego adresu IP jest już w omawianym polu wypełniona przez program. Dzieje się tak, ponieważ taki nowy węzeł musi należeć do logicznej sieci IP, którą reprezentuje wybrana mapa.*
- *Nowo wstawiany węzeł może zostać umieszczony na mapie w sposób nieprawidłowy. Aby umieścić go we właściwym położeniu, należy z menu **Mapa** wybrać polecenie **Rozmieść węzły**.*

Wstawianie węzła na mapę w sekcji Widoki własne

Sekcja *Widoki własne* grupuje mapy, które stanowią jedynie częściowy widok logicznej reprezentacji sieci (takiej, jaka wyświetlana jest w sekcji *Sieci IP*). Wstawienie węzła na mapę należącą do sekcji *Widoki własne* możliwe jest tylko w przypadku, gdy mapa ta została utworzona ręcznie (jest typu statycznego). Ręczne wstawienie węzła nie jest możliwe w przypadku mapy widoku filtrowanego, której elementy są dynamiczne (to znaczy są automatycznie aktualizowane przez program).

Aby wstawić węzeł na mapę w sekcji Widoki własne

1. W oknie **Atlas sieci** zaznacz dowolną ręcznie utworzoną mapę z sekcji *Widoki własne*.
2. Z menu **Wstaw** wybierz polecenie **Węzeł**. Zamiast tego możesz kliknąć prawym klawiszem myszy dowolne miejsce w oknie **Widok sieci**, wskazać w menu podręcznym polecenie **Wstaw**, a następnie w tak otwartym menu kliknąć pozycję **Węzeł**.
3. Jeżeli znasz nazwę lub adres IP nowo wstawianego węzła, wpisz jeden z tych identyfikatorów w polu **Adres IP lub nazwa DNS węzła**. Kliknij przycisk **OK**. W przeciwnym przypadku kliknij ikonę ***Wybierz węzeł***.
4. Z listy wyświetlanej w oknie **Wybierz węzeł** wybierz węzeł lub węzły, które zamierzasz wstawić na mapę należącą do sekcji *Widoki własne*, a następnie kliknij przycisk **OK**.

Uwagi

- *Możliwe jest jednoczesne wstawienie na pustą mapę więcej niż jednego węzła. W tym celu w punkcie 4. należy, korzystając z klawisza **Ctrl**, zaznaczyć te węzły, które mają być dodane do ręcznie utworzonej mapy.*
- *Jeżeli węzeł, który chcielibyśmy dodać, nie jest widoczny na liście w oknie **Wybierz węzeł** (w punkcie 4.), oznacza to, że węzeł ten jest dla programu nieznany (nie jest on aktualnie monitorowany). Albo nie*

został on wykryty podczas skanowania sieci, albo nie wstawiono go na żadną z map należących do sekcji Sieci IP. *O tym jak dodać nowy węzeł do mapy należącej do sekcji* Sieci IP *traktuje rozdział* Wstawianie węzła na mapę w sekcji Sieci IP *na stronie 177.*

Wstawianie urządzeń warstwy 2

Po włączeniu – przy użyciu specjalnego kreatora – funkcji prezentacji map topologii segmentów fizycznych, NetCrunch próbuje utworzyć najbardziej optymalne odwzorowanie fizycznej warstwy sieci. Topologia segmentów fizycznych w NetCrunchu jest odwzorowywana w postaci drzewa, którego korzeniem w każdym przepadku jest most, do którego podłączony jest węzeł z NetCrunchem. Później może zajść potrzeba ręcznego wstawienia dodatkowych urządzeń warstwy 2, takich jak przełączniki lub koncentratory, które nie zostały znalezione i umieszczone na mapie przez Kreatora konfiguracji segmentów fizycznych. W korzeniu mapy segmentów fizycznych można dodawać tylko urządzenia warstwy 2. Jednakże kiedy owe urządzenia zostaną skonfigurowane – poprzez wypełnienie ich tablic przekazywania – program odpowiednio skoryguje ich położenie w obrębie drzewa w trybie automatycznym.

Aby wstawić urządzenie warstwy 2

1. Kliknij sekcję *Segmenty fizyczne* w oknie Atlas sieci.
   Korzeń mapy topologii segmentów fizycznych wyświetli okno **Widok sieci**.
2. W menu **Wstaw** wybierz opcję **Urządzenie warstwy 2**.
   Otworzy się kreator *Dodaj urządzenie warstwy 2*.
3. Kliknij przycisk opcji **Dodaj urządzenie warstwy 2**, jeśli chcesz ręcznie dodać nowe urządzenie, np. przełącznik. Przejdź do punktu 4.
   Wybierz przycisk opcji **Dodaj most statyczny**, jeśli chcesz ręcznie dodać urządzenie statyczne, jak np. koncentrator. Przejdź do punktu 7.
4. W polu **Nazwa** lub **Adres IP** wpisz adres IP lub nazwę DNS nowego urządzenia warstwy 2. Możesz kliknąć ikonę *Przeglądaj*, aby odszukać żądany węzeł na liście.
5. W polu **Port SNMP** wpisz numer portu SNMP używany przez usługę SNMP na węźle.
6. W rozwijanej liście **Profil SNMP** wybierz profil SNMP i kliknij **Dalej**.
7. Kliknij **OK**.
   Nowe urządzenie wyświetli się w mapie segmentów fizycznych.

Uwagi

- *Dodawanie urządzeń warstwy 2 jest możliwe tylko wówczas, gdy w programie włączone jest monitorowanie segmentów fizycznych. Czynność ta odbywa się w opcjach programu lub poprzez kliknięcie sekcji* Segmenty fizyczne *w oknie* ***Atlas sieci****.*
- *W punkcie 6 można kliknąć ikonę* ***Edytuj profil****, aby zmodyfikować właściwości profilu SNMP lub utworzyć nowy – np. by używać innej wspólnoty odczytu (SNMPv1) lub zapisać dane uwierzytelnienia i hasło użytkownika (SNMPv3).*
- *Jeśli po wykonaniu kroku opisanego w punkcie 6 NetCrunch nie zdołał uzyskać odpowiednich informacji SNMP, wskazane urządzenie można dodać jako zdefiniowany przez użytkownika most*

*statyczny (którego można później skonfigurować). W tym celu zaznacz pole wyboru **Utwórz most statyczny** przed kliknięciem **OK**.*

- *Aby dowiedzieć się, jak konfiguruje się umieszczony przez użytkownika most statyczny, zapoznaj się z poniższą sekcją* Konfigurowanie mostu statycznego.
- *Choć węzłów wyświetlanych na mapach segmentów fizycznych nie można usuwać, można usuwać mosty statyczne ręcznie wstawione i skonfigurowane przez użytkownika – nie są one bowiem traktowane jako właściwe węzły. Po udanych usunięciu mostu statycznego, mapy segmentów fizycznych są automatycznie korygowane w celu uwzględnienia zmian.*

Konfigurowanie mostu statycznego

Most statyczny nie jest traktowany jako węzeł programu NetCrunch – przykładowo nie można go w żaden sposób monitorować. Po umieszczeniu mostu statycznego w mapie segmentów fizycznych zostanie on natychmiast wyświetlony w drzewie mapy segmentów fizycznych. Następnie należy go odpowiednio skonfigurować, aby został właściwie zaprezentowany w sekcji segmentów fizycznych atlasu sieci. W pierwszej kolejności należy sprawdzić, czy urządzenie jest podłączone do nadrzędnego w stosunku do niego urządzenia warstwy 2 (tj. rodzica, który znajduje się bliżej korzenia drzewa segmentów fizycznych), a jeśli jest, sprawdzić na którym porcie jest ono podłączone. Następnie należy wypełnić tablicę przekazywania dla wszystkich dodatkowych mostu.

Aby skonfigurować most statyczny

1. Kliknij prawym przyciskiem myszy most statyczny znajdujący się na mapie segmentów fizycznych i w jego podręcznym menu wybierz polecenie **Konfiguracja mostu statycznego**.
   Otworzy sie kreator *Konfiguracja mostu statycznego*.
2. W polu **Nazwa** określ nazwę urządzenia, którą będzie posługiwał się NetCrunch.
3. W polu **Liczba portów** wpisz liczbę portów mostu i kliknij **Dalej**.
4. Jeśli chcesz umieścić most statyczny na szczycie drzewa segmentów fizycznych, wybierz przycisk opcji **Most statyczny nie jest podłączony do innych urządzeń warstwy 2** i przejdź do punktu 8.
   Jeśli urządzenie posiada nadrzędne w stosunku do siebie urządzenie warstwy 2 (tj. rodzica), które znajduje się bliżej drzewa segmentów fizycznych, wybierz przycisk opcji **Most statyczny posiada nadrzędne urządzenie warstwy 2**.
5. Używając rozwijanej listy **Rodzic**, wybierz istniejące urządzenie warstwy 2, które ma być rodzicem mostu statycznego.
6. Korzystając z rozwijanej listy **Port rodzica** wybierz numer portu, do którego podłączony jest most statyczny na urządzeniu nadrzędnym (rodzicu).
7. Korzystając z rozwijanej listy **Port mostu statycznego** wybierz numer portu, do którego podłączone jest urządzenie nadrzędne (rodzic) na moście statycznym, a następnie kliknij **Dalej**.

8. Wybierz port w polu **Porty** i kliknij ikonę ***Dodaj***.
   Otworzy się okno **Wybierz węzeł lub mapę**.

9. Wybierz węzeł podłączony do tego portu i kliknij **OK**.
   Węzeł pojawi się w polu **Port tablicy przekazywania**.
10. Powtórz kroki opisane w punktach 8 i 9 dla każdego portu, dla którego należy skonfigurować połączenie.
11. Kliknij **OK**.
    Most statyczny zostanie automatycznie przeniesiony w odpowiednie miejsce w drzewie mapy segmentów fizycznych, a same mapy segmentów fizycznych zostaną ponownie narysowane.

Uwagi

- *Okno **Wybierz węzeł lub mapę** będzie prezentować tylko te węzły, które aktualnie nie znajdują się w żadnej strukturze segmentów fizycznych oraz te, które można podłączyć do przełącznika stosownie do ich aktualnego położenia drzewie segmentów fizycznych.*
- *W punkcie 8 można wybrać określony port – w tym celu kliknij ikonę **Właściwości** i w nowo otwartym oknie dialogowym wpisz inną nazwę portu.*
- *Aby usunąć określony węzeł z połączenia portu na tablicy przekazywania, wybierz port w polu **Porty** oraz węzeł w polu **Port tablicy przekazywania**, a następnie kliknij ikonę **Usuń**.*
- *Wstawianie urządzenia warstwy 2 do drzewa mapy segmentów fizycznych opisuje zamieszczona powyżej sekcja* Wstawianie urządzeń warstwy 2 .

Wstawianie odsyłacza do innej mapy

Na mapie należącej do sekcji *Sieci IP* lub *Widoki własne* można umieścić odsyłacz do innej mapy (poprzez wstawienie specjalnej ikony odsyłacza). Opcja ta jest szczególnie przydatna w sytuacji, gdy do danego atlasu należy wiele różnych map. Wstawianie na różnych mapach odpowiednich odsyłaczy do innych map pozwala w wygodny przechodzić do wyświetlania wskazywanych w ten sposób map bez konieczności ich wcześniejszego odszukiwania w oknie **Atlas sieci**. Aby w szybki sposób wyświetlić daną mapę w oknie **Widok sieci**, należy dwukrotnie kliknąć ikonę jej odsyłacza, umieszczoną na innej mapie.

Ikona odsyłacza symbolizująca inną mapę może, przez zmianę swojego koloru, sygnalizować aktualny stan takiej mapy. Jeżeli ikona taka wyświetlana jest w kolorze domyślnym, oznacza to, że wszystkie węzły należące do danej mapy odpowiadają. Jeżeli ikona zmieni kolor na żółty, oznacza to, że co najmniej jeden węzeł znajduje się w stanie ostrzegawczym, lub co najmniej jeden z węzłów nie odpowiada. Jeżeli wreszcie ikona odsyłacza zmieni kolor na czerwony, świadczy to o tym, że wszystkie węzły mapy docelowej nie odpowiadają.

Aby wstawić odsyłacz do innej mapy

1. W oknie **Atlas sieci** zaznacz wybraną mapę.
2. Z menu **Wstaw** wybierz polecenie **Odsyłacz do mapy**.
3. W oknie **Wstaw odsyłacz do mapy** wybierz mapę, do której chcesz wstawić odsyłacz.

Uwaga

Nowo utworzony odsyłacz do mapy zostanie umieszczony na mapie w sposób zupełnie przypadkowy. Aby umieścić taki odsyłacz w żądanym położeniu, należy kliknąć ikonę **Edytuj mapę**, *przeciągnąć go do wybranego miejsca i upuścić.*

Usuwanie węzłów

Węzły mogą być usuwane z map należących do sekcji *Sieci IP* lub *Widoki własne*. Jednakże podczas usuwania węzłów z map logicznych znajdujących się w sekcji *Sieci IP* należy zachować szczególną ostrożność. Podyktowane jest to tym, że taki usuwany węzeł zostanie także usunięty ze wszystkich innych map (należących do sekcji *Widoki własne*). Gdy natomiast dany węzeł jest usuwany z mapy należącej do sekcji *Widoki własne*, nie ma to żadnego wpływu na którąkolwiek z pozostałych map atlasu. Na przykład usunięty w ten sposób węzeł będzie nadal wyświetlany na mapie w sekcji *Sieci IP*.

Aby usunąć węzeł z mapy

1. W oknie **Widok sieci** wybierz węzeł, który chcesz usunąć.
2. Z menu **Edycja** wybierz polecenie **Usuń** lub naciśnij bezpośrednio klawisz **Delete**.
3. Kliknij przycisk **Tak**, aby potwierdzić usunięcie węzła.

Uwaga

Zaleca się usuwanie węzłów wyłącznie z map należących do sekcji Widoki własne.

Kopiowanie węzła na mapę

Węzły mogą być kopiowane na dowolną inną mapę należącą do sekcji *Widoki własne*, pod warunkiem, że mapa ta została utworzona ręcznie (tzn. nie jest rodzajem widoku filtrowanego, którego zawartość jest automatycznie uaktualniana przez program).

Aby skopiować węzeł na mapę w sekcji Widoki własne

1. W oknie **Widok sieci** kliknij prawym przyciskiem myszy węzeł, który chcesz skopiować na inną mapę, a następnie z menu podręcznego wybierz polecenie **Skopiuj do**.
2. W oknie **Skopiuj węzły do** wybierz mapę, na którą powinien zostać skopiowany wybrany węzeł.

Uwagi

- *Jeżeli w punkcie 2. mapa docelowa nie jest widoczna, należy dwukrotnie kliknąć wyświetlany folder, co spowoduje natychmiastowe pojawienie się należących do niego map.*
- *W punkcie 2. mapy, na które nie można kopiować węzłów, są automatycznie wygaszane.*
- *Na wybraną mapę można równocześnie skopiować kilka węzłów. W tym celu w oknie* ***Widok sieci*** *należy zaznaczyć wszystkie te węzły, która mają być skopiowane, a następnie przejść do wykonania opisanych powyżej czynności.*

Rozmieszczanie węzłów

Na dowolnej mapie (należącej do sekcji *Sieci IP* lub *Widoki własne*) węzły mogą być rozmieszczane albo w sposób ręczny, albo automatyczny z wykorzystaniem okna **Rozmieść węzły**. W tym ostatnim przypadku program może to zrobić samodzielnie, na podstawie pewnych zdefiniowanych przez użytkownika reguł, określających sposób grupowania węzłów oraz styl ramki służącej do takiego grupowania, a także decydujących o tym, czy mają być rysowane połączenia pomiędzy węzłami, czy też nie.

Aby umożliwić ręczne rozmieszczanie węzłów na określonej mapie, konieczne jest wcześniejsze włączenie edycji takiej mapy. Gdy zostanie to już zrobione, możliwe staje się przenoszenie węzłów do nowego miejsca, ich wzajemne łączenie oraz umieszczanie dodatkowych obiektów graficznych, takich jak różnego rodzaju kształty, teksty lub rysunki. Więcej informacji na temat tych funkcji zawiera rozdział *Edytowanie map* na stronie 184.

Aby rozmieścić węzły na mapie

1. Z menu **Mapa** wybierz polecenie **Rozmieść węzły**. Spowoduje to wyświetlenie okna **Rozmieść węzły**.
2. Jeżeli chcesz grupować węzły według ich lokalizacji (łańcucha znaków, za pomocą którego jest ona określona), zaznacz pole wyboru **Lokalizacja SNMP**.
3. Jeżeli chcesz grupować węzły według ich sieci IP, zaznacz pole wyboru **Sieć**.
4. Jeżeli wybrane zostało grupowanie węzłów, możesz dodatkowo wybrać styl ramki służącej do takiego grupowania.
5. Aby rysowane były linie łączące węzły na mapie, zaznacz pole wyboru **Rysuj połączenia między węzłami**.
6. Kliknij przycisk **Podgląd**, aby obejrzeć nowy sposób rozmieszczenia węzłów na mapie.

Uwaga

Węzły na mapie zostaną przez program ponownie rozmieszczone w oparciu o ustawienia wprowadzone w punktach 2-5.

Ustalanie map, do których należy węzeł

NetCrunch umożliwia szybkie ustalenie, do jakich map należy dany węzeł, a nawet bezpośrednie lokalizowanie danego węzła na takich mapach. Powyższa funkcja została udostępniona w menu podręcznym węzła.

Aby zlokalizować węzeł na innych mapach

1. Wybierz węzła na mapie.
2. W menu podręcznym węzła wskaż opcję **Znajdź na**.
   Pojawi się lista pozostałych map, do których należy dany węzeł.
3. Wybierz żądaną mapę.
   Wskazana mapa wyświetli się z zaznaczonym węzłem.

Zarządzanie Notatnikiem węzła

W określonych sytuacjach zachodzi potrzeba zapisania istotnych informacji na temat konkretnych węzłów, na przykład w celu opisania charakterystyki ich funkcjonowania lub właściwości monitorowania. NetCrunch umożliwia wykonywanie tej czynności udostępniając funkcję o nazwie **Notatnik węzła**. Do tworzenia, usuwania lub edycji notatek w programie służy okno **Notatki** bądź okno właściwości danego węzła (karta **Notatki**) – w tym ostatnim wypadku por. sekcję *Notatki węzła* na stronie 145.

W oknie **Notatki** możliwe jest wyszukiwanie notatek węzłów według wybranej mapy i daty. Każda notatka składa się z tematu, daty utworzenia, opisywanego węzła, kategorii i właściwej treści zapisków.

Aby przeglądać notatki węzłów dla mapy

1. Z menu **Widok** wybierz opcję **Notatnik węzła**.
   Otworzy się okno **Notatki**.
2. W pasku narzędzi wskaż mapę, dla której zostaną wyświetlone notatki węzłów.

Uwagi



- *Aby z powyższego okna dodać nową notatkę dla węzła, kliknij ikonę **Dodaj**, a następnie w oknie **Nowa notatka** wpisz treść notatki.*
- *Aby zredagować notatkę węzła, wskaż ją na liście i kliknij ikonę **Edytuj**.*
- *Aby usunąć notatkę, wskaż ją na liście i kliknij ikonę **Usuń**.*

Edytowanie map

W oknie **Widok sieci** można w dowolnej chwili przeprowadzić edycję aktualnej zawartości mapy. Widoczna w nim mapa składa się z ikon węzłów oraz z obiektów dodatkowych, takich jak rysunki, teksty oraz różnego rodzaju kształty w tle. Ponadto dowolne dwa lub więcej spośród takich obiektów może zostać połączonych za pomocą linii połączeń.

Włączanie trybu edycji

Aby możliwe było wprowadzanie zmian w obiektach graficznych na mapach, należy włączyć tryb edycji mapy.

Aby włączyć tryb edycji mapy

1. Kliknij ikonę ***Edytuj mapę***, znajdującą się na pasku narzędzi w oknie **Widok sieci**. Jeżeli ikona ta wyświetlana jest jako wciśnięta, oznacza to, że edycja danej mapy została już włączona. Jeżeli natomiast przycisk ten nie jest wyświetlany jako wciśnięty, edycja mapy jest wyłączona.

Uwagi

- *Domyślnie tryb edycji mapy jest wyłączony.*
- *Tryb edycji mapy może zostać również włączony przez kliknięcie prawym przyciskiem myszy dowolnego miejsca w obszarze stanowiącym tło mapy, a następnie wybranie z menu podręcznego polecenia **Edytuj mapę** lub skorzystanie z kombinacji klawiszy **Ctrl+E**.*

- *Po włączeniu trybu edycji mapy w prawej części okna **Widok sieci** wyświetlony zostaje pasek narzędzi* Edytuj mapę.
- *Jeżeli włączony jest tryb edycji określonej mapy, a w tym czasie zaznaczona zostanie jakakolwiek inna mapa w drzewie atlasu sieci, wówczas tryb edycji zostanie automatycznie wyłączony, a wprowadzone zmiany – zapisane.*

Zmiana położenia obiektów

Gdy tryb edycji mapy jest włączony, ikony węzłów oraz inne obiekty graficzne mogą być w dowolny sposób przenoszone.

Aby przenieść ikonę węzła do nowego miejsca na mapie

1. Zaznacz obiekty (możesz zaznaczyć większą ich liczbę, korzystając z klawisza **Ctrl**), które chcesz przenieść do nowego miejsca na mapie. Gdy zaznaczysz obiekt, który jest tekstem lub kształtem w tle, wówczas na jego bokach oraz w jego narożach pojawią się niewielkie kwadraciki. Gdy natomiast zaznaczysz obiekt, który jest ikoną, wokół niej pojawi się kwadratowa otoczka.
2. Przeciągnij go do nowego miejsca.
   Jeżeli chcesz przenieść taki obiekt za pomocą klawiatury, przytrzymaj wciśnięty klawisz **Ctrl**, a w tym czasie, za pomocą klawiszy strzałek, przenieś go do nowego miejsca na mapie.

Uwagi

- *Jeżeli określony węzeł jest połączony z innymi węzłami i zostanie przeniesiony do nowego miejsca na mapie, jego połączenia pozostaną nadal widoczne.*
- *Użytkownik ma możliwość zaznaczenia wielu węzłów i przeniesienia ich do dowolnego nowego miejsca na mapie. W tym celu należy upewnić się, że tryb edycji mapy jest włączony, a następnie, przytrzymując wciśnięty klawisz **Ctrl**, kliknąć każdy węzeł, który ma zostać przeniesiony. Gdy wszystkie wybrane węzły zostaną w ten sposób zaznaczone, należy przeciągnąć je jednym ruchem do nowego położenia i upuścić lub indywidualnie zmienić ich położenia.*
- *Przy przenoszeniu ikony dowolnego węzła na nowe miejsce na mapie możliwa jest zmiana wykorzystywanego podczas tej operacji skoku siatki. Ponadto można wyłączyć opcję wyrównania do siatki. W takim przypadku, podczas ręcznej zmiany położenia, ikony węzła będą przemieszczane co jeden piksel. Aby zmienić te ustawienia, należy z menu **Narzędzia** wybrać polecenie **Opcje**, a następnie przejść do strony **Mapa**. W otwartym w ten sposób oknie należy zmienić odpowiednie ustawienia.*

Wyrównywanie obiektów

Za pomocą okna **Wyrównanie** program pozwala wyrównywać ikony węzłów oraz inne obiekty, rozproszone na mapie w sposób całkowicie przypadkowy.

Aby wyrównać obiekty na mapie

1. Przytrzymaj wciśnięty klawisz **Ctrl** i zaznacz te obiekty, które chcesz wyrównać. Na pasku narzędzi *Edytuj mapę* kliknij ikonę ***Wyrównaj***.
   Możesz również kliknąć prawym przyciskiem myszy dowolną z zaznaczonych ikon węzła, w menu podręcznym wskazać pozycję **Pozycja**, a następnie wybrać polecenie **Wyrównaj**.

2. Podejmij decyzję o pionowym lub poziomym wyrównaniu węzłów, wybierając odpowiedni przycisk opcji w jednym z dwóch obszarów otwartego w ten sposób okna.
3. Kliknij przycisk **Zastosuj**.

Uwagi

Jeżeli wybrane zostanie zarówno poziome, jaki i pionowe wyrównanie zaznaczonych obiektów, wówczas obiekty zostaną wyrównane w taki sposób, że będą ułożone bezpośrednio jeden na drugim.

Zmiana tła

Tło mapy może zostać zmienione na jeden z następujących rodzajów:

- jednolity kolor wypełnienia,
- wstępnie zdefiniowany rysunek mapy,
- wstępnie zdefiniowana tekstura,
- dowolny obraz wstawiony z pliku (w dowolnie wybranym formacie graficznym),
- cieniowanie.

Aby zmienić właściwości tła mapy

1. Kliknij prawym przyciskiem myszy dowolne miejsce tła mapy i z menu podręcznego wybierz polecenie **Tło**.
2. Z listy rozwijanej **Tło** wybierz odpowiedni rodzaj tła.

Wybór obiektów

Wybór pojedynczego obiektu

Wyboru pojedynczego obiektu w programie dokonuje się po prostu przez zaznaczenie go myszą.

Wybór wielu obiektów

Równoczesnego wyboru wielu obiektów w programie NetCrunch można dokonać na kilka sposobów: wyłącznie za pomocą myszy, przy wykorzystaniu myszy wraz z klawiszami **Ctrl** lub **Shift**, względnie wyłącznie za pomocą klawiszy na klawiaturze.

Pierwsza metoda polega na przeciągnięciu kursora myszy po odpowiednim obszarze (w trakcie tej czynności widoczna będzie tymczasowa prostokątna ramka). Po zwolnieniu klawisza obiekty, które zostały objęte tą ramką, zostaną zaznaczone.

Druga metoda polega na przytrzymaniu wciśniętego klawisza **Ctrl** lub **Shift** i klikaniu tych obiektów, które mają zostać wybrane. Gdy przy wciśniętym klawiszu **Ctrl** kolejno klikane są różne obiekty, wszystkie one zostają wybrane (zaznaczone). Gdy przy wciśniętym klawiszu **Shift** kliknięty zostanie określony obiekt, w programie wybrane (zaznaczone) zostaną równocześnie wszystkie obiekty położone pomiędzy tym obiektem a obiektem wybranym wcześniej.

Jeżeli chcemy dokonać wyboru wielu obiektów wyłącznie za pomocą klawiatury, należy przytrzymać wciśnięty klawisz **Ctrl**, a następnie za pomocą klawiszy strzałek przenieść się do innego obiektu i nacisnąć klawisz **Spacja**. Procedurę tę należy powtórzyć dla wszystkich pozostałych obiektów, które mają zostać wybrane.

Wstawianie obiektów graficznych

W ogólnym zarysie procedura wstawiania na mapę nowych obiektów dla wszystkich trzech rodzajów obiektów wygląda podobnie.

Kształt

Kształty służą w programie do lepszego organizowania informacji na mapach. Umieszczane są one obok węzłów i pomagają podzielić je na różne kategorie, w zależności od sieci, do której należą, lokalizacji SNMP lub innych cech określanych przez użytkownika.

Rysunek

Podczas opracowywania określonej mapy przydatne może okazać się dodanie do niej pewnych nowych rysunków. Takie elementy graficzne, jak na przykład logo lub wizerunek danej firmy, mogą być umieszczane w dowolnym miejscu określonej mapy, poprawiając w ten sposób jej czytelność. Po wstawieniu rysunku na mapę można go łatwo przenieść do dowolnego innego miejsca, oczywiście pod warunkiem, że nadal włączony jest tryb edycji mapy.

Aby wstawić rysunek z pliku

1. Kliknij ikonę ***Wstaw rysunek***, znajdującą się na pasku narzędzi *Edytuj mapę* lub z menu **Wstaw** wybierz polecenie **Rysunek**.
   Spowoduje to wyświetlenie standardowego okna **Otwieranie**.
2. Wybierz w tym oknie ścieżkę oraz nazwę pliku zawierającego rysunek, który chcesz wstawić. Kliknij przycisk **Otwórz**, aby zatwierdzić wybór.
3. Nowo wstawiony rysunek pojawi się na mapie.

Tekst

Podczas edytowania mapy przydatne może się okazać wstawienie dodatkowego tekstu, który pomoże przedstawić informacje związane z daną siecią w sposób bardziej jasny i zrozumiały. Podczas wstawiania tekstu wykorzystane mogą być następujące style domyślne:

Nagłówek	Ten rodzaj tekstu służy do wstawienia na mapę odpowiedniego nagłówka. Z nagłówkami związane jest z reguły określone tło.
Tytuł	Ten rodzaj tekstu służy do wstawiania w dowolnym miejscu mapy odpowiedniego tytułu. Tekst tytułu z reguły nie ma skojarzonego z nim żadnego tła.
Standard	Zgodnie ze swoją nazwą, tekst standardowy może być wstawiany w dowolnym miejscu mapy. Z tym rodzajem tekstu nie jest skojarzone żadne tło.

Układ	Ten rodzaj tekstu jest wstawiany wraz tłem, które jest tłem domyślnym dla danego układu mapy.
Własny	Ten rodzaj tekstu jest umieszczany przy zastosowaniu zdefiniowanych przez użytkownika: koloru, rodzaju i rozmiaru czcionki, jak również charakterystycznego położenia na mapie.

Aby wstawić tekst na mapie

1. Kliknij ikonę ***Wstaw tekst***, znajdującą się na pasku narzędzi *Edytuj mapę* lub z menu **Wstaw** wybierz polecenie **Tekst**.
2. Wybierz odpowiednią czcionkę, korzystając z listy rozwijanej **Rodzaj czcionki**.
3. W polu **Rozmiar** wpisz rozmiar czcionki w punktach.

4. Kliknij ikonę ***Kolor***, aby zmienić kolor czcionki.
5. Kliknij jedną z wyświetlanych ikon formatowania, aby tekst wyświetlany był czcionką pogrubioną, podkreśloną lub kursywą.
6. Za pomocą dwóch list rozwijanych wybierz rodzaj poziomego i pionowego wyrównania tekstu w przeznaczonym dla niego prostokątnym polu tekstowym na mapie.
7. Jeżeli chcesz, aby tekst wyświetlany był pod określonym kątem, wpisz w polu **Kąt** odpowiednią wartość z zakresu od 0 do 360 stopni.
8. W głównym obszarze tego okna wpisz dokładnie tekst, który ma zostać wstawiony.
9. Jeżeli chcesz, aby tekst był zawijany do nowego wiersza wewnątrz przeznaczonego dla niego pola tekstowego, zaznacz pole wyboru **Zawijaj tekst**.

Uwagi

- *Zamiast wprowadzać własne ustawienia dla wstawianego tekstu, można w oknie **Nowy tekst** wybrać od razu jeden ze wstępnie zdefiniowanych stylów. W tym celu należy skorzystać z listy rozwijanej **Styl**.*
- *Aby zmienić rozmiar pola tekstowego, należy zaznaczyć wybrany tekst i odpowiednio przeciągnąć jeden z widocznych wokół niego niewielkich kwadracików. Czynność ta nie spowoduje zmiany rozmiaru samego tekstu.*
- *Style tekstowe* Nagłówek, Tytuł, Standard *oraz* Układ *są stylami wstępnie zdefiniowanymi w programie NetCrunch, a ich ustawienia mogą być zmieniane w oknie **Opcje**.*

Wstawianie kształtu

Oprócz ikon reprezentujących węzły lub odsyłacze do innych map, NetCrunch umożliwia wstawienie dowolnego rodzaju kształtów. W tym celu wykorzystane mogą być następujące style:

- Prostokąt
- Prostokąt zaokrąglony (prostokąt z zaokrąglonymi wierzchołkami)
- Owal
- Koło

- Tło gradientowe (prostokąt z cieniowaniem)
- Układ (jest to domyślny styl dla map z automatycznym rozmieszczaniem)
- Własny

Aby wstawić kształt na mapę

1. Kliknij ikonę ***Wstaw kształt***, znajdującą się na pasku narzędzi *Edytuj mapę*, lub z menu **Wstaw** wybierz polecenie **Kształt**.
2. Wybierz odpowiedni wstępnie zdefiniowany styl kształtu, korzystając z listy rozwijanej **Styl**.
3. Wybierz kształt, korzystając z pola **Kształt**.
4. Jeżeli chcesz, aby kształt związany z tłem zachował stosunek swoich wymiarów, zaznacz pole wyboru **Zachowaj stosunek wymiarów**.

Łączenie obiektów

Ikony na mapie mogą być łączone ze sobą za pomocą linii połączeń.

Aby połączyć obiekty

1. Zaznacz obiekt, od którego chcesz poprowadzić linię połączenia.
2. Kliknij zaznaczony obiekt prawym przyciskiem myszy, w menu podręcznym wskaż pozycję **Linie**, a następnie wybierz polecenie **Połącz z**.

Uwagi

- *Użytkownik ma możliwość równoczesnego wybrania ikon kilku węzłów i wstawienia linii połączeń prowadzących od tych węzłów do dowolnego innego węzła. W tym celu należy upewnić się, że tryb edycji mapy jest włączony, a następnie, przytrzymując wciśnięty klawisz* ***Ctrl****, kliknąć każdą ikonę węzła, od której ma zostać poprowadzona linia połączenia. Po zaznaczeniu wszystkich takich ikon należy kliknąć prawym przyciskiem myszy którąkolwiek z nich, w menu podręcznym wskazać pozycję* ***Linie****, a następnie wybrać polecenie* ***Połącz z*** *i kliknąć dowolny inny węzeł, do którego mają prowadzić linie połączeń rozpoczynające się w zaznaczonych węzłach.*
- *Każda linia połączenia poprowadzona pomiędzy dwiema ikonami węzłów, która albo została dodana, albo znajdowała się już wcześniej na mapie, może zostać w dowolnej chwili usunięta. Więcej informacji na ten temat zawiera rozdział* Usuwanie obiektów z mapy *na stronie 191.*

Zmiana właściwości obiektu

Właściwości obiektu, które mogą być zmieniane przez użytkownika, można podzielić na trzy podstawowe kategorie:

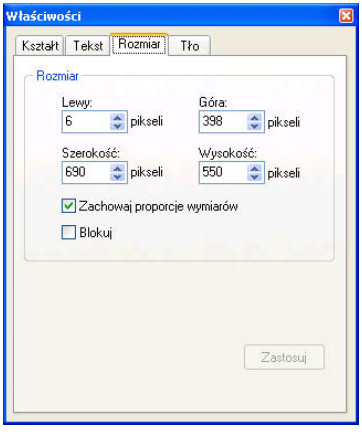
Ogólne (rysunek, tekst, kształt)	Właściwości charakterystyczne dla określonego obiektu. Różnią się one w zależności od rodzaju obiektu. Przykładami takich właściwości ogólnych są: tekst napisu (w przypadku obiektu tekstowego), kształt (w przypadku obiektu, który jest kształtem w tle) czy ścieżka pliku (w przypadku obiektu, który jest rysunkiem).

Rozmiar	Właściwości związane z rozmiarem obiektu.
Tło	Właściwości związane z tłem obiektu (w tym obramowanie i cieniowanie).

Uwaga

*Użytkownik może zaznaczyć dowolną liczbę obiektów graficznych (tekstów, rysunków lub kształtów) i równocześnie zmienić ich właściwości. W tym celu należy najpierw upewnić się, że włączony jest tryb edycji mapy. Następnie, przytrzymując wciśnięty klawisz **Ctrl**, należy kliknąć każdy z obiektów, zaznaczając ja kolejno. Kolejny krok to kliknięcie prawym przyciskiem myszy dowolnego z zaznaczonych obiektów i wybranie z menu podręcznego polecenia **Właściwości**. W otwartym w ten sposób oknie należy wprowadzić odpowiednie zmiany we właściwościach zaznaczonych obiektów.*

Aby zmienić rozmiar obiektu



1. Zaznacz wybrany obiekt i otwórz okno **Właściwości**.
2. Kliknij kartę **Rozmiar**.
3. W obszarze **Rozmiar** zmień rozmiar obiektu (w pikselach).
4. Jeżeli zachodzi taka potrzeba, zaznacz pole wyboru **Zachowaj proporcje wymiarów**, aby zachować taki sam stosunek szerokości do wysokości.

Aby zmienić właściwości tła obiektu

1. Zaznacz wybrany obiekt i otwórz okno **Właściwości**.
2. Kliknij kartę **Tło**.
3. Jeżeli chcesz, aby za obramowaniem obiektu pojawiał się cień, zaznacz pole wyboru **Rysuj cień**. Za pomocą suwaka **Rozmiar** ustaw grubość cienia. Można wybrać dowolną wartość z zakresu od 0 do 10.
4. Za pomocą ikon **Pozycja** wybierz położenie cienia w stosunku do tekstu.

Aby zmienić właściwości rysunku

1. Zaznacz obiekt będący rysunkiem.
2. Klikając ikonę ***Przeglądaj*,** możesz zmienić nazwę pliku z rysunkiem.
3. Zaznacz pole wyboru **Przezroczysty**. Niektóre rodzaje rysunków (PSD, TIFF) mogą zawierać informacje związane z przezroczystością.
   W takim przypadku należy pozostawić to pole niezaznaczone.
4. Jeżeli chcesz zmienić rozmiar rysunku poprzez jego rozciągnięcie, zaznacz pole wyboru **Rozciągnij**.
5. Jeżeli chcesz zachować stosunek szerokości do długości danego rysunku, zaznacz pole wyboru **Zachowaj proporcje wymiarów**.

6. Aby zachować oryginalne wymiary rysunku, zaznacz pole wyboru **Rozmiar automatyczny**.

Aby zmienić właściwości tekstu

1. Zaznacz obiekt będący tekstem.
2. Korzystając z listy rozwijanej **Rodzaj czcionki**, wybierz odpowiednią czcionkę, którą ma być wyświetlany zaznaczony tekst.
3. Za pomocą listy rozwijanej **Rozmiar** wybierz rozmiar czcionki dla tego tekstu.
4. Kliknij ikonę **Kolor**, aby zmienić kolor czcionki, którą ma być wyświetlany zaznaczony tekst.
5. Aby umieścić tekst pod określonym kątem, skorzystaj z pola **Kąt**.
6. W polu przeznaczonym na tekst wpisz tekst, który ma być wyświetlany.
7. Aby zawijać tekst, który nie mieści się w jednym wierszu, zaznacz pole wyboru **Zawijaj tekst**.
8. Styl obiektu tekstowego może być zmieniany za pomocą listy rozwijanej **Styl**. Wybierz jeden ze wstępnie zdefiniowanych stylów lub pozostaw wybrany styl *Własny* (jeżeli w punktach 3-7 wprowadzone zostały przez Ciebie jakiekolwiek zmiany).

Aby zmienić właściwości kształtu

1. Zaznacz wybrane obiekty.
2. Zmień styl obiektu, korzystając z listy rozwijanej **Styl**.
3. Za pomocą listy **Kształt** wybierz odpowiedni kształt.

Aby zmienić właściwości linii połączenia

1. Zaznacz linię połączenia.
2. Skorzystaj z poziomego suwaka **Grubość**, aby zmienić grubość linii połączenia. Można wybrać wartość z zakresu od 1 do 10.
3. Kliknij ikonę ***Kolor***, aby wybrać odpowiedni kolor linii.
4. Wybierz **Rodzaj połączenia**, klikając ikonę *Ukośny*, *Prostokątny* lub *Magistrala*.
5. Po wybraniu rodzaju połączenia w obszarze **Punkty połączeń** wybierz metodę łączenia ze sobą dwóch ikon (uzależnioną od wybranego rodzaju połączenia – ukośnego, prostokątnego bądź magistralowego). Jeżeli chcesz, aby program automatycznie wybrał metodę najkrótszej ścieżki, zaznacz pole wyboru **Wybór automatyczny**.

Usuwanie obiektów z mapy

Wszelkie obiekty dodatkowe, takie jak rysunki, tekst czy kształty w tle, mogą w dowolnej chwili zostać usunięte z mapy. Usuwać można również linie połączeń oraz ikony węzłów. Jednakże usunięcie ikony węzła z mapy sieci pociągnie za sobą usunięcie rekordu tego węzła z bazy danych monitorowania oraz usunięcie tego węzła z pozostałych map, na których węzeł

ten występuje. Natomiast usunięcie węzła z mapy własnej spowoduje jedynie usunięcie ikony reprezentującej ten węzeł na mapie, natomiast obiekt związany z tym węzłem będzie nadal obecny na pozostałych mapach, jak również w bazie danych monitorowania.

Aby usunąć wybrany obiekt(y) z mapy

1. Zaznacz jeden lub więcej wybranych obiektów.
2. Kliknij prawym przyciskiem myszy jeden z zaznaczonych obiektów, a następnie z menu podręcznego wybierz polecenie **Usuń**.
   Wyświetlone zostanie okno potwierdzenia.
3. Kliknij przycisk **Tak**, aby potwierdzić usunięcie.

Korzystanie z funkcji zdalnego dostępu

Zdalny dostęp z przeglądarki internetowej pozwala na bezpośrednie, zdalne łączenie się za pomocą standardowej przeglądarki z komputerem, na którym zainstalowane jest oprogramowanie NetCrunch. Dzięki temu udogodnieniu niektóre standardowe funkcje programu, takie jak tworzenie map, monitorowanie, alertowanie czy raportowanie, stają się dostępne z dowolnego komputera podłączonego do Internetu. Program udostępnia także profile zdalnego dostępu, dzięki czemu można sprecyzować zestaw funkcji NetCruncha, do korzystania z których – w trybie „odczyt/zapis" bądź „tylko do odczytu"—uprawniony będzie każdy zdalny użytkownik.

Z oferowanego w programie mechanizmu zdalnego dostępu można skorzystać niemal natychmiast. Wcześniej jednak konieczne jest skonfigurowanie kilku opcji programu. Należy zatem:

- zdefiniować i włączyć – przez podanie hasła – użytkowników, którzy będą mogli korzystać z dostępu przez WWW
- upewnić się, że funkcja zdalnego dostępu została w programie włączona.

Po wykonaniu tych dwóch czynności, aby korzystać z funkcji programu NetCrunch zdalnie (z dowolnego miejsca w sieci), za pomocą standardowej przeglądarki WWW, należy wpisać w niej adres IP lub nazwę urządzenia, w którym aktualnie uruchomiony jest NetCrunch. Na otwartej w ten sposób stronie WWW należy zalogować się w programie jako zdefiniowany wcześniej użytkownik. Por. sekcję *Zdalny dostęp do programu NetCrunch* na stronie 202 w celu uzyskania dodatkowych informacji.

Uwaga

Funkcja zdalnego dostępu w NetCrunchu pozwala na korzystanie z większości popularnych przeglądarek WWW, w tym Microsoft Internet Explorer 5.5 i nowsze, Firefox 1.0 i nowsze, Mozilla oraz Netscape.

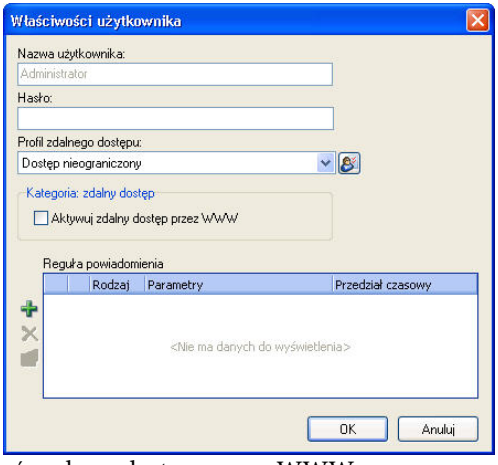
Definiowanie użytkowników ze zdalnym dostępem przez przeglądarkę

Na potrzeby zdalnego dostępu i powiadamiania można zdefiniować dowolną liczbę użytkowników. Logika nakazuje, aby dla zdefiniowanego użytkownika najpierw ustalić metody powiadamiania (czyli w jaki sposób i kiedy ma on być powiadamiany). Następnie dla powiadamianego użytkownika można włączyć opcję zdalnego dostępu przez przeglądarkę oraz wybrać profil zdalnego dostępu. Gdy użytkownik taki zostaje powiadomiony o określonym problemie w sieci, jest bardzo prawdopodobne, że będzie chciał zalogować się w programie NetCrunch przez sieć WWW, aby poznać przyczynę danego problemu oraz znaleźć jego rozwiązanie.

Aby zdefiniować użytkownika ze zdalnym dostępem z przeglądarki

1. Na głównym pasku narzędzi programu kliknij ikonę ***Użytkownicy***. Spowoduje to wyświetlenie okna **Ustawienia użytkowników i grup**.

2. Zaznacz użytkownika, któremu chcesz włączyć dostęp przez WWW, a następnie kliknij ikonę ***Edytuj***.
Jeżeli chcesz utworzyć całkowicie nowego użytkownika, kliknij zamiast tego ikonę ***Nowy użytkownik***.
Spowoduje to wyświetlenie okna **Właściwości użytkownika**.



3. Jeżeli przeprowadzasz edycję istniejącego użytkownika, pozostaw niezmienione pole **Nazwa użytkownika**. Będzie to nazwa, za pomocą której użytkownik będzie się logować podczas dostępu przez WWW.
W innym wypadku wpisz nazwę logowania nowego użytkownika.
4. W polu **Hasło** wpisz hasło użytkownika wykorzystywane podczas dostępu przez WWW.
5. Zaznacz pole wyboru **Aktywuj zdalny dostęp przez WWW**. Spowoduje to włączenie danemu użytkownikowi dostępu przez WWW.
6. Zdefiniuj profil zdalnego dostępu dla użytkownika posługując się rozwijaną listą **Profil zdalnego dostępu** lub użyj ikony ***Edytuj profil***, aby zmodyfikować istniejący profil lub utworzyć nowy.

Uwagi

- *Standardowo program udostępnia kilka profili zdalnego dostępu, takich jak na przykład **Dostęp nieograniczony** czy **Dostęp tylko do odczytu**. Jak sama nazwa wskazuje pierwszy profil daje pełne prawa do zdalnego używania programu, natomiast drugi profil pozwala na zdalny dostęp tylko w zakresie odczytywania danych. Powyższe predefiniowane profile są nieusuwalne, natomiast pozostałe predefiniowane profile zdalnego dostępu mogą być kasowane.*
- *Możliwe jest utworzenie nowego profilu zdalnego dostępu – w tym celu należy skorzystać z okna **Menedżer profili zdalnego dostępu**. Szczegółowo opisuje to zamieszczona poniżej sekcja* Zarządzanie profilami zdalnego dostępu *na stronie 196.*
- *Więcej informacji na temat zarządzania powiadamianiem użytkowników lub grup zawiera rozdział* Zarządzanie powiadamianiem użytkowników i grup *na stronie 237.*

Zarządzanie użytkownikami zdalnego dostępu

Po otwarciu okna **Ustawienia użytkowników i grup** wyświetlani są zdefiniowani użytkownicy i grupy. W przypadku prezentowanych na liście użytkowników, w osobnej kolumnie pokazywany jest również ich aktualny status zdalnego dostępu (możliwe wartości to ”Nie przyłączony” i ”Przyłączony”. Z kolei po rozwinięciu listy związanej

z aktualnie przyłączonym użytkownikiem zdalnego dostępu prezentowany jest również adres IP, z którego nawiązano zdalne połączenie oraz dokładny czas zalogowania użytkownika. Każdego przyłączonego użytkownika można szybko rozłączyć z NetCruncha – w tym celu należy zaznaczyć użytkownika i w podręcznym menu wybrać opcję **Rozłącz**. Istnieje także opcja redagowania komunikatu rozłączenia, jaki ukazuje się zdalnemu użytkownikowi przed rozłączeniem.

Uwaga

Z zależności od rodzaju zakupionej licencji programu, z opcji zdalnego dostępu do programu z przeglądarki WWW można korzystać następująca liczba użytkowników: 0, 3 lub nieograniczona.

Dziennik kontroli sesji zdalnego dostępu

Ilekroć jakiś użytkownik łączy się zdalnie z NetCrunchem z przeglądarki internetowej, zainicjowana przez niego sesja jest automatycznie zapisywana w specjalnym pliku rejestru. Powyższy plik rejestru sesji zdalnego dostępu wyświetlany jest w oknie **Dziennik dostępu przez WWW** po wybraniu odpowiedniego polecenia z menu **Widok**. Zawiera on następujące informacje dotyczące każdej sesji z logowaniem:

- użytkownik NetCruncha, który korzystał ze zdalnego połączenia
- dokładny okres czasu, w którym użytkownik pozostawał zalogowany
- moment rozpoczęcia sesji
- moment zakończenia sesji.

Ponadto po wybraniu konkretnej wyszczególnionej na liście sesji użytkownika i wskazaniu w jej podręcznym menu opcji **Szczegóły**, wyświetli się okno **Podgląd dziennika sesji** zawierające informacje o operacjach, jakie użytkownik wykonał w NetCrunchu zdalnie za pomocą przeglądarki internetowej. W skład listy wchodzą następujące rodzaje informacji (z odpowiednim znacznikiem czasowym):

- użytkownik połączył się z określonego adresu IP
- dokonano modyfikacji właściwości węzła
- dokonano modyfikacji właściwości monitorowania węzła
- dodano węzeł do monitorowania
- na określonej mapie umieszczono węzeł
- nastąpiło sprawdzenie statusu usług sieciowych na określonym węźle
- na określonym węźle przeprowadzono procedurę wykrywania usług sieciowych,
- nastąpiło rozłączenie zdalnego użytkownika.

Aby przeglądać zawartość pliku dziennika sesji dostępu przez WWW

1. Z menu **Widok** wybierz **Dzienniki**, a następnie opcję **Kontrola dostępu przez WWW**. Otworzy się okno **Dziennik dostępu przez WWW** zawierające aktualnie zalogowane sesje zdalnego dostępu z ostatnich 24 godzin.
2. Korzystając z opaska narzędzi w powyższym oknie, wybierz inny okres, dla którego mają być wyświetlane sesje.

3. Wybierz sesję użytkownika z listy, a następnie w jej podręcznym menu wskaż opcję **Szczegóły**.
   Okno **Dziennik kontroli sesji** pokaże wszystkie zadania, jakie w trakcie tejże sesji wykonał dany użytkownik.

Uwagi

- *W punkcie 2 można wyświetlić wszystkie zapisane w rejestrze sesje z ostatnich 24 godzin, lub z dowolnie wskazanego dnia, tygodnia czy miesiąca.*
- *Używając udostępnionego w oknie paska narzędzi można wydrukować treść rejestru zdalnego dostępu lub wyeksportować ją do plików HTML, XML i tekstowego.*
- *W opcjach programu, w karcie **Konserwacja**, można określić, jak długo mają być przechowywane rejestry sesji zdalnego dostępu. Oznacza to, że sesje, które miały miejsce przez wskazanym okresem będą automatycznie usuwane z rejestru.*

Zarządzanie profilami zdalnego dostępu

Profil zdalnego dostępu zawiera wszystkie prawa dostępu zdefiniowane dla określonych obiektów NetCruncha i stosowanych operacji. Uściślając, możliwe jest przydzielanie użytkownikom praw dostępu do następujących funkcji programu (a także zapisywanie ich w profilach zdalnego dostępu):

FUNKCJA PROGRAMU	*UDOSTĘPNIANY OBIEKTU*	*RODZAJ DOSTĘPU*
Modyfikacja opcji zdalnego dostępu	Program	Przyznany lub Zablokowany
Modyfikacja hasła zdalnego dostępu	Program	Przyznany lub Zablokowany
Używanie Narzędzi IP i SNMP	Program	Przyznany lub Zablokowany
Odczyt alertów	Atlas, mapa lub folder	Odczyt/zapis, Tylko do odczytu lub Zablokowany
Odczyt raportów	Atlas, mapa lub folder	Przyznany lub Zablokowany
Odczyt mapy	Atlas, mapa lub folder	Przyznany lub Zablokowany
Przeglądanie notatek	Atlas, mapa lub folder	Odczyt/zapis, Tylko do odczytu lub Zablokowany
Dodawanie węzłów do monitorowania	Program	Przyznany lub Zablokowany
Wykrywanie usług sieciowych	Atlas, mapa lub folder	Przyznany lub Zablokowany
Odczyt ustawień monitorowania węzła	Atlas, mapa lub folder	Odczyt/zapis, Tylko do odczytu lub Zablokowany

Odczyt serwisów systemu NT na węźle	Atlas, mapa lub folder	Przyznany lub Zablokowany
Odczyt właściwości węzła	Atlas, mapa lub folder	Odczyt/zapis, Tylko do odczytu lub Zablokowany
Odczyt statusu węzła	Atlas, mapa lub folder	Przyznany lub Zablokowany

Jak wynika z powyższej tabeli, NetCrunch oferuje szeroką gamę praw dostępu do swoich funkcji za pośrednictwem przeglądarki internetowej. Przykładowo pewnym funkcjom programu można przypisać różne rodzaje dostępu do różnych obiektów bądź utworzyć wyjątki od dziedziczonego poziomu dostępu dla obiektu.

Tworzenie profilu zdalnego dostępu

Procedura definicji profilu zdalnego dostępu odbywa się w oknie **Menedżer profili zdalnego dostępu**. Umożliwia ono tworzenie, edytowanie oraz usuwanie profili zdalnego dostępu. Należy pamiętać, że program zawiera kilka predefiniowanych profili zdalnego dostępu, w tym profil typu „Dostęp nieograniczony" oraz profil dostępu w trybie „tylko do odczytu". Choć usuwanie dwóch wymienionych powyżej profili predefiniowanych jest niemożliwe, dopuszczalne jest kasowanie innych predefiniowanych profili.

Aby utworzyć nowy profil zdalnego dostępu

1. W menu **Atlas** wskaż pozycję **Profile** i wybierz opcję **Zdalny dostęp**.
   Pojawi się okno **Menedżer profili zdalnego dostępu** prezentujące listę aktualnie zdefiniowanych profili zdalnego dostępu.
2. 
   Kliknij ikonę ***Dodaj profil***.
   Wyświetli się okno **Właściwości profilu zdalnego dostępu**.
3. Wprowadź własne ustawienia związane ze zdalnymi uprawnieniami oraz rodzajem dostępu do każdego obiektu programu.
4. Kliknij przycisk **Zapisz profil jako**.
   Wyświetli się okno dialogowe **Zapisz profil jako**.
5. W polu **Nazwa profilu** określ nazwę profilu.

Uwaga

W oknie wymienionym w punkcie 3 można zarządzać prawami i zakresem dostępu do obiektów programu. Por. następujące sekcje: Dodawanie praw dostępu *na stronie 199,* Edytowanie praw dostępu *na stronie 200 oraz* Usuwanie praw dostępu *na stronie 200 w celu uzyskania szczegółowych informacji.*

Edytowanie profilu zdalnego dostępu

Możliwe jest edytowanie wszystkich profili zdalnego dostępu za wyjątkiem dwóch profili predefiniowanych: „Dostęp nieograniczony" oraz profil dostępu w trybie „Tylko do odczytu".

Aby dokonać edycji istniejącego profilu zdalnego dostępu zdefiniowanego przez użytkownika

1. W menu **Atlas** wskaż pozycję **Profile** i wybierz opcję **Zdalny dostęp**.
   Pojawi się okno **Menedżer profili zdalnego dostępu** prezentujące listę aktualnie zdefiniowanych profili zdalnego dostępu.
2. Wybierz profil zdalnego dostępu do edycji.
3.  Kliknij ikonę ***Edytuj profil***.
   Wyświetli się okno **Właściwości profilu zdalnego dostępu**.
4. Dokonaj stosownych zmian w obiektach programu, dla których chcesz zmodyfikować prawa użytkowników i odpowiadający im poziom dostępu.

Uwaga

W oknie wymienionym w punkcie 4 można zarządzać prawami i zakresem dostępu do obiektów programu. Por. następujące sekcje: Dodawanie praw dostępu na stronie 199, Edytowanie praw dostępu na stronie 200 oraz Usuwanie praw dostępu na stronie 200 w celu uzyskania szczegółowych informacji.

Usuwanie profilu zdalnego dostępu

Możliwe jest usuwanie wszystkich profili zdalnego dostępu za wyjątkiem dwóch profili predefiniowanych: „Dostęp nieograniczony" oraz profil dostępu w trybie „Tylko do odczytu".

Aby usunąć istniejący profil zdalnego dostępu zdefiniowanego przez użytkownika

1. W menu **Atlas** wskaż pozycję **Profile i** wybierz opcję **Zdalny dostęp**.
   Pojawi się okno **Menedżer profili zdalnego dostępu** prezentujące listę aktualnie zdefiniowanych profili zdalnego dostępu (w tym dwa profile predefiniowane).
2. Wybierz z listy profil zdalnego dostępu do usunięcia.
3. Kliknij ikonę *Edytuj profil*.

Zarządzanie prawami dostępu

Okno **Właściwości profilu zdalnego dostępu** służy do zarządzania wszystkimi prawami dostępu i rodzajami dostępu do różnorodnych obiektów programu dla aktualnie zaznaczonego profilu zdalnego dostępu. Można również przypisywać obiektom nowe prawa dostępu z odpowiednim poziomem dostępu lub ograniczać dziedziczone prawa dostępu do obiektu.

Aby otworzyć okno Właściwości profilu zdalnego dostępu

1. W menu **Atlas** wskaż pozycję **Profile i** wybierz opcję **Zdalny dostęp**.
   Okno **Właściwości profilu zdalnego dostępu** wyświetli listę zdefiniowanych profili zdalnego dostępu.
2.  Zaznacz profil i kliknij ikonę ***Edytuj profil,*** jeśli chcesz edytować istniejący profil zdalnego dostępu.
    Kliknij ikonę ***Dodaj profil***, jeśli zamierzasz utworzyć nowy profil zdalnego dostępu.
   Wyświetli się okno **Właściwości profilu zdalnego dostępu**.

Dodawanie obiektu do właściwości profilu

Aby przyznać bądź ograniczyć prawa do wykonywania na określonych obiektach programu wskazanych funkcji, należy w pierwszej kolejności dodać obiekt do listy obiektów dla aktualnie wskazanego profilu zdalnego dostępu.

Aby dodać obiekt do listy profili

1. Otwórz okno **Właściwości profilu zdalnego dostępu** dla profilu zdalnego dostępu.
2.  Kliknij strzałkę znajdującą się na prawo od ikony ***Dodaj obiekt***.
3. W zaprezentowanym menu wskaż obiekt do dodania (program, atlas, węzeł/mapa/folder).
   Obiekt natychmiast zostanie wyświetlony w liście obiektów.

Uwaga

Jeśli w punkcie 3 wybrano dodanie węzła/mapy/folderu, należy także wskazać folder, mapę lub węzeł w oknie ***Wybierz węzeł lub mapę****.*

Usuwanie obiektu z właściwości profilu

Usunięcie obiektu z listy obiektów w wybranym profilu zdalnego dostępu powoduje utracenie wszystkich uprawnień do określonych funkcji programu dla danego obiektu. Z tego powodu należy zachować szczególną ostrożność przy wykonywaniu tej operacji.

Aby usunąć obiekt z właściwości profilu

1. Otwórz okno **Właściwości profilu zdalnego dostępu**.
2. W liście obiektów wskaż obiekt do usunięcia.
   Zdefiniowane dla tego obiektu prawa dostępu natychmiast wyświetlą się liście poniżej.
3.  Kliknij ikonę ***Usuń obiekt***.

Dodawanie praw dostępu

W oknie **Właściwości profilu zdalnego dostępu** można wybrać obiekt programu (program, atlas, dowolna mapa, folder lub węzeł) a także przyznać lub zablokować dostęp do tego obiektu dla określonej funkcji programu. Kolejność czynności przedstawia się następująco:

- Wybór obiektu (program, atlas, dowolny folder, mapa lub węzeł), któremu zostaną przyznane/ograniczone prawa użytkownika.
- Wybór funkcji programu, do której dostęp zostanie przyznany/zablokowany użytkownikowi.
- Wybór rodzaju dostępu (Odczyt/zapis, Tylko do odczytu lub Zablokowany; Przyznany lub Zablokowany).
- Dla każdego kolejnego obiektu, dla którego są przyznawane lub ograniczane prawa dostępu należy powtórzyć opisane powyżej czynności.

Aby dodać nowe prawo dostępu

1. Otwórz okno **Właściwości profilu zdalnego dostępu** dla profilu zdalnego dostępu.
2. Wybierz obiekt z listy obiektów lub dodaj go bezpośrednio.

3. Aby przyznać/zablokować określone prawo dostępu dla zaznaczonego obiektu, należy kliknąć ikonę ***Dodaj uprawnienie***.

Pojawi się okno **Właściwości praw dostępu**.
4. W rozwijanej liście **Kategoria** wskaż kategorię, do której należy prawo dostępu.
5. Z rozwijanej listy **Nazwa prawa dostępu** wybierz prawo dostępu, które ma zostać przyznane/ograniczone dla wybranego obiektu.
6. W polu **Dostęp** wybierz odpowiedni przycisk opcji (Odczyt/zapis, Tylko do odczytu, Zablokowany, Przyznany lub Zablokowany).

Uwaga

W punkcie 2, przy dodawaniu obiektu do listy, warto zapoznać się z sekcją Dodawanie obiektu do właściwości profilu *na stronie 199.*

Edytowanie praw dostępu

Aby dokonać edycji istniejącego prawa dostępu

1. Otwórz okno **Właściwości profilu zdalnego dostępu** dla profilu zdalnego dostępu.
2. Wybierz żądany obiekt z listy obiektów.
Na dole zostaną wyświetlone prawa dostępu przyznane/ograniczone dla określonych funkcji programu.
3. Z listy praw dostępu wybierz prawo dostępu odpowiadające funkcji programu, której właściwości zostaną zmienione.
4. Kliknij ikonę ***Edytuj uprawnienie***.

Pojawi się okno **Właściwości praw dostępu**.
5. W polu **Dostęp** wybierz odpowiedni przycisk opcji odpowiadający żądanemu rodzajowi dostępu (Odczyt/zapis, Tylko do odczytu, Zablokowany; Przyznany lub Zablokowany).

Usuwanie praw dostępu

Aby usunąć istniejące prawo dostępu

1. Otwórz okno **Właściwości profilu zdalnego dostępu** dla profilu zdalnego dostępu.
2. Wybierz żądany obiekt z listy obiektów.
Na dole zostaną wyświetlone prawa dostępu przyznane/zablokowane dla określonych funkcji programu.
3. Wybierz prawo dostępu do usunięcia dla aktualnie zaznaczonego obiektu z wybranego profilu zdalnego dostępu.
4. Kliknij ikonę ***Usuń uprawnienie***.


Włączanie dostępu przez przeglądarkę internetową

Po utworzeniu użytkowników z dostępem przez WWW należy sprawdzić w opcjach programu, czy funkcja dostępu przez WWW jest włączona. W tym celu trzeba otworzyć okno **Opcje**, a następnie wybrać stronę **Dostęp przez WWW** i skorzystać z Kreatora konfiguracji dostępu przez WWW.

Aby włączyć w programie dostęp przez WWW

1. Z menu **Narzędzia** wybierz polecenie **Opcje**.
   Spowoduje to wyświetlenie okna **Opcje**.
2. W lewej części okna wybierz stronę **Dostęp przez WWW**.
3. Aby włączyć funkcję zdalnego dostępu, zaznacz pole wyboru **Włącz**. Pojawi się *Kreator konfiguracji dostępu przez WWW*.
4. Jeśli podczas zdalnego łączenia się za pośrednictwem przeglądarki internetowej chcesz stosować protokół Secure Socket Layer (SSL), wybierz przycisk opcji **Tak**.
   W innym wypadku wybierz przycisk **Nie**.
5. Kliknij **Dalej**.
6. Jeśli w punkcie 4 kliknąłeś **Tak**, określ plik klucza, plik certyfikatu oraz plik głównego certyfikatu (Root Certification File), a następnie kliknij **Dalej**.
   W innym wypadku przejdź prosto do punktu 7.
7. W polu **Port serwera** określ port serwera dla połączenia przez WWW.
8. W polu **Częstotliwość automatycznego odświeżania strony** określ ilość w minutach okres, w którym program będzie czekał przed odświeżeniem aktualnej strony.
9. Kliknij **Dalej**.
10. Wybierz co najmniej jednego użytkownika dostępu przez WWW o żądanych uprawnieniach (w profilu), a następnie kliknij **Dalej**.
    Kreator wskaże, co należy wpisać w przeglądarce internetowej, aby zdalnie używać NetCruncha.
11. Kliknij **OK**, aby zapisać zmiany.

Uwaga

- *W katalogu `..\WebAccess\ssl`, w którym został pierwotnie zainstalowany program, znajdują się przykładowe pliki klucza, certyfikatu i certyfikatu głównego do SSL. Mogą one posłużyć do przetestowania funkcjonalności bezpiecznego dostępu przez WWW.*
- *Po wykonaniu czynności opisanych w punkcie 10 można także zaznaczyć pole wyboru* ***Uruchom domyślną przeglądarkę z dostępem internetowym***, aby otworzyć przeglądarkę ze zdalnym ekranem NetCruncha.
- *Aby wyłączyć funkcję zdalnego dostępu, tak aby żaden zdalny użytkownik nie miał prawa logowania się i używania funkcji programu przez Internet, odznacz pole wyboru* ***Włącz dostęp przez WWW****.*

Zdalny dostęp do programu NetCrunch

Po zdefiniowaniu użytkowników i włączeniu dostępu przez przeglądarkę internetową możliwe staje się zdalne korzystanie z funkcji programu, za pośrednictwem sieci WWW. W tym celu należy otworzyć standardową przeglądarkę WWW i wpisać w niej adres IP lub nazwę DNS komputera, na którym uruchomiony jest NetCrunch. Jeżeli na przykład program został zainstalowany na komputerze, którego adres IP to `123.43.2.10`,
w polu **Adres** w przeglądarce należy wpisać:

```
http://123.43.2.10
```

Uwaga

*Aby wylogować się z programu NetCrunch, należy z menu **Plik**, umieszczonego w górnej części wyświetlanej strony, wybrać polecenie **Wyloguj się**.*

Zmiana opcji zdalnego dostępu

Po zalogowaniu się w programie NetCrunch możliwe staje się zdalne wprowadzenie zmian we właściwościach zdalnego dostępu. W szczególności można zmienić hasło służące do logowania (dla określonego użytkownika) lub określić inną częstotliwość, z jaką odświeżane mają być wyświetlane strony (w minutach).

Aby zmienić opcje klienta zdalnego dostępu

1. Zaloguj się zdalnie, przez przeglądarkę internetową, w programie NetCrunch.
2. Z menu **Narzędzia**, znajdującego się w górnej części wyświetlanej strony WWW, wybierz polecenie **Opcje**.
3. Aby zmienić interwał czasowy, w jakim odświeżana ma być w przeglądarce aktualnie wyświetlana strona, określ odpowiednią wartość w polu **Odświeżaj strony co**.
4. Aby zmienić hasło służące do logowania, kliknij kartę **Hasło**.
5. W polu **Stare hasło** wpisz dotychczasowe hasło, a w polach **Nowe hasło** oraz **Potwierdzenie nowego hasła** podaj nowe hasło.
   Po kliknięciu przycisku **OK** opcje dostępu przez WWW zostaną zmienione, a okno **Opcje** zostanie zamknięte.

Uwaga

Opisane powyżej zmiany opcji zdalnego dostępu dotyczą wyłącznie tego użytkownika, który zdalnie loguje się w programie NetCrunch.

Opcje programu

NetCrunch pozwala użytkownikowi konfigurować niektóre opcje programu i tym samym tak ustawić działanie programu, by odpowiadało ono obranej strategii monitorowania i specyfice sieci. Konfigurowalne opcje programu można podzielić na pięć podstawowych grup związanych z monitorowaniem, powiadamianiem, mapami, raportami oraz dostępem przez WWW.

Monitorowanie

Opcje monitorowania umożliwiają użytkownikowi wykonywanie następujących operacji związanych ze zmianą powyższych ustawień programu:

- stosowanie usługi WINS w celu ustalania właściwości węzła [odczytu nazwy NetBIOS oraz adresy sprzętu (MAC)].
- ustawianie domyślnych właściwości identyfikacji, monitorowania i zarządzania za pośrednictwem standardu SNMP dla nowych węzłów
- określanie domyślnego konta Windows używanego do logowania się do węzłów Windows
- określanie domyślnych danych uwierzytelnienia w drzewie eDirectory używanym do logowania się do węzłów (serwerów NetWare)
- zmiana strategii funkcjonowania wątków monitorujących w celu podniesienia wydajności programu,
- wybór domyślnej listy usług sieciowych, które mają być wykrywane w każdym węźle,
- dodawanie do domyślnej listy monitorowanych usług nowych definicji usług sieciowych (tak, aby mogły one być przygotowane do monitorowania w każdym węźle),
- włączanie lub wyłączanie monitorowania topologii fizycznej,
- Włączanie/wyłączanie monitorowania segmentów fizycznych
- nasłuch programu w celu przechwytywania przychodzących trapów SNMP,
- przekierowywanie przychodzących trapów SNMP bezpośrednio do dowolnego innego węzła TCP/IP,

Ustawianie domyślnych właściwości monitorowania oraz zarządzania przez SNMP dla węzła

W opcjach programu można zdefiniować dla węzłów domyślny czas monitorowania, profil SNMP oraz port SNMP (w stosownych przypadkach). Dzięki temu, nowo wykryte lub umieszczone w atlasie węzły będą miały automatycznie przypisywane domyślne ustawienia zdefiniowane w powyższych opcjach. W ten sposób nie trzeba ustawiać bądź modyfikować owych opcji za każdym razem, gdy dowolny pojedynczy węzeł lub grupa węzłów zostaje wykryta przez program lub umieszczona w atlasie przez użytkownika.

Uwaga

Po wstępnej instalacji programu i wykryciu sieci, domyślny czas monitorowania dla węzłów ustawiony jest na 5 minut, natomiast domyślnym portem SNMP jest port numer 161.

Zmiana domyślnego konta dla systemu Windows NT

Gdy NetCrunch używany jest jako program na pulpicie, współdzieli on sesje zabezpieczeń z procesem pulpitu. Innymi słowy, program uzyskuje dostęp do tych samych zasobów systemu Windows, do których uzyskał dostęp użytkownik pulpitu.

Sytuacja zmienia się, gdy program uruchamiany jest jako usługa i wówczas, aby uzyskać dostęp do monitorowanych zasobów, konieczne jest jego zalogowanie się do domeny w systemie Windows lub do odpowiednich komputerów. Jeżeli dla danego węzła nie zostały określone żadne parametry konta, program zastosuje domyślne ustawienia konta.

Uwagi

- *Jeżeli z zastosowanymi nazwą i hasłem nie są związane pełne uprawnienia administratora systemu Windows, program jedynie zaloguje się w lokalnym węźle Windows, aby uzyskać odczyty liczników wydajności Windows dla celów monitorowania. Pole* ***Domena*** *jest opcjonalne.*

Dane uwierzytelniania w drzewie eDirectory

Aby program mógł łączyć się z monitorowanymi serwerami NetWare i odczytywać z nich liczniki wydajności, należy określić odpowiednie dane uwierzytelniania w drzewie eDirectory, do którego należą dane serwery. Odbywa się to na stronie **Monitorowanie – Domyślne właściwości węzła - NetWare** znajdującej się w oknie opcji programu. Można w nim dodawać wszelkie niezbędne dane uwierzytelnienia w drzewie eDirectory (nazwę użytkownika, kontekst i hasło), a później zmieniać lub usuwać przechowywane w nim właściwości.

Zmiana ustawień wątków

Wydajność programu NetCrunch można zwiększyć poprzez zmianę szeregu opcji związanych z jego wątkami monitorowania. Jednakże tego rodzaju ustawienia konfiguracyjne należy traktować jako zaawansowane i z tego względu, podczas ich modyfikacji, wymagane jest zachowanie szczególnej ostrożności. W zasadzie zalecane jest pozostanie przy ustawieniach domyślnych, jednakże w pewnych przypadkach konieczna może się okazać ich zmiana. Jeżeli komputer, na którym uruchomiony jest program, ma ograniczoną ilość zasobów (procesora, pamięci itp.), zmiana strategii przydziału wątków może doprowadzić do zmniejszenia w programie liczby wątków monitorujących. Jeżeli zaś NetCrunch uruchomiony jest na wysokiej klasy komputerze, przeznaczonym wyłącznie do wykonywania zadań związanych z monitorowaniem, wówczas zmiana ustawień wątków może przyczynić się do wzrostu wydajności samego procesu monitorowania. Można wówczas wprowadzić takie ustawienia, które pozwolą maksymalnie usprawnić proces monitorowania. Można również zmienić częstotliwość kontroli liczby wątków oraz maksymalną liczbę wątków monitorujących wykorzystywanych przez program.

Czas kontroli liczby wątków określa częstotliwość, z jaką mechanizm zarządzania wątkami monitorującymi przydziela lub zwalnia nieużywane wątki monitorujące. Jeżeli chcemy, aby

decyzje takie podejmowane były przez program częściej, kosztem zwiększonego wykorzystania zasobów komputera, należy wartość tę odpowiednio zmniejszyć. Z kolei jej zwiększenie ogranicza proces zarządzania watkami, przyczyniając się do mniejszego obciążenia cennych zasobów, takich jak na przykład procesory.

W praktyce maksymalna liczba wątków monitorujących może być podwojona, a nawet potrojona w stosunku do jej wartości domyślnej. Jednak nie powinna ona zazwyczaj przekraczać wartości 400. Zwiększenie tej wartości okazuje się szczególnie pożyteczne w sytuacji, gdy oprogramowanie NetCrunch monitoruje wiele węzłów pracujących pod kontrolą systemu Windows.

Domyślne usługi sieciowe

Jedną z istotnych konfigurowalnych opcji programu jest lista usług sieciowych, które będą przez program domyślnie wykrywane w każdym węźle. W rzeczywistości, gdy użytkownik przeprowadza operację wykrywania usług sieciowych w danym węźle, sprawdzana jest jedynie dostępność usług sieciowych określonych na tej właśnie specjalnej liście monitorowanych usług. Opcja te jest niezwykle wygodna, gdyż eliminuje konieczność wykrywania wszystkich możliwych usług sieciowych zdefiniowanych w programie. W opcjach programu użytkownik może dodawać usługi sieciowe do tej listy lub je z niej usuwać.

Zmiana definicji usług sieciowych

W programie NetCrunch użytkownik ma możliwość definiowania własnych usług sieciowych, jeżeli aktualnie nie są one wyszczególnione na domyślnej liście programu. Dzięki tej funkcji monitorowanie usług odbywa się w sposób bardziej elastyczny, gdyż za jej pomocą może zostać zdefiniowana praktycznie każda usługa sieciowa. Omówienie usług sieciowych dostępnych dla monitorowania w różnego rodzaju urządzeniach można znaleźć w rozdziale *Usługi sieciowe w urządzeniach* w publikacji **NetCrunch – Podręcznik monitorowania sieci**.

Tworzenie nowej definicji

Dodanie nowej definicji usługi sieciowej możliwe jest albo poprzez utworzenie całkowicie nowej definicji, albo przez skopiowanie definicji już istniejącej i odpowiednią zmianę jej parametrów. Wszystkie wstępnie zdefiniowane usługi sieciowe są przeznaczone tylko do odczytu, a po takim ich skopiowaniu zmieniony może być jedynie odpowiedni numer portu. Na przykład możliwe jest, w stosunkowo prosty sposób, utworzenie kopii usługi HTTP z innym ustawieniem portu, natomiast nie jest możliwa zmiana wewnętrznych danych związanych z taką usługą.

Aby utworzyć kopię usługi, należy kliknąć ikonę *Duplikuj*, znajdującą się na lewo od listy usług.

Przy dodawaniu definicji nowej usługi sieciowej (aby umożliwić programowi monitorowanie jej statusu) należy określić odpowiednie zapytanie, jakie będzie wysyłane do węzła, na którym uruchomiona jest nowo zdefiniowana usługa, a także oczekiwaną wartość wzorcową, która będzie porównywana z odpowiedzą otrzymaną od usługi sieciowej.

Aby dodać definicję nowej usługi

1. Otwórz okno **Opcje** wskazując pozycję **Opcje** w menu **Narzędzia**.
2. Wybierz stronę **Monitorowanie** – **Usługi** – **Definicja** znajdującą się po lewej stronie okna. Spowoduje to wyświetlenie listy usług sieciowych zdefiniowanych w programie.
3. Aby dodać nową usługę sieciową do listy zdefiniowanych w programie usług, kliknij ikonę ***Dodaj***. Pojawi się okno **Edytor usług**.
4. Wpisz nazwę nowej usługi w polu **Nazwa protokołu/usługi**.
5. Wybierz rodzaj protokołu (UDP, TCP lub IPX) dla nowej usługi używając rozwijanej listy **Rodzaj protokołu**.
6. Wpisz numer portu nowej usługi sieciowej w polu **Port**.
7. Zredaguj krótki opis nowej usługi sieciowej w polu **Opis**.
8. Zdefiniuj zapytanie, które będzie zawsze wysyłane do usługi sieciowej w celu sprawdzenia jej statusu. Por. poniższą sekcję *Definiowanie zapytania* w celu uzyskania dodatkowych informacji.
9. Określ oczekiwane wartości wzorcowe, które będą porównywane z odpowiedzą otrzymaną z nowej usługi sieciowej. Por. zamieszczoną poniżej sekcję *Definiowanie odpowiedzi* na stronie 206 w celu uzyskania dodatkowych informacji.

Definiowanie zapytania

Podczas definiowania zapytania należy precyzyjnie określić dane, jakie będą wysyłane przez program w celu sprawdzenia stanu nowej usługi sieciowej. Dane zapytania można zdefiniować i wysyłać w formacie tekstowym lub szesnastkowym. Aby zagwarantować poprawne działanie tej funkcji, można także ustawić wartość opóźnienia podczas wysyłania każdego zapytania.

Aby zdefiniować zapytanie

1. W oknie **Edytor usług** wybierz kartę **Zapytanie**.
2. W rozwijanej liście **Wyślij** wskaż format danych zapytania (tekstowy lub szesnastkowy).
3. W polu poniżej wpisz zapytanie, jakie za każdym będzie wysyłane w celu sprawdzenia statusu usługi sieciowej.
4. Jeśli zachodzi potrzeba zdefiniowania opóźnienia podczas wysyłania zapytania, należy zaznaczyć pole wyboru **Ustaw opóźnienie podczas wysyłania**.

Definiowanie odpowiedzi

Definiowanie odpowiedzi polega na utworzeniu wzorca lub zestawu wzorców, które pokrywają się (lub nie pokrywają się) z oczekiwaną odpowiedzią otrzymaną od nowo zdefiniowanej usługi sieciowej. Można zatem wskazać, że odpowiedź będzie poprawna, jeśli pokrywa się z dowolnym wzorcem, jeśli pokrywa się ze wszystkimi wzorcami, lub jeśli nie pokrywa się z żadnym wzorcem. Każdy wzorzec tworzony jest osobno w oknie **Właściwości wzorca odpowiedzi** poprzez wpisanie odpowiednich informacji w wyrażeniu warunku

logicznego. Należy także określić format wzorca warunku – może to być format tekstowy, szesnastkowy lub wyrażenie regularne.

Instrukcja warunku przybiera różne formy w zależności od tego, czy wybrano format tekstowy, szesnastkowy czy też wyrażenie regularne. W pierwszym przypadku należy określić następujące informacje:

Dopasuj/Szukaj	Określa, czy wzorzec ma idealnie pokrywać się z pozycją porównania bajta początkowego, a także definiuje wyszukiwanie wzorca w przedziale między pozycją bajta początkowego a bajta końcowego.
Wzorzec	Określa wzorzec (np. 'ABCD123'), która ma znaleźć wierne dopasowanie lub ma być wyszukiwany w otrzymanej odpowiedzi.
Jest równy/ Nie jest równy/ Większy niż/ Mniejszy niż	Określa logiczny związek między wiernie dopasowanym lub wyszukiwanym wzorcem a odpowiedzią.
Pozycja porównania bajta początkowego	Określa początkowy bajt odpowiedzi, względem którego wzorzec będzie wiernie dopasowywany lub wyszukiwany.
Pozycja wyszukiwania bajta końcowego	Określa końcowy bajt odpowiedzi, w stosunku do którego będzie wyszukiwany wzorzec.

W przypadku wyrażenia regularnego, w instrukcji warunku należy określić następujące informacje:

Bajt początkowy	Określa pozycję bajta początkowego odpowiedzi, od której będzie wyszukiwane wyrażenie regularne.
Bajt końcowy	Określa pozycję bajta końcowego odpowiedzi, do której będzie wyszukiwane wyrażenie regularne.
Wzorzec	Określa wyrażenie regularne, które będzie dopasowywane w odpowiedzi.

Aby zdefiniować odpowiedź

1. W oknie **Edytor usług** kliknij kartę **Odpowiedź**.
2. W rozwijanej liście **Poprawna gdy:** wskaż odpowiedni rodzaj dopasowania wzorca (dowolny, wszystkie lub żaden).
3.  Kliknij ikonę ***Dodaj***.
   Otworzy się okno **Właściwości wzorca**.
4. W polu **Format** wpisz format wzorca, które będzie porównywany do odpowiedzi otrzymanej od nowej usługi sieciowej.
5. W polu **Warunek** wpisz stosowne informacje (opisane w powyższych tabelach).

6. Kliknij **OK**.
   Zdefiniowany wzorzec zostanie wyświetlony w tabeli.
7. Powtórz czynności opisane w punktach 3-6, aby zdefiniować kolejny wzorzec, który będzie porównywany z odpowiedzią.

Uwagi


- *Możliwe jest łatwe edytowanie lub usuwanie zdefiniowanych już warunków wzorca wyszczególnionych w tabeli. W tym celu wybierz warunek wzorca w tabeli i kliknij ikony* **Edytuj** *lub* **Usuń**.
- *Wyrażenia regularne umożliwiają niezwykle wszechstronne i zaawansowane wyszukiwanie wzorców w łańcuchach danych. Szczegółowy opis tego zagadnienia wykracza poza założenia i ramy niniejszej publikacji. Tworzeniu wyrażeń regularnych poświęcona jest witryna internetowa* ***http://www.regular-expressions.info/****.*
- *Po zdefiniowaniu wszystkich wzorców można łatwo zweryfikować poprawność ich funkcjonowania, klikając przycisk* ***Testuj*** *w oknie* ***Edytor usług****. Otworzy się okno* ***Test wzorców odpowiedzi****, w którym należy wpisać oczekiwaną odpowiedź usługi, a następnie kliknąć przycisk* ***Testuj*** *w celu sprawdzenia, czy zdefiniowane wzorce znalazły dopasowanie.*

Zmiana definicji

W łatwy sposób można także zmienić właściwości dowolnej definicji usługi sieciowej (spośród definicji usług utworzonych przez użytkownika i wymienionych na odpowiedniej liście). W tym celu w oknie **Opcje** należy zaznaczyć usługę sieciową, której właściwości mają być zmienione, a następnie otworzyć okno **Edytor usług** (klikając ikonę ***Zmień definicję usługi***).

Uwaga

Zmieniane mogą być właściwości tylko tych definicji usług sieciowych, które zostały utworzone podczas korzystania z programu. Wprowadzanie zmian w którejkolwiek ze wstępnie określonych definicji usług sieciowych nie jest możliwe.

Topologia segmentów fizycznych

NetCrunch potrafi prezentować w postaci graficznej połączenia fizyczne między komputerami a zarządzalnymi przełącznikami (i urządzeniami warstwy 2 zgodnymi ze standardem Bridge MIB [RFC 1493]) w sieciach lokalnych i zdalnych. Podczas rysowania topologii segmentów fizycznych program przetwarza tabele przekazywania, a także opcjonalnie używa dodatkowych metod analizy, takich jak: tabele protokołu spanning tree (STP), Cisco Discovery Protocol (CDP) oraz SynOptics Network Management Protocol (SONMP). Ponadto program pozwala użytkownikom na dodawanie własnych niezarządzalnych urządzeń (mostów statycznych), w celu uzupełnienia struktury segmentów fizycznych wykrytej przez program – do wykonywaniu tej operacji w NetCrunchu służy specjalny kreator. Odwzorowanie topologii fizycznej w Netcrunch może być dowolnie modyfikowane przez użytkowników stosownie do potrzeb wizualizacji i zarządzania.

Uwaga

- *W chwili obecnej NetCrunch obsługuje rysowanie sieci wirtualnych VLAN w kontekście przełączników Cisco i 3Com. Oznacza to, że wszystkie urządzenia przyłączone do przełączników Cisco lub 3Com w sieciach wirtualnych są odpowiednio odwzorowywane w tworzonych przez program schematach segmentów fizycznych.*
- *Jeśli struktura segmentów fizycznych utworzona przy użyciu kreatora nie w pełni odzwierciedla daną sieć, można w każdej chwili dodać własne urządzenia warstwy 2, w tym urządzenia niezarządzalne (mosty statyczne). Por. sekcję* Wstawianie urządzeń warstwy 2 *na stronie 179.*

Procedura nasłuchu trapów SNMP

W NetCrunchu przewidziane zostały dwa sposoby nasłuchu trapów SNMP. Pierwszy to wbudowana procedura nasłuchująca, która może być dostosowana do prowadzenia nasłuchu na porcie innym niż domyślny. Drugi polega na wykorzystaniu usługi obsługi trapów SNMP firmy Microsoft o nazwie *SNMP Trap Service*, o ile usługa ta jest zainstalowana i uruchomiona na komputerze, na którym działa program. Takie rozwiązanie zapewnia wysoki poziom zgodności
z innymi produktami, które mogą być zainstalowane na tym samym komputerze.

Należy pamiętać, że na określonym porcie może prowadzić nasłuch wyłącznie jeden program, a zatem jeżeli informacja o trapach SNMP ma być udostępniana innemu programowi – albo na tym samym, albo na innym komputerze – konieczne będzie włączenie przekazywania trapów dalej, czego dokonuje się przez zaznaczenie pola wyboru **Przekierowuj trapy SNMP** i podanie adresu oraz portu innej procedury prowadzącej nasłuch trapów.

Komunikaty Syslog

Można zażądać od programu, aby na dowolnie wybranym porcie nasłuchiwał przychodzących komunikatów Syslog (dokonuje się tego w oknie **Opcje**, na stronie **Monitorowanie – Syslog**). Można również zdecydować, aby program kierował przychodzące komunikaty Syslog do dowolnego innego węzła – w takim przypadku konieczne jest podanie nazwy urządzenia lub adresu IP węzła oraz określenie portu, na którym będzie on prowadził nasłuch.

Powiadamianie

W grupie opcji związanych z powiadamianiem zmieniane może być tylko jedno ustawienie ogólne. Użytkownik może dokładnie określić przez jak długi okres czasu informacja o zdarzeniu wygenerowanym w programie NetCrunch ma być przechowywana w bazie danych SQL – zanim zostanie usunięta. Innymi słowy, jeżeli informacje o jakimkolwiek zdarzeniu są już przechowywane dłużej niż zadana ilość dni, zostaną one automatycznie usunięte.

Mowa

Jeżeli w programie NetCrunch do generowania alertów głosowych ma być wykorzystywany aparat syntezy mowy, konieczne jest skonfigurowanie jego opcji. Jeżeli na komputerze

z uruchomionym programem NetCrunch aparat syntezy mowy został zainstalowany prawidłowo, możliwe będzie wybranie go z listy rozwijanej, a nawet przetestowanie przed wykorzystaniem. Można również, posługując się poziomym suwakiem, wybrać odpowiednią szybkość wzorca mowy.

ICQ

Ustawienia udostępniane w tej grupie pozwalają użytkownikom prawidłowo skonfigurować powiadamianie za pomocą komunikatów ICQ. W szczególności należy określić serwer lub serwery ICQ (podając albo odpowiedni adres IP, albo nazwę komputera), a także unikatowy numer, nazwę oraz hasło, które mają być wykorzystywane przy tego rodzaju powiadamianiu. Po prawidłowym skonfigurowaniu wszystkich tych informacji można rozpocząć korzystanie z powiadamiania za pomocą komunikatów ICQ.

E-mail

W celu wysyłania za pomocą NetCruncha powiadomień pocztą e-mail, użytkownik ma możliwość skorzystania albo z wbudowanego serwera SMTP, albo z jakiegokolwiek innego zewnętrznego serwera poczty. Jeżeli ma być wykorzystywany zewnętrzny serwer poczty, konieczne jest określenie jego nazwy oraz portu służącego do komunikacji. Natomiast w przypadku wbudowanego serwera SMTP konieczne jest jedynie podanie adresu zwrotnego. Podany adres zwrotny będzie wykorzystywany przez każdą wiadomość powiadamiającą wysyłaną przez program w ramach procesu alertowania.

Ustawienia pagera

Innym ważnym sposobem wysyłania powiadomień jest wysyłanie wiadomości na pager. Przed skorzystaniem z niego konieczne jest prawidłowe skonfigurowanie ustawień związanych z wysyłaniem wiadomości na pagery. NetCrunch pozwala na zastosowanie dwóch niezależnych metod powiadamiania na pager. Może się ono odbywać albo za pośrednictwem standardowego modemu zainstalowanego w komputerze, na którym uruchomiony jest program NetCrunch, albo bezpośrednio za pośrednictwem Internetu. Należy więc określić, która z tych metod powinna być stosowana domyślnie podczas wysyłania powiadomienia na pager.

W przypadku powiadamiania na pager za pośrednictwem modemu należy skonfigurować trzy ustawienia. Za pomocą listy rozwijanej należy wybrać urządzenie wykorzystywane jako modem w komputerze, na którym uruchomiony jest NetCrunch. Konieczne jest także podanie liczby prób wybierania numeru przez modem. I wreszcie musi zostać wybrana i skonfigurowana usługa TAP. TAP to standardowy protokół wykorzystywany do transmisji danych na wszelkiego rodzaju pagery alfanumeryczne.

Urządzenie telefonii komórkowej GSM (telefon lub modem)

Powiadomienie może zostać wysłane za pośrednictwem telefonu komórkowego GSM, który został w jakiś sposób podłączony do komputera z uruchomionym programem NetCrunch. Możliwe jest przy tym zastosowanie połączenia za pomocą przewodu, technologii Bluetooth,

łącza podczerwieni (IrDA) lub jakiegokolwiek innego rodzaju połączenia – o ile tylko z punktu widzenia komputera wykorzystuje ono jeden z jego portów COM. W programie konieczne jest określenie ustawień dla urządzenia komórkowego GSM. Służy do tego okno **Wykryj urządzenie GSM**, w którym można określić właściwe parametry portu COM, a następnie przetestować dane urządzenie. Ponadto można zdecydować, czy program ma automatycznie rozdzielać wiadomości liczące więcej niż 160 znaków na dwie lub więcej wiadomości. Można wreszcie podać numer centrum wiadomości SMS oraz określić wszelkie dodatkowe polecenia inicjalizujące AT+C.

Mapa

Ogólne opcje mapy znajdują zastosowanie w szczególności przy włączonym trybie edycji mapy. Użytkownik może zażyczyć sobie, aby ikony, podczas ich przenoszenia w inne miejsca mapy, były wyrównywane do siatki. Gdy włączony jest tryb edycji mapy, taki sposób działania programu pozwala ręcznie umieścić odpowiednie ikony węzłów w wybranych miejscach mapy bez korzystania ze standardowej funkcji „przeciągnij i upuść". Jeżeli funkcja wyrównywania do siatki jest wyłączona, ikony mogą być ręcznie przesuwane co jeden piksel w dowolnym kierunku.

Ponadto możliwe jest ustawienie przez użytkownika stopnia przezroczystości okna z właściwościami obiektu przy wyświetlaniu tego okna podczas edycji. Pozwala to użytkownikowi, podczas wprowadzania za pomocą okna **Właściwości** zmian w określonym węźle lub w dodatkowym obiekcie na mapie, widzieć wszystkie informacje umieszczone na danej mapie.

Ikony

NetCrunch umożliwia użytkownikowi zarządzanie ikonami na mapach (tymi ikonami, które służą do reprezentowania różnego rodzajów węzłów). Może on także dodawać nowe rodzaje ikon. W tym celu wystarczy jedynie określić obraz graficzny, który w programie ma reprezentować nowy rodzaj węzła (można przy tym wykorzystać rozbudowaną listę typów obrazów), a ponadto podać krótką nazwę opisową, która będzie służyć jako nazwa danego rodzaju węzła. Po ich określeniu użytkownik może bez ograniczeń w oknie **Właściwości** przyporządkowywać ten nowo utworzony rodzaj ikony dowolnej ikonie węzła.

Uwagi

- *Nie ma potrzeby wprowadzania na udostępnianą przez program listę kilku odmian danej ikony, różniących się jedynie kolorem (reprezentujących poszczególne stany, takie jak NIEDOPOWIADA, OSTRZEŻENIE lub NIEZNANY), gdyż NetCrunch automatycznie zmienia kolor ikony, dostosowując go do aktualnego stanu węzła. Do listy takiej należy dodać tylko jedną ikonę o normalnej kolorystyce.*
- *Aby uzyskać możliwie najlepsze rezultaty, należy stosować ikony o rozmiarach 32x32, zawierające informacje dotyczące przezroczystości, w formacie Adobe Photoshop (*`PSD`*) lub pliku* `TIFF`*.*
- *Dodawanie nowych ikon do listy w programie służy jeszcze jednemu celowi. Dzięki temu program może podczas skanowania wykrywać nowe rodzaje węzłów oraz umieszczać je na mapach w postaci takich właśnie nowo zdefiniowanych ikon. Więcej informacji na ten temat zawiera rozdział* Udoskonalona identyfikacja urządzeń sieciowych *na stronie 243.*

Podpisy

Domyślnie w popisie pod każdą ikoną węzła na mapie program automatycznie wyświetla nazwę DNS danego węzła. Jednakże to predefiniowane ustawienie może zostać zmienione na jedno z następujących:

Nazwa systemowa SNMP	Jest to zawartość pola *Nazwa systemu*, odczytana z agenta SNMP uruchomionego w danym węźle.
Adres IP	Program w podpisie wyświetla adres IP węzła.
Nazwa DNS	Program wyświetla nazwę DNS urządzenia znajdującego się w danym węźle.

Można również ustawić, aby do podpisu dodawany był zawsze adres IP węzła.

Podczas pomniejszania mapy jej skala może ulec zmniejszeniu poniżej domyślnej wartości 100%. Gdy rozmiar ikon węzłów staje się na tyle mały, że ich rozpoznanie mogłoby sprawić trudność, program może automatycznie ukryć ikony węzłów i wyświetlać je jako kolorowe prostokąty. Progowa wartość skali, przy której to następuje, ustawiona jest domyślnie na 50%. Ustawienie to może zostać przez użytkownika zmienione lub całkowicie wyłączone.

Style

NetCrunch pozwala użytkownikom wstawiać na mapę obiektów graficznych (kształtów i tekstów). Korzystanie ze stylów graficznych znacznie ułatwia wprowadzanie zmian w wyglądzie tych obiektów na mapie.

Nowy styl może zostać zdefiniowany dla określonego obiektu – kształtu lub tekstu. Co więcej, można łatwo rozróżnić, do jakiego obiektu dany styl się odnosi – wystarczy w oknie **Opcje**, na stronie **Mapa – Style**, spojrzeć na niewielki element graficzny umieszczony po lewej stronie nazwy tego stylu:

- styl wyłącznie dla kształtów,

- styl wyłącznie dla tekstów,

- styl zarówno dla kształtów, jak i dla tekstów.

Tworzenie nowego stylu

Dodawanie w programie nowego stylu dla tekstów, kształtów bądź dla obu tych rodzajów obiektów, jest czynnością niezwykle prostą.

Uwaga

*Zmiany w nowym stylu wprowadzone w oknie **Właściwości stylu mapy** są natychmiast aktualizowane na mapie.*

Tło

Na tej stronie zmieniony może zostać domyślny kolor mapy. Ściślej mówiąc możliwe jest wybranie jednego z następujących rodzajów tła:

Kolor jednolity	Tło mapy będzie jednolicie jednobarwne. Konieczne jest przy tym również określenie koloru, jaki ma zostać zastosowany.
Mapa	Tłem mapy będzie jeden ze zdefiniowanych w programie obrazów przedstawiających mapę (takich, jak na przykład mapa Polski czy Europy). Do listy map można ręcznie dodać swoje własne obrazy zawierające mapy. W celu uzyskania dalszych informacji należy zapoznać się z zamieszczonymi poniżej uwagami.
Tekstura	Tło mapy będzie wypełnione jedną ze wstępnie zdefiniowanych tekstur. Do zdefiniowanej listy tekstur można ręcznie dodać swoje własne obrazy zawierające tekstury. W celu uzyskania dalszych informacji należy zapoznać się z zamieszczonymi poniżej uwagami.
Obraz	Tło mapy będzie wypełnione obrazem zapisanym w dowolnym pliku graficznym, wybranym spośród plików zapisanych w katalogu o podanej ścieżce. Użytkownik ma także możliwość rozciągnięcia obrazu umieszczonego w tle danej mapy tak, aby dopasował się on do jej obszaru.
Cieniowanie	Tło mapy będzie wypełnione gradientowo. Należy przy tym wybrać kolor początkowy i kolor końcowy takiego cieniowania oraz zdecydować, od której strony obszaru mapy (górnej, dolnej, lewej czy prawej) ma się rozpocząć zmiana koloru.

Uwagi

- *Chcąc dołączyć do domyślnej listy programu określone obrazy przedstawiające mapy, należy najpierw zamienić je na pliki w formacie* `.JPG`*,* `.GIF` *lub* `.PSD`*. Następnie należy je skopiować do podkatalogu* `\Background\Maps` *w katalogu, w którym zainstalowany jest program NetCrunch.*
- *Chcąc zastosować jako tło map własne obrazy z teksturami, należy je zamienić na pliki w formacie* `.JPG`*,* `.GIF` *lub* `.PSD`*. Następnie należy je skopiować do podkatalogu* `\Background\textures` *w katalogu, w którym zainstalowany jest NetCrunch.*

Linia połączenia

W tym miejscu programu możliwa jest zmiana ustawień domyślnych dla wyświetlanych na mapach linii połączeń. Zmieniane mogą być następujące parametry związane z liniami połączeń:

- grubość linii,
- kolor linii,
- rodzaj połączenia przekątnego (ukośny, prostokątny lub typu magistrala danych).

Sygnalizacja stanu węzła

Domyślnie, gdy zmienia się stan danego węzła, program zmienia kolor ikony takiego węzła, aby odzwierciedlał on aktualny stan węzła. Niezmieniony kolor ikony wskazuje, że określony węzeł znajduje się w stanie OK – węzeł taki odpowiada (działa prawidłowo) oraz wszystkie

monitorowane w nim usługi sieciowe odpowiadają prawidłowo. Natomiast kolor żółty oznacza, że określony węzeł znajduje się w stanie OSTRZEŻENIE – co prawda sam węzeł odpowiada, jednak niektóre z monitorowanych w nim usług sieciowych nie odpowiadają. Z kolei czerwony kolor ikony informuje, że określony węzeł znajduje się w stanie NIE ODPOWIADA – sam węzeł nie odpowiada ani żadna z monitorowanych w nim usług sieciowych nie odpowiada prawidłowo. Wreszcie szary kolor ikony sygnalizuje, iż odpowiedni węzeł znajduje się w stanie NIEZNANY – albo monitorowanie w danym węźle zostało całkowicie wyłączone, albo nie jest w nim monitorowana żadna usługa sieciowa. Więcej informacji na temat różnych stanów węzłów, z jakimi spotkać się można w programie, zawiera rozdział *Określanie stanu węzła* na stronie 70.

Omówiona powyżej domyślna metoda sygnalizacji aktualnego stanu danego węzła, polegająca na nadawaniu jego ikonie odpowiedniego koloru, może zostać zmieniona. Program udostępnia jeszcze dwie inne metody sygnalizowania stanu węzła:

- wyświetlanie za ikoną otaczającego ją kolorowego prostokąta,
- otaczanie ikony kolorową ramką.

Ponadto wszystkie te metody (łącznie z metodą domyślną, polegająca na zmianie koloru ikony) pozwalają użytkownikowi na włączenie w programie opcji migotania ikony. Gdy jest ona włączona (domyślne ustawienie w programie), wówczas przez określony czas po zmianie stanu danego węzła odpowiadająca mu ikona będzie migotać. Za pomocą dodatkowej opcji można zdecydować, aby linie połączeń (reprezentujące rzeczywiste przewody fizyczne) umieszczone na dowolnych mapach topologii fizycznej sieci migotały, gdy przewody te są odłączane od urządzeń. Możliwa jest również zmiana okresu czasu, przez jaki migotać mają ikony lub linie połączeń fizycznych.

Pamięć podręczna obrazów map

Aby udoskonalić mechanizm rysowania zawartości map, program używa pamięci podręcznej map. Przechowuje ona najczęściej używane na mapach obrazy, co pozwala zminimalizować pamięć wykorzystywaną w czasie rysowania. W opcjach programu związanych z tym zagadnieniem można wskazać maksymalny rozmiar owej pamięci podręcznej (w megabajtach) a także minimalny rozmiar obrazu, który może być w niej przechowywany (w kilobajtach).

Raporty

Gdy generowane automatycznie raporty przesyłane są użytkownikowi, mogą one być wyeksportowane w jednym z dostępnych formatów. Domyślnie wybrany jest format HTML, jednakże może on zostać zamieniony na jeden z następujących formatów:

- Quick Report QRP
- Microsoft Excel
- Dokument HTML
- Dokument XHTML

- Obraz JPEG
- Portable Document Format (PDF)
- Rich Text Format (RTF)
- Tekst

Ustawienia zdalnego dostępu

Do zapewnienia zdalnego dostępu przez przeglądarkę NetCrunch wykorzystuje wbudowany serwer HTTP. Na tej stronie możliwe jest włączanie i wyłączanie serwera HTTP programu NetCrunch oraz zmiana portu wykorzystywanego przez ten serwer (domyślnie jest to port numer 80). Jeżeli zastosowane ma być bezpieczne zdalne połączenie z programem NetCrunch, należy dodatkowo włączyć protokół SSL. W takim przypadku konieczne jest określenie plików klucza, certyfikatu oraz certyfikatu głównego. Można wreszcie zmienić przedział czasu (w minutach), w jakim w przeglądarce ma być odświeżana aktualnie oglądana strona (domyślną wartością jest jedna minuta).

Ustawienia wykrywania sieci

Możliwe jest modyfikowanie określonych parametrów, jakie NetCrunch wykorzystuje podczas procedury wykrywania sieci, w celu zwiększenia jej wydajności i skuteczności. Można zatem zmienić maksymalny czas skanowania (w sekundach), jaki NetCrunch zastosuje w celu uzyskania wszelkich niezbędnych informacji na temat nowo znalezionego węzła. Należy pamiętać, że zmniejszenie tej wartości może spowodować, że NetCrunch uzyska niepełne informacje o węźle. Z drugiej strony zwiększenie tej wartości może wydłużyć procedurę wykrywania sieci.

Kolejny parametr, jakie można ustawiać, to liczba prób pakietów ICMP oraz timeout – czyli czas odpowiedzi – w sekundach. Oba wspomniane parametry bezpośrednio decydują o tym, czy NetCrunch wykryje w sieci dany węzeł. Można także włączyć lub wyłączyć ostrzeżenie, które będzie wyświetlane przed próbą skanowania sieci obcych lub internetowych (opcja ta jest domyślnie włączona).

Konserwacja

NetCrunch pozwala określać, jak długo przechowywane będą wygenerowane zdarzenia w bazie SQL, zanim zostaną z niej usunięte. Innymi słowy, jeśli jakieś zdarzenia będą przetrzymywane dłużej niż określona maksymalna liczba dni, zostaną one automatycznie skasowane. Analogicznie w ustawieniach konserwacji można wskazać, jak długo będą trzymane na dysku zebrane trendy, zanim zostaną usunięte. Dzięki wspomnianym opcjom można uniknąć sytuacji, w której nadmierną przestrzeń na dysku NetCruncha zajmują zebrane trendy i wygenerowane zdarzenia. Z reguły zalecane jest przechowywanie trendów i zdarzeń tylko przez niezbędną liczbę dni.

Program umożliwia także użytkownikom określenie w dniach okresu, przez który przechowywane będą rejestry sesji zdalnego dostępu. W celu uzyskania dodatkowych informacji o tej funkcji, por. sekcję *Dziennik kontroli sesji zdalnego dostępu* na stronie 195.

Ponadto na stronie **Konserwacja** w opcjach programu możliwe jest modyfikowanie ścieżki katalogu, w którym zapisywana jest – a także ewentualnie odtwarzana – kopia zapasowa atlasu. Ścieżka domyślna to `../Data/Backup` w katalogu, w którym został pierwotnie zainstalowany NetCrunch.

Zgłaszanie błędów

Aby usprawnić pracę nad dalszym udoskonalaniem programu, firma AdRem Software umożliwia użytkownikom wysyłanie z NetCruncha raportu o błędzie dokumentującego określony problem. Można również w nim podać własny adres mailowy, na który producent oprogramowania NetCrunch może ewentualnie skontaktować się z użytkownikiem w celu udzielenia wskazówek lub naprawienia zaistniałego problemu.

Menedżer licencji

Wybierając stronę **Menedżer licencji** w oknie **Opcje** można przeglądać listę aktualnie zainstalowanych licencji NetCruncha (ich rodzaj, liczbę, datę ważności i numer seryjny). W oknie tym można także zainstalować nową licencję.

Eksport trendów

NetCrunch udostępnia opcję automatycznego eksportu zgromadzonych trendów (określonego węzła i rodzaju) do zewnętrznej bazy danych SQL. W tym celu należy w pierwszej kolejności włączyć tę funkcję w opcjach programu, a następnie określić wszystkie niezbędne szczegóły definiujące zewnętrzną bazę danych (rodzaj serwera bazy danych, nazwa serwera, nazwa bazy danych, rodzaj uwierzytelnienia, nazwa logowania i hasło). Powyższa opcje jest udostępniona wyłącznie w edycji Premium XE programu.

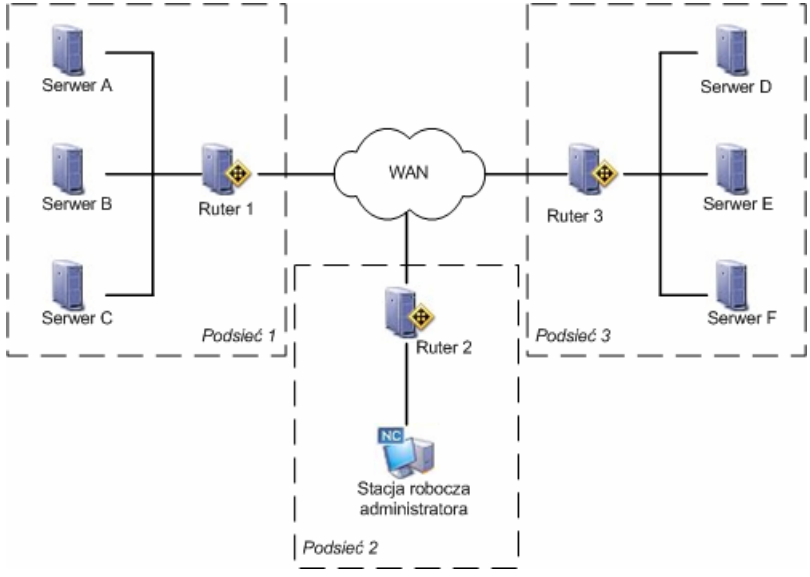
Koncepcje zaawansowanego monitorowania węzłów

Funkcjonowanie zależności sieciowych

Kolejnym zagadnieniem odgrywającym ważną rolę w zarządzaniu siecią jest mechanizm zależności sieciowych. Zależności sieciowe określają relacje między węzłami oraz rządzącą nimi hierarchię. Ma to szczególne znaczenie w monitorowaniu sieci. W wielu sytuacjach konieczne może okazać się monitorowanie określonego węzła `A` i węzła `B` w sieci, wyłącznie wtedy, gdy jakiś inny węzeł, węzeł `C`, odpowiada poprawnie (czyli jest sprawny). Kiedy natomiast ów węzeł `C` nie odpowiada, monitorowanie węzłów `A` i `B` staje się niepotrzebne, co sprawia, że ich monitorowanie powinno zostać czasowo wyłączone na mocy reguły zależności (do momentu, kiedy węzeł `C` znów zacznie odpowiadać poprawnie).

Przykład 1.

W przykładzie 1 sieć średniej wielkości zawiera kilka podsieci znajdujących się w kilku oddziałach przedsiębiorstwa i połączonych ze sobą specjalnym rodzajem węzłów sieciowych zwanych ruterami. Na rys. 1 pokazano przykładową sieć korporacyjną.



Rys. 14 Przykładowa sieć przedsiębiorstwa

Przyjmijmy założenie, że administrator sieci ma zainstalowane na swojej stacji roboczej oprogramowanie NetCrunch. Za pomocą programu administrator może monitorować

dowolną ilość węzłów dostępnych w sieci, w tym węzły krytyczne, takie jak rutery i serwery w kilku podsieciach. Jest wielce prawdopodobne, że ów administrator nadzoruje znaczną liczbę węzłów, co dodatkowo komplikuje zadanie monitorowania. W takiej sytuacji pomocny w strategii monitorowania sieci okazuje właśnie mechanizm zależności sieciowych.

Uznając, że niektóre ważne węzły są zależne w stosunku do określonego węzła nadrzędnego, NetCrunch automatycznie wstrzymuje monitorowanie węzłów podrzędnych w momencie, gdy węzeł nadrzędny przestaje odpowiadać. Będą one monitorowane tylko wtedy gdy węzeł krytyczny odpowiada poprawnie. Na podstawie rysunku 2 można wysnuć wniosek, że jeśli rutery w podsieci 1 i 3 są niesprawne, program czasowo wyłączy monitorowanie serwerów należących do podsieci, które te rutery obsługują. Dzieje się tak, ponieważ gdy określone rutery nie działają poprawnie, stacja robocza administratora nie ma łączności z obsługiwanymi przez te rutery podsieciami. Wówczas serwery należące do podsieci rutera będą czasowo wyłączone z monitorowania.

Podsumowując, administrator sieci przedsiębiorstwa może wykorzystać zawarty w NetCrunchu mechanizm zależności sieciowych w celu monitorowania kluczowych serwerów w podsieci tylko wtedy, gdy ich ruter działa poprawnie. Gdy tylko ów ruter staje się niesprawny, serwery tracą z nim łączność. W takich wypadkach NetCrunch – korzystając z zależności monitorowania – automatycznie wyłącza monitorowanie kluczowych węzłów (serwerów) zależnych od węzła krytycznego (rutera), który właśnie uległ awarii. Dzięki temu administrator może natychmiast dostrzec, że określony ruter jest niesprawny, bez potrzeby analizy awarii innych węzłów, które przestały odpowiadać na skutek awarii rutera (węzły te są wyłączane z monitorowania na czas niesprawności rutera).

Uwagi

- *Węzeł, na którym jest zainstalowany NetCrunch – dla rozróżnienia go od pozostałych węzłów – jest oznakowany specjalną ikoną z literami „NC". Wszystkie inne węzły są od niego zależne – ustawienie to nie podlega modyfikacji.*
- *Szczegółową prezentację podstawowych zagadnień związanych z mechanizmem wstrzymywania zdarzeń i jego związkiem z funkcją zależności sieciowych w NetCrunchu zawiera zamieszczona poniżej sekcja. Należy pamiętać, że wstrzymywanie zdarzeń jest dostępne wyłącznie w edycji Premium XE programu.*

Wprowadzenie do mechanizmu wstrzymywania zdarzeń

Charakterystyka ustawień monitorowania zaawansowanego

W dostępnym w NetCrunchu mechanizmie zaawansowanego wstrzymywania zdarzeń zastosowano następujące cztery ustawienia:

Wstrzymuj zdarzenia z podrzędnych węzłów	Opcja ta znajduje zastosowanie wyłącznie w przypadku węzłów figurujących w drzewie zależności monitorowania – czyli takich węzłów, która posiadają co najmniej jeden podlegający im węzeł. Gdy jest włączona, nie jest widoczna w ustawieniach węzłów zależnych od danego węzła. Opcja ta zakłada, że gdy z jakiegokolwiek powodu węzeł ulega awarii, zdarzenia o treści "Węzeł nie odpowiada" lub "Usługa nie odpowiada" NIE SĄ generowane dla węzłów zależnych od tego węzła (zostaną one wyłączone na mocy reguły zależności). Gdy opcja ta jest wyłączona, wszystkie zdarzenia o treści "Węzeł nie odpowiada" lub "Usługa nie odpowiada" SĄ generowane dla wszystkich węzłów zależnych od tego węzła (przy równoczesnym uwzględnieniu ustawienia na tych węzłach opcji **Wstrzymuj zdarzenia związane z usługami węzła**).
Wyklucz z mechanizmu wstrzymywania zdarzeń	Opcja dotyczy wyłącznie węzłów zależnych, których węzeł nadrzędny posiada włączoną opcję **Wstrzymuj zdarzenia z podrzędnych węzłów**. Ustawienie opcji **Wyklucz z mechanizmu wstrzymywania zdarzeń** na węźle podrzędnym oznacza, że węzeł zostanie pominięty w mechanizmie wstrzymywanie zdarzeń włączonym na jego węźle nadrzędnym. Gdy opcja ta jest włączona, wszystkie zdarzenia o treści "Węzeł nie odpowiada" lub "Usługa nie odpowiada" SĄ generowane dla takiego węzła (przy równoczesnym uwzględnieniu ustawienia na tym węźle opcji **Wstrzymuj zdarzenia związane z usługami węzła**).
Wstrzymuj zdarzenia związane z usługami węzła	Gdy niniejsza opcja jest włączona na węźle i węzeł ten przestaje odpowiadać, NIE SĄ GENEROWANE dodatkowe zdarzenia o treści "Usługa nie odpowiada". Generowane jest wówczas dla węzła tylko jedno zdarzenie o treści "Usługa nie odpowiada".
Wyklucz wstrzymywanie zdarzeń na usługach sieciowych	Opcja ta obowiązuje tylko wtedy, gdy równocześnie włączona jest na węźle opcja **Wstrzymuj zdarzenia związane z usługami węzła**. Gdy dla usługi na węźle włączona jest funkcja **Wyklucz wstrzymywanie zdarzeń na usługach sieciowych**, oznacza to, że zdarzenie o treści "Usługa nie odpowiada" JEST generowane tylko dla tej konkretnej usługi, mimo iż obowiązuje reguła, że wszystkie zdarzenia związane z usługami na danym węźle mają być wstrzymywane (zgodnie z ustawieniem **Wstrzymuj zdarzenia związane z usługami węzła**).

Uwagi

- *Powyższe ustawienia zostały opisane w porządku od najważniejszego do najmniej ważnego priorytetu logicznego.*

- *Pierwsze trzy powyższe ustawienia można modyfikować w karcie **Zaawansowane** okna **Monitorowanie** na węźle, lub bezpośrednio w Menedżerze wstrzymywania zdarzeń.*
- *Ostatnia opcja jest ustawiania w oknie **Właściwości usługi** dla określonej usługi na węźle.*

Ważne informacje na temat mechanizmu wstrzymywania zdarzeń

Gdy NetCrunch wstrzymuje jakiekolwiek zdarzenie związane z usługą lub węzłem (”Węzeł nie odpowiada” lub ”Usługa nie odpowiada”), ustawione na czas późniejszy komplementarne zdarzenia o treści ”Węzeł odpowiada” lub ”Usługa odpowiada” także nie będą generowane, mimo zaistnienia odpowiednich warunków.

Domyślnie opcja **Wstrzymuj zdarzenia z podrzędnych węzłów** włączona jest dla wszystkich węzłów wykrytych na drodze skanowania lub ręcznie umieszczonych na mapie. Pozostałe trzy ustawienia są na nich zawsze wyłączone. Jedynym wyjątkiem jest węzeł, na którym zainstalowany jest NetCrunch, na których wszystkie powyższe opcje są zawsze włączone.

Gdy po przeniesieniu atlasu na inny komputer sieciowy (także na komputer z zainstalowanym NetCrunchem) dany atlas zostaje otworzony, ów nowy komputer sieciowy automatycznie staje się węzłem z NetCrunchem. W takich wypadkach aktualne ustawienie opcji **Wstrzymuj zdarzenia z podrzędnych węzłów** dla poprzedniego węzła z NetCrunchem (włączona/wyłączona) zostanie automatycznie zduplikowane na węźle oznaczonym jako nowy węzeł z NetCrunchem.

Po włączeniu opcji **Wstrzymuj zdarzenia z podrzędnych węzłów** na węźle nadrzędnym, opcja ta zostanie automatycznie włączona na wszystkich węzłach od niego zależnych. Co więcej nie będzie wówczas można wyłączyć tego ustawienia na pokrewnych węzłach podrzędnych (będzie ono wyszarzone). Aby utworzyć wyjątek od tej reguły na poszczególnych węzłach podrzędnych, należy włączyć dostępną na nich opcję **Wyklucz z mechanizmu wstrzymywania zdarzeń**.

Jednakże wyłączenie na węźle nadrzędnym opcji **Wstrzymuj zdarzenia z podrzędnych węzłów** NIE OZNACZA, że opcja ta zostanie także automatycznie wyłączona na wszystkich węzłach zależnych od tego węzła. Aby zmienić to ustawienie na tych węzłach, należy je zaznaczyć, a następnie odznaczyć opcję **Wstrzymuj zdarzenia z podrzędnych węzłów** (na przykład w **Menedżerze wstrzymywania zdarzeń** lub na mapie **Zależności monitorowania**).

Ilustracja

Gdy węzeł B jest zależny od węzła A, zachodzi następująca sytuacja:

- Opcja **Wyklucz z mechanizmu wstrzymywania zdarzeń** na podrzędnym węźle B ma zastosowanie jedynie wtedy, gdy na węźle nadrzędnym włączona jest opcja **Wstrzymuj zdarzenia z podrzędnych węzłów** .
- Opcja **Wstrzymuj zdarzenia związane z usługami węzła** na węźle podrzędnym B ma zastosowanie jedynie, gdy:
  - na węźle nadrzędnym A wyłączona jest opcja **Wstrzymuj zdarzenia z podrzędnych węzłów**.

  lub
  - na węźle nadrzędnym A włączona jest opcja **Wstrzymuj zdarzenia z podrzędnych węzłów**, a na węźle podrzędnym B włączona jest opcja **Wyklucz z mechanizmu wstrzymywania zdarzeń**.

- Opcja **Wyklucz wstrzymywanie zdarzeń na usługach sieciowych** na węźle zależnym B ma zastosowanie jedynie, gdy na zależnym węźle B jest włączona opcja **Wstrzymuj zdarzenia związane z usługami węzła**.

Rozumienie stanu usługi typu „Nieokreślony"

Konsekwencją stosowania powyższych czterech ustawień jest fakt, iż generowanie zdarzeń typu "NIE ODPOWIADA" na węźle zależnym będzie opóźniane do momentu, kiedy program wykryje, że nadrzędny w stosunku do niego węzeł odpowiada i jest sprawny lub z jakiegoś powodu jest wyłączony z monitorowania (nie odpowiada). Jeśli węzeł nadrzędny jest z kolei zależny od innego węzła, program będzie dodatkowo starał się ustalić stan tego węzła.

W przypadku opcji **Wstrzymuj zdarzenia z podrzędnych węzłów**, powyższe opóźnienie nie przekracza 30 sekund, ponieważ usługa wiodąca na węźle nadrzędnym zawsze będzie monitorowana w przybliżeniu co 30 sekund. W trakcie tego opóźnienia usługi sieciowe węzła podrzędnego są oznaczane tymczasowym statusem o nazwie „Nieokreślony". Ów specjalny przypadek stanu definiuje usługę sieciową, której stan przejściowo nie można zostać ustalony, ponieważ węzeł wciąż oczekuje na potwierdzenie statusu węzła nadrzędnego.

Uwaga

*Gdy ustawiona jest opcja **Wstrzymuj zdarzenia związane z usługami węzła**, opóźnienie nigdy nie przekracza czasu monitorowania usługi sieciowej. Jeśli dla każdej usługi sieciowej ustawione są różne czasy monitorowania, w celu ustalenia, czy węzeł odpowiada, program zawsze będzie używał czasu najkrótszego.*

Ilustracja

Przyjmijmy, że na nadrzędnym węźle A usługą wiodącą jest usługa sieciowa PING, a na zależnym od niego węźle B usługą wiodącą jest SNMP.

Jeśli na węźle nadrzędnym A odznaczona została opcja **Wstrzymuj zdarzenia z podrzędnych węzłów,** a na zależnym od niego węźle B usługa SNMP przestaje odpowiadać, status usługi SNMP na węźle B zmieni się do wartości BŁĄD (nie odpowiada), a ponadto na węźle B zostanie wygenerowane zdarzenie o treści a "Usługa SNMP nie odpowiada".

Jeśli na węźle nadrzędnym A włączona jest opcja **Wstrzymuj zdarzenia z podrzędnych węzłów,** a na zależnym od niego węźle B usługa SNMP przestaje odpowiadać, program będzie oczekiwał na ustalenie statusu sprawności/niesprawności nadrzędnego węzła A, od którego zależy węzeł B. W międzyczasie usługa SNMP na zależnym węźle B będzie tymczasowo posiadać status „Nieokreślony". W trakcie 30-sekundowego opóźnienia – czyli w okresie, w jakim program sprawdza stan usługi wiodącej na nadrzędnym węźle A – mogą zaistnieć co najwyżej trzy zdarzenia:

- **Usługa SNMP na węźle podrzędnym B wznawia poprawne odpowiadanie** – status usługi SNMP wraca do wartości "OK", a na węźle B generowane są zdarzenia o treści "Usługa SNMP nie odpowiada" oraz "Usługa SNMP odpowiada".
- **Działająca na węźle nadrzędnym usługa (wiodąca) PING odpowiada poprawnie (Stan "OK") –** status usługi SNMP zmienia się na "BŁĄD" i generowane jest zdarzenie o treści "Usługa SNMP nie odpowiada" na węźle B.

- **Usługa (wiodąca) PING na węźle nadrzędnym nie odpowiada (stan „BŁĄD”)** – usługa SNMP otrzymuje status „BŁĄD”, natomiast zdarzenie ”Usługa SNMP nie odpowiada” NIE JEST generowane (na mocy reguły wstrzymywania zdarzeń zdefiniowanej na nadrzędnym węźle A). Natomiast na węźle A generowane jest zdarzenie o treści „Węzeł nie odpowiada”.

Przykładowy scenariusz

Dla wszystkich czterech poniższych przypadków zachodzą następujące warunki:

- węzeł A posiada usługę PING w charakterze usługi wiodącej, a inną usługą na liście monitorowanych usług tego węzła jest usługa SNMP.
- węzeł B, zależny od węzła A, także posiada usługę PING jako usługę wiodącą, a inną usługą na liście monitorowanych usług tego węzła jest usługa SNMP.
- węzeł C, zależny od węzła B, także posiada usługę PING jako usługę wiodącą,; inną usługą na liście monitorowanych usług tego węzła jest usługa FTP.

Rys. 15 Przykładowa hierarchia węzłów

Przypadek 1

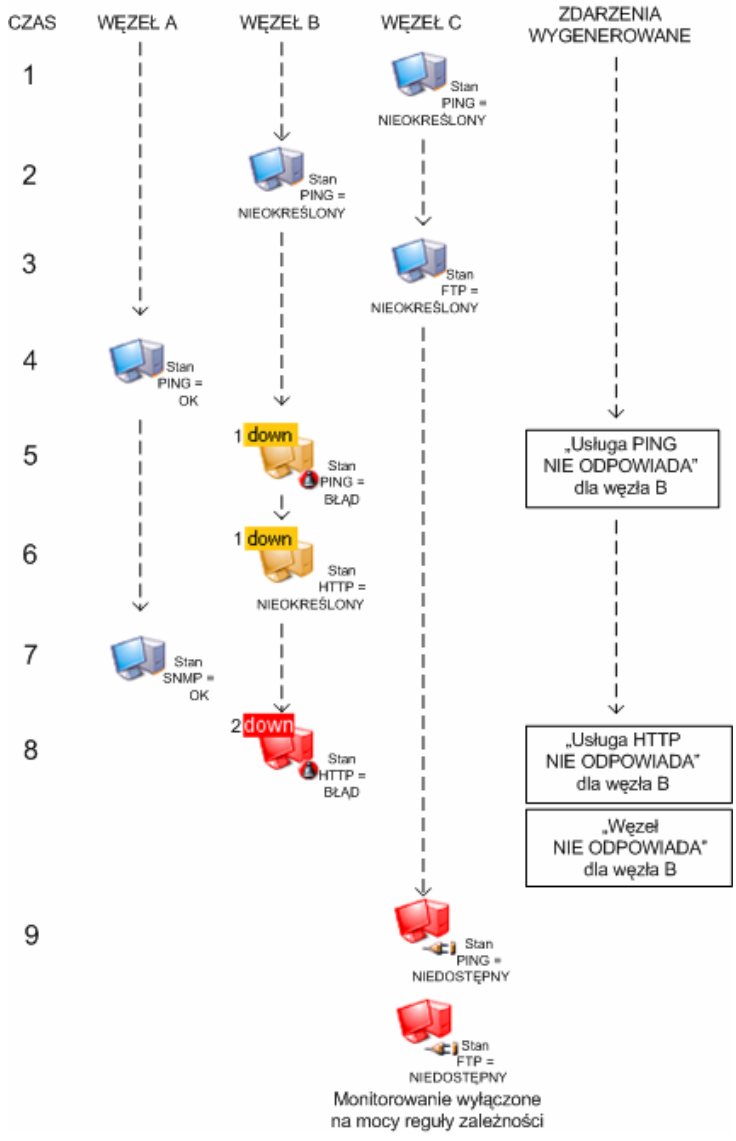
Na każdym z powyższych węzłów wyłączone są wszystkie cztery opcje wstrzymywania zdarzeń.

W takim przypadku wszystkie zdarzenia o treści ”Węzeł nie odpowiada” i „Usługa nie odpowiada”, oraz o treści ”Węzeł odpowiada” i „Usługa odpowiada” będą generowane w porządku określonym przez stosowaną w NetCrunchu procedurę monitorowania.

Przypadek 2

Opcja **Wstrzymuj zdarzenia z węzłów podrzędnych** jest włączona na węźle A.
W konsekwencji jest ona także automatycznie włączona na zależnym od węzła A węźle B, który posiada co najmniej jeden węzeł zależny, węzeł C. Jednakże ustawienie to nie obowiązuje (jest wyłączone) na węźle C, ponieważ węzeł ten nie posiada żadnych węzłów od niego zależnych.

W momencie gdy węzeł B przestaje odpowiadać, zachodzą następujące zdarzenia (pokazane na poniższym rysunku):

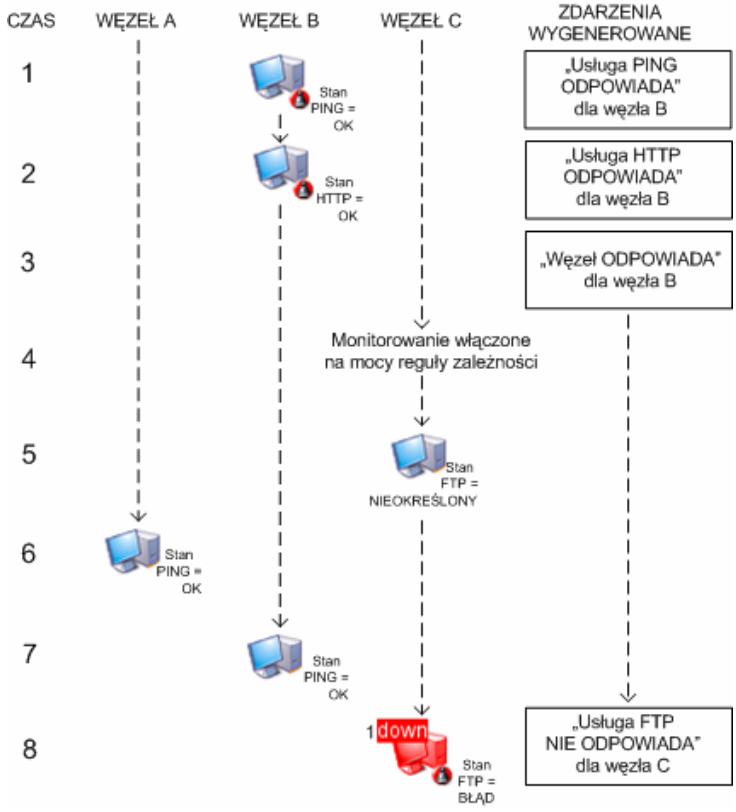


Rys. 16 Przypadek 2 A

Warto zauważyć, że choć usługi PING i FTP na węźle C stają się niedostępne (na mocy reguły zależności), nie są generowane żadne stosowne zdarzenia. Zdarzenia o treści ”Usługa PING nie odpowiada”, ”Usługa FTP nie odpowiada” oraz ”Węzeł C nie odpowiada” są

wstrzymywane, ponieważ na węźle B zaznaczone jest pole wyboru **Wstrzymuj zdarzenia z podrzędnych węzłów**.

Z kolei, gdy później węzeł B zaczyna odpowiadać poprawnie i jednocześnie usługa FTP na węźle C przestaje odpowiadać, następują zamieszczone poniżej zdarzenia:



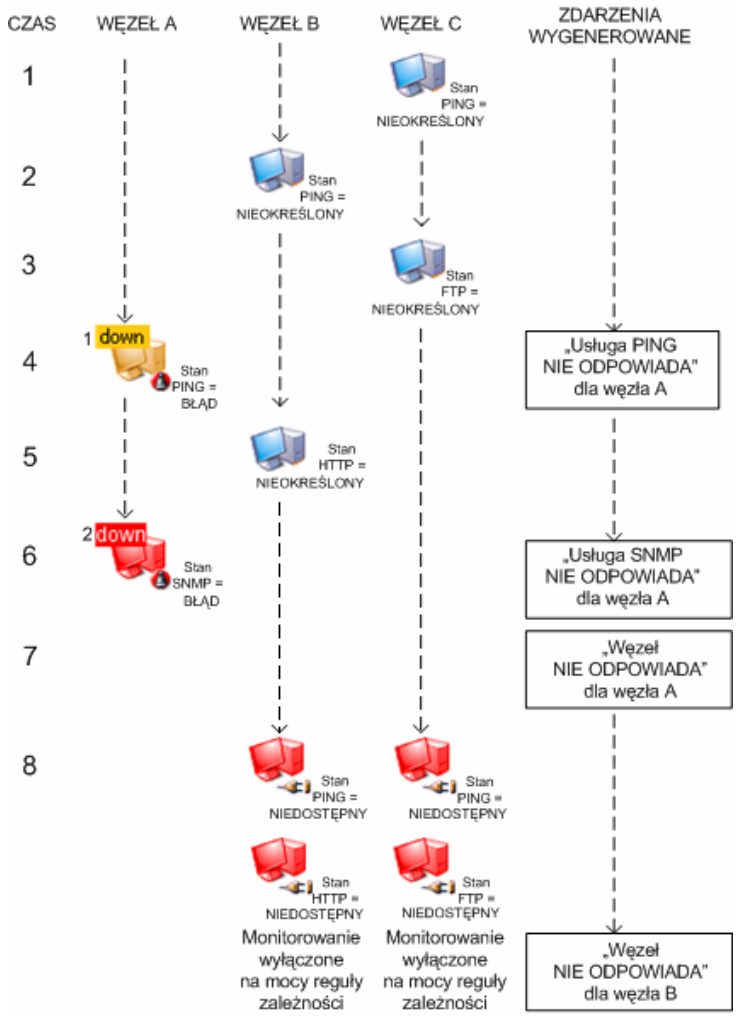
Rys. 17 Przypadek 2 B

Warto zauważyć, że w tym przypadku zdarzenia typu „ODPOWIADA" związane z węzłem B są generowane, ponieważ przeciwstawne w stosunku do nich zdarzenia „NIE ODPOWIADA" zostały wcześniej wygenerowane (co zostało opisane w poprzednim przykładzie). Jednakże dla węzła C generowane jest jedynie zdarzenie o treści „Usługa FTP nie odpowiada", ponieważ ta właśnie usługa przestała odpowiadać. Zdarzenia wywołane stanem „ODPOWIADA" na węźle C nie są generowane, ponieważ komplementarne w stosunku do nich zdarzenia „NIE ODPOWIADA" zostały wstrzymane i z tego powodu nie zostały wygenerowane (co zostało opisane w poprzednim przykładzie).

Przypadek 3

Na węźle A włączona jest opcja **Wstrzymuj zdarzenia z podrzędnych węzłów** (która jest także włączona na węźle B, ponieważ ów węzeł posiada co najmniej jeden węzeł od siebie zależny). Ponadto na węźle B włączone są opcje **Wyklucz z mechanizmu wstrzymywania zdarzeń** oraz **Wstrzymuj zdarzenia związane z usługami węzła**.

Zatem kiedy węzeł A staje się niesprawny, zachodzą następujące reakcje:

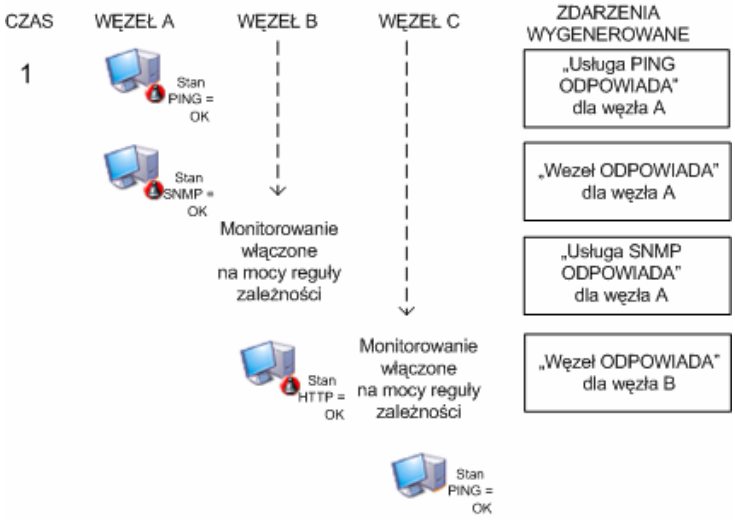


Rys. 18 Przypadek 3 A

Jak widać powyżej, dla węzła A, który stał się niesprawny, generowane są zgodnie z oczekiwaniami wszystkie trzy zdarzenia o treści ”Węzeł nie odpowiada”, ”Usługa SNMP nie

odpowiada" oraz "Usługa PING nie odpowiada". W międzyczasie wszystkie trzy zdarzenia dla węzła C są wstrzymywane, ponieważ na węźle B włączona jest opcja **Wstrzymuj zdarzenia z podrzędnych węzłów**. Wreszcie na węźle B generowane jest zdarzenie "Węzeł nie odpowiada", ponieważ z uwagi na włączone ustawienie **Wyklucz z mechanizmu wstrzymywania zdarzeń** nie są wstrzymywane dla tego węzła zdarzenia związane ze stanem usługi i węzła (choć jest to zasygnalizowane w odpowiednim ustawieniu na węźle A, od którego ów węzeł jest zależny). Z drugiej strony zdarzenia o treści „Usługa PING nie odpowiada" i „Usługa HTTP nie odpowiada" nie będą generowane, ponieważ nie węźle B włączona jest opcja **Wstrzymuj zdarzenia związane z usługami węzła**.

Kiedy węzeł A ponownie zaczyna odpowiadać, zachodzą następujące reakcje:



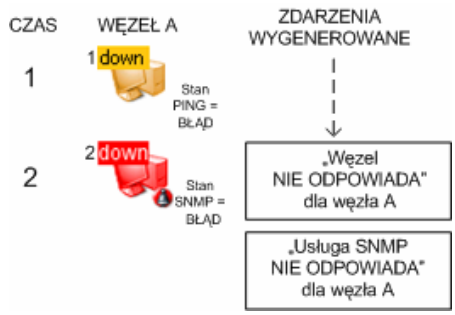
Rys. 19 Przypadek 3 B

Warto odnotować, że generowane są jedynie zdarzenia typu „ODPOWIADA, dla których zostały poprzednio wygenerowane komplementarne w stosunku do nich zdarzenia typu „NIE ODPOWIADA". Dla węzła C nie zostały wygenerowane żadne zdarzenia, ponieważ wszystkie związane z nim zdarzenia o treści „Usługa/węzeł nie odpowiada" zostały wstrzymane. Analogicznie na węźle B nie zostaną wygenerowane żadne zdarzenia o treści „Usługa PING odpowiada" i „Usługa HTTP odpowiada", ponieważ komplementarne w stosunku do nich zdarzenia typu "NIE ODPOWIADA" zostały wstrzymane.

Przypadek 4

W tym przypadku w centrum uwagi jest wyłącznie węzeł A. Wyłączona jest na nim opcja **Wstrzymuj zdarzenia z podrzędnych węzłów**, natomiast włączona jest opcja **Wstrzymuj zdarzenia związane z usługami węzła**. Ponadto dla działającej na tym węźle usługi SNMP włączona jest opcja **Wyklucz wstrzymywanie zdarzeń na usługach sieciowych**.

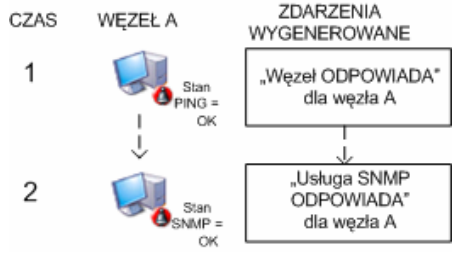
Gdy węzeł A przestaje odpowiadać, zachodzą następujące okoliczności:



Rys. 20 Przypadek 4 A

Warto zauważyć, że choć na węźle A zdarzenia związane ze stanem usług sieciowych są wstrzymywane (na mocy włączonej opcji **Wstrzymuj zdarzenia związane z usługami węzła**), zostanie wygenerowane zdarzenie o treści „Usługa SNMP nie odpowiada", ponieważ opcja **Wyklucz wstrzymywanie zdarzeń na usługach sieciowych** została włączona na działającej na tym węźle usłudze sieciowej SNMP.

Gdy węzeł A ponownie zaczyna odpowiadać, zachodzą następujące zdarzenia:



Rys. 21 Przypadek 4 B

Godny uwagi jest fakt, iż wygenerowane zostaną jedynie dwa zdarzenia o treści „ODPOWIADA", dla których poprzednio zostały wygenerowane komplementarne w stosunku do nich zdarzenia typu "NIE ODPOWIADA". Innymi słowy, zdarzenia komplementarne w stosunku do zdarzeń wstrzymanych – czyli zdarzenie o treści "Usługa PING odpowiada" – również nie zostaną wygenerowane.

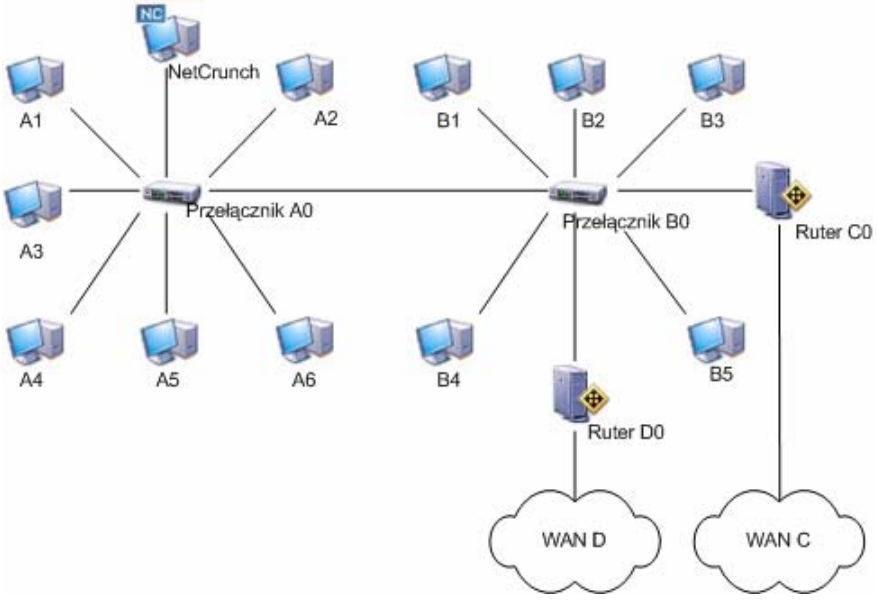
Wstrzymywanie zdarzeń wywołanych zależnościami sieciowymi

Podczas tworzenia zależności sieciowych między węzłami sieciowymi ważne jest kontrolowanie zdarzeń, które mają być generowane lub wstrzymywane na każdym poziomie zależności. Z reguły praktyczne okazuje się wstrzymywanie zdarzeń z węzłów podrzędnych, chyba że dany węzeł odgrywa w danej sieci krytyczne znaczenie lub jest urządzeniem sieciowym (serwem, ruterem, przełącznikiem, itp.). Wówczas warto tworzyć wyjątki od reguły

wstrzymywania zdarzeń, dzięki czemu można zawsze szybko dowiadywać się o awariach takich krytycznych węzłów dzięki zdarzeniom i akcjom inicjowanym przez NetCruncha.

Przykład 2

Zamieszczony niżej diagram przedstawia typowy schemat sieci komputerowej. Komputer, na którym zainstalowany jest NetCrunch, znajduje się w lewym górnym rogu i opatrzony jest charakterystyczną ikoną. Jak widać na rysunku, sieć składa się z dwóch przełączników, do których podłączone są dwie lokalne stacje robocze; ponadto funkcjonują w niej dwa rutery zapewniające komunikację z innymi węzłami w rozległej sieci przedsiębiorstwa.



Rys. 22 Przykład sieci przedsiębiorstwa

W tym przypadku kluczowe znaczenie dla ogólnego stanu sieci mają dwa przełączniki i dwa rutery. Wobec powyższego w pierwszym rzędzie należy:

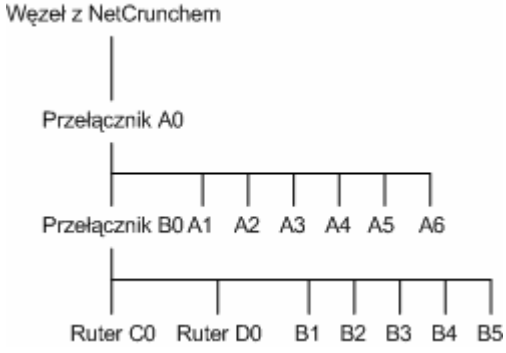
- **Krok 1:** ustawić odpowiednie zależności sieciowe na krytycznych urządzeniach sieciowych i innych węzłach.
- **Krok 2:** ustawić wstrzymywanie zdarzeń (dotyczących stanu usług i węzłów sieciowych) na węzłach podrzędnych na każdym poziomie zależności.
- **Krok 3**: wykluczyć wstrzymywanie zdarzeń na krytycznych urządzeniach sieciowych tak, aby generowane na nich zdarzenia dotyczące stanu urządzeń i usług były zawsze generowane, gdy nadrzędny w stosunku do nich węzeł przestaje odpowiadać.

Krok 1: Ustawianie zależności sieciowych

W pierwszej kolejności należy ustawić odpowiednie zależności sieciowe na krytycznych urządzeniach sieciowych oraz innych rodzajach węzłów. W pierwszym rzędzie warto ustawić zależność rutera C0 i rutera D0 na przełączniku B0. Należy również zdefiniować zależność węzłów B1, B2, B3, B4 i B5 na przełączniku B0. Wówczas, gdy przełącznik B0 z jakiegokolwiek powodu przestanie odpowiadać, monitorowanie zarówno rutera C0 jak i rutera D0 (oraz oczywiście węzłów od B1 do B5) zostanie automatycznie wyłączone przez NetCruncha na mocy reguły zależności.

Następnie należy ustawić zależność przełącznika B0 na przełączniku A0, tak, by w momencie awarii tego ostatniego, monitorowanie przełącznika B0 było automatycznie wyłączone na mocy reguły zależności. Ponadto należy podporządkować węzły A1, A2, A3, A4, A5 i A6 przełącznikowi A0.

W kolejnym kroku należy ustawić w programie odpowiednie zależności sieciowe: ruter C0 jest zależny od przełącznika B0, a ruter D0 także jest zależny od przełącznika B0. Węzły B1-B5 również są podrzędne w stosunku do przełącznika B0. Z kolei przełącznik B0 jest zależny od przełącznika A0, od którego zależne są także węzły A1-A6. Wreszcie przełącznik A0 jest zależny od węzła z NetCrunchem. Ustawione poziomy zależności zostały pokazane na poniższym diagramie.



Rys. 23 Diagram poziomów zależności

Uwagi

- *Nie ma potrzeby ustawiania na przełączniku A0 zależności od węzła z NetCrunchem, ponieważ program automatycznie uzależnia nowo wykrywane węzły od węzła z NetCrunchem.*
- *Zależności węzłów ustawia się w oknie* ***Monitorowanie*** *pojedynczego węzła, w którym należy kliknąć kartę* ***Ogólne*** *a następnie w polu* ***Monitorowanie jest zależne od stanu:*** *zaznaczyć inny węzeł, od którego dany węzeł ma zależeć.*

Krok 2: Ustawianie wstrzymywania zdarzeń

Gdy ustawiono już odpowiednie zależności, można przejść do kroku 2 polegającego na definiowaniu reguł wstrzymywania zdarzeń na wszystkich węzłach zależnych na każdym poziomie zależności. W efekcie gdy węzeł przestanie odpowiadać (przez co wszystkie zależne od niego węzły zostaną wyłączone na mocy reguły zależności), na węzłach zależnych nie będą

generowane żadne zdarzenia (takie jak ”Węzeł nie odpowiada” lub ”Usługa nie odpowiada”). Innymi słowy zostanie wygenerowane tylko jedno zdarzenie (o treści „Węzeł nie odpowiada”), mimo iż węzły zależne także nie odpowiadają (zostały wyłączone na mocy reguły zależności).

Aby wstrzymać zdarzenia z węzłów zależnych, należy wybrać odpowiednią opcję monitorowania na samym węźle. W praktyce wystarczy wybrać taką opcję na węźle stojącym na najwyższym poziomie zależności (nie uwzględniając węzła z NetCrunchem), ponieważ wszystkie węzły zależne od danego węzła i posiadające co najmniej jeden węzeł zależny (na każdym poziomie) także będą wówczas miały automatycznie włączoną tę opcję.

Na omawianym powyżej rysunku 32 węzłem na najwyższym poziomie zależności (poza węzłem z NetCrunchem) jest przełącznik A0. Dlatego też należy w takim przypadku wstrzymywać jedynie zdarzenia z węzłów zależnych od węzła A0 – ustawienie do zostanie przypisane wszystkim węzłom zależnym, które posiadają co najmniej jeden węzeł zależny (na każdym poziomie).

Uwaga

*Aby ustawić tę opcję, należy otworzyć dla węzła okno **Monitorowanie**, kliknąć kartę **Zaawansowane**, a następnie zaznaczyć pole wyboru **Wstrzymuj zdarzenia z węzłów podrzędnych**.*

Krok 3: Tworzenie wyjątków od reguły wstrzymywania zdarzeń

Po odpowiednim zdefiniowaniu wstrzymywania zdarzeń z węzłów podrzędnych (związanych ze stanem węzła lub usług), w momencie awarii węzła, np., przełącznika A0, wyłączone zostaną na mocy reguły zależności wszystkie zależne od niego węzły (na każdym poziomie). Z kolei z powodu ustawionej reguły wstrzymywania zdarzeń na węzłach zależnych nie będą generowane zdarzenia o treści ”Węzeł nie odpowiada” lub ”Usługa nie odpowiada”.

Aby mieć pewność, że będziemy powiadamiani o wszystkich awariach zachodzących na ważnych węzłach wyłączonych przez regułę zależności, należy dodatkowo na takich węzłach wykluczyć wstrzymywanie zdarzeń. W tym celu na każdym takim urządzeniu należy – w powyższym przypadku na przełącznikach A0 i B0 oraz na ruterach i D0 – włączyć wykluczenie z reguły wstrzymywania zdarzeń.

Uwaga

*Aby utworzyć wyjątek od reguły wstrzymywania zdarzeń, należy otworzyć okno **Monitorowanie** dla węzła, kliknąć kartę **Zaawansowane**, a następnie zaznaczyć pole wyboru **Wyklucz z mechanizmu wstrzymywania zdarzeń**.*

Zakończenie

Do stosowania zawartych w programie mechanizmów wstrzymywania zdarzeń i zależności sieciowych konieczne jest uprzednie posiadanie sprecyzowanych założeń i strategii. Przed podjęciem opisanych powyżej procedur w zaawansowanych ustawieniach węzłów, należy ustalić, które węzły mają w danej sieci krytyczne znaczenie i jakie są między nimi zależności. Aby wykonać trzy opisane powyżej kroki, należy zawęzić listę urządzeń krytycznych dla danej infrastruktury sieciowej (dla których chcemy zawsze otrzymywać zdarzenia o treści ”Węzeł nie odpowiada” lub ”Usługa nie odpowiada”).

Powyższe procedury pozwalają ustawić w programie zaawansowany mechanizm monitorowania i alertowania. Przykładowo w sieci pokazanej na rysunku 30 na stronie 227 można powiązać powiadomienie pocztą elektroniczną ze zdarzeniami o treści „Węzeł nie odpowiada" dla różnych urządzeń infrastruktury o ważnym znaczeniu. Główny administrator sieci może wówczas otrzymywać email w momentach, gdy jakieś urządzenie – przełącznik A0, przełącznik B0, ruter C0 i ruter D0 – przestaje odpowiadać (z jakiegokolwiek powodu, w tym na mocy reguły zależności). Ponadto inny administrator odpowiedzialny wyłącznie za sieć rozległą C mógłby otrzymywać wiadomość mailową, gdy ruter C0 przestaje odpowiadać. Analogicznie trzeci administrator, odpowiedzialny za sieć rozległą D, mógłby otrzymywać powiadomienie pocztą elektroniczną o awarii rutera D0 (także spowodowanej wyłączeniem na mocy reguły zależności). W ten sposób, stosując wstrzymywanie zdarzeń i zależności sieciowe program pozwala odpowiednim fachowcom o zróżnicowanym zakresie obowiązków na natychmiastowe otrzymywanie informacji o zdarzeniach w zarządzanej przez nich sieci. W ten sposób mogą poświęcić więcej czasu i uwagi na problemy pojawiające się w najważniejszych komponentach sieci.

Wstrzymywanie zdarzeń na usługach sieciowych

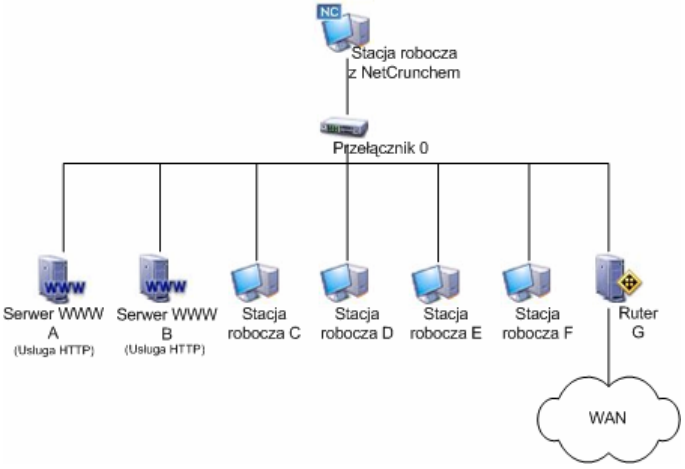
Kolejnym zaawansowanym ustawieniem monitorowania w programie jest wstrzymywanie zdarzeń związanych z usługami sieciowymi w momencie, gdy węzeł przestaje odpowiadać (i w rezultacie nie opowiadają wszystkie działające na nim usługi sieciowe). Oznacza to, że w momencie awarii węzła, liczne zdarzenia o treści „Usługa sieciowa nie odpowiada" dotyczące usług monitorowanych na tym węźle zostaną wstrzymane i nie będą generowane. Także w tym przypadku można definiować wyjątki od reguły wstrzymywania zdarzeń dla usługi sieciowej, która odgrywa w danej sieci istotne znaczenie – wówczas dla usługi tej będzie generowane zdarzenie o treści „Usługa sieciowa odpowiada".

Przykład 3

Zamieszczony niżej diagram przedstawia typowy schemat sytuacyjny sieci komputerowej. Komputer, na którym zainstalowany jest NetCrunch znajduje się na czele hierarchii i jest podłączony do przełącznika 0. Do wspomnianego przełącznika przyłączone są różne inne węzły: serwer webowy A, serwer webowy B, stacja robocza C, stacja robocza D, stacja robocza E, stacja robocza F oraz ruter G. Warto odnotować, że ruter G służy także za punkt dostępu do sieci rozległej.

Załóżmy, że na wszystkich węzłach podpiętych do przełącznika interesuje nas tylko otrzymywanie zdarzeń wywołanych stanem węzła („Węzeł nie odpowiada"). Chcemy natomiast uniknąć dodatkowych zdarzeń dotyczących stanu usługi („Usługa sieciowa nie odpowiada") w momencie, gdy określony węzeł jest wyłączony na mocy reguły zależności z powodu awarii przełącznika. Jedynym wyjątkiem od tej reguły są dwa serwery webowe, na których działa usługa HTTP. W tym przypadku chcemy otrzymywać powiadomienia w momencie, gdy krytyczna usługa HTTP na tych dwóch węzłach staje się niedostępna – także z powodu wyłączenia węzła przez regułę zależności. Wówczas należy ustawić wyjątek od wstrzymywania zdarzeń na usłudze HTTP działającej na serwerach A i B.

W omawianym przypadku dla uproszczenia nie zostanie użyta funkcja wstrzymywania zdarzeń z węzłów podrzędnych.



Rys. 24 Przykład sieci

Ogólna zasada postępowania przedstawia się następująco:

- **Krok 1:** upewnij się, że wstrzymywanie zdarzeń w węzłów podrzędnych nie jest włączone na węźle nadrzędnym w stosunku do węzłów, których zdarzenia związane z usługami mają być wstrzymywane.
- **Krok 2:** ustaw wstrzymywanie zdarzeń związanych z usługami na wszystkich odpowiednich węzłach.
- **Krok 3:** utwórz wyjątek od wstrzymywania zdarzeń związanych ze stanem usług na węźle dla działającej na serwerach webowych usługi sieciowej HTTP.

Krok 1: Wyłączanie wstrzymywania węzłów zależnych

W przedstawionej wyżej sieci węzłem rządzącym węzłami, których zdarzenia związane z usługami mają być wstrzymywane, jest przełącznik 0. Z tego powodu należy w zaawansowanych opcjach tego węzła wyłączyć wstrzymywanie zdarzeń z węzłów podrzędnych.

Uwaga

*Aby ustawić tę opcję, należy otworzyć dla węzła okno **Monitorowanie**, kliknąć kartę **Zaawansowane**, a następnie odznaczyć pole wyboru **Wstrzymuj zdarzenia z podrzędnych węzłów**.*

Krok 2: Ustawianie wstrzymywania zdarzeń związanych ze stanem usług

Następnie na wszystkich węzłach podpiętych do przełącznika 0 (za wyjątkiem stacji roboczej z NetCrunchem), należy włączyć wstrzymywanie zdarzeń związanych z usługami węzła. Dzięki temu gdy dowolny z tych węzłów zostanie wyłączony na mocy reguły zależności z powodu awarii węzła nadrzędnego (przełącznika 0) (i gdy wygenerowane zostanie zdarzenie ”Węzeł nie odpowiada”), na usługach sieciowych monitorowanych na każdym takim węźle

nie zostaną wygenerowane żadne dodatkowe zdarzenia związane ze stanem usługi sieciowej (czyli mające treść "Usługa sieciowa nie odpowiada").

Uwaga

Aby ustawić tę opcję, należy otworzyć – dla dowolnej ilości zaznaczonych węzłów – okno ***Monitorowanie****, kliknąć kartę* ***Zaawansowane****, a następnie zaznaczyć pole wyboru* ***Wstrzymuj zdarzenia z podrzędnych węzłów****.*

Krok 3: Tworzenie wyjątków od reguły wstrzymywania zdarzeń związanych z usługami

W tym momencie interesuje nas otrzymywanie powiadomień w momencie, gdy jeden z serwerów webowych nie odpowiada i w rezultacie monitorowana na nich usługa HTTP jest niedostępna. Ponieważ zdarzenia dotyczące stanu usług sieciowych („Usługa sieciowa nie odpowiada") są wstrzymywane na serwerach webowych A i B (co zostało ustawione w poprzednim kroku), należy teraz utworzyć wyjątek od wstrzymywania zdarzeń związanych z usługami na działającej na tych dwóch węzłach usłudze HTTP.

Uwaga

Aby utworzyć wyjątek od wstrzymywania zdarzeń związanych z usługą dla określonej monitorowanej usługi sieciowej na węźle, należy otworzyć stosowne dla węzła okno ***Monitorowanie****, kliknąć kartę* ***Usługi sieciowe****, a następnie zaznaczyć interesującą nas usługę sieciową i kliknąć ikonę* **Właściwości**. *W oknie* ***Właściwości usługi*** *należy zaznaczyć pole wyboru* ***Wyklucz wstrzymywanie zdarzeń na usługach sieciowych****.*

Zakończenie

W ten sposób wykonanie trzech powyższych czynności pozwoliło nam na zdefiniowanie w programie następujących procedur:

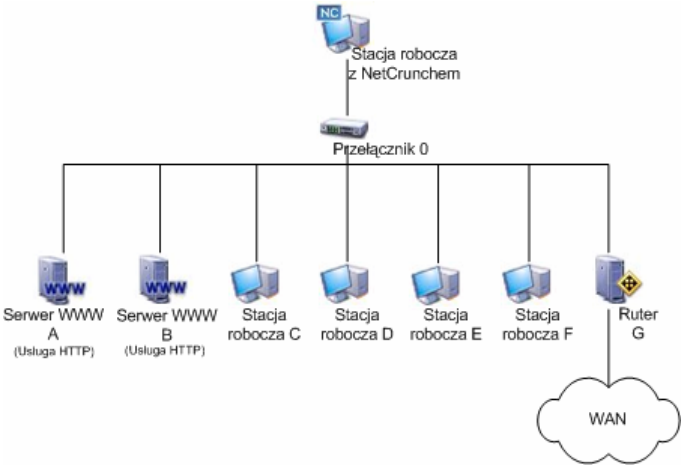
- Gdy dowolny węzeł podpięty do przełącznika 0 będzie wyłączany przez regułę zależności (za wyjątkiem stacji roboczej z NetCrunchem), dla każdego z nich będzie generowane jedynie zdarzenie o treści „Węzeł nie odpowiada" (czyli dla każdej usługi sieciowej działającej na pojedynczym węźle nie będą generowane żadne dodatkowe zdarzenia o treści „Usługa sieciowa nie odpowiada").
- Wyjątkiem od tej reguły są dwa serwery webowe (A i B). Gdy którykolwiek z nich zostanie wyłączony na mocy reguły zależności, poza zdarzeniem „Węzeł nie odpowiada" zostanie także wygenerowane zdarzenie o treści „Usługa HTTP nie odpowiada".

W ten sposób zyskujemy gwarancję, że będziemy na bieżąco otrzymywać informacje o niedostępności krytycznej usługi HTTP na serwerach webowych (także spowodowanej regułą zależności), jednocześnie wstrzymując inne zdarzenia dotyczące stanu usług sieciowych na wszystkich węzłach podpiętych do przełącznika 0.

Przykład 4

Podsumowując, zagadnienia opisane w dwóch powyższych sekcjach mogą znaleźć wspólne zastosowanie. Można więc używać wstrzymywania zdarzeń przy użyciu zależności sieciowych razem ze wstrzymywaniem zdarzeń związanych z usługami sieciowymi na węzłach

sieciowych. Taki wariant zostanie zaprezentowany w poniższej sekcji na przykładzie takiej samej sieci, jak w ostatniej sekcji niniejszego rozdziału.



Rys. 25 Przykładowa sieć

Załóżmy, że domyślnie dla całej sieci włączone zostaje wstrzymywanie zdarzeń z węzłów podrzędnych. Ponadto na węzłach krytycznych (dwóch serwerach webowych i ruterze) zostaje zdefiniowany wyjątek od reguły wstrzymywania zdarzeń, jeśli węzeł nadrzędny w stosunku do nich (przełącznik lub stacja robocza z NetCrunchem) przestaje odpowiadać. Na ruterze ustawione jest także otrzymywanie tylko zdarzeń o treści „Węzeł nie odpowiada", pomijając zdarzenia „Usługa nie odpowiada" wywoływane w momencie awarii węzła nadrzędnego (czyli wyłączanie rutera przez regułę zależności). Ponadto na dwóch serwerach webowych włączone jest otrzymywanie nie tylko zdarzeń o treści „Węzeł nie odpowiada", lecz także zdarzenia „Usługa nie odpowiada" dla krytycznej usługi sieciowej HTTP, w momencie gdy dowolny z tych węzłów zostaje wyłączony przez regułę zależności.

A zatem gdy przełącznik lub stacja robocza z NetCrunchem z jakiegokolwiek powodu przestaje odpowiadać, na mocy reguły zależności wszystkie zależne od nich węzły zostaną automatycznie wyłączone. Wówczas program będzie generował zdarzenia „Węzeł nie odpowiada" tylko dla krytycznych urządzeń infrastruktury sieciowej (czyli dla obu serwerów webowych i rutera), oraz zdarzenie „Usługa nie odpowiada" tylko dla krytycznej usługi sieciowej HTTP na obu serwerach webowych. W przypadku czterech pozostałych stacji roboczych wstrzymywane będą zdarzenia o treści „Węzeł nie odpowiada" i „Usługa nie odpowiada". Innymi słowy, gdy przełącznik lub stacja robocza z NetCrunchem przestaje odpowiadać, będziemy dodatkowo dowiadywać się, że oba serwery webowe oraz ruter są w danym momencie wyłączone na mocy reguły zależności oraz że usługa HTTP na tych serwerach także nie odpowiada.

Ogólna zasada postępowania powinna wyglądać następująco:

- **Krok 1:** ustaw odpowiednie zależności sieciowe na wszystkich węzłach sieciowych; przełącznik jest zależny od stacji roboczej z NetCrunchem, a wszystkie pozostałe węzły są zależne od przełącznika.

- **Krok 2:** włącz wstrzymywanie zdarzeń z węzłów zależnych (na wszystkich poziomach zależności); ustawienie to powinno zostać włączone na stacji roboczej z NetCrunchem oraz przełączniku.
- **Krok 3:** zdefiniuj wyjątki od reguły wstrzymywania zdarzeń dla krytycznych urządzeń infrastruktury sieciowej (czyli dla przełącznika oraz dwóch serwerów webowych) tak, aby zdarzenia związane ze stanem usług i węzłów były na nich zawsze generowane w momencie awarii węzła, od którego są zależne.
- **Krok 4:** włącz wstrzymywanie zdarzeń związanych z usługami na wszystkich urządzeniach infrastruktury sieciowej (czyli na przełączniku oraz dwóch serwerach webowych) tak, aby nie były generowane żadne zdarzenia związane ze stanem usług w momencie, gdy dany węzeł zostaje wyłączony przez regułę zależności.
- **Krok 5:** zdefiniuj wyjątki od reguły wstrzymywania zdarzeń związanych z usługą HTTP działającą na dwóch serwerach webowych (tak, aby w momencie wyłączenia serwerów webowych przez regułę zależności zawsze generowane było zdarzenie dotyczące usługi HTTP o treści "Usługa nie odpowiada".

Dostosowywanie programu NetCrunch

Zarządzanie powiadamianiem użytkowników i grup

W programie możliwe jest określenie ustawień profilów użytkowników i grup. Jest to dość istotna czynność, gdyż profile znajdują zastosowanie w następujących obszarach:

- **Dostęp przez WWW** – profil użytkownika służy do określania jego nazwy i hasła, wykorzystywanych podczas logowania w programie NetCrunch za pomocą przeglądarki WWW.
- **Alertowanie** – profil użytkownika służy do oznaczenia użytkownika lub grupy w celu szybkiego określenia rodzaju akcji powiadamiającej, podejmowanej w ramach alertowania. W profilu użytkownika lub grupy ustalana jest metoda powiadamiania, wymagane przez nią parametry oraz czas, w jakim takie powiadamianie ma następować (lub związane z tym przedziały czasowe).
- **Raportowanie** – profil użytkownika stwarza możliwość szybkiego wybrania użytkownika lub grupy, usprawniając w ten sposób przesyłanie wygenerowanych raportów. W profilu użytkownika lub grupy musi być zapisana metoda wysyłania wyników za pomocą poczty e-mail oraz wszelkie przedziały czasowe.

Aby określić lub zmienić ustawienia powiadamiania użytkowników lub grup

1. Na głównym pasku narzędzi kliknij ikonę ***Profile użytkowników***.
   Spowoduje to otwarcie okna **Ustawienia użytkowników i grup** z listą aktualnie zdefiniowanych użytkowników i grup.




2. Wybierz użytkownika lub grupę, których ustawienia chcesz zmienić, a następnie kliknij ikonę ***Edytuj*** i wprowadź w tak otwartym oknie odpowiednie zmiany.
   Aby dodać nowego użytkownika, kliknij ikonę ***Nowy użytkownik***, a następnie w tak otwartym oknie określ profil powiadamiania lub dostępu przez WWW.
   Aby dodać nową grupę, kliknij ikonę ***Nowa grupa***, a następnie w tak otwartym oknie wskaż nowych członków, którzy mają należeć do danej grupy.
   Aby usunąć użytkownika lub grupę, zaznacz dany element, a następnie kliknij ikonę ***Usuń***.

Uwagi

- *Możliwe jest dodawanie, usuwanie lub modyfikowanie właściwości profili grup i użytkowników. Grupy służą do przechowywania dowolnej ilości zdefiniowanych użytkowników.*
- *Istnieje opcja sprawdzania statusu połączenia dowolnych użytkowników zdalnego dostępu, a nawet rozłączania ich. Por. sekcję* Zarządzanie użytkownikami zdalnego dostępu *na stronie 194 w celu uzyskania szczegółowych informacji.*

Zarządzanie profilami SNMP

Profile SNMP przechowują ustawienia związane z upoważnieniami do oglądania i modyfikowania informacji na węzłach za pośrednictwem protokołu SNMP. Z reguły profil SNMP zawiera następujące informacje (czyli indywidualne ustawienia dotyczące odczytu i zapisu danych przy użyciu SNMP):

- Stosowana wersja standardu SNMP (SNMPv1, SNMPv2c, lub SNMPv3).
- Wspólnota odczytu i zapisu SNMP (dotyczy jedynie wersji SNMPv1 i SNMPv2c).
- Opcje mechanizmu uwierzytelnienia: brak uwierzytelnienia, uwierzytelnienie, uwierzytelnienie z szyfrowaniem danych (dotyczy wyłącznie SNMPv3).
- Nazwa i hasło użytkownika uwierzytelnienia, protokół uwierzytelnienia, hasło szyfrowania (wszystkie powyższe dotyczą wyłącznie SNMPv3) – w zależności o tego, jakie opcje zostały wybrane w poprzednich punktach.

Zdefiniowany w ten sposób profil SNMP może wówczas być stosowany pojedynczo dla każdego węzła z agentem SNMP. Por. sekcję *Właściwości zarządzania poprzez agenta SNMP* na stronie 143 w celu uzyskania dodatkowych informacji. Ponadto w opcjach programu można określić domyślny profil SNMP dla wszystkich nowo wykrywanych w atlasie, lub dodawanych do atlasu ręcznie, węzłów. Por. sekcję *Ustawianie domyślnych właściwości monitorowania oraz zarządzania przez SNMP* na stronie 203 w celu uzyskania dodatkowych informacji.

Aby ustawić/zmodyfikować profil SNMP

1. W menu **Atlas** wskaż pozycję **Profile** i wybierz opcję **SNMP**.
   Otworzy się okno **Profile SNMP**.



2. Aby dodać nowy profil SNMP, kliknij ikonę ***Dodaj nowy***, a następnie w oknie **Właściwości profilu SNMP** określ dane profilu SNMP.
   Aby zmodyfikować istniejący profil SNMP, wybierz go z listy i kliknij ikonę ***Edytuj***. W oknie **Właściwości profilu SNMP** dokonaj stosownych zmian.
   Aby usunąć istniejący profil SNMP, wybierz go z listy i kliknij ikonę ***Usuń***. Następnie w oknie dialogowym kliknij **Tak**.

Uwagi

- *Domyślnie NetCrunch oferuje dwa predefiniowane profile SNMP o nazwie* ***Default (read only)*** *i* ***Default (read-write)****. Oba są związane z wersją 1 protokołu SNMP i używają odpowiednio wspólnoty* ***public*** *i* ***private*** *we właściwościach odczytu i zapisu SNMP.*
- *Możliwe jest także tworzenie, edytowanie lub usuwanie profili SNMP bezpośrednio we właściwościach SNMP dowolnego węzła lub w opcjach programu. Jednakże przy dokonywanej w ten sposób edycji lub usuwaniu profilu SNMP, profil SNMP węzła zostanie automatycznie ustawiony jako "'Własny". Aby globalnie zmodyfikować lub usunąć profil SNMP używany na węzłach atlasu, sugerowane jest korzystanie bezpośrednio z okna* ***Profile SNMP*** *zgodnie ze wskazówkami zawartymi w niniejszej sekcji.*

Menedżer wstrzymywania zdarzeń

Odpowiednia parametryzacja mechanizmu wstrzymywania zdarzeń na węzłach sieciowych wymaga posiadania jasno sprecyzowanej strategii monitorowania. Procedurę tą w znaczny stopniu ułatwia **Menedżer wstrzymywania zdarzeń** umożliwiający graficzną prezentację oraz sprawne zarządzanie wstrzymywaniem zdarzeń z jednego okna. Menedżer wstrzymywania zdarzeń wyświetla wszystkie zależności sieciowe, a także wszystkie trzy z czterech istniejących ustawień wstrzymywania (czwarte ustawienie jest definiowane we właściwościach usługi sieciowej). Każde z powyższych trzech ustawień jest prezentowane w osobnej tabelarycznej kolumnie. Ponadto można modyfikować owe ustawienia dla węzła na liście. Por. sekcję *Modyfikowanie ustawień wstrzymywania zdarzeń* na stronie 239 w celu uzyskania dodatkowych informacji.

Uwaga

***Menedżer wstrzymywania zdarzeń** jest dostępny wyłącznie w edycji Premium XE programu.*

Otwieranie Menedżera wstrzymywania zdarzeń

Po otworzeniu Menedżera wstrzymywania zdarzeń można natychmiast przeglądać relacje między poszczególnymi węzłami i zachodzące między nimi związki zależności. Co więcej w przypadku każdego wyszczególnionego na liście węzła można stwierdzić, czy jest włączone jakiekolwiek z trzech ustawień wstrzymywania zdarzeń (zielona ikona zaznaczenia wskazuje, że dane ustawienie jest włączone).

Aby otworzyć Menedżera wstrzymywania zdarzeń

1. W menu **Atlas** wskaż **Monitorowanie** i wybierz opcję **Menedżer wstrzymywania zdarzeń**.
   Wyświetli się okno **Zależności sieciowe** z wybraną kartą **Menedżer wstrzymywania zdarzeń**.

Uwaga

*W razie potrzeby modyfikacji zależności monitorowania między węzłami należy kliknąć kartę **Zależności monitorowania** i dokonać stosownych zmian. Aby powrócić do Menedżera wstrzymywania zdarzeń, należy kliknąć kartę **Menedżer wstrzymywania zdarzeń**.*

Modyfikowanie ustawień wstrzymywania zdarzeń dla węzłów

Modyfikowanie ustawień wstrzymywania zdarzeń zdefiniowanych dla konkretnego węzła odbywa się w oknie **Właściwości wstrzymywania**. Po dokonaniu zmian lista węzła w Menedżerze wstrzymywania zdarzeń będzie wyświetlać włączone ustawienia wstrzymywania dla danego węzła (w razie włączenia prezentowana będzie zielona ikona zaznaczenia, w przypadku niedostępności tej opcji ikona ta będzie oznaczona kolorem szarym, natomiast brak powyższej ikony wskazuje na wyłączenie opcji).

Aby zmodyfikować ustawienia wstrzymywania zdarzeń na węźle

1. Otwórz Menedżera wstrzymywania zdarzeń.
   Wyświetli się okno **Zależności sieciowe** z wybraną kartą **Menedżer wstrzymywania zdarzeń**.
2. Na liście zależności sieciowych kliknij dwa razy dany węzeł (może zaistnieć potrzeba przewinięcia listy w dół).
   Otworzy się okno **Właściwości wstrzymywania**.
3. Aby ustawić wstrzymywanie zdarzeń związanych z usługami na węźle („Usługa nie odpowiada") wywoływanych niedostępnością węzła z jakiejkolwiek przyczyny, zaznacz pole wyboru **Wstrzymuj zdarzenia związane z usługami węzła**.
4. Aby ustawić wstrzymywanie zdarzeń z węzłów zależnych w momencie spowodowanej dowolną przyczyną niedostępnością węzła, zaznacz pole wyboru **Wstrzymuj zdarzenia z podrzędnych węzłów**.
5. Aby utworzyć wyjątek od reguły wstrzymywania (zdefiniowanej na węźle nadrzędnym w stosunku do danego węzła), zaznacz pole wyboru **Wyklucz z mechanizmu wstrzymywania zdarzeń**.

Uwagi

- *Nie wszystkie z trzech powyższych pól wyboru mogą być dostępne na danym węźle; przykładowo zależy to od tego, czy ów węzeł posiada co najmniej jeden zależny od siebie węzeł oraz od tego, czy na węźle nadrzędnym w stosunku do tego węzła włączone zostało wstrzymywanie zdarzeń z węzłów zależnych.*
- *Aby uzyskać więcej informacji na temat opcji opisanych w krokach 3-5, por. także sekcje* Wstrzymywanie zdarzeń związanych ze stanem usług sieciowych *na stronie 161,* Wstrzymywanie zdarzeń z węzłów podrzędnych *na stronie 161, oraz* Tworzenie wyjątków od wstrzymywania zdarzeń *na stronie 163.*
- *Aby uzyskać więcej informacji na temat zastosowanego w programie zaawansowanego mechanizmu wstrzymywania zdarzeń, por. sekcję* Koncepcje zaawansowanego monitorowania węzłów *na stronie 217.*

Konfigurowanie menu Narzędzia dla węzła

Po kliknięciu węzła prawym przyciskiem myszy pojawia się menu podręczne, za pomocą którego przeprowadzane mogą być różnego rodzaju standardowe operacje, związane ze stanem węzła, monitorowaniem, usługą sieciową SNMP, alertowaniem, raportowaniem, zmianą właściwości węzła czy zastosowaniem dodatkowych narzędzi.

Za pomocą dodatkowego menu narzędzi (wyświetlanego po wybraniu z menu podręcznego polecenia **Narzędzia**) można uruchomić kilka przydatnych funkcji narzędziowych udostępnianych w oddzielnym programie **Narzędzia IP i SNMP** (takich jak Ping, Traceroute, Lookup itp.), a także pewną liczbę wybranych przez użytkownika poleceń związanych z węzłem (takich jak na przykład otwarcie standardowej przeglądarki WWW z adresem IP danego węzła).

Innymi słowy, użytkownik ma możliwość skonfigurowania menu narzędzi tak, aby zawierało ono dowolną liczbę poleceń uruchamianych dla określonego węzła (będą one wyszczególnione jako oddzielne pozycje menu). Ponadto ma on możliwość zadecydowania, czy każda z pozycji menu ma być dodawana do menu wszystkich węzłów, menu wybranego węzła lub tylko do menu określonego rodzaju węzłów (takich jak na przykład węzły Windows, Unix, NetWare lub routery).

Konfigurowanie pozycji w menu narzędzi jest bardzo proste. Należy w tym celu kliknąć prawym przyciskiem myszy dowolny węzeł na mapie, w menu podręcznym wskazać pozycję **Narzędzia**, a następnie wybrać polecenie **Konfiguruj narzędzia**. Spowoduje to wyświetlenie okna **Konfiguruj narzędzia**, za pomocą którego można dodawać nowe, względnie usuwać lub zmieniać istniejące pozycje menu.

W oknie **Konfiguruj narzędzia** można przeprowadzać następujące operacje:

- dodawać nową pozycję menu do wyświetlanej listy,
- dodawać nowy separator do wyświetlanej listy,
- usuwać pozycję menu z wyświetlanej listy,
- zmieniać właściwości dowolnej wcześniej określonej pozycji menu,
- przenosić pozycję menu w górę lub w dół wyświetlanej listy.

Uwaga

*Standardowe pozycje menu, odpowiadające wszystkim tym narzędziom, które dostępne są w samodzielnym programie **Narzędzia IP i SNMP** (takim jak Ping, Traceroute, Lookup itp.), nie mogą zostać usunięte. Można je jedynie przenosić w górę lub w dół listy.*

Dodawanie nowej pozycji menu

Możliwość zdefiniowania nowego rodzaju poleceń, które mogą być uruchamiane po kliknięciu węzła prawym przyciskiem myszy i wybraniu z menu podręcznego pozycji **Narzędzia**, może się okazać niezwykle pożyteczna. W praktyce dowolne nowe polecenie tego rodzaju może zostać w łatwy sposób dodane jako nowa pozycja w podręcznym menu narzędzi związanych z danym węzłem.

Aby dodać nowe polecenie jako pozycję menu

1. W oknie **Widok sieci** kliknij prawym przyciskiem myszy wybrany węzeł, w menu podręcznym wskaż pozycję **Narzędzia**, a następnie wybierz polecenie **Konfiguruj narzędzia**.
   Spowoduje to pojawienie się okna **Konfiguruj narzędzia** z listą aktualnie określonych pozycji menu wyświetlaną dokładnie w takiej kolejności, w jakiej pozycje te występują w odpowiednim menu podręcznym (stanowiącym podmenu polecenia **Narzędzia**).
2. Kliknij ikonę ***Dodaj nowy***.
   Spowoduje to wyświetlenie okna **Właściwości menu**.
3. W polu **Nazwa** wpisz nazwę polecenia, która ma się pojawiać jako nowa pozycja menu.

4. W polu **Polecenie** wpisz nazwę programu, który ma być uruchamiany po kliknięciu nowo tworzonej pozycji menu. Być może konieczne będzie także określenie ścieżki tego programu.
5. W polu **Argumenty** wpisz wszelkie argumenty, jakie mają być przekazane do wywoływanego polecenia. Jeżeli w polu tym wpisujesz więcej niż jeden argument, oddziel każdy z nich spacją.
6. W dolnej części okna wybierz przycisk opcji określający miejsca w programie, w których ta nowa pozycja menu ma się pojawiać (możesz ją dodać do wszystkich węzłów, wyłącznie do wybranego węzła lub do węzłów określonego rodzaju – Windows, Unix, NetWare lub do węzła będącego ruterem).

Uwaga

- *W punkcie 4. można kliknąć ikonę* **Przeglądaj**, *a następnie w otwartym oknie* ***Przeglądaj*** *znaleźć dokładną ścieżkę oraz nazwę pliku, który ma być uruchamiany w wyniku wybrania danego polecenia. Po wybraniu nazwy programu należy kliknąć przycisk* ***Otwórz****, aby zamknąć okno* ***Przeglądaj****. W polu* ***Polecenie*** *widoczna będzie teraz pełna nazwa programu wraz z jego ścieżką.*

- *Klikając specjalną ikonę* **Wybierz argument**, *można również dodać jeden z następujących argumentów:* Nazwa urządzenia, Adres IP, Nazwa urządzenia SNMP, Nazwa NetBIOS *dla danego węzła*, Info1, Info2, Stan, Wspólnota odczytu/zapisu, Rodzaj, Identyfikacja oraz Adres sprzętowy.

Dodawanie separatora pozycji menu

W dowolnym miejscu podmenu **Narzędzia** możliwe jest umieszczanie odpowiednich separatorów, porządkujących aktualnie istniejące lub nowo dodawane pozycje tego menu. Jest to szczególnie przydatne w sytuacji, gdy chcemy, aby pewne polecenia (np. standardowe narzędzia programu **Narzędzia IP i SNMP**) były zgrupowane razem i oddzielone od pozostałych rodzajów poleceń dostępnych w podmenu **Narzędzia**.

Aby dodać nowy separator pozycji menu

1. W oknie **Widok sieci** kliknij prawym przyciskiem myszy wybrany węzeł, w menu podręcznym wskaż pozycję **Narzędzia**, a następnie wybierz polecenie **Konfiguruj narzędzia**.
   Spowoduje to pojawienie się okna **Konfiguruj narzędzia**, a w nim aktualnej listy pozycji menu dla wybranego węzła.

2. Kliknij ikonę ***Nowy separator***, aby dodać do listy nowy separator pozycji menu. Zostanie on automatycznie umieszczony na dole listy.

3. Korzystając z ikon **Przenieś w górę** lub **Przenieś w dół**, przenieś nowo dodany separator w wybrane miejsce na liście pozycji menu.

Usuwanie pozycji menu

Polecenia lub separatory, które zostały dodane do listy pozycji menu **Narzędzia**, mogą zostać w łatwy sposób usunięte. Jednakże nie jest możliwe usunięcie poleceń związanych ze standardowymi narzędziami sieciowymi, dostępnymi w programie **Narzędzia IP i SNMP** (Ping, Traceroute, Lookup itp.).

Aby usunąć pozycję menu stanowiącą polecenie lub separator

1. Kliknij wybrany węzeł prawym przyciskiem myszy, w menu podręcznym wskaż pozycję **Narzędzia**, a następnie wybierz polecenie **Konfiguruj narzędzia**.

   Spowoduje to pojawienie się okna **Konfiguruj narzędzia**, z aktualną listą pozycji menu wyświetlaną dokładnie w takiej kolejności, w jakiej pozycje te występują w odpowiednim menu podręcznym, stanowiącym podmenu polecenia **Narzędzia**.

2. Na liście pozycji menu zaznacz polecenie lub separator, który chcesz usunąć.

3. Kliknij ikonę ***Usuń***, aby z listy pozycji menu usunąć zaznaczone polecenie lub separator.

Uwaga

Po kliknięciu danego węzła prawym przyciskiem myszy i wybraniu z menu podręcznego polecenia ***Narzędzia*** *wyświetlona zostanie lista, na której już nie pojawi się usunięte przed chwilą polecenie czy separator.*

Udoskonalona identyfikacja urządzeń sieciowych

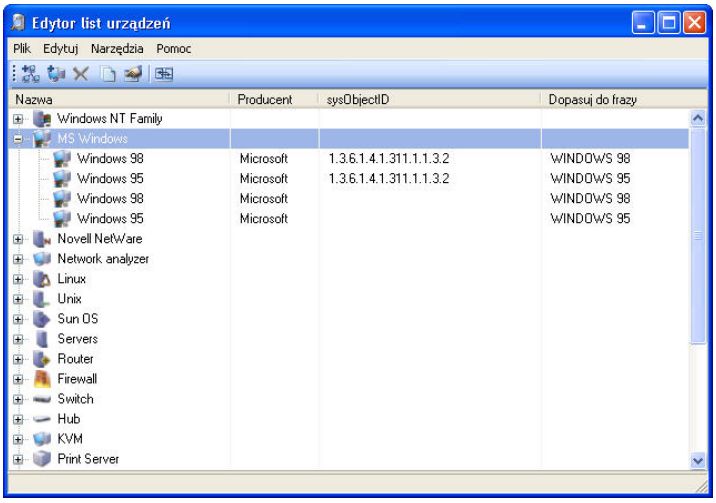
Gdy program przeprowadza skanowanie określonej sieci w poszukiwaniu węzłów, równocześnie automatycznie identyfikuje on rodzaj wykrytych węzłów (za pomocą usługi SNMP) i przypisuje każdemu z nich jedną z domyślnych ikon. Wszystkie dostępne ikony widoczne są na liście w oknie **Opcje**, po wybraniu strony **Mapa – Ikony**.

NetCrunch rozpoznaje różnego rodzaju urządzenia na podstawie zmiennych sysObjectID oraz sysDescr, wykorzystywanych przez protokół SNMP. Oba rodzaje zmiennych MIB są odpowiedzialne za identyfikację urządzenia w sieci. Mogą one posłużyć do udoskonalenia procesu prawidłowego rozpoznawania ikon dla urządzeń o podobnym charakterze.

Lista aktualnie rozpoznawanych urządzeń zapisana jest w programie NetCrunch w specjalnym pliku o nazwie `devices.xml`, umieszczonym w katalogu, w którym zainstalowany został sam program. W praktyce do wprowadzania zmian w tym pliku można wykorzystać samodzielny program **Edytor listy urządzeń**, wchodzący w skład pakietu NetCrunch. Do listy takiej może również zostać dodana definicja całkowicie nowego urządzenia.

Korzystanie z Edytora listy urządzeń

Aby przejść do programu **Edytor listy urządzeń**, należy bezpośrednio z menu **Narzędzia** wybrać polecenie **Edytor listy urządzeń**. Okno programu wygląda podobnie do tego, jakie zostało przedstawione na rysunku poniżej.



Rys. 26 Edytor listy urządzeń

W przejrzystej, podzielonej na sekcje tabeli wyświetlana jest lista wszystkich urządzeń sieciowych aktualnie rozpoznanych przez NetCruncha. Poszczególne sekcje, zwane także grupami urządzeń, mogą zostać rozwinięte poprzez kliknięcie znaku „+", umieszczonego się przy ich nazwie. W wyniku tego pod nazwą danej grupy pojawi się natychmiast lista należących do niej zdefiniowanych urządzeń sieciowych. Każde urządzenie wyświetlane w tabeli opisane może być za pomocą następujących informacji:

- **Ikona** – określa ikonę, która ma reprezentować dane urządzenie w programie NetCrunch. Ikona o tej nazwie i o odpowiedniej treści graficznej musi być bezpośrednio związana z jedną z ikon zdefiniowanych na liście w oknie **Opcje** (na stronie **Mapa – Ikony**). Podczas skanowania sieci, gdy na podstawie wartości identyfikatora sysObjectID program NetCrunch rozpozna dane urządzenie, wówczas do wyświetlenia takiego urządzenia w oknie **Widok sieci** zastosuje określoną w tym miejscu ikonę.
- **Nazwa** – określa nazwę urządzenia. Innymi słowy, jest to nazwa, która w programie będzie kojarzona z danym urządzeniem.
- **Producent** – określa nazwę firmy produkującej dane urządzenie. Pole to jest wygodne, gdyż pozwala grupować urządzenia wytwarzane przez różnych producentów, ułatwiając ich rozróżnianie.
- **sysObjectID** – dla danego urządzenia określa identyfikator obiektu w bazie MIB (na podstawie unikatowej wartości sysObjectID). Jest to praktycznie najważniejsze z pól. Jeżeli zostanie w nim wpisana nieprawidłowa wartość, podczas przeprowadzania procesu skanowania NetCrunch nie będzie w stanie ani wykryć i rozpoznać danego urządzenia, ani umieścić na mapie w oknie **Widok sieci** odpowiadającej mu ikony.
- **Tekst wzorcowy** – podaje krótką informację związaną z danym urządzeniem, określoną na podstawie wartości parametru sysDescr. Niektóre urządzenia mogą być rozpoznawane przez program jedynie na podstawie wartości ich parametru sysDescr, a nie na podstawie identyfikatora sysObjectID.

Aby dodać nowe urządzenie lub grupę

1. Z menu **Edycja** wybierz polecenie **Dodaj urządzenie** lub **Dodaj grupę**, względnie kliknij odpowiednią ikonę na pasku narzędzi.
2. W przypadku dodawania nowej grupy wpisz w oknie **Dodaj nową grupę urządzeń** jej nazwę, a z listy rozwijanej **Ikona** wybierz ikonę, która będzie reprezentować tę grupę. W przypadku dodawania nowego urządzenia wpisz w oknie **Dodaj nowe urządzenie** jego nazwę, producenta oraz identyfikator sysObjectID lub tekst wzorcowy (względnie oba te parametry). Przejdź do listy rozwijanej **Ikona** i wybierz ikonę, która ma reprezentować dane urządzenie.
3. Kliknij przycisk **OK**.
   Nowe urządzenie lub grupa zostaną natychmiast wyświetlone w tabeli **Edytora listy urządzeń**.
4. Przeciągnij i upuść nowo utworzone urządzenie lub grupę w dowolnie wybranym miejscu wyświetlanej listy.
5. Aby zapisać wprowadzone zmiany, z menu **Plik** wybierz polecenie **Zapisz**.

Uwagi

- *Jeżeli w punkcie 2. znalezienie stosownej ikony dla grupy lub urządzenia nie jest możliwe, konieczne jest zdefiniowanie – na odpowiedniej liście w programie – nowej ikony. Jest to możliwe w oknie **Opcje** poprzez wybór strony **Mapa – Ikony**.*
- *Chcąc w punkcie 5. anulować zmiany, które zostały już wprowadzone w punktach 1-4, należy z menu **Plik** wybrać polecenie **Cofnij**.*
- *Aby w późniejszym czasie zmienić właściwości zdefiniowanej uprzednio grupy lub urządzenia (jego nazwę, producenta, identyfikator sysObjectID, tekst wzorcowy lub ikonę), należy zaznaczyć dany element w wyświetlanej tabeli, a następnie z menu **Edycja** wybrać polecenie **Właściwości**. W przypadku ikon zdefiniowanych przez użytkownika zmieniana może być zawartość wszystkich pól. W przypadku ikon związanych z urządzeniami standardowymi (takimi, które są już zdefiniowane w programie w chwili jego instalacji) zmieniany może być tylko rodzaj ikony.*
- *Aby szybko odszukać w tabeli definicję grupy lub urządzenia, należy z menu **Edycja** wybrać polecenie **Znajdź**, a następnie, w otwartym w ten sposób oknie, wpisać te parametry, według których ma być przeprowadzone poszukiwanie.*
- *Po dodaniu nowej grupy lub urządzenia, względnie po przeprowadzeniu ich edycji lub po ich usunięciu, odpowiednie zmiany zostaną automatycznie zapisane w pliku `devices.xml`. Jednakże taki zmieniony plik zostanie zapisany w podkatalogu `../data` w katalogu, w którym zainstalowany został NetCrunch. Będzie on dostępny dla wszystkich atlasów, które zostały zdefiniowane przez użytkownika i które będą otwierane w programie. Oryginalna wersja pliku (z chwili instalacji programu) pozostanie niezmieniona i będzie dostępna w głównym katalogu, w którym zainstalowany został NetCrunch.*

Automatyczna aktualizacja pliku DEVICES.XML

Program **Edytor listy urządzeń** pozwala użytkownikowi w łatwy sposób pobierać zaktualizowaną listę urządzeń bezpośrednio z witryny WWW firmy AdRem Software. Lista taka będzie okresowo aktualizowana przez firmę AdRem Software na podstawie informacji otrzymywanych od klientów, a następnie udostępniana w nowej wersji. Każdy użytkownik może także przesyłać do firmy AdRem utworzone przez siebie definicje, tak aby inni

użytkownicy programu NetCrunch mogli w ten sposób aktualizować swoje listy. Obie te czynności przeprowadzane są bezpośrednio w programie **Edytor listy urządzeń**, poprzez wybranie z menu **Narzędzia** polecenia **Uaktualnij** (lub kliknięcie odpowiedniej ikony na pasku narzędzi). Następnie wystarczy postępować zgodnie ze wskazówkami podawanymi w kreatorze *Aktualizacja listy urządzeń*.

Dodawanie nowej definicji urządzenia

W NetCrunchu można w łatwy sposób dodać całkowicie nową definicję urządzenia, tak aby program mógł prawidłowo rozpoznawać dany rodzaj urządzenia (wraz z odpowiadającą mu ikoną) i przeprowadzać wykrywanie sieci, monitorowanie, alertowanie i raportowanie. Do tego celu służy specjalny kreator. Definicja nowego urządzenia może być utworzona w oparciu o już istniejący węzeł lub utworzona od podstaw. W pierwszym przypadku nowa definicja zostanie automatycznie zastosowana do tego węzła, który został wybrany jako wzorzec przy jej tworzeniu. W drugim przypadku konieczne jest wypełnienie pola sysObjectID lub sysDescr, względnie obu tych pól, a także skojarzenie z danym urządzeniem pewnej już istniejącej ikony lub utworzenie nowej i dodanie jej do listy ikon.

Aby dodać nową definicję urządzenia

1. W menu **Narzędzia** wskaż pozycję **Zadania**, a następnie wybierz polecenie **Dodaj definicję nowego urządzenia**.
   Wyświetlone zostanie okno kreatora *Definicja nowego urządzenia*.
2. Jeżeli planujesz utworzyć definicję nowego urządzenia na podstawie już istniejącego węzła, kliknij ikonę ***Wybierz węzeł***, a następnie, w otwartym w ten sposób oknie, wybierz żądany węzeł.
   Jeżeli planujesz utworzyć definicję nowego urządzenia od podstaw, pomiń ten punkt.
3. Kliknij przycisk **Dalej**.
4. Jeżeli to konieczne, zmień odpowiednio parametry identyfikacyjne nowego urządzenia (pola sysObjectID lub sysDescr, lub oba z nich).
5. Kliknij przycisk **Dalej**.
6. Z wyświetlanej listy wybierz dla nowo definiowanego urządzenia jedną z już istniejących ikon.
7. Kliknij przycisk **OK**.

Uwagi

- *Jeżeli definicja nowego urządzenia ma być utworzona na podstawie już istniejącego węzła, możliwe jest przyspieszenie tego procesu. W tym celu należy dla takiego węzła otworzyć okno* ***Właściwości*** *(wystarczy wybrać z jego menu podręcznego polecenie* ***Właściwości****), a następnie kliknąć ikonę* **Dodaj**, *znajdującą się na lewo od listy rozwijanej* ***Rodzaj****. Spowoduje to wyświetlenie okna kreatora* Definicja nowego urządzenia, *a w jego polu* ***Węzeł odniesienia*** *wpisane będą automatycznie dane identyfikujące wcześniej wybrany węzeł. Teraz należy przejść bezpośrednio do punktu 3.*
- *Jeżeli w punkcie 6. nie zostanie znaleziona odpowiednia ikona, która nadawałaby się do reprezentowania nowego rodzaju urządzenia na liście, należy taką ikonę dodać do listy, klikając ikonę* **Dodaj** *i wybierając odpowiedni plik graficzny z katalogu o podanej ścieżce.*

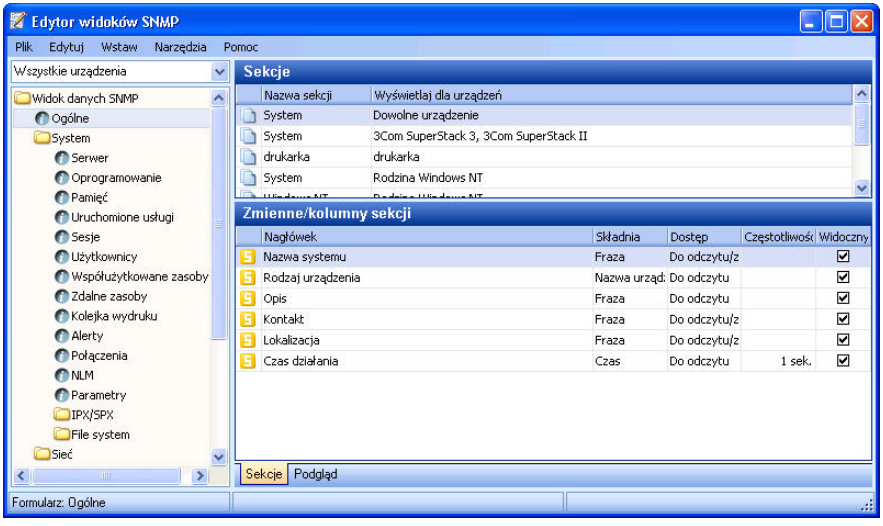
- *Po zakończeniu wszystkich opisanych powyżej czynności nowa definicja urządzenia jest automatycznie dołączana do pliku* `devices.xml`. *Oznacza to, że na tego rodzaju węzłach możliwe jest przeprowadzanie wszystkich operacji programu, takich jak wykrywanie sieci, monitorowanie, alertowanie czy raportowanie. Jeżeli teraz otwarte zostanie okno programu* ***Edytor listy urządzeń****, pojawi się ono pod nową grupą o nazwie* ***Kreator rodzaju urządzenia****. Można je teraz przeciągnąć do którejkolwiek z już istniejących grup i tam upuścić.*

Dostosowywanie widoków SNMP

W programie NetCrunch możliwe jest przeglądanie lub zmiana danych związanych z węzłami za pomocą usługi sieciowej SNMP. W tym celu wystarczy w menu podręcznym danego węzła wskazać pozycję **SNMP**, a następnie wybrać polecenie **Widok**. Do tworzenia swoich własnych, personalizowanych widoków SNMP – obejmujących wszystkie rodzaje węzłów lub dowolnie wybrane ich rodzaje (Windows, NetWare, rutery itp.), względnie do wprowadzenia zmian w widokach już istniejących, można wykorzystać samodzielny program **Edytor widoków SNMP**. Narzędzie to ułatwia dostosowywanie do własnych potrzeb sposobów wyświetlania informacji SNMP o węźle podczas ich przeglądania w programie. Lista aktualnie zdefiniowanych widoków SNMP zapisana jest w NetCrunchu w specjalnym pliku o nazwie snmpview.xml, umieszczonym w katalogu, w którym zainstalowany został sam program.

Korzystanie z Edytora widoków SNMP

Aby przejść do programu **Edytor widoków SNMP**, należy bezpośrednio z menu **Narzędzia** wybrać polecenie **Edytor widoków SNMP**. Okno programu wygląda podobnie do tego, jakie zostało przedstawione na rysunku poniżej.



Rys. 27 Edytor widoków SNMP

W lewej części okna, poniżej menu, wyświetlana jest lista rozwijana **Wybierz widok** służąca do filtrowania informacji SNMP, która ma być przedstawiana na poszczególnych widokach. Dzięki niej możliwe jest wyświetlanie lub edycja widoków SNMP związanych ze wszystkimi urządzeniami lub tylko z określonymi ich rodzajami. Poniżej tej listy rozwijanej przedstawione jest drzewo widoków SNMP. Wyświetlana jest w nim dokładnie taka zawartość, jaka oglądana byłaby podczas korzystania w programie NetCrunch z przeglądarki SNMP (Eksploratora MIB-ów). W drzewie tym widoczne są grupy i formularze. Grupy pełnią rolę folderów i stanowią listę zdefiniowanych wcześniej formularzy. Natomiast zawartość formularza wyświetlana jest wówczas, gdy któryś z nich zostanie wybrany w przeglądarce SNMP. Formularze składają się z różnych sekcji, i mogą mieć albo styl tabeli, albo panelu. W tabeli znajdującej się w prawej górnej części okna wyświetlana jest lista sekcji zdefiniowanych w wybranym formularzu drzewa widoków SNMP. Po wybraniu jednej z takich sekcji w okienku znajdującym się w prawej dolnej części okna wyświetlone zostają wszystkie pola lub kolumny (odpowiednio dla sekcji mającej styl panelu lub tabeli), które są aktualnie zdefiniowane w tej sekcji.

Podczas dodawania do formularza nowej sekcji konieczne jest podanie następujących informacji:

- **Nazwa** – określa nazwę służącą do oznaczenia danej sekcji zarówno w omawianym tutaj programie, jak i podczas przeglądania w programie informacji zapisanych w bazie MIB.
- **Urządzenia** – określa rodzaje urządzeń, dla których dana sekcja ma się pojawiać w przeglądarce SNMP (Eksploratorze MIB-ów). Można zażyczyć sobie, aby dana sekcja pojawiała się dla dowolnego rodzaju urządzeń – wystarczy w tym celu zaznaczyć odpowiednie pole wyboru.
- **Wysokość** – określa, jaką wysokość (w pikselach) będzie miała dana sekcja, gdy będzie ona wyświetlana podczas korzystania z funkcji przeglądania.
- **Styl** – określa, czy sekcja ma mieć styl tabeli, czy panelu. W sekcjach o stylu tabeli dodawana może być dowolna liczba kolumn. W sekcjach o stylu panelu dodawana może być dowolna liczba pól.

Podczas dodawania do sekcji nowej kolumny lub nowego pola (odpowiednio dla stylu tabeli lub panelu), konieczne jest podanie następujących informacji:

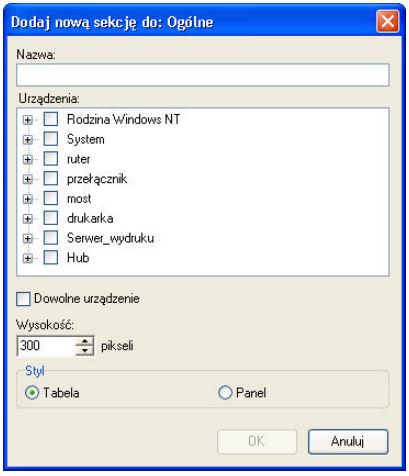
- **Nagłówek** – określa nazwę kolumny lub pola.
- **Składnia** – określa składnię wartości podawanej w danej kolumnie lub w danym polu. Do dyspozycji mamy następujące typy wartości: łańcuch znaków, liczba całkowita (Integer), data i czas, adres fizyczny, nazwa urządzenia lub czas.
- **Czas odświeżania** – określa odstęp czasu (w sekundach), w jakim następować będzie cykliczne odświeżanie wartości podawanej w danej kolumnie lub polu. Jeżeli nie zostanie tutaj wpisana żadna wartość, dana kolumna lub pole nie będą odświeżane.
- **Dostęp** – informuje, czy dana kolumna lub pole jest udostępnione zarówno do odczytu jak i do zapisu, czy też jest przeznaczone tylko do odczytu odpowiedniej wartości.
- **Widoczny** – określa czy dana kolumna lub pole są w określonej sekcji widoczne, czy też nie.

Aby dodać nową grupę lub formularz do drzewa widoków SNMP

1. W lewej części okna wybierz miejsce w drzewie widoków SNMP, w którym wstawiona ma zostać nowa grupa lub nowy formularz.

2. Z menu **Edycja** wybierz polecenie **Dodaj grupę** lub **Dodaj formularz**.
3. W otwartym w ten sposób oknie wpisz nazwę nowo tworzonej grupy lub nowo tworzonego formularza.

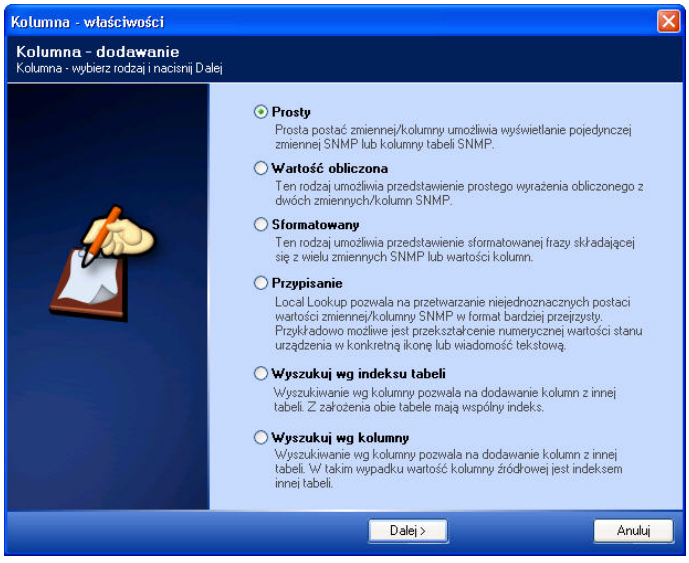
Aby dodać sekcję do formularza



1. W lewej części okna wybierz formularz, do którego chcesz dodać nową sekcję.
2. Z menu **Edycja** wybierz polecenie **Dodaj sekcję**.
3. W oknie **Dodaj nową sekcję do <NAZWA_FORMULARZA>** wpisz nazwę nowej sekcji.
4. Zaznacz rodzaje urządzeń, dla których pojawiać się ma dana sekcja, lub zaznacz pole wyboru **Dowolne urządzenie**, aby była ona widoczna dla wszystkich rodzajów urządzeń.
5. Wybierz styl sekcji – tabela lub panel.
6. W przypadku, gdy wybrany został styl tabeli, wpisz wysokość danej sekcji (w pikselach).

Aby dodać do sekcji nową kolumnę lub nowe pole

1. W prawej górnej części okna wybierz sekcję, do której chcesz dodać nową kolumnę lub nowe pole. Jeżeli nie jest ona widoczna, najpierw wybierz odpowiednią sekcję w drzewie widoków SNMP, wyświetlanym w lewej części okna.
2. Z menu **Wstaw** wybierz polecenia **Kolumna** lub **Pole** (w zależności od tego, czy dana sekcja ma styl tabeli, czy panelu).
3. Postępuj zgodnie ze wskazówkami podawanymi w otwartym w ten sposób oknie i wpisz informacje związane z nową kolumną lub nowym polem.



Rys. 28 Okno właściwości kolumny

Uwagi

- *Aby uzyskać podgląd edytowanej sekcji, należy skorzystać z karty **Podgląd**, dostępnej w dolnej części wyświetlanego okna. Kliknięcie karty **Sekcje** spowoduje powrót do widoku edycyjnego (sekcji oraz, odpowiednio, zmiennych w tych sekcjach lub tabel z kolumnami).*
- *Aby po pewnym czasie zmienić zdefiniowaną już wcześniej grupę, formularz, sekcję lub kolumnę/pole, należy taki element zaznaczyć, a następnie z menu **Edycja** wybrać polecenie **Właściwości**. W otwartym w ten sposób oknie należy wprowadzić odpowiednie zmiany.*
- *Aby natychmiast zapisać zmiany wprowadzone w widokach SNMP, należy z menu **Plik** wybrać polecenie **Zapisz**. Jeżeli jednak użytkownik będzie próbował zakończyć pracę z programem **Edytor widoków SNMP** bez wcześniejszego zapisania wprowadzonych zmian, wyświetlone zostanie okno ostrzeżenia, pozwalające na ich zapisanie przed zamknięciem aplikacji.*
- *Aby przeglądnąć lub przeprowadzić edycję aktualnie wykorzystywanych tabel wyszukiwania, należy z menu **Narzędzia** wybrać polecenie **Tabele wyszukania**, a następnie, w otwartym w ten sposób oknie, wprowadzić odpowiednie zmiany.*
- *Po utworzeniu nowych widoków SNMP, względnie po przeprowadzeniu edycji lub po usunięciu widoków już istniejących, odpowiednie zmiany zostaną automatycznie zapisane w pliku `snmpview.xml`. Jednakże taki zmieniony plik zapisany zostanie w podkatalogu `../data` w katalogu, w którym zainstalowany został NetCrunch. Będzie on dostępny dla wszystkich atlasów, które zostały zdefiniowane przez użytkownika i które będą otwierane w programie. Oryginalna wersja pliku (z chwili instalacji programu) pozostanie niezmieniona i będzie dostępna w głównym katalogu, w którym zainstalowany został NetCrunch.*

Zmiana domyślnych szablonów wiadomości

Większość alertów w programie (wiążących się albo z powiadomieniami, albo podejmowaniem określonych akcji – oprócz powiadomienia na pulpicie) musi zawierać informacje związane z wygenerowanym zdarzeniem, któremu alerty te zostały przypisane. Jest to konieczne do właściwego opisania wszelkich szczegółów zdarzenia, które właśnie wystąpiło. Informacje takie mogą zostać przekazane za pomocą wiadomości o różnym formacie: tekstowym, HTML, XML lub własnym. Uściślając, użytkownik wybiera jeden z tych czterech formatów wiadomości w kreatorze **Utwórz akcję**, podczas definiowania akcji dla danego zdarzenia.

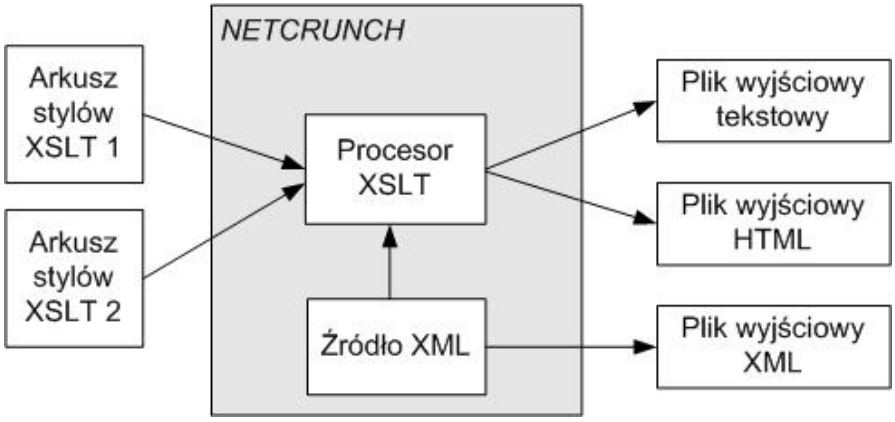
O ile wybranie własnego formatu wiadomości pozwala użytkownikowi dowolnie edytować to, co ma w takiej wiadomości zostać zawarte, o tyle pozostałe trzy formaty (XML, HTML oraz tekstowy) są już w programie wstępnie zdefiniowane.

Jednakże, w razie potrzeby, styl wyświetlania informacji o zdarzeniu w wiadomościach o formacie HTML lub tekstowym może zostać przez użytkownika ręcznie zmieniony – oddzielnie dla każdej z dostępnych klas zdarzeń. Oznacza to, że standardowy format prezentacji dowolnej, zdefiniowanej w programie wiadomości o zdarzeniu może zostać ręcznie zmieniony poprzez edycję odpowiednich plików.

Wprowadzenie do języka XSLT

Do zmiany formatu wiadomości NetCrunch wykorzystuje język XSLT (Transformacje XSL). Język XSLT jest językiem służącym do konwersji dokumentu z formatu XML na inny. Domyślnie dla każdej klasy zdarzeń w programie zdefiniowane są dwa oddzielne arkusze stylów XSLT (służące do konwersji wiadomości w formacie XML na wiadomość w formacie – odpowiednio – HTML lub tekstowym). Ponieważ formatem wykorzystywanym wewnętrznie przez program dla potrzeb wszelkiego rodzaju konfiguracji jest format XML, zatem styl wiadomości XML nie może być zmieniany.

W ogólnym zarysie przeprowadzany przez NetCruncha proces konwersji formatu wiadomości na inny przedstawiony został poniżej, na Rys. 29. Warto zwrócić uwagę fakt, iż format danych zamieniany jest na standardowy format prezentacji (HTML lub tekstowy) za pomocą różnych arkuszy stylów. Chcąc więc zmienić domyślny sposób prezentacji wiadomości w formacie HTML lub tekstowym, wystarczy wprowadzić zmiany w odpowiednim arkuszu stylów.



Rys. 29 Proces konwersji XSLT w programie NetCrunch

Aby móc wprowadzać zmiany w arkuszu stylów, konieczna jest podstawowa znajomość języka XSLT. Dostarczanie tego rodzaju wiedzy wykracza poza zakres niniejszego podręcznika. Więcej informacji na ten temat można znaleźć w dokumentacji technicznej służącej do nauki i praktycznego zastosowania języka XSLT, dostępnej na przykład na stronie http://www.w3.org/Style/XSL/WhatIsXSL.html.

Arkusze stylów XSL programu NetCrunch

Wszystkie arkusze stylów XSL programu znajdują się w podkatalogu `/Alerts` katalogu, w którym zainstalowany został program NetCrunch. Ponadto w katalogu tym znajduje się dwanaście podkatalogów, z których każdy odpowiada jednej z dostępnych w programie klas zdarzeń. Katalogi te wymienione zostały poniżej (w przypadkowej kolejności):

- Map Action (Akcja na mapie),
- NetWare Performance (Wydajność NetWare),
- Network Interface State (Stan interfejsu sieciowego),
- Network Service Performance (Wydajność usługi sieciowej),
- Network Service State (Stan usługi sieciowej),
- Node Action (Akcja na węźle),
- Node State (Stan węzła),
- SNMP Performance (Wydajność SNMP),
- SNMP Trap (Trap SNMP),
- Syslog (Komunikat Syslog),
- Windows NT Performance (Wydajność Windows NT),
- Windows Service State (Stan usługi Windows).

W każdym z tych katalogów znajdują się dwa arkusze stylów XSL o nazwach `HTML.xsl` i `text.xsl`. Aby zmienić sposób prezentowania w programie informacji o zdarzeniach

w formacie HTML lub tekstowym, konieczne jest przeprowadzenie edycji tych plików (dla poszczególnych klas zdarzeń). W tym celu niezbędna jest biegła znajomość języka XSLT. Przed przystąpieniem do wprowadzania zmian w plikach zalecane jest zapoznanie się z odpowiednimi materiałami źródłowymi, zawierającymi informacje techniczne dotyczące języka XSLT. Po zaktualizowaniu właściwych plików, wprowadzone w nich zmiany znajdą swoje odzwierciedlenie w wiadomościach o formacie HTML lub tekstowym, wyświetlanych w ramach poszczególnych akcji.

Uwaga

Zalecane jest utworzenie kopii zapasowej domyślnych arkuszy stylów XSL, znajdujących się w folderze `/Alerts`*, przed wprowadzeniem do nich jakichkolwiek zmian.*

Zmiana arkuszy stylów XSL w programie NetCrunch

Arkusze stylów XSL wykorzystywane w NetCrunchu (zarówno `text.xls`, jak i `HTML.xls`) mają wstępnie zdefiniowany format. Zawierają dowolną liczbę następujących standardowych elementów XSL (określanych jako tagi XML):

xsl:stylesheet	Jest to najbardziej zewnętrzny element każdego arkusza stylów XSL programu. Za jego pomocą musi zostać zadeklarowana wersja oraz przestrzeń nazw. Jest on definiowany tylko raz, na początku danego arkusza stylów XSL.
xls:template	Element ten określa kontekst, według którego przetwarzany ma być wejściowy dokument XML. Służy on do odszukania określonego taga zdefiniowanego w wejściowym dokumencie XML i odpowiedniego przetworzenia zawartej w nim informacji (danych lub wartości parametryzujących określone atrybuty).
xls:value of select=""	Element ten umieszczany jest z reguły pomiędzy tagami definiującym i element <xls:template>. Pozwala na wybranie (z wejściowego dokumentu XML) określonych danych zdefiniowanych w danym tagu lub określonej wartości jego atrybutu.
xsl:apply templates	Element ten służy do kontroli strumienia przetwarzania szablonu w wejściowym dokumencie XML. Ściślej mówiąc, każe on procesorowi języka XSL dopasowywać zadaną liczbę elementów do innych szablonów w dokumencie. W programie element ten wykorzystywany jest do przetwarzania wszystkich bezpośrednich węzłów (czyli elementów) potomnych w stosunku do aktualnie przetwarzanego elementu z pliku XML.

Przykład

Pokażmy na prostym przykładzie, w jaki sposób fragment wejściowego dokumentu XML z programu NetCrunch jest przetwarzany z wykorzystaniem standardowego arkusza stylów XSL, oraz jak później wygląda wynik takiego przetwarzania. W naszym przypadku

wykorzystamy arkusz stylów XSL o nazwie *text.xls*, który został utworzony dla potrzeb generowania pliku w formacie tekstowym, zawierającego wiadomość o zdarzeniu.

Wejściowy plik XML został wygenerowany w programie, a jego zawartość przedstawia się następująco (umieszczona poniżej numeracja wierszy nie występuje w rzeczywistym pliku):

```
1   <alert  id="1234" received="10/28/03 15:37:59">
2   <from  id="1024" name="cheops.adrem.com" address="192.168.1.10"/>
3   <type  id="1007" name="Próg wydajności Novell NetWare"/>
4   <rule  id="101" name="WYSOKI poziom wykorzystania pamięci"
severity="Krytyczna" state="Sprawny"/>5 </alert>
```

Jak widać, ma on związek z alertem, który generowany jest dla zdarzenia polegającego na przekroczeniu progu wydajności systemu NetWare.

Arkusz stylów XSL o nazwie `text.xls`, znajdujący się w podkatalogu `/Alerts/NetWare Performance` katalogu, w którym zainstalowany został program, został zmieniony i przedstawia się następująco (umieszczona poniżej numeracja wierszy nie występuje w rzeczywistym pliku):

```
1  <?xml version="1.0" encoding="ISO-8859-1"?>
2  <xsl:stylesheet version="1.0"  xmlns:xsl="http://www.w3.org/TR/WD-xsl">
3    <xsl:template match="/">
4
5    |===============|
6    |Alert NetCrunch|
7    |===============|
8
9      <xsl:apply-templates/>
10   </xsl:template>
11
12   <xsl:template match="alert">
13   --------------------
14   Odebrane: <xsl:value-of select="@received"/>
15     <xsl:apply-templates/>
16   </xsl:template>
17
18   <xsl:template match="from">
19   Od: <xsl:value-of select="@name"/> (<xsl:value-of select="@address"/>)
20   --------------------
21   </xsl:template>
22
23   <xsl:template match="type">
24   Rodzaj: <xsl:value-of select="@name"/>
25   </xsl:template>
26
27   <xsl:template match="rule">
28   Opis: <xsl:value-of select="@name"/>
29   Ranga: <xsl:value-of select="@severity"/>
```

```
30   Stan działania: <xsl:value-of select="@state"/>
31   </xsl:template>
32 </xsl:stylesheet>
```

I wreszcie wynikowa wiadomość generowana przez program (na podstawie wejściowego pliku XML oraz arkusza stylów XSL), wyświetlana w formacie tekstowym, przedstawiać się będzie następująco:

```
|===============|
|Alert NetCrunch|
|===============|

--------------------
Odebrane: 10/28/03 15:37:59
Od: cheops.adrem.com (192.168.1.10)
--------------------

Rodzaj: Próg wydajności Novell NetWare
Opis: WYSOKI poziom wykorzystania pamięci
Ranga: Krytyczna
Stan działania: Sprawny
```

W jaki sposób wygenerowany został plik wyjściowy

NetCrunch rozpoczyna przetwarzanie arkusza stylów XSL (`text.xls`) wczytując go wiersz po wierszu. Pierwsze dwa wiersze pliku występują domyślnie. W szczególności wiersz 2. (czyli tag <xsl:stylesheet>) określa najbardziej zewnętrzny element tego pliku XSL.

W wierszu 3. arkusza stylów XSL (czyli w tagu <xls:template match=”/”>) zdefiniowany jest rzeczywisty kontekst w wejściowym pliku XML. Informuje on procesor języka XSL, aby rozpoczął przetwarzanie wejściowego pliku XML od pierwszego wiersza. Wiersze 4-8 przetwarzane są jako regularny tekst i dołączane do wyjściowego pliku tekstowego. Wiersz 9. (czyli tag <xsl:apply-templates/>) nakazuje programowi, aby przetwarzał wszystkie bezpośrednie elementy potomne wejściowego pliku XML. W wierszu 10. zamykany jest tag, który został określony w wierszu 3.

Wiersz 12. arkusza stylów XSL (czyli tag <xsl:template match=”alert”>) informuje procesor programu NetCrunch, aby odszukał w wejściowym pliku XML element „<alert>” i rozpoczął jego przetwarzanie. Wiersz 13. jest wczytywany i dołączany bez zmian do wyjściowego pliku tekstowego. Następnie przetwarzany jest wiersz 14. Najpierw do pliku wyjściowego dodawany jest tekst „Odebrane:”. Następnie tag <xsl:value-of select=”@received”/> poszukuje atrybutu *received* należącego do elementu <alert> w pliku XML. Gdy zostanie on znaleziony, do wyjściowego pliku tekstowego przepisywana jest wartość tego parametru (czyli „10/28/03 15:37:59”).

Wiersz 15. informuje procesor programu NetCrunch, aby rozpoczął przetwarzać wszelkie elementy potomne aktualnego elementu <alert>. Ponieważ pierwszym elementem potomnym taga <ALERT> jest element <from>, zatem przetwarzany jest jego szablon znajdujący się w wierszu 18. Wiersz 19. przepisuje tekst „Od:” wraz z wartościami atrybutów *name* i *address*

znalezionymi w wejściowym pliku XML. Wiersz 20. jest przepisywany bez zmian do wyjściowego pliku tekstowego.

Ponieważ następnym elementem potomnym elementu <alert> jest element <type>, zatem, jako kolejne, przetwarzane są wiersze 23-25. Jak widać w wierszu 24. arkusza stylów XSL, tekst „Rodzaj:" przepisywany jest do wyjściowego pliku tekstowego wraz z wartością atrybutu *name* taga <type> (czyli określeniem „Próg wydajności Novell NetWare").

Ostatnim elementem potomnym elementu <alert> (w wejściowym pliku XML) jest element <rule>, a zatem, jako kolejne, przetwarzane są wiersze 27-31. Można ponownie zauważyć, że tag <xsl:value-of select/> służy do odszukania trzech wartości atrybutów elementu <rule> (czyli atrybutów *name*, *severity* i *state*) i przepisania ich do wyjściowego pliku tekstowego wraz z określonym tekstem.

Wreszcie wiersz 32. informuje procesor programu NetCrunch, że osiągnięty został koniec arkusza stylów XSL.

Jak wprowadzać zmiany w arkuszu stylów XSL

Zaleca się, aby przed próbą wprowadzenia zmian w domyślnych arkuszach stylów (związanych z wyjściowym formatem tekstowym i HTML) dla jakiegokolwiek rodzaju zdarzenia, sporządzić najpierw kopię zapasową każdego z nich. Zapobiega to różnym nieprzewidzianym problemom, jakie mogą pojawić się w przypadku, gdy zmieniony plik XSL nie może być poprawnie przetwarzany przez program (można wówczas powrócić do zapisanych wcześniej kopii).

W zasadzie zaleca się wprowadzanie jedynie drobnych zmian w domyślnych arkuszach stylów XSL. Można na przykład zmienić kolejność, w jakiej pewne elementy pojawiać się będą w plikach wyjściowych – tekstowym lub HTML. Można również zmienić tekst, który zapisany jest na takich arkuszach stylów XSL, a który ma być wiernie przepisywany do pliku wyjściowego. W przypadku plików wyjściowych HTML możliwa jest ponadto zmiana standardowych tagów formatujących tak, aby określone informacje o zdarzeniach prezentowane były w postaci tabeli.

Zmiana formatu wiadomości związanych z akcjami

W przypadku kilku rodzajów akcji udostępniane jest dodatkowe okno **Format wiadomości**, w którym może zostać dokładnie zdefiniowany format wiadomości, jaka ma być w takiej sytuacji wysyłana. Okno to wyświetlane jest w kreatorze *Utwórz akcję*, podczas czynności dodawania akcji do zdarzenia.

Wiadomość może być zapisana w jednym z następujących formatów:

- Tekst
- HTML
- XML
- Własny

Jeżeli wybrana zostanie jedna z pierwszych trzech opcji (tekst, HTML lub XML), informacje związane z alertem, a dotyczące danego zdarzenia, otrzymywane będą w ustalonym w ten sposób formacie. Natomiast po wybraniu opcji **Własny** możliwe staje się ułożenie własnej treści wiadomości, przy wykorzystaniu do tego celu zestawu dostępnych parametrów (ich dokładna liczba uzależniona jest od zdarzenia, z którym skojarzona jest wybrana akcja). Parametr wybierany jest przez kliknięcie prawym przyciskiem myszy pustego miejsca w panelu edycyjnym okna, a następnie wybranie jednej z pozycji wyświetlanych w menu podręcznym. Parametr taki zostanie automatycznie wstawiony do tekstu aktualnie edytowanego w panelu edycji. Można również skorzystać z parametrów zawierających ogólne informacje o zdarzeniu (grupy *Common* i *Properties*). Są one zawsze dostępne dla wszystkich rodzajów zdarzeń. Pozostałe grupy parametrów dostępne są jedynie dla określonych rodzajów zdarzeń, dla których definiowana jest dana akcja. W pierwszej z zamieszczonych poniżej tabel wymienione zostały parametry dostępne w przypadku każdego zdarzenia. Podane w niej zostały: nazwa, krótki opis oraz przykładowa wartość każdego z nich. W drugiej tabeli wymienione są pozostałe dostępne parametry. Dla wybranego zdarzenia może pojawiać się tylko jedna taka grupa parametrów (na przykład *NetworkService*, *MapAction* lub *InterfaceState*). W tabeli tej także podane zostały: nazwa, krótki opis oraz przykładowa wartość każdego z parametrów.

Uwaga

Można również dodawać zmienne do własnych rodzajów wiadomości właściwych dla producenta. W tym celu umieść '$' przed nazwą parametru specyficznego dla producenta we własnej wiadomości, jeśli chcesz, aby zastąpiła go aktualna wartość, która znalazła się w otrzymanym trapie. Parametry właściwe dla producenta zawsze zaczynają się od 'Event.'. Przykładowo, jeśli jednym z otrzymanych w trapie parametrów producenta jest 'Event.1.3.6.1.4.1.4331.3.3', należy wpisać '$Event.1.3.6.1.4.1.4331.3.3' we własnej wiadomości, aby wyświetlić wartość, jaką otrzymał ten konkretny parametr w akcji wysyłki wiadomości email (związanej ze zdarzeniem typu trap SNMP).

NAZWA ZMIENNEJ	*OPIS*	*PRZYKŁADOWA WARTOŚĆ*
$Common.Id	Numer identyfikacyjny przypisany danemu zdarzeniu, umożliwiający rozróżnianie poszczególnych zdarzeń zewnętrznych (pochodzących od trapów SNMP lub komunikatów Syslog). W aktualnej wersji programu dla wszystkich zdarzeń wewnętrznych identyfikator ten ma wartość 0.	0
$Common.Time	Dokładna data i czas przetwarzania zdarzenia.	2004-04-01 10:40:47[1]

[1] Format daty i czasu uzależniony jest od ustawień wprowadzonych przez użytkownika na komputerze, na którym uruchomiony jest NetCrunch.

$Common.EventType	Rodzaj zdarzenia.	`Zdarzenie trap SNMP`
$Common.Description	Nazwa zdarzenia – taka, jaka została podana podczas jego definiowania.	`Trap`
$Common.Severity	Ranga zdarzenia – taka, jaka podana została podczas jego definiowania (KRYTYCZNA, OSTRZEŻENIE, INFORMACYJNA lub NIEISTOTNA).	`Krytyczna`
$Common.State	Informuje, czy wystąpienie danego zdarzenia spowodowało przejście węzła, w którym miało ono miejsce, względnie zasobów zainstalowanych w tym węźle, w stan sprawności, czy też nie.	`Niesprawny`
$Common.Application	Określa zastosowanie, do której należy dane zdarzenie. Jest to to samo zastosowanie, w której zdefiniowane zostało dane zdarzenie.	`Windows NT Server`
$Common.XML	Pełna informacja o zdarzeniu w formacie XML (czyli taka sama informacja, jaka generowana jest wówczas, gdy wybrany zostaje format XML wiadomości).	
$Common.AlertInfo	Krótki opis zdarzenia.	`Trap SNMP Właściwy dla producenta od przełącznik01 w test15.adrem (192.168.1.65)`
$Properties.DisplayName	Określa nazwę DNS i adres IP węzła, w którym nastąpiło zdarzenie, w formacie <NAZWA_DNS>(<ADRES_IP>).[2]	`test15.adrem(192.168.1.65)`

[2] Pole **Nazwa wyświetlana**, należące do właściwości węzła, dotyczy jedynie tekstu, który jest wyświetlany na mapie. Należy również pamiętać, że ten sam węzeł może być na różnych mapach wyświetlany
z coraz to inną nazwą.

$Properties.HostName	Określa nazwę urządzenia, w którym nastąpiło zdarzenie.	`test15`
$Properties.Address	Określa adres IP urządzenia, w którym nastąpiło zdarzenie.	`192.168.1.65`
$Properties.ComputerName	Określa nazwę komputera w węźle, w którym nastąpiło zdarzenie.	
$Properties.HardwareAddress	Określa adres MAC węzła.	`0004760DF61C`
$Properties.Info1	Udostępnia zawartość pola o tej samej nazwie, znajdującego się w oknie właściwości węzła. W przypadku map dynamicznych należących do widoków własnych pole to może być wykorzystywane do tworzenia warunku w ramach określania kryteriów filtrowania.	`Biuro`
$Properties.Info2	Udostępnia zawartość pola o tej samej nazwie, znajdującego się w oknie właściwości węzła. W przypadku map dynamicznych należących do widoków własnych pole to może być wykorzystywane do tworzenia warunku w ramach określania kryteriów filtrowania.	`Piętro 1`
$Properties.Type	Określa rodzaj węzła, w którym nastąpiło zdarzenie.	`Stacja robocza Windows 2000`
$Properties.ReadCommunity	Określa wspólnotę odczytu SNMP wykorzystywaną przez węzeł, o ile ma ona zastosowanie.	`Public`
$Properties.WriteCommunity	Określa wspólnotę zapisu SNMP wykorzystywaną przez węzeł, o ile ma ona zastosowanie.	`Private`

NAZWA ZMIENNEJ	***OPIS***	***PRZYKŁADOWA WARTOŚĆ***
$NetworkService.Status	Charakter zmiany stanu związanej z danym progiem (tj. *wystąpił* lub *skasował się*).	`Skasował się`

$NetworkService.Counter	Określa licznik wydajności, który jest monitorowany w danym węźle.	PING/Czas odpowiedzi (RTT)
$NetworkService.Value	Podaje wartość odczytaną z licznika wydajności w chwili, gdy wygenerowane zostało zdarzenie związane z wartością progową.	80
$NetworkService.Kind	Określa, czy wartość znajduje się powyżej czy poniżej wartości progowej.	Powyżej
$NetworkService.Threshold	Wartość progowa, która, gdy zostanie przekroczona, powoduje generowanie zdarzenia.	82
$NetworkServiceState.Status	Określa, jaki rodzaj zmiany nastąpił (*Odpowiada* lub *Nie odpowiada*)	Odpowiada
$NetworkServiceState.Service	Określa usługę sieciową, dla której nastąpiło zdarzenie związane z wartością progową (np. PING, HTTP itp.).	HTTP
$MapAction.Action	Określa, jaki rodzaj akcji został przeprowadzony na mapie.	Usuń
$MapAction.MapId	Określa numer identyfikacyjny mapy, na której wprowadzone zostały zmiany.	3
$MapAction.MapName	Określa nazwę mapy, na której wprowadzone zostały zmiany.	Grupa robocza
$InterfaceState.Status	Określa rodzaj zmiany, jaka nastąpiła w interfejsie (*Odpowiadający* lub *Nieodpowiadający*)	Odpowiada
$InterfaceState.Interface	Określa nazwę interfejsu, w związku z którym nastąpiło dane zdarzenie.	RMON Port 09 w jednostce 1
$InterfaceState.Index	Określa indeks interfejsu sieciowego, w związku z którym nastąpiło dane zdarzenie (np. 109 oznacza jednostkę 1, port 09).	109

$InterfaceState.HardwareAddress	Określa adres sprzętowy (MAC) interfejsu sieciowego, w związku z którym generowane jest dane zdarzenie.	`0004762221D2`
$NodeAction.Action	Określa rodzaj akcji, jaka została przeprowadzona na danym węźle.	`Usunięty`
$NodeState.Status	Określa stan węzła (np. *Odpowiada* lub *Nie odpowiada*).	`Nie odpowiada`
$Syslog.Facility	Udostępnia zawartość pola **Facility**, otrzymaną w przychodzącym komunikacie Syslog.	`User level`
$Syslog.Severity	Udostępnia zawartość pola **Severity**, otrzymaną w przychodzącym z urządzenia komunikacie Syslog.	`Error`
$Syslog.Process name	Określa proces, który wywołał komunikat Syslog.	`gsview`
$Syslog.Content	Określa zawartość wywołanego komunikatu Syslog.	
$Syslog.Host name	Określa adres IP lub nazwę urządzenia, który wywołał komunikat Syslog.	`182.35.3.11`
$Netware.Status	Charakter zmiany stanu (*wystąpił* lub *skasował się*).	`Wystąpił`
$Netware.Counter	Licznik wydajności w węźle NetWare, który jest monitorowany pod kątem zdarzeń związanych z wartością progową.	`Serwer\% Wykorzystania pamięci`
$NetWare.Value	Podaje wartość odczytaną z licznika wydajności w chwili, gdy wygenerowane zostało zdarzenie związane z wartością progową.	`2000`
$NetWare.Kind	Określa, czy dana wartość znajduje się powyżej czy poniżej wartości progowej.	`Powyżej`
$NetWare.Threshold	Określa wartość progową, która, gdy zostanie przekroczona, powoduje generowanie zdarzenia.	`2100`

$Snmp.Status	Charakter zmiany stanu (np. *wystąpił* lub *skasował się*).	`Skasował się`
$Snmp.Counter	Licznik wydajności w węźle zarządzanym za pomocą agenta SNMP, który jest monitorowany pod kątem zdarzeń związanych z wartością progową.	`Zbiorczy\Czas prawidłowego działania`
$Snmp.Value	Podaje wartość odczytaną z licznika wydajności w chwili, gdy wygenerowane zostało zdarzenie związane z wartością progową.	`22`
$Snmp.Kind	Określa, czy wartość znajduje się powyżej czy poniżej wartości progowej.	`Powyżej`
$Snmp.Threshold	Określa wartość progową, która, gdy zostanie przekroczona, powoduje generowanie zdarzenia.	`20`
$Snmp.OID	Określa identyfikator OID licznika w węźle, który jest monitorowany pod kątem zdarzeń związanych z wartością progową.	`1.3.6.1.2.1.2.2.1.20`
$SnmpTrap.GenericType	Określa ogólny rodzaj trapu SNMP.	`Cold Start`
$SnmpTrap.SpecificType	Określa szczególny rodzaj trapu SNMP.	`resStateChange (44)`
$SnmpTrap.OID	Określa identyfikator OID nadawcy oraz pole Szczególny rodzaj trapu.[3]	`1.3.6.1.4.1.43.2.1.3`
$SnmpTrap.Enterprise	Identyfikator OID nadawcy.	`a3Com (1.3.6.1.4.1.43)`
$SnmpTrap.Community	Określa wspólnotę trapów SNMP.	`Private`

[3] Zmiennej tej jest nadawana określona wartość tylko w przypadku węzła wykorzystującego protokół SNMPv2.

$SnmpTrap.Info	Opisowa informacja na temat wygenerowanego szczególnego rodzaju trapu SNMP.	`Ten trap generowany jest wówczas, gdy zmiana stanu jednego z portów pary elastycznej (resilient pair)nie wpływa na przełączenie portu aktywnego. Gdyby miało nastąpić takie przełączenie, wiązałoby się to z wygenerowaniem trapu resResilienceSwitch.`
$WindowsNT.Status	Rodzaj zmiany stanu.	`Wystąpił`
$WindowsNT.Counter	Określa licznik wydajności w węźle typu Windows, który jest monitorowany pod kątem zdarzeń związanych z wartością progową.	`Pamięć\Dostępnych bajtów`
$WindowsNT.Value	Wartość odczytana z licznika wydajności Windows w chwili, gdy przekroczona została wartość progowa.	`320`
$WindowsNT.Kind	Określa, czy wartość znajduje się powyżej czy poniżej wartości progowej.	`Poniżej`
$WindowsNT.Threshold	Określa wstępnie zdefiniowaną wartość progową, która, gdy zostanie przekroczona, powoduje generowanie zdarzenia.	`380`
$WindowsService.Status	Określa zmieniony stan usługi Windows (np. *Uruchomiona*, *Wstrzymana* lub *Zatrzymana*).	`Uruchomiona`

$WindowsService.Service	Określa usługę Windows, dla której wystąpiło dane zdarzenie.	MSSQLSERVER
$Heartbeat.ActiveAtlasName	Określa nazwę aktualnie otwartego atlasu NetCruncha.	Sieć(192.168.1.0)
$Heartbeat.ActiveAtlasDescription	Podaje zwięzły opis aktualnie otwartego atlasu.	Atlas lokalny
$Heartbeat.ActiveAtlasUptime	Określa, jak długo otwarty atlas jest załadowany w NetCrunchu.	2 dni 20 h 51 min. 30 sek.
$Heartbeat.ActiveMonitoringStatus	Określa status monitorowania aktywnego atlasu.	Włączone
$Heartbeat.HeartbeatInterval	Określa, jak często w NetCrunchu było wygenerowane zdarzenie typu Heartbeat.	Codziennie, o 12:00:00
$Heartbeat.NodeCount	Określa liczbę węzłów w aktywnym atlasie.	85
$Heartbeat.NodeDown	Określa liczbę węzłów nieodpowiadających w aktywnym atlasie.	21
$Heartbeat.NodesUnknown	Określa liczbę nieznanych węzłów w aktywnym atlasie.	0
$Heartbeat.NetworkServiceCount	Określa liczbę usług monitorowanych w aktywnym atlasie.	130
$Heartbeat.NetworkServiceErrors	Określa liczbę błędów usług sieciowych w aktywnym atlasie.	25
$Heartbeat.NetworkServiceWarnings	Określa liczbę usług sieciowych oznaczonych ostrzeżeniem w aktywnym atlasie.	0
$Heartbeat.NetworkServicesUnknown	Określa liczbę nieznanych węzłów w aktywnym atlasie.	4
$Heartbeat.NetCrunchMemoryStatus	Określa status pamięci uruchomionego Netcruncha.	Zaalokowana: 15360kB, Wolna: 3514kB
$Heartbeat.NetCrunchCPUUtilization	Określa obciążenie procesora generowane przez NetCruncha.	7%

$NodeStateMon.State	Określa niepożądane stany węzła – wywołujące zdarzenie w momencie, gdy zachodzą przez określony okres czasu.	`Nie odpowiada`
$NodeStateMon.ExpectedState	Określa oczekiwany stan węzła.	`OK`
$NodeStateMon.TimeRange	Określa okres czasu monitorowania stanu węzła.	`Pn, Wt, Śr, Czw, Pt od 9:00 do 17:30`

Indeks

X

Z