AdRem NetCrunch

Wersja 4.x

„Pierwsze kroki”

Poradnik dla początkujących użytkowników NetCruncha

Monitorowanie i zarządzanie siecią

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

Omówienie

Niniejszy poradnik przeznaczony jest dla administratorów sieci oraz innych specjalistów zajmujących się zarządzaniem infrastrukturą sieciowa. Pokaże on, jak zainstalować oprogramowanie AdRem NetCrunch i natychmiast przystąpić do korzystania z udostępnionych w nim funkcji. Zasadniczym przeznaczeniem programu jest monitorowanie infrastruktury sieciowej z wykorzystaniem mechanizmów wizualizacji sieci, wykrywania usterek, powiadamiania o nich oraz raportowania.

Nowe funkcje programu

Edycja 4.x NetCruncha doczekała się kilku wersji (4.0, 4.1 i 4.2), w których wprowadzono szereg udoskonaleń i nowych funkcji:

1. Wykrywanie sieci

- Opcja ponownego skanowania domen Windows. Nowa wersja umożliwia powtórne skanowanie lub tworzenie map domen Windows.
- Domyślne ustawienia monitorowania dla nowo wykrytych węzłów: program umożliwia ustawianie domyślnych opcji dla nowo wykrytych lub ręcznie dodanych węzłów (takich jak czas monitorowania, profil SNMP i port SNMP).
- Możliwość pomijania wybranych węzłów w procedurze wykrywania węzłów(4.1).

2. Wizualizacja map

- Usprawiony mechanizm tworzenia map topologii fizycznej wyposażone o nowe metody analizy (4.1).
- Udoskonalony mechanizm filterowania map dynamicznych.
- Możliwość modyfikowania układu graficznego segmentów fizycznych (4.1).
- Funkcja "Cofnij" w edycji map.
- Udoskonalone wyświetlanie podpisów węzłów.
- Nowe opcje edycji mapy.
- Nowy domyślny układ graficzny.

3. Monitorowanie sieci

- Kompletna obsługa wersji 3 protokołu SNMP (uwierzytelnienie i szyfrowanie); użytkownicy mogą wybierać wersje 1, 2 i 3 standardu SNMP.
- Priorytety monitorowania usług sieciowych.
- Mechanizm wstrzymywania zdarzeń.

- Opcja tworzenia wirtualnych liczników wydajności w postaci wyrażenia opartego o zebrane dane licznika.
- Nowe rodzaje warunków progowych: nagła zmiana (narastający/opadający), stan (jest równe/jest różne), obecność (odebrano dowolną wartość/nie odebrano żadnej wartości).
- Opcja ustawiania innego niż domyślny portu SNMP na dowolnym węźle.
- Udoskonalone monitorowanie zależności sieciowych: zastosowanie trybu wielokrotnego wyboru w oknie **Zależności sieciowe**; węzeł lokalny, na którym uruchomiony jest NetCrunch jest oznaczany za pomocą specjalnego znaczka graficznego, a monitorowanie wszystkich innych węzłów jest od niego zależne.
- Możliwość otrzymywania zdarzeń informujących o zresetowaniu progu.
- Opcja wyboru wiodącej usługi węzła. Usługa wiodąca to jedyna usługa monitorowana w momencie, gdy węzeł nie odpowiada w celu ustalenia jego statusu.
- Poszerzone parametry monitorowania usług sieciowych (nowe pole **Dodatkowa liczba powtórzeń**).
- Nowe profile SNMP: umożliwiają wskazanie dostępu w trybie "tylko do odczytu" oraz "odczyt-zapis" dla każdego węzła.
- Mapa Zależności monitorowania jest dynamiczna.
- Usprawnione definiowanie nowych usług sieciowych.
- W Widoku SNMP liczniki mogą być odświerzane w odstępach sekundowych.
- Poszerzone statystyki monitorowania węzła.

4. Alertowanie

- Zdarzenie o nazwie Heartbeat. Informuje użytkownika, czy NetCrunch jest uruchomiony i działa poprawnie (4.1).
- Zdarzenie związane z monitorem stanu węzła - informuje użytkownika, czy w określonym czasie węzeł niezmiennie znajduje się w żądanym stanie (ODPOWIADA lub NIE ODPOWIADA) [4.1].
- Nowe akcje:
  - ustaw zmienną SNMP.
  - uruchom/zatrzymaj/wtrzymaj/ponownie uruchom/kontynuuj usługę Windows.
  - ustaw stan monitorowania węzła.
  - ponowne uruchomienie/wyłączenie komputera.
  - zakończenie procesu Windows.
  - wykonanie polecenia „Wake on LAN”.
  - dodanie statusu usługi sieciowej do treści komunikatu alertu.
  - zapisanie informacji o zdarzeniu w dzienniku zdarzeń systemu Windows.
- Uruchamianie programu lub skryptu na dowolnym węźle - nie tylko na węźle, na którym wystąpiło zdarzenie.
- Opcja logowania się do serwera SMTP -- zamiast wbudowanego serwera server.

5. Zdalny dostęp

- Ograniczanie dostępu użytkowników do funkcji programu: można określić odpowiedni poziom dostępu do funkcjonalności udostępnianej zdalnie za pomocą przeglądarki internetowej dla każdego użytkownika zdefiniowanego w profilach użytkownika (brak dostępu, tylko do odczytu, odczyt/zapis) [4.1].
- Udoskonalone zarządzanie kontami dostępu zdalnych użytkowników: można oglądać, kto korzysta zdalnie z programu i rozłączyć dowolnego użytkownika.
- Dziennik kontroli sesji zdalnego dostępu umożliwia weryfikowanie akcji wykonanych przez zdalnego użytkownika (4.1).
- Obsługa popalrnych przeglądarek internetowych: Internet Explorer, Mozilla, Firefox i Netscape.
- Szybkie modyfikowanie profili dostępu do poszczgólnych obiektów (węzeł, mapa lub atlas).
- Ulepszony interfejs użytkownika i grafika dla zdalnego dostępu przez WWW (4.2).

6. Raportowanie

- Nowy **Generator raportów wydajności**: umożliwia tworzenie własnych raportów trendów i szablonów raportów
- Nowa **Przeglądarka trendów**.

7. Nowy Kompilator MIB-ów SNMP

- Udoskonalone przeglądanie i zarządzanie modułami MIB.
- Edycja MIB-ów z podświetlaniem składni.
- Filttrowanie drzew MIB-ów według poszczególnych modułów.

8. Kompatybilność i konserwacja

- Opcja automatycznego eksportu trendów do bazy danych SQL (4.1).
- Opcja wyboru lokalizacji plików kopii zapasowej.
- Opcja usuwania trendów starszych niż określona liczba dni.
- Uwierzytelnianie podczas łączenia się z zewnętrznym serwerem SMTP.
- Import danych atlasu wersji 3.x NetCruncha

9. lTools 4.5

- Obsługa wersji 3 protokołu SNMP.
- Nowe narzędzie do weryfikowania jakości połączeń.
- Udoskonalony interfejs użytkownika.
- Udoskonalona funkcja wyszukiwania MIB-ów (według OID-ów lub nazwy).

10. Inne

- Nowa aplikacja **WinTools** udostępniająca prkatyczne informacje Windows WMI (4.1).

- Edycja Premium XE NetCrunch działa na platformach 64-bitowych (zarówno wesji Windows XP Professional x64 jak i Windows Server 2003 x64) [4.1].
- Przeglądarka rejestrów w celu oglądania rejestrów wygenerowanych przez program (4.1).
- Notatnik węzła umożliwiający zamieszczanie w formie tekstowej komentarzy na temat poszczególnych węzłów (4.1).
- W podręcznym menu węzła można oglądać listę innych map, które zawierają wybranego węzła (np. mapa segmentów fizycznych) [4.1].

Instalacja

Procedura instalacji licencji

Podczas potwierdzenia procesowania zamówienia dostaniesz odsyłacz i hasło do portalu **myadrem.com**. Po zalogowaniu się do tego portalu, będziesz mógł ściągnąć plik zawierający instalację programu oraz stosowne pliki licencji.

Aby zainstalować licencję, należy ściągnąć pliki z rozszerzeniami **.als** oraz **.key**. Podczas otwarcia programu bez uprzednio zainstalowanej licencji, program zapyta się o lokalizację tych plików.

W celu uzyskaniu więcej informacji nt instalacji licencji, proszę odnieść się do **Podręcznika instalacji licencji** do programu Netcrunch.

Instalacja NetCruncha

NetCrunch może zostać zainstalowany na dwa sposoby:

- **Jako standardowy program na pulpicie** – wówczas użytkownik uruchamia go otwierając standardowy program wykonywalny Windows. Program będzie uruchomiony do momentu wylogowania się z systemu Windows.
- **Jako usługa Windows** – wówczas NetCrunch będzie działał wyłącznie jako usługa Windows. Znaczy to, że program zostanie automatycznie uruchomiony podczas startu systemu i będzie działał w tle. W wypadku, kiedy jesteś zalogowany jako administrator, będziesz miał dostęp do interfejsu programu poprzez kliknięcie na stosowną ikonę w pasku narzędzi. Inny sposób dostępu do programu to użycie przeglądarki (lokalnie i zdalnie). Jeżeli używasz użytkownika Windows podczas działania programu (kiedy jest uruchomiony jako usługa Windows), taki użytkownik musi mieć prawa administratora, aby program ten działał poprawnie.

Wymagania systemowe

Instalacja edycji Premium lub Premium XE NetCruncha 4.x zalecana jest na oddzielnym komputerze służącym do tego celu.

Wymagania systemu zależne są od liczby monitorowanych węzłów. W wypadku monitorowania powyżej 100-200 węzłów, powinno się używać zalecane wymagania systemowe wymienione poniżej.

Komponent	Minimum	Zalecane
Procesor	Intel Pentium 4 / AMD Athlon64	Dual-core Intel Pentium D/Core2 Duo or AMD Athlon64 X2 lub szybsze modele
System Operacyjny	Windows 2000, Windows XP SP2 (z zastrzeżeniami opisanymi poniżej) lub Windows Server 2003	Windows Server 2003
Pamięć	512 MB RAM	1 GB RAM
Twardy dysk	100 MB wolnego miejsca na dysku na pliki programu po instalacji; 200 MB na zapisywanie trendów	100 MB wolnego miejsca na dysku na pliki programu po instalacji; 1 GB na zapisywanie trendów
Grafika	1280 x 1024 pikseli (SXGA) High Color (16 bit)	Widescreen - 1680 x 1050 pikseli (WSXGA+) lub wyżej. True Color (32 bit)
Przeglądarka internetowa	Firefox, Mozilla, Netscape, Microsoft Internet Explorer 5.5 lub nowsza	Firefox, Mozilla, Netscape, Microsoft Internet Explorer 6.0 lub nowsza

Uwagi

- *Edycja Premium XE Netcrunch może zostać uruchomiona na 64-bitowych systemach operacyjnych: edycja Windows XP Professional x64 jak i również edycja Windows Server 2003 x64 jest obsługiwana.*
- *System operacyjny Windows XP Service Pack 2 ogranicza liczbę równoczesnych niekompletnych przychodzących prób połączeń (SYN) za pomocą protokołu TCP do 10 (w wersji systemu operacyjnego Windows XP Service Pack 1 ten limit był ustawiony na 65,000). Niedogodność tego ograniczenia połączeń znaczy, że funkcjonalność oprogramowania monitorujących sieci takiego jak NetCrunch, może zostać ujemnie ograniczona. Proces monitorowania sieci oraz opóźnienie połączeń do bazy danych zdarzeń może zostać tymczasowo wstrzymane.*

Krótka prezentacja programu

Poniższy rozdział pokazuje, jak uruchomić NetCruncha i pokrótce wyjaśnia przeznaczenie wszystkich okien programu.

Uruchamianie Programu

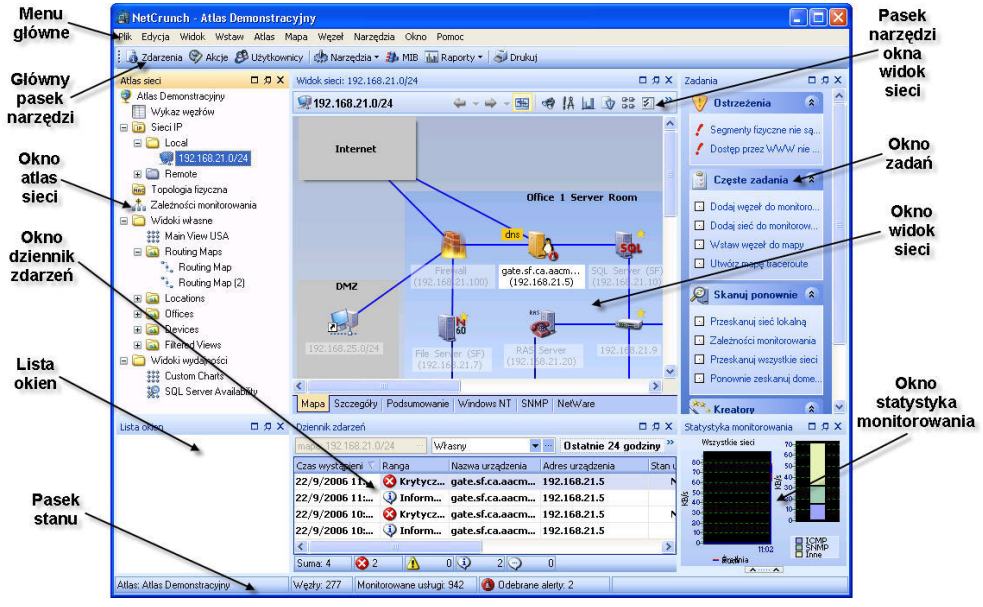
NetCrunch może być uruchomiany na jeden z następujących sposobów:

- Dwukrotne kliknięcie ikony programu na pulpicie (jeśli oczywiście został a ona uprzednio utworzona).
- Wybór opcji *Programy* | *Adrem NetCrunch 4.2* | *NetCrunch* z menu Start na pulpicie Windows.
- Dwukrotne kliknięcie pliku *iMonitor.exe* w katalogu o ścieżce `c:\Program Files\Adrem\NetCrunch\4.0` (lub o innej ścieżce określonej przez użytkownika podczas instalacji programu).

Po pomyślnym otwarciu programu możliwe jest wykrycie sieci i utworzenie atlasu. Więcej szczegółów na ten temat zawiera sekcja pt. *Wykrywanie struktury* sieci na stronie 27.

Opis/charakterystyka programu

Po otwarciu programu po raz pierwszy (po przeprowadzaniu procedury wykrycia sieci), ukaże się okno przedstawione na Rys. 1.



Rys. 1 Przykład głównego okna NetCruncha

Program zawiera zastępujące okna (nie wszystkie z nich muszą być wyświetlane jednocześnie):

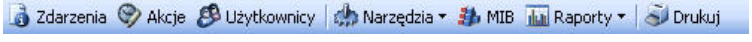
Główny pasek narzędzi	Zawiera przyciski umożliwiające dostęp do zasadniczych funkcji programu.
Atlas sieci	Organizuje informacje atlasu w trzech sekcjach drzewa: *Sieci IP* (widoki logiczne), *Segmenty fizyczne* (widoki fizyczne), i *Widoki własne* (zdefiniowane przez użytkownika).
Widok sieci	Wyświetla topologię sieci na graficznej mapie lub w tabeli.
Dziennik zdarzeń	Wyświetla i umożliwia zarządzanie zdarzeniami wygenerowanymi w monitorowanych sieciach.
Lista okien	Wyświetla listę okien programu aktualnie otwartych poza głównym oknem.
Zadania	Zawiera wykaz najczęściej używanych zadań programu dostępnych za jednym kliknięciem myszy.
Statystyka Monitorowania	Wyświetla bieżące informacje o ruchu w sieci generowanym przez monitorowanie NetCruncha, a także umożliwia ustawianie na podsieciach limitów dla ruchu monitorującego.
Pasek stanu	Wyświetla ogólne informacje o atlasie i należących do niego mapach.

Uwagi

- *Położenie wszystkich wyszczególnionych powyżej okien można zmieniać za pomocą opcji dokowania/oddokowywania. Więcej informacji na ten temat zawiera sekcja* Dostosowywanie interfejsu użytkownika *na stronie 47.*
- *Dodatkowo NetCrunch zawiera kilka niezależnych programów:* ***Przeglądarkę Raportów*** *(służącą do generowania i wyświetlania predefiniowanych raportów),* ***Generatora raportów wydajności*** *(służącego do tworzenia, generowania i wyświetlania własnych raportów trendów),* ***Narzędzia IP i SNMP*** *(pakiet przydatnych sieciowych narzędzi diagnostycznych) i* ***WinTools*** *(pakiet przydatnych narzędzi dotyczących węzłów z systemem operacyjnym Windows).*

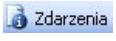
Główny pasek narzędzi

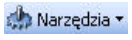
Główny pasek narzędzi zawiera listę często używanych globalnych funkcji, umożliwiając tym samym szybki do nich dostęp w dowolnej chwili. Przykładowy pasek tego typu został pokazany na poniższym Rys. 2.



Rys. 2 Przykład głównego paska narzędzi

Omawiany pasek składa się z następujących ikon:

	**Zdarzenia**	Otwiera okno **Dziennik zdarzeń**, w którym można przeglądać wygenerowane zdarzenia przechowywane w bazie Dziennika zdarzeń.

	**Akcje**	Otwiera okno **Zdefiniowane Akcje**, w którym można zarządzać zdefiniowanymi akcjami programu (dodawać, kasować, lub modyfikować ich właściwości). Akcje te mogą być kojarzone z dowolnym zdefiniowanym zdarzeniem.
	**Profile użytkowników**	Otwiera okno, w którym definiuje się użytkowników i grupy używane w powiadomieniach i dostępie przez WWW.
	**Narzędzia**	Otwiera niezależny program **Narzędzia IP i SNMP** lub **WinTools**. Program **Narzędzia IP i SNMP** zawiera zestaw standardowym narzędzi sieciowych (np. Ping, Traceroute, DNS Lookup, Przepustowość, Skaner i SNMP). Natomiast program **WinTools** pozwala uruchomić narzędzia dotyczące węzłów z systemem operacyjnym Windows.
	**Menedżer MIB-ów**	Otwiera program o nazwie **Menedżer MIB-ów** służący do edytowania i rekompilowania MIB-ów producentów.
	**Raporty**	Otwiera niezależny program o nazwie **Przeglądarka raportów** lub program o nazwie **Generator raportów wydajności**, za pomocą których można utworzyć, oglądać i drukować raporty.
	**Drukuj**	Otwiera okno **Podgląd wydruku** dla aktualnie wyświetlanej mapy.

Uwaga

*Aby włączyć lub wyłączyć pokazywanie głównego paska narzędzi, należy wybrać pozycję **Główny pasek narzędzi** z menu **Widok**.*

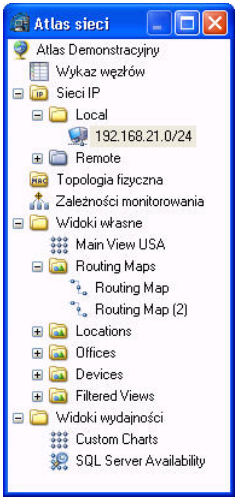
Atlas sieci

Okno **Atlas sieci** zawiera drzewo porządkujące informacje o aktualnie otwartym atlasie. Drzewo to składa się z czterech zasadniczych sekcji, opisanych w poniższej tabeli:

Sieci IP	Wyszczególnia zeskanowane logiczne mapy IP sieci (zarówno lokalne jak i zdalne).
Segmenty fizyczne	Pokazuje sieć lokalną, a w szczególności połączenia fizyczne między znajdującymi się w niej elementami.
Widoki własne	Grupuje widoki własne zawierające węzły wchodzące w skład dwóch opisanych powyżej sekcji atlasu. Widoki własne mogą mieć charakter dynamiczny (widoki filtrowane) lub statyczny (widoki własne utworzone ręcznie przez użytkownika).
Widoki wydajności	Prezentuje wykresy (wykres liniowy, wskaźnik wychyłowy, wykres słupkowy) obrazujące wyniki pomiaru liczników wydajności w węzłach.

Drzewo atlasu niezmiennie zawiera Wykaz węzłów wyszczególniający wszystkie węzły wykryte podczas skanowania lub dodane ręcznie przez użytkownika. Należy pamiętać, że węzły na tej liście niekoniecznie należą do mapy atlasu (a wiec do widoku logicznego, fizycznego lub własnego).

Co więcej, głównym obiektem okna **Atlas sieci** jest sam atlas. Przykładowe okno **Atlas sieci** zostało pokazane na Rys. 3. Jak można zauważyć, sekcja *Widoki własne* zawiera foldery i widoki o nazwie Main View USA, Routing Map itd.



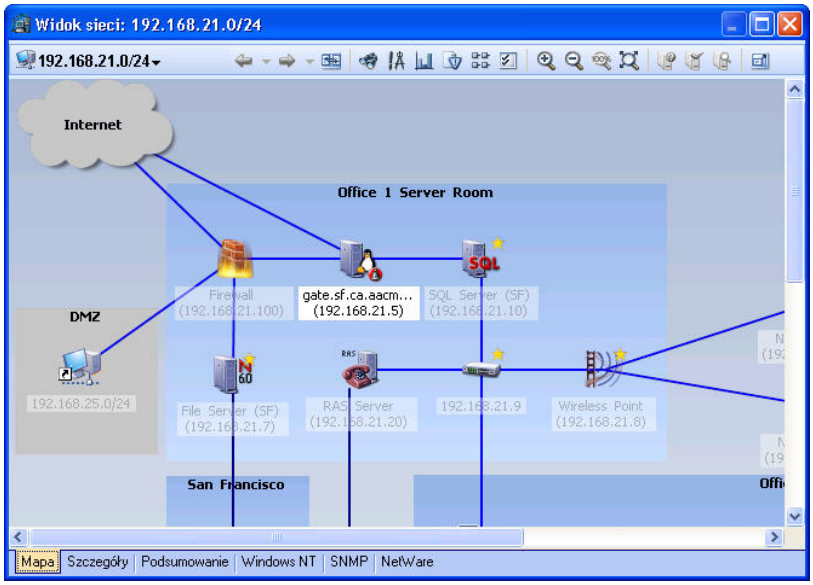
Rys. 3 Drzewo Atlasu sieci

Możliwe jest przenoszenie map z sekcji *Widoki własne* do innych grup. Mapy z sekcji *Segmenty fizyczne* nie mogą być modyfikowane w żadnym zakresie.

Dowolne okna sekcji **Widok sieci** i okna **Dziennika zdarzeń** można zsynchronizować z Atlasem sieci. Oznacza to, że przy wyborze określonej mapy z drzewa atlasu, okno lub okna w **Widoku sieci** natychmiast wyświetlą jej zawartość. Analogicznie, okno **Dziennik zdarzeń** pokaże wygenerowane zdarzenia dla węzłów należących do wybranej mapy.

Widok sieci

Okno **Widok sieci** służy do wyświetlania zawartości podświetlonego obiektu np. mapy sekcji **Atlas sieci**. Właściwe okno składa się z wygodnego paska narzędzi umożliwiającego dostęp do najczęściej używanych funkcji programu, panelu wyświetlania elementów sieci oraz zestawu kart umożliwiających przełączanie się między mapami i tabelarycznymi widokami sieci. W oknie **Widok sieci** można również edytować zawartość mapy (zmieniać rozmieszczenie węzłów i modyfikować graficzne obiekty na mapie, takie jak kształty w tle lub obrazy).



Rys. 4 Okno Widok sieci

Pasek narzędzi okna Widok sieci

Pasek narzędzi usytuowany w oknie **Widok sieci** umożliwia dostęp do najczęściej używanych funkcji programu związanych z mapami i ich zawartością. Aktualna liczba dostępnych ikon zależy od tego, czy w **Atlasie sieci** wybrano atlas, mapę czy grupę, oraz od aktualnie wybranego rodzaju karty. Rys. 5 ilustruje przykładowy pasek narzędzi okna **Widok sieci**. Na lewo od ikon wyświetlana jest nazwa aktualnie wybranej mapy w drzewie **Atlas sieci**.

Rys. 5 Przykładowy pasek narzędzi okna Widok sieci

Pasek narzędzi okna **Widok sieci** zawiera następujące ikony:

	Wstecz	Pozwala wrócić do poprzednio oglądanej mapy.
	Dalej	Wyświetla następną stronę (tylko wtedy, gdy uprzednio użytkownik wrócił z wcześniejszej mapy).
	Synchronizuj z atlasem sieci	Synchronizuje zawartość okna **Widok sieci** z obiektem wybranym w oknie **Atlas sieci**.
	Znajdź	Umożliwia znalezienie węzła w wybranej mapie lub gdziekolwiek w atlasie.
	Edytuj mapę	Włącza lub wyłącza tryb edycji zawartości wyświetlanej mapy.
	Raporty dla mapy	Otwiera niezależną **Przeglądarkę raportów** służącą do oglądania i drukowania wygenerowanych w tej mapie raportów.
	Alerty mapy	Otwiera okno **Dziennik zdarzeń** dla wyświetlanej mapy.

	**Rozmieść węzły**	Umożliwia rozmieszczanie węzłów w oknie **Widok sieci**.
	**Właściwości mapy**	Wywołuje okno, w którym można zmieniać właściwości wybranej mapy.
	**Powiększ**	Zwiększa rozmiar wyświetlanej mapy.
	**Pomniejsz**	Zmniejsza rozmiar wyświetlanej mapy.
	**Powiększenie do 100%**	Ustawia powiększenie na domyślnej wartości 100%.
	**Dostosuj do rozmiaru okna**	Dostosowuje wyświetlaną mapę do rozmiaru, który umożliwia wyświetlenie wszystkich węzłów w oknie **Widok sieci**.
	**Stan węzła**	Wywołuje okno stanu wybranego węzła.
	**Sprawdź węzeł teraz**	Weryfikuje kondycję wybranego węzła, w tym stan monitorowanych na nim usług sieciowych i wskazania związanych z nim liczników wydajności.
	**Wykryj usługi sieciowe**	Wykrywa wszystkie usługi aktualnie działające na wybranym węźle.
	**SNMP**	Otwiera okno służące do przeglądania lub edytowania informacji SNMP dostępnych na wybranych węźle.
	**Wyślij wiadomość**	Umożliwia wysłanie wiadomości NetWare lub Windows do węzła.
	**Pełny ekran**	Przycisk ten umożliwia wyświetlenie oddokowanego okna **Widok sieci** na całym ekranie. Aby przełączyć się między widokiem normalnym a trybem pełnoekranowym, należy nacisnąć kombinację klawiszy **CTRL+ALT+F**.
	**Automatyczna szerokość kolumn**	Umożliwia ustawienie w programie, aby automatycznie dostosowywał szerokość kolumny dla tabeli w oknie **Widok sieci**.
	**Dostosuj kolumny**	Umożliwia dodawanie lub usuwanie kolumn z aktualnego widoku mapy w formacie tabeli.
	**Grupuj wg**	Umożliwia grupowanie węzłów wyświetlanych w formie tabeli w oparciu o właściwości jednego z pól tabeli.

Następujące ikony są dodatkowo dostępne w oknie Widoku sieci, w wypadku kiedy widok wydajności zawierający wykresy jest zaznaczony w oknie Atlasu sieci.

	**Wstaw wykres liniowy**	Dodaje wykres liniowy to bieżącego widoku wydajnościowego.
	**Wstaw wykres słupkowy**	Dodaje wykres słupkowy to bieżącego widoku wydajnościowego.
	**Wstaw wskaźnik**	Dodaje wskaźnik to bieżącego widoku wydajnościowego.
	**Właściwości panelu**	Otwiera panel z właściwościami wybranego wykresu liniowego, słupkowego lub wskaźnika na widocznym widoku wydajnościowym.
	**Historia licznika**	Otwiera **Przeglądarkę trendów**, gdzie można przeglądać szczegółową statystykę liczników dotyczącą bieżącego wykresu lub wskaźnika w wybranym widoku wydajnościowym.

	**Eksport trendów**	Pozwala wyeksportować trendy licznika dotyczącą wybranego wykresu do dowolnej zdalnej bazy danych SQL.

Karty w oknie Widok sieci

Karty znajdujące się w oknie **Widok sieci** pozwalają przełączać się między różnymi obiektami zawierającymi informacje na temat wybranej mapy. Dostępne są następujące rodzaje kart:

Mapa	Stanowi graficzną prezentację sieci. Mapę w tym widoku edytuje się, klikając ikonę **Edytuj mapę** w pasku narzędzi okna **Widok sieci**. Wszystkie węzły na wybranej mapie są wyświetlane za pomocą odpowiednich graficznych ikon, które uzależnione są od rodzaju węzła. Ponadto kolor tych ikon sygnalizuje stan węzła.
Szczegóły	Zawiera tabelaryczną listę węzłów składającą się z różnorodnych kolumn. Prezentowane informacje dotyczą statystyk i parametrów monitorowania dla każdego węzła.
Podsumowanie	Zestawia zbiorcze informacje o stanie mapy a także inne dane prezentowane na wykresach słupkowych.
Windows NT	Zawiera tabelę wyszczególniającą węzły działające pod kontrolą systemu operacyjnego z rodziny Windows NT (NT/2000/XP). Kolumny wyświetlają informacje otrzymane bezpośrednio od węzłów Windows.
NetWare	Zawiera tabelę wyszczególniającą węzły działające pod kontrolą systemu operacyjnego NetWare, od wersji 4.11 wzwyż. Kolumny wyświetlają informacje otrzymane bezpośrednio od węzłów NetWare.
SNMP	Zawiera tabelę wyszczególniającą węzły z działającymi agentami SNMP. Kolumny wyświetlają informacje otrzymane bezpośrednio od agentów SNMP na węzłach.

Informacje prezentowane w tabelach Szczegóły, Windows NT, NetWare i SNMP można wygodnie przegrupowywać. Dane na każdej tabeli można sortować (klikając na odpowiedni nagłówek kolumny); można też dostosowywać okno **Widok sieci**, dodając bądź usuwając z niego kolumny. Ponadto informacje w tabelach można grupować w sekcje na podstawie kilku kolumn. Użytkownik może tworzyć własne reguły filtrowania określając, co ma być wyświetlane w każdej z czterech stron tabeli. Więcej informacji na ten temat zawiera sekcja *Dostosowywanie tabel* na stronie 51.

Informacje na karcie Szczegóły

Tabela Szczegóły zawiera następujące informacje (w porządku alfabetycznym):

Adres	Oznacza adres IP węzła.
Adres MAC	Określa unikatowy numer seryjny karty Ethernet urządzenia; numer ten służy do odróżniania karty sieciowej w węźle od innych. Adres MAC jest uzyskiwany w NetCrunchu jedynie w kontekście sieci lokalnych.
Alerty	Pokazuje liczbę nieprzyjętych alertów (uprzednio zdefiniowanych w węźle), które zostały odnotowane w węźle.

Interfejsy	Wyszczególnia interfejsy sieciowe na węźle. Dotyczy to jedynie węzłów z uruchomionymi agentami SNMP, w których dodatkowo poprawnie określono Wspólnotę odczytu.
Lokalizacja	Precyzuje umiejscowienie węzła w sieci. Wartość ta jest otrzymywana automatycznie z węzła za pośrednictwem SNMP. Nazwy lokalizacji mogą być używane w charakterze kryteriów wyboru przy tworzeniu dynamicznych map w sekcji *Widoki własne* okna **Atlas sieci**.
Maks. RTT	Określa maksymalny czas odpowiedzi wysyłanych pakietów (w milisekundach).
Monitorowanie uproszczone	Wskazuje, czy włączona jest opcja monitorowania uproszczonego.
Nazwa	Informuje o nazwie DNS węzła.
Nie odpowiada od	Wskazuje okres czasu, w którym węzeł nie odpowiadał.
Ostatni alert	Pokazuje dokładny czas wystąpienia w węźle ostatniego alertu.
Ostatnia odpowiedź	Pokazuje dokładny czas i datę otrzymania od węzła ostatniej odpowiedzi.
% Czas działania	Określa procentowy czas niezakłóconego działania węzła.
% Dostępności	Określa procentowy czas, w którym węzeł odpowiadał poprawnie. Parametr ten bierze pod uwagę okres czasu, w którym NetCrunch monitorował dany węzeł.
% Utraconych	Oznacza procent pakietów utraconych w czasie monitorowania.
Stan monitorowania	Wskazuje aktualny status monitorowania węzła (włączony, wyłączony lub trwa oczekiwanie na odpowiedź).
System	Informuje, jaki system operacyjny jest aktualnie uruchomiony w węźle. Informacja ta jest dostępna jedynie dla węzłów z włączonymi agentami SNMP, w których określono Wspólnotę odczytu.
Średni RTT	Oznacza średni czas odpowiedzi (w milisekundach) wszystkich pakietów wysyłanych do węzła.
Typ	Pokazuje rodzaj węzła i przypisaną mu ikonę.
Usługi	Wyszczególnia usługi aktualnie monitorowane w węźle. Domyślnie w węźle monitorowana jest usługa sieciowa PING; w razie potrzeby można dodać dowolne inne usługi.
Wspólnota odczytu	Informuje, jakiej Wspólnoty odczytu używa węzeł zarządzany przy użyciu SNMP.
Wspólnota zapisu	Określa Wspólnotę zapisu węzła zarządzanego przez SNMP.

Informacje na karcie Windows NT

Tabela Windows NT wyświetla następujące kolumny (wyszczególnione poniżej w porządku alfabetycznym):

Adres	Adres IP węzła Windows.
Czas monitorowania	Informuje, jaki jest interwał monitorowania wydajności Windows w węźle. Jeśli wartość ta nie została określona, używany jest ogólny interwał monitorowania dla węzła.

Czas odczytu danych wydajności (ms)	Określa w milisekundach, że NetCrunch odebrał informacje nt wydajności systemu Windows na węźle.
Domena	Nazwa domeny Windows, do której należy węzeł.
Komputer	Nazwa lub adres IP urządzenia.
Liczba bajtów na sek.	Całkowita liczba bajtów przesłanych przez interfejs/interfejsy sieciowe na węźle podczas jednosekundowego interwału.
Nazwa NetBIOS	Nazwa NetBIOS urządzenia – o ile ma zastosowanie.
Ostatni błąd	Określa rodzaj błędu, jaki po raz ostatni został odebrany z węzła podczas próby do zalogowania się.
Ostatnia odpowiedź	Określa czas uzyskania ostatniej odpowiedzi z węzła systemu Windows.
% Obciążenia procesora	Procent czasu, w którym procesor węzła znajdował się w użyciu.
% Obciążenia sieci	Procentowe obciążenie sieci generowane przez węzeł.
% Wykorzystania pamięci	Procent czasu, w którym pamięć dostępna w węźle była wykorzystywana w określonym przedziale czasu.
Rozmiar danych wydajności	Określa rozmiar w bajtach danych wydajności systemu Windows, jakie zostały odczytane od węzła po raz ostatni.
Sesje	Liczba aktywnych sesji w węźle Windows.
Stan logowania	Aktualny stan zalogowania węzła. Możliwe są następujące stany: POŁĄCZONY, TRWA ŁĄCZENIE, NIEPOPRAWNE HASŁO i NIEDOSTĘPNY.
Stan monitorowania	Stan monitorowania węzła. Gdy węzeł znajduje się w stanie *Trwa oczekiwanie na odpowiedź*, jakiekolwiek monitorowanie i alertowanie jest wyłączone, a sprawdzany jest jedynie stan PING-a lub innej usługi wiodącej.
System	Informuje, jaki system operacyjny działa w węźle.
Zalogowany użytkownik	Nazwa logowania użytkownika domeny Windows w węźle. W celu logowania się w węźle NetCrunch używa domyślnej nazwy użytkownika i hasła, określonej w opcjach programu. Aby zalogować się w węźle za pomocą innej nazwy użytkownika i hasła, kliknij prawym przyciskiem myszy na tę nazwę i wybierz opcję menu **Monitorowanie ► Wydajność Windows**. W wywołanym oknie określ nową nazwę użytkownika i hasło.

Informacje na karcie NetWare

Tabela na stronie NetWare umożliwia dostosowywanie następujących kolumn (wyszczególnionych poniżej w porządku alfabetycznym):

Adres	Adres TCP/IP lub IPX/SPX węzła (w zależności od tego, który z nich jest używany przez określone urządzenie NetWare).
Czas monitorowania	Informuje, jaki jest interwał monitorowania wydajności NetWare w węźle. Jeśli wartość ta nie została określona, używany jest domyślny interwał monitorowania dla węzła.
Drzewo	Określa drzewo eDirectory, do którego zalogowany jest węzeł.
Liczba połączeń	Liczba połączeń NetWare z serwerem.

Nazwa eDirectory	Określa nazwę eDirectory, do jakiej należy węzeł.
Ostatni błąd	Określa rodzaj błędu, jaki po raz ostatni został odebrany z węzła podczas próby do zalogowania się w drzewie NetWare.
Ostatnia odpowiedź	Określa czas uzyskania ostatniej odpowiedzi z węzła systemu NetWare.
% Wykorzystania	Licznik właściwy systemowi NetWare; określa procent czasu, w którym serwer znajdował się w użyciu.
Protokół	Protokół używany przez węzła w komunikacji sieciowej (możliwy jest albo TCP/IP albo IPX/SPX).
Serwer	Nazwa NetWare węzła lub odpowiadający jej adres sieciowy.
Stan monitorowania	Stan monitorowania węzła. Gdy znajduje się on w stanie *Trwa oczekiwanie na odpowiedź*, wszelkie monitorowanie i alertowanie jest wyłączone, a sprawdzany jest jedynie stan PING-a lub innej usługi wiodącej.
Status	Określa jeden z następujących stanów węzła NetWare: *połączony*, *zalogowany* lub *wyłączony*.
System	Aktualna wersja systemu operacyjnego NetWare uruchomionego w węźle.
Typ	Rodzaj połączenia z węzłem. Możliwe rodzaje to albo bezpośrednio z NDS-u, albo za pomocą bazy obiektów sieci (Bindery).
Zalogowany użytkownik	Nazwa użytkownika aktualnie zalogowanego w węźle NetWare. W celu logowania się w węźle NetCrunch używa domyślnej nazwy użytkownika i hasła, określonej w opcjach programu. Aby zalogować się w węźle za pomocą innej nazwy użytkownika i hasła systemu NetWare, kliknij prawym przyciskiem myszy na tę nazwę i wybierz opcję menu **Monitorowanie ► Wydajność NetWare**.W wywołanym oknie określ nową nazwę użytkownika i hasło dla NetWare.
Żądania/sek.	Całkowita liczba pakietów NCP żądanych na węźle podczas jednosekundowego interwału.

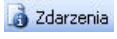
Informacje na karcie SNMP

Kliknięcie karty SNMP w oknie **Widok sieci** wyświetla informacje o węzłach uzyskane w nich bezpośrednio od agentów SNMP. Tabela zawiera następujące kolumny (wyszczególnione poniżej w porządku alfabetycznym):

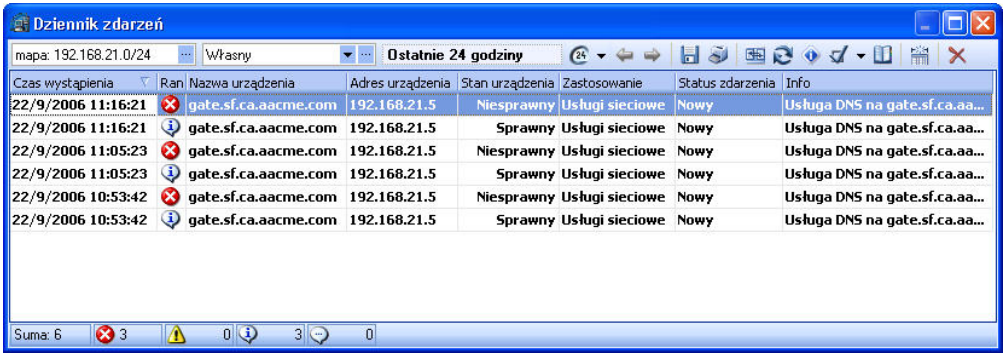
Adres	Adres TCP/IP lub IPX/SPX węzła.
Czas działania	Dokładna ilość czasu, w którym węzeł był dostępny i odpowiadał. Uwaga: wartość ta nie zależy od tego, czy i jak długo działał NetCrunch – jest ona przechowywana na samym węźle w postaci danych SNMP.
Czas monitorowania	Informuje, jaki jest interwał monitorowania wydajności SNMP w węźle. Jeśli wartość ta nie została określona, używany jest ogólny interwał monitorowania dla węzła.
Komputer	Nazwa lub adres IP węzła.
Liczba procesów	Liczba procesów aktualnie mających miejsce w węźle.

Liczba użytkowników	Liczba użytkowników aktualnie przyłączonych do węzła.
Nazwa DNS	Nazwa serwera DNS w notacji kropkowej.
Nazwa systemu	Nazwa sieciowa urządzenia, zdefiniowana w SNMP.
Ostatnia odpowiedź	Określa czas uzyskania ostatniej odpowiedzi węzła.
Stan monitorowania	Stan monitorowania węzła. Gdy ma on wartość *Trwa oczekiwanie na odpowiedź*, wszelkie monitorowanie i alertowanie jest wyłączone, a sprawdzany jest jedynie stan PING-a lub innej usługi wiodącej.
Stan połączenia	Stan połączenia (status logowania) węzła. Możliwe są trzy stany: *połączony*, *niepoprawna wspólnota* lub *niedostępny*.
Suma przesłanych bajtów	Całkowita liczba bajtów wysłanych lub otrzymanych przez interfejsy sieciowe w węźle.
Wspólnota	Nazwa wspólnoty SNMP określonej w węźle. Nazwy te są swego rodzaju hasłem – ich znajomość jest niezbędna do uzyskania dostępu do danych SNMP w sieci.

Okno Dziennik zdarzeń



Klikając ikonę ***Zdarzenia*** na głównym pasku narzędzi otwiera okno o nazwie **Dziennik zdarzeń**. Okno umożliwia zarządzanie zdarzeniami przetwarzanymi w programie, a więc zdarzeniami wewnętrznymi generowanymi przez NetCruncha – i zewnętrznymi, pochodzącymi z innych źródeł, np. z trapu SNMP. Wszystkie zdarzenia są przechowywane w SQL-owej bazie zdarzeń, a wszelkie zapytania bazy danych są wyświetlane w oknie **Dziennik zdarzeń**.



Rys. 6 Okno Dziennik zdarzeń

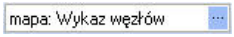
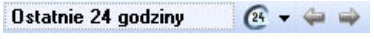
Okno **Dziennik zdarzeń** (zob. Rys. 6) składa się z paska narzędzi, tabeli zdarzeń prezentującej szczegóły dotyczące zdarzenia, i panelu podglądu (widocznego lub ukrytego). Panel podglądu umożliwia szybki dostęp do istotnych informacji o wybranym zdarzeniu (takich jak np. ustawione parametry i wykonane akcje alertujące).

Pasek narzędzi Dziennika zdarzeń

Rys. 7 Przykładowy pasek narzędzi Dziennika zdarzeń

Poza prezentacją listy często używanych ikon, pasek narzędzi Dziennika zdarzeń pełni kilka innych funkcji. Umożliwia zmianę zakresu wyświetlanych danych, czyli np. sprecyzowanie, jakie zdarzenia z danej mapy/widoku, grupy lub pojedynczego węzła powinny być wyświetlane. Następnie pozwala wybrać widok bazy danych i/lub utworzyć własny widok na podstawie wielu kryteriów. Istnieje także opcja modyfikowania zakresu czasu i interwału, dla których mają być wyświetlane przetworzone zdarzenia.

Poniższa tabela opisuje trzy części paska narzędzi pełniące powyższe funkcje.

	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 użyć ikony ***Wybierz zakres danych***.
	Informuje o aktualnie wybranym rodzaju widoku, a także umożliwia utworzenie lub wybranie innego rodzaju widoku. Aby wybrać istniejący widok, należy użyć 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***.

Poniższa tabela opisuje ikony wyświetlane w pasku narzędzi Dziennika zdarzeń:

	**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**	Umożliwia ustawienie w programie, aby automatycznie dostosowywał szerokość kolumny dla tabeli w oknie **Dziennika zdarzeń**.
	**Usuń**	Usuwa wybrane zdarzenie z bazy danych.

Kolumny tabeli Dziennika zdarzeń

Tabela ta wyświetla zdarzenia przetworzone przez program. Składa się z następujących kolumn (wyszczególnionych w porządku alfabetycznym):

Adres urządzenia	Adres IP węzła, w którym nastąpiło zdarzenie.
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.
Identyfikator zdarzenia	Numer identyfikacyjny zdarzenia, odróżniający go od innych zdarzeń (pochodzących z aplikacji zewnętrznych). W aktualnej wersji programu wszystkie zdarzenia wewnętrzne, wygenerowane przez program, mają identyfikator równy 0.
Info	Krótki opis zdarzenia.
Kategoria	Dodatkowa kategoria, do której należy wygenerowane zdarzenie (np. Inicjalizacja, Sieć lub Pamięć).
Nazwa urządzenia	Nazwa węźła, w którym nastąpiło zdarzenie.
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.
Opis	Krótki tekst opisujący zdarzenie. Jest on określany przez użytkownika podczas definicji danego zdarzenia.

Rodzaj	Nazwa opisująca rodzaj zdarzenia, zgodnie z określeniem, które zostało podane w polu **Opis** podczas definiowania danego zdarzenia.
Rodzaj zdarzenia	Określa typ zdarzenia, do którego należy dane zdarzenie (np. *Stan węzła* lub *Stan usługi sieciowej*).
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.
Status zdarzenia	Aktualny status zdarzenia. Stan taki może przybierać następujące wartości: tuż po wystąpieniu zdarzenia określane jest ono jako *Nowy*, natomiast później, podczas korzystania z okna **Dziennik zdarzeń**, jego stan może zostać zmieniony i na przykład może on przybrać status *Przyjęty* lub *Zamknięty*.
Ranga	Stopień ważności zdarzenia, zgodnie z tym, który został podany podczas definiowania danego zdarzenia (ranga zdarzenia może przyjąć następujące wartości: KRYTYCZNA, OSTRZEŻENIE, INFORMACYJNA lub NIEISTOTNA).
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**.
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.
Źródło	Nazwa podsystemu, który wygenerował dane zdarzenie w węźle (np. serwer DNS lub serwer sieci WWW).

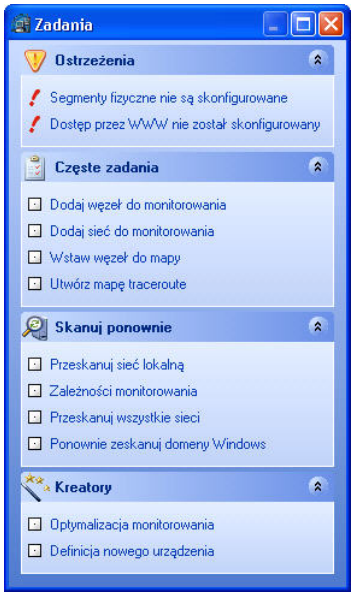
Właściwą liczbę kolumn wyświetlanych w widoku dziennika zdarzeń można dostosowywać (Kolumny są wybierane lub usuwane podczas tworzenia/edycji widoków własnych definiowanych przez użytkowników.) Ponadto jedno kliknięcie nagłówka kolumny umożliwia sortowanie informacji o zdarzeniach.

Lista okien

Aby wyświetlić listę okien, należy z menu **Widok** wskazać pozycję **Lista okien**. Okno to pełni funkcję wykazu otwartych okien programu, które aktualnie nie są zadokowane w obszarze dokowania, którego częścią jest okno **Lista okien**. Aby wyświetlić ukryte okno, kliknij jego nazwę w liście okien.

Okno Zadania

Aby wyświetlić okno o nazwie **Zadania**, należy w menu **Widok** wskazać pozycję menu **Zadania**. Daje ono natychmiastowy dostęp do najczęściej używanych lub najbardziej przydatnych funkcji i kreatorów programu. Pozwala również skonfigurować segmenty fizyczne i dostęp poprzez WWW (z sekcji **Ostrzeżenia**). W tym celu wystarczy kliknąć żądaną funkcję lub kreatora.



Rys. 8 Okno Zadania

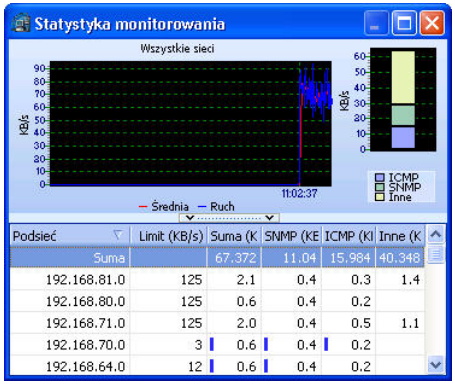
Poniższa tabela zestawia wszystkie funkcje programie dostępne poprzez kliknięcie okna **Zadania**:

Definicja nowego urządzenia	Tworzy definicję nowego urządzenia, dzięki czemu NetCrunch będzie poprawne rozpoznawał dane urządzenie.
Dodaj sieć do monitorowania	Uruchamia *Kreatora wykrywania sieci* służącego do dodawania nowych zdalnych sieci do monitorowania. Istnieje kilka opcji pozwalający na określenie, które nowo wykryte węzły w sieci mają być dodawane do listy monitorowanych węzłów.
Dodaj węzeł do monitorowania	Wprowadza nowy węzeł do monitorowania. Jeśli węzeł należy do nieznanej (tj. aktualnie nie monitorowanej) sieci IP, sieć taka zostanie dodana do sekcji *Sieci IP* w oknie **Atlas sieci**.
Optymalizacja monitorowania	Umożliwia wybór strategii monitorowania dla aktualnie otwartego atlasu.
Przeskanuj sieć lokalną	Powtórnie skanuje – w celu wykrycia nowych węzłów – aktualnie monitorowaną sieć lokalną.
Przeskanuj wszystkie sieci	Powtórnie skanuje aktualnie zdefiniowane lokalne i zdalne sieci w celu wykrycia nowych węzłów.
Ponownie przeskanuj domeny Windows	Powtórnie skanuje wszystkie aktualnie wykryte domeny Windows.
Utwórz mapę Traceroute	Tworzy mapę trasy pakietów z lokalnego komputera, na którym uruchomiony jest NetCrunch, do wybranego urządzenia.

Wstaw węzeł do mapy	Umieszcza węzła w mapie aktualnie wybranej w oknie **Atlas sieci** (jej zawartość wyświetlana jest w oknie **Widok sieci**).
Zależności monitorowania	Otwiera okno **Zależności monitorowania**, w którym można ustawiać zależności monitorowania między węzłami atlasu.

Okno Ruch monitorowania

Aby otworzyć okno **Statystyka monitorowania**, należy z menu **Widok** kliknąć pozycję **Statystyka monitorowania**. Pozwala ono przeglądać aktualne statystyki dla poszczególnych podsieci związane z ruchem w sieci generowanym przez proces monitorowania – lub inne operacje wykonywane przez NetCruncha. Ponadto dla każdej monitorowanej sieci można ustawić limit ruchu w sieci, którego program nie może przekroczyć podczas monitorowania. Funkcja ta jest szczególnie przydatna, gdy istnieje potrzeba kontrolowania i ograniczania ilości ruchu w sieci. Ustawiając maksymalne wartości, użytkownik zyskuje gwarancję, że monitorowanie NetCruncha nigdy nie będzie nadmiernie obciążać wydajności całej sieci.



Rys. 9 Okno Statystyka monitorowania

Okno to składa się z dwóch sekcji (porównaj Rys. 9).

Panel wyświetlania	Ilustruje na wykresie aktualne statystyki podsieci, która została wskazana w znajdującej się pod panelem tabeli. Na panel składają się dwa osobne wykresy. Pierwszy wyświetla dane o ruchu do wybranej podsieci, drugi zaś pokazuje średni poziom ruchu do tej sieci.
Tabela podsieci	Wskazuje aktualną ilość ruchu przychodzącego do wszystkich podsieci (wyświetlanych w osobnych rzędach tabeli). Dostępne w tabeli pola to *Suma*, *SNMP*, *ICMP* oraz *Inne*. Ponadto tabela informuje, czy na danej podsieci został zdefiniowany jakiś limit, oraz pokazuje całkowitą ilość ruchu monitorowania wywołanego przez program.

Uwaga

W aktualnie monitorowanych w programie podsieciach można ustawić limit ruchu sieciowego, którego NetCrunch nie powinien przekraczać. W tym celu należy kliknąć prawym przyciskiem myszy nazwę podsieci w tabeli i wybrać stosowną opcję.

Wykrywanie struktury sieci

Pierwsze uruchomienie programu wywołuje *Kreatora wykrywania sieci*, który umożliwia utworzenie atlasu sieci. Po wykonaniu tej procedury można natychmiast przystąpić do zadań związanych z wizualizacją, alertowanie i raportowaniem.

Tworzenie map sieci

Rysowanie map sieci to zasadnicza – a zarazem często używana – funkcja programu. Bez utworzenia mapy sieci nie jest możliwe pełne korzystanie z programu, gdyż wówczas nie będą istnieć węzły podlegające monitorowaniu i raportowaniu. Automatyczne wykrywanie sieci IP (przy użyciu *Kreatora wykrywania sieci*) odbywa się podczas uruchamiania programu po raz pierwszy lub podczas definiowania nowej sieci IP.

Wykonanie procedury automatycznego wykrywania prowadzi do utworzenia graficznej reprezentacji sieci zawierającej zestaw map. *Kreator wykrywania sieci* tworzy mapy logiczne w sekcji *Sieci IP* (a uściślając, w podsekcjach *Lokalne* i *Zdalne*). Jednocześnie w sekcji *Widoki własne* okna **Atlas sieci** umieszczane są dwie domyślne grupy: *Domeny Windows* (wyszczególniające mapy węzłów należących do Domen Windows istniejących w sieci IP) i *eDirectory* (zawierające węzłów należących do eDirectory istniejących w sieci IP).

Po wstępnym przeprowadzeniu wykrycia struktury sieci, można rozpocząć tworzenie widoków własnych świeżo wykrytej i naniesionej na mapę sieci IP. Widoki własne mogą przybrać postać widoków filtrowanych lub pierwotnie pustych map. W późniejszym czasie można ponownie uruchomić *Kreatora wykrywania sieci* w celu otrzymania kolejnej sieci IP, która nie została jeszcze zeskanowana przez program i ukazana na mapie.

Wstępne wykrywanie sieci

Wykrywanie sieci odbywa się podczas pierwszego uruchomienia programu. Skanujący sieci IP *Kreator wykrywania sieci* udostępnia szeroką gamę opcji i przechowuje rezultaty przeszukiwania sieci w nowym atlasie. Atlas ten zapisuje wszelkie informacje związane z określoną mapą, w tym grupy, mapy, węzły, ich określone położenie na mapie i w innych obiektach.

Kreator umożliwia wykrycie sieci na dwa sposoby: ręczny i automatyczny. Metoda automatyczna jest zalecana, gdy zachodzi potrzeba szybkiego utworzenia atlasu sieci za pomocą zestawu wstępnie zdefiniowanych w programie reguł. W tym wypadku kreator programu będzie wyszukał węzły posiłkując się różnorodnymi metodami (np. SNMP, eDirectory, Active Directory i Domeny Windows), a następnie rozmieści je na mapach. Określi również, które usługi sieciowe powinny być monitorowane na każdym wykrytym węźle atlasu.

Ręczne wykrywanie sieci umożliwia wybór różnorodnych opcji. Użytkownik ma do wyboru trzy metody: Ping, Domeny/Grupy robocze Windows i eDirectory i może np. zdecydować się na wszystkie z nich. Może również określić listę usług sieciowych, które automatycznie będą monitorowane na każdym wykrytym węźle.

Poniższe dwie sekcje tego poradnika przedstawiają szczegółowe przykłady tego, jak używać *Kreatora wykrywania sieci* w zależności od rozmiaru sieci. W pierwszym scenariuszu NetCrunch będzie monitorował względnie małą lub średnią sieć firmową. Zostanie wówczas użyta metoda automatycznego wykrywania sieci, znacznie przyspieszająca utworzenie nowego atlasu. Drugi scenariusz pokaże, jak ustawić parametry przy wykrywaniu sieci o większych rozmiarach, zawierającej sporą liczbę węzłów takich jak serwery, przełączniki i stacje robocze. Ponieważ w takim przypadku procedura wykrywania sieci jest bardziej złożona, zostanie użyta ręczna metoda wyboru opcji kreatora, która daje użytkownikowi większe pole manewru w konfiguracji parametrów skanowania.

Wykrywanie niewielkiej lub średniej sieci

Załóżmy, że mała sieć firmowa zawiera do 500 węzłów takich jak rutery, serwery, przełączniki i stacje robocze. 25 węzłów spośród tej pięćsetki ma znaczenie krytyczne – zazwyczaj są nimi serwery, rutery i przełączniki. Przyjmijmy także, że sieć średniej wielkości składa się z 2000 węzłów, z których około 100 pełni strategiczne funkcje – innymi słowy, od ich stabilnego funkcjonowania uzależniona jest wydajność i dostępność całej sieci. Każda ilość węzłów przekraczająca tę granicę oznacza, że mamy do czynienia z dużą siecią.

Zanim jednak uruchomimy program po raz pierwszy i przejdziemy do skanowania sieci, należy przyjąć strategię określającą, jak poprawnie i optymalnie wykryć – a następnie monitorować – małą lub średnią sieć firmową. Następnie – już w *Kreatorze wykrywania sieci* – należy zdecydować, czy program ma wykrywać wszystkie typy węzłów, czy tylko te krytyczne, a więc serwery i rutery. Ponieważ mała lub średnia sieć zawiera nie więcej niż 2000 węzłów, zaleca się wybór opcji wykrywania węzłów wszystkich typów.

W przypadku małej sieci sugerowane jest wybranie w *Kreatorze wykrywania sieci* opcji monitorowania wszystkich węzłów w pełnym zakresie. Natomiast dla średnich sieci lepszym wyjściem może okazać się monitorowanie jedynie ważnych węzłów: serwerów i ruterów i wówczas należy wybrać odpowiednią opcję kreatora. W takim wypadku NetCrunch będzie monitorował w pełnym zakresie wszystkie krytyczne węzły, które zostały wykryte. Uściślając, na węzłach tego typu będzie można monitorować ich liczniki wydajności (SNMP, Windows i/lub NetWare) i wykryte usługi sieciowe, a także wykonywać zadania związane z alertowaniem i raportowaniem. W przypadku pozostałych węzłów – np. stacji roboczych – monitorowany będzie tylko ich status (odpowiada/nie odpowiada), natomiast nie będą mierzone wskazania żadnych liczników wydajności i usług sieciowych. Ponadto, dla nieistotnych węzłów wyłączone będzie alertowanie i raportowanie.

Już po wykryciu sieci i utworzeniu atlasu z mapami dla mniej ważnych węzłów – takich jak np. stacje robocze – w dowolnym momencie można indywidualnie zmodyfikować opcje monitorowania, przykładowo włączając w nich monitorowanie usług sieciowych i liczników wydajności.

Podsumowując, w przypadku małych i średnich sieci sugerowane jest, aby program:

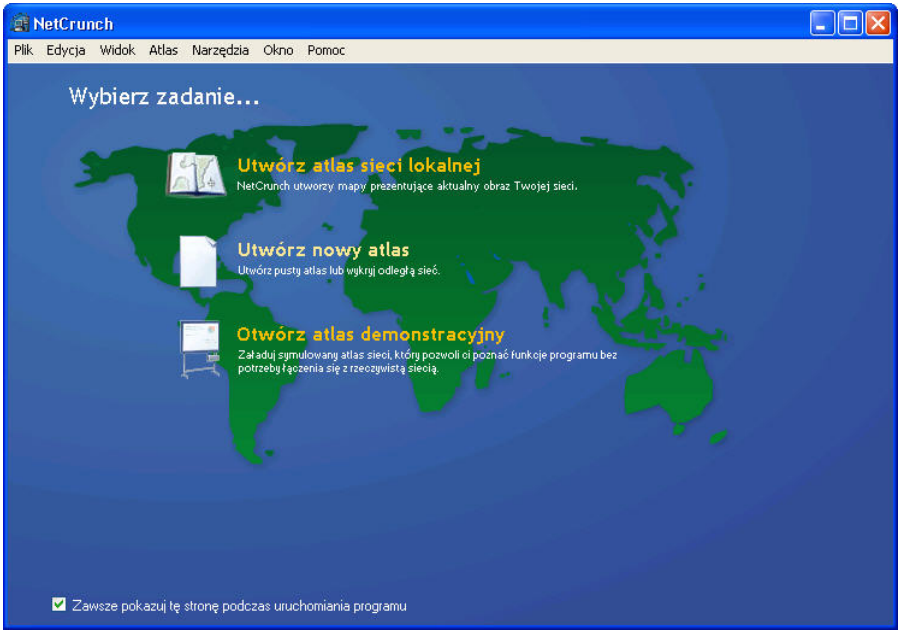
- Automatycznie wykrywał sieć przy użyciu domyślnych ustawień kreatora,
- Wykrywał wszystkie rodzaje węzłów.

Dodatkowo, kiedy atlas zostanie utworzony, tylko krytyczne węzły będą monitorowane w pełnym zakresie.

Szczegółowe instrukcje

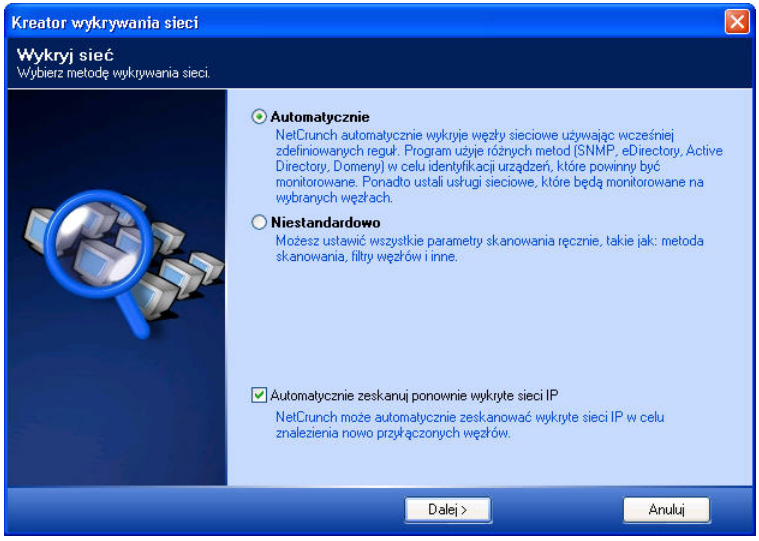
Aby wykryć małą/średnią sieć

1. Uruchom NetCruncha po raz pierwszy. Otworzy się ekran *Wybierz zadanie*, przedstawiony na Rys. 10.



Rys. 10 Ekran *Wybierz zadanie*

2. Aby utworzyć nowy atlas, wybierz opcję **Utwórz atlas sieci lokalnej**.
Otworzy się pierwsze okno *Kreatora wykrywania sieci* przedstawione na Rys. 11.



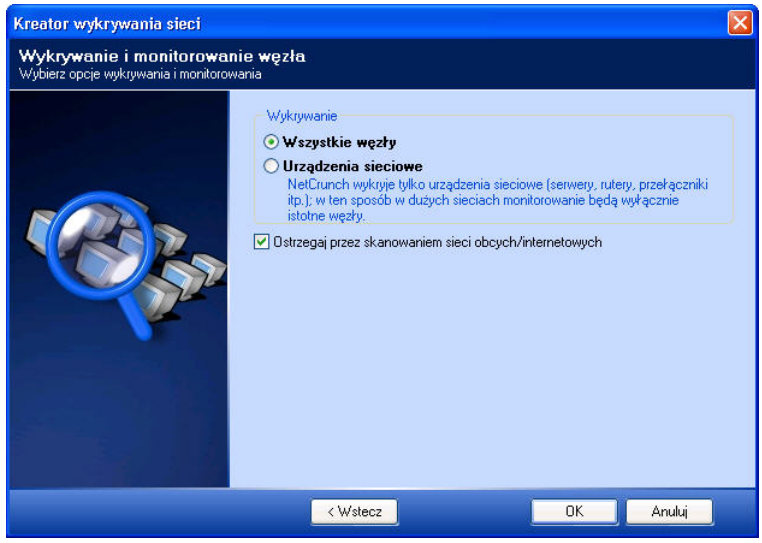
Rys. 11 Pierwszy ekran *Kreatora wykrywania sieci*

3. Ponieważ wykrywana ma być mała lub średnia sieć, wybierz przycisk opcji **Automatycznie**.

Uwaga

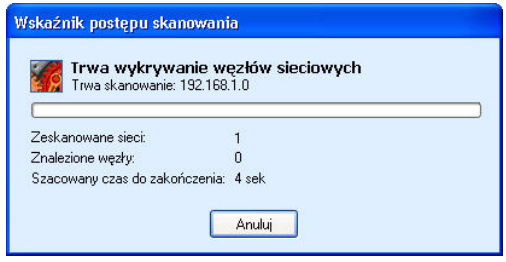
*Jednocześnie zaznacz pole wyboru **Automatycznie zeskakuj ponownie wykryte sieci IP**. Pozwala to później programowi automatycznie przeskanować wykryte sieci w określonych odstępach czasu.*

4. Kliknij przycisk **Dalej**.
   Otworzy się ekran *Wykrywanie i monitorowanie węzłów*, jak widać na Rys. 12.



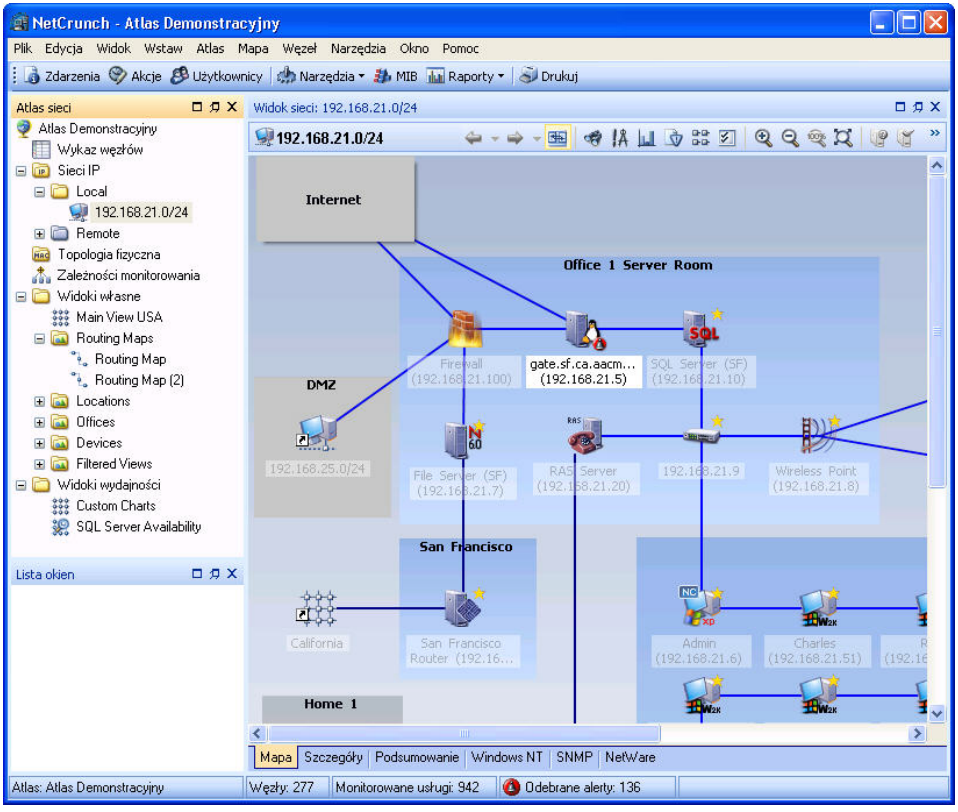
Rys. 12 Ekran Wykrywanie i monitorowanie węzłów

5. W polu **Wykrywanie** okna wybierz przycisk opcji **Wszystkie węzły**.
6. Kliknij **OK**, aby zamknąć *Kreatora wykrywania sieci*.
   NetCrunch przystąpi do wykrywania sieci lokalnej, wyświetlając okno **Wskaźnik postępu skanowania**, jak widać na Rys. 13.



Rys. 13 Okno wskaźnika postępu skanowania

7. Po zakończeniu skanowania sieci (może to potrwać od kilku sekund do kilkunastu minut w zależności od liczby węzłów w danej sieci), zostanie utworzony nowy atlas, zawierający wszystkie wykryte mapy sieci i węzły, jak widać na Rys. 14.



Rys. 14 Ekran nowego Atlasu sieci

Uwaga

Więcej informacji o korzystaniu z funkcji i kreatorów programu udostępnia ***Podręcznik użytkownika*** *programu NetCrunch.*

Wykrywanie dużej sieci

Duża sieć firmowa zawiera od 2000 do 5000 i więcej węzłów, z których mniej więcej 250 to węzły o krytycznym znaczeniu: serwery, rutery lub przełączniki. W sieci o takich rozmiarach użycie *Kreatora wykrywania sieci* wymaga przyjęcia odmiennej strategii.

Sugerowane jest wybranie metody ręcznej konfiguracji opcji w kreatorze. W ten sposób można wybrać metodę wykrywania, filtry dla wyszukiwanych węzłów i listę usług sieciowych, które mają podlegać skanowaniu. W kontekście metod wykrywania istnieje możliwość wyboru jednej, wielu lub wszystkich z następujących opcji: Ping (wówczas zastosowany zostanie protokół ICMP), Domeny i Grupy robocze Windows i katalogi eDirectory. Jeśli skanowanie ma obejmować Domeny i Grupy robocze Windows i eDirectory, można wówczas precyzyjnie określić, które kontenery domen Windows i eDirectory powinny być skanowane podczas wyszukiwania węzłów. Taka możliwość okaże się szczególnie przydatna właśnie w dużych sieciach, gdzie w domenach Windows i katalogach eDirectory z reguły istnieje kilka kontenerów i tylko niektóre z nich mają istotne znaczenie.

Ponadto możliwe jest wybranie protokołu SNMP jako metody uzyskania dodatkowych informacji o znalezionych węzłach, a także określenie konkretnych wspólnot odczytu SNMP, które powinny zostać wykorzystane do uzyskania tych informacji. Istnieje też możliwość uruchomienia skanowania sieci sąsiednich i użycia kryteriów filtrowania węzłów za pomocą SNMP. Kolejnym zaleceniem przy skanowaniu dużej sieci jest zmiana listy usług sieciowych, które mają być wykrywane
w węzłach.

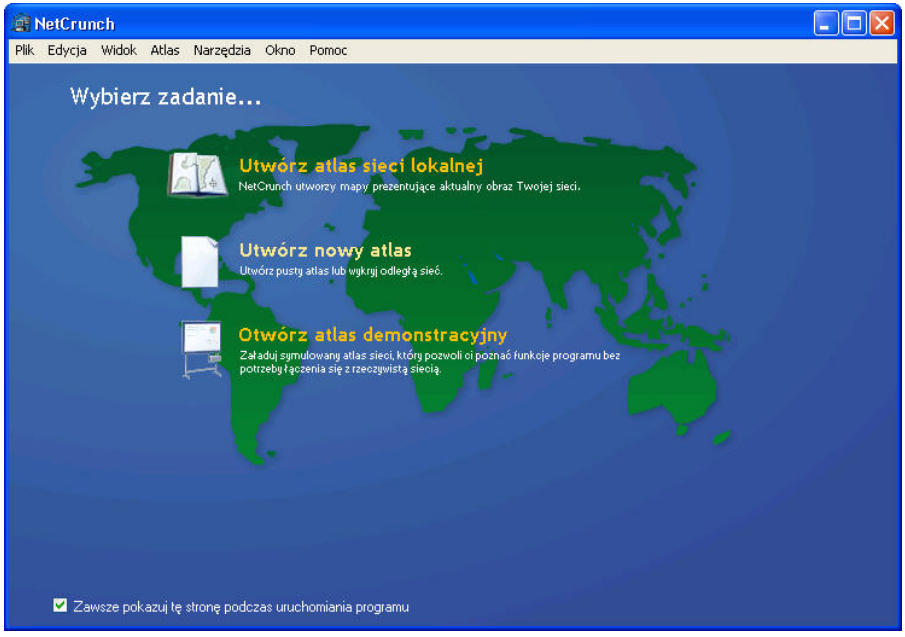
Podsumowując, w dużych sieciach firmowych warto tak ustawić program, aby:

- Wykrywał sieć używając opcji niestandardowo (ręcznie) wybranych przez użytkownika,
- Użył wszystkich trzech metod wykrycia (Ping, Domeny/Grupy robocze Windows i katalogi eDirectory),
- Użył wszystkich stosownych wspólnot odczytu SNMP,
- Nie skanował sieci sąsiednich,
- Wykrywał wyłącznie węzły spełniające kryteria filtrowania SNMP,
- Monitorował jedynie węzły krytyczne,
- Sprawdzał w każdym wykrytym węźle usługi sieciowe wyszczególnione na liście,
- Jeżeli jest to istotne, również zdefiniuj listę węzłów, które powinny być ominięte z procesu wykrywania.

Szczegółowe instrukcje

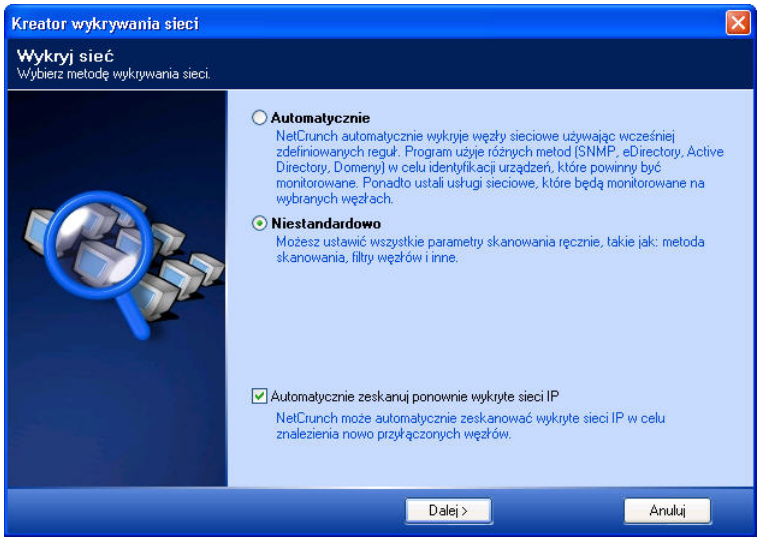
Aby wykryć dużą sieć

1. Uruchom po raz pierwszy NetCruncha. Otworzy się ekran **Wybierz zadanie**, jak na Rys. 15.



Rys. 15 Okno wyboru zadań

2. Aby utworzyć nowy atlas, wybierz opcję **Utwórz atlas sieci lokalnej**.
Otworzy się pierwsze okno *Kreatora wykrywania sieci* przedstawione na Rys. 16.



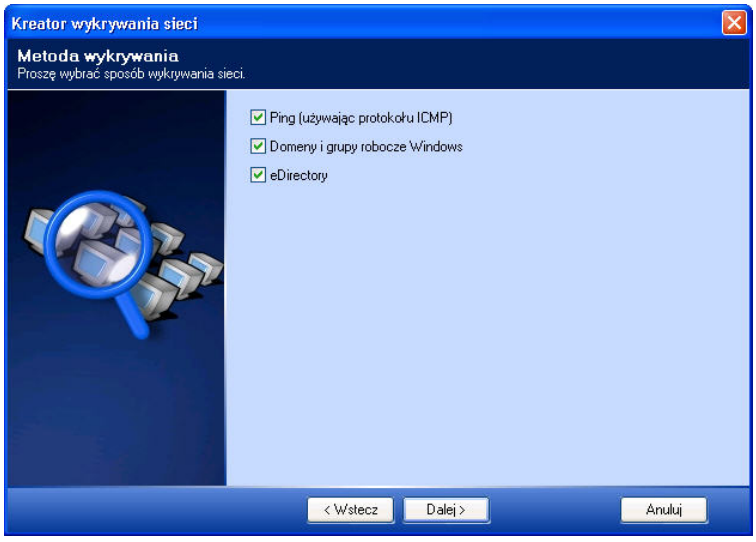
Rys. 16 Pierwszy ekran *Kreatora wykrywania sieci*

3. Ponieważ wykrywana jest sieć o dużych rozmiarach, wybierz przycisk opcji **Niestandardowo**.

Uwaga

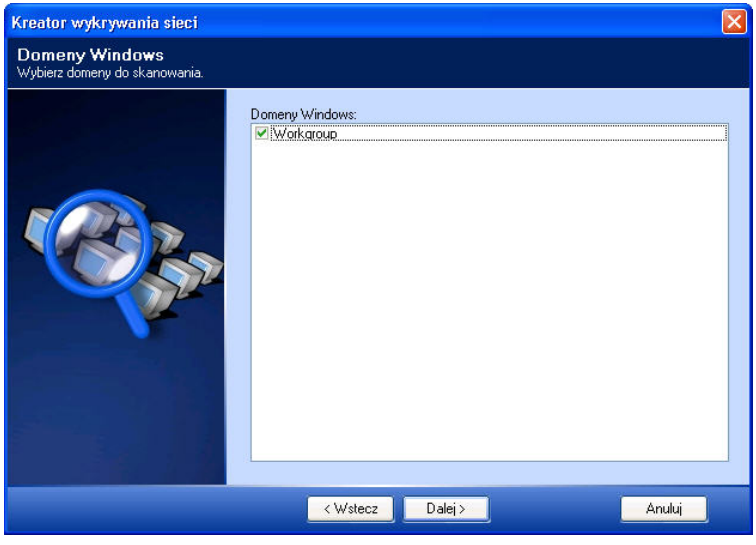
*Dodatkowo odznacz pole wyboru **Automatycznie zeskakuj ponownie wykryte sieci IP**. To pozwala programowi później nie skanować ponownie wcześniej wykrytych sieci, w celu znalezienia nowych węzłów. Oczywiście, można w późniejszym czasie tą opcję włączyć (w oknie **Właściwości mapy** i na karcie **Automatyczne wykrywanie**).*

4. Kliknij przycisk **Dalej**.
   Otworzy się ekran **Metoda wykrywania** widoczny na Rys. 17.



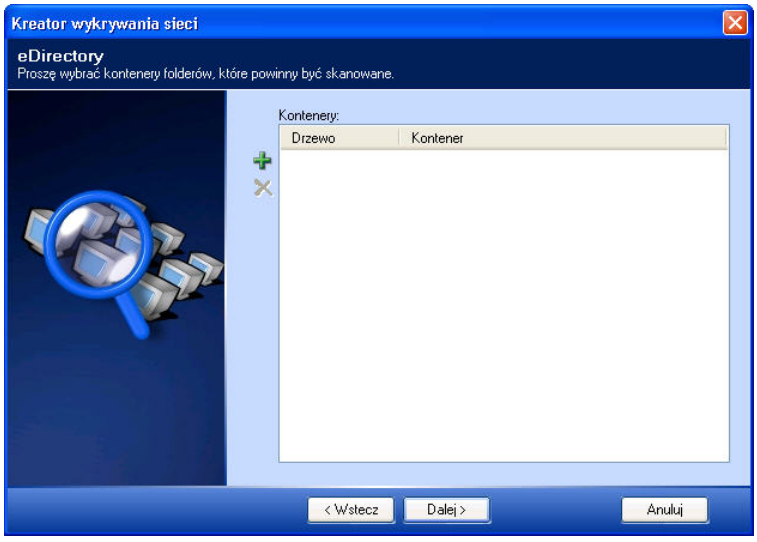
Rys. 17 Ekran wyboru metody wykrywania sieci

5. Wybierz wszystkie trzy metody wykrywania, zaznaczając odpowiednie pola wyboru odpowiadające każdej metodzie. Kliknij **Dalej**.
   Otworzy się okno **Domeny Windows** przedstawione na Rys. 18.



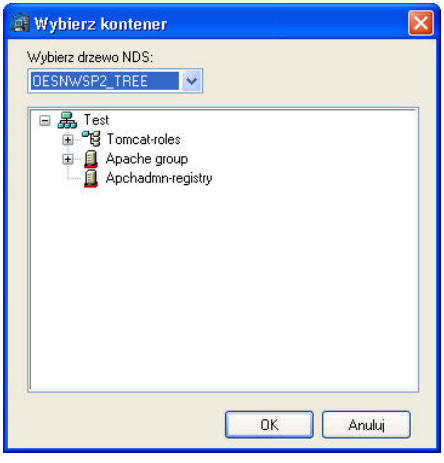
Rys. 18 Ekran Domeny Windows

6. Wybierz Domeny Windows, które ma zeskanować NetCrunch zaznaczając stosowne pola wyboru odpowiadające nazwom domen. Kliknij **Dalej**.
   Wówczas otworzy się ekran kreatora o nazwie *eDirectory* przedstawiony na Rys. 19.



Rys. 19 Ekran eDirectory

7. Kliknij ikonę ***Dodaj***, aby otworzyć okno **Wybierz kontener**, przedstawione na Rys. 20.



Rys. 20 Okno wyboru kontenera

8. Na rozwijanej liście **Wybierz drzewo NDS** wskaż drzewo NDS zawierające kontenery, które mają zostać poddane skanowaniu przez program.
9. Wybierz kontener eDirectory z listy i kliknij **OK**.

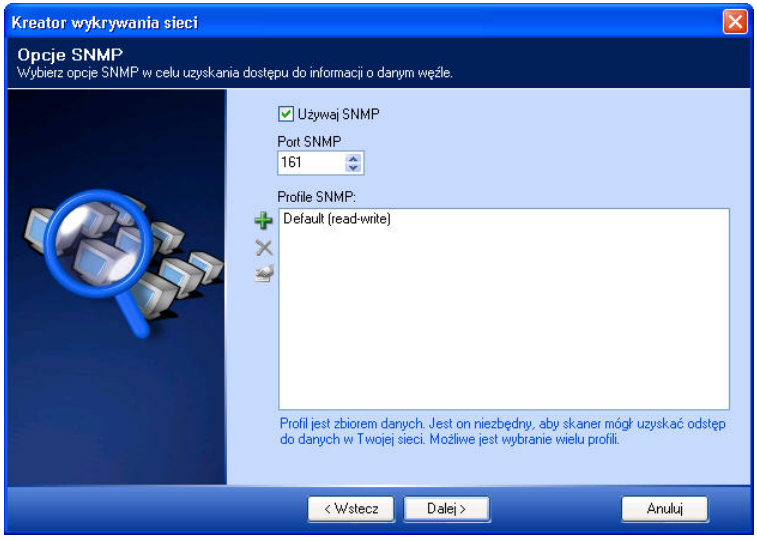
Okno **Wybierz drzewo NDS** zostanie zamknięte.

10. Ekran *eDirectory* wyświetli nowo dodany kontener.

    Powtórz czynności opisane w punktach 7-9, aby dodać kolejne kontenery eDirectory, które mają zostać przeskanowane w celu wykrycia węzłów w sieci.

11. Kliknij **Dalej**.

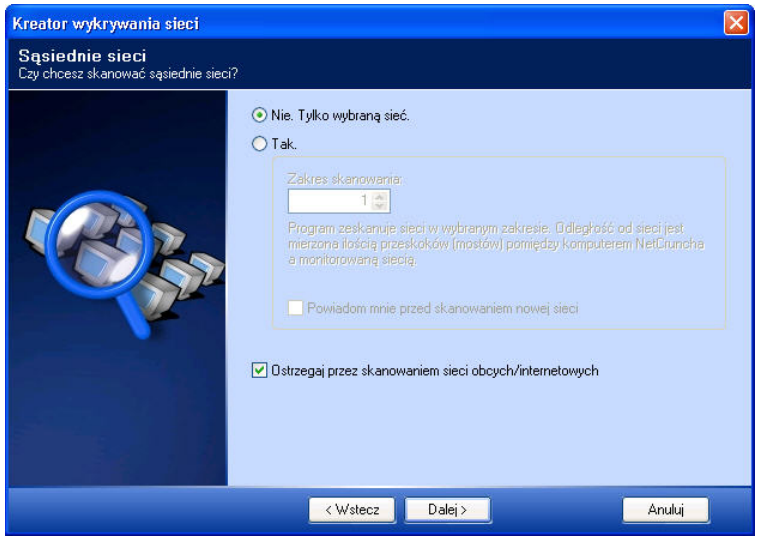
    Wyświetli się ekran *Opcje SNMP*, przedstawiony na Rys. 21.



Rys. 21 Ekran opcji SNMP

12. Zaznacz pole wyboru **Używaj SNMP**, za sprawą którego kreator uzyska dostęp do informacji SNMP o wykrytych węzłach.
13. W polu **Port SNMP**, określ domyślny port SNMP, na którym NetCrunch będzie odpytywał węzły w twojej sieci.
14. Kliknij ikonę ***Dodaj***, aby dodać profil SNMP.
    W takim wypadku otworzy się okno **Wybierz profil SNMP**, gdzie możesz określić chciany profil SNMP, zmienić jego właściwości lub utworzyć nowy (wersję SNMP, która ma być użyta oraz dodatkowe ustawienia dla danej wersji – do odczytu i zapisu).
15. Powtórz czynności opisane w punkcie 14, aby dodać kolejny profil SNMP lub zmienić jego właściwości.
16. Następnie kliknij przycisk **Dalej**.

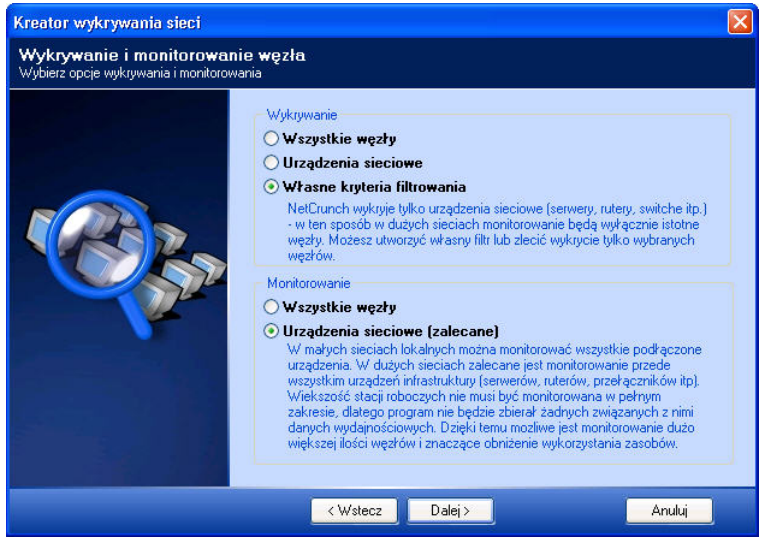
    Wówczas otworzy się ekran *Sąsiednie sieci*, przedstawiony Rys. 22.



Rys. 22 Ekran Sąsiednie sieci

17. Ponieważ nie będzie skanowania sieć zdalna, wybierz przycisk opcji **Nie. Tylko wybraną sieć** i kliknij ikonę **Dalej**.

Pojawi się ekran o nazwie *Wykrywanie i monitorowanie węzła*, przedstawiony na Rys. 23.

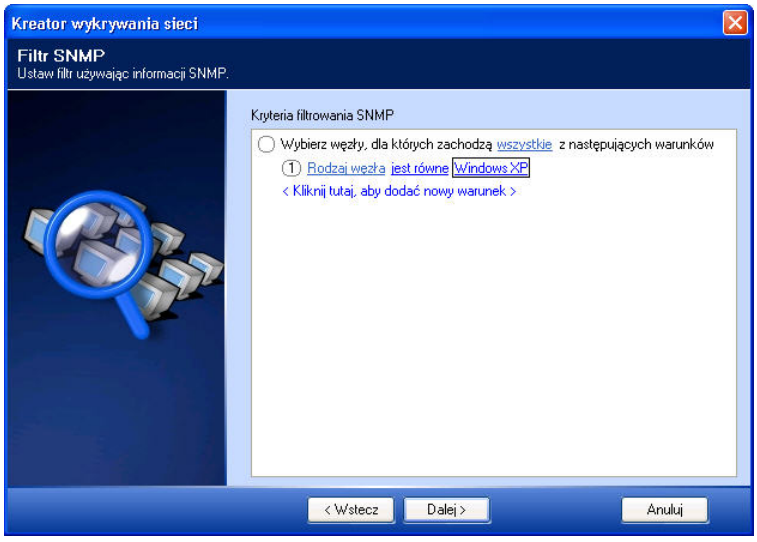


Rys. 23 Ekran Wykrywanie i monitorowanie węzła

18. W polu **Wykrywanie** wybierz przycisk opcji **Własne kryteria filtrowania**, który pozwala wybrać kryteria użytkownika, jakie mają zostać użyte w wykrywaniu węzłów.

19. W polu **Monitorowanie**, wybierz przycisk opcji **Urządzenia sieciowe (zalecane)**, dzięki któremu jedynie znalezione węzły krytyczne będą monitorowane w pełnym zakresie.
20. Kliknij **Dalej**.

Otworzy się ekran *Filtr SNMP*, przedstawiony na Rys. 24.



Rys. 24 Ekran filtra SNMP

21. Aby dodać kilka warunków filtrowania i upewnić się, że zostaną one użyte przy dodawaniu węzłów, wybierz **wszystkie** w wyrażeniu *Wybierz węzły, dla których zachodzą wszystkie z następujących warunków*, a następnie w menu podręcznym wybierz **dowolne**.
22. Kliknij zdanie **< Kliknij tutaj, aby dodać nowy warunek>**, aby dodać warunek.
23. W przypadku warunku filtrowania *Rodzaj węzła jest równe___*, kliknij podkreślone puste pole i z podręcznego menu wybierz rodzaj węzła, który ma posłużyć jako kryterium filtrowania.
24. Aby dodać kolejną regułę filtrowania, powtórz czynności opisane w punkcie 20.

Pod warunkiem filtrowania – zdefiniowanym jako pierwszy w kolejności – wyświetli się kolejny warunek. Powtórz czynności opisane w punkcie 21 za każdym razem, gdy istnieje potrzeba użycia nowego rodzaju węzła w charakterze kryterium filtrowania.

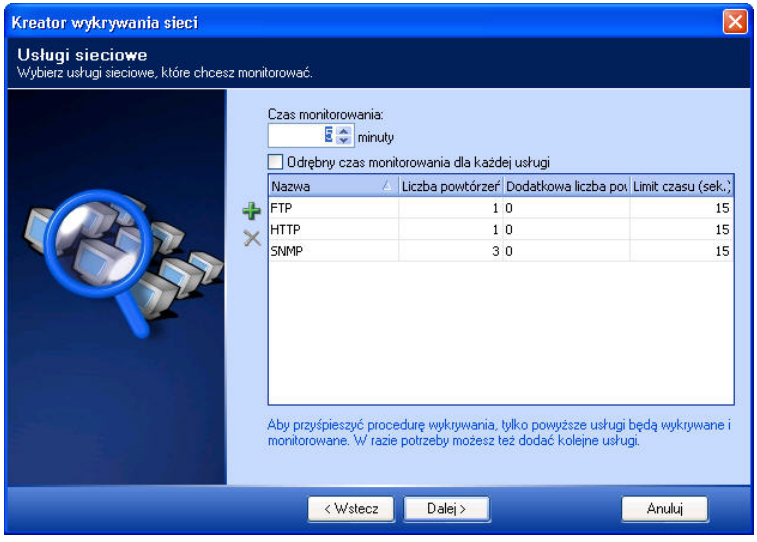
W kryteriach filtrowania można również zmienić rodzaj filtra SNMP. W tym celu należy kliknąć **Rodzaj węzła**, a następnie z podręcznego menu wybrać inną wartość jak np. *Lokalizacja* lub *Usługi sieciowe TCP*.

Uwaga

Może się zdarzyć, że po wybraniu określonej usługi sieciowej w charakterze własnego kryterium filtrowania węzły posiadające tą usługę nie zostaną poprawnie wykryte. Dzieje się tak, gdy wybrany filtr opiera się na danych SNMP, a agent SNMP nie jest dostępny w danym węźle

*(a więc za pomocą SNMP nie da się go wykryć i dodać do monitorowania). Aby uniknąć takiej ewentualności, należy upewnić się, że agenty SNMP są poprawnie uruchomione w węzłach, które będą wskazane na ekranie **Filtr SNMP** w ręcznym trybie wykrycia sieci.*

25. Po zdefiniowaniu wszystkich reguł filtrowania, kliknij **Dalej**.
Wyświetli się ekran *Usługi sieciowe* przedstawiony na Rys. 25.

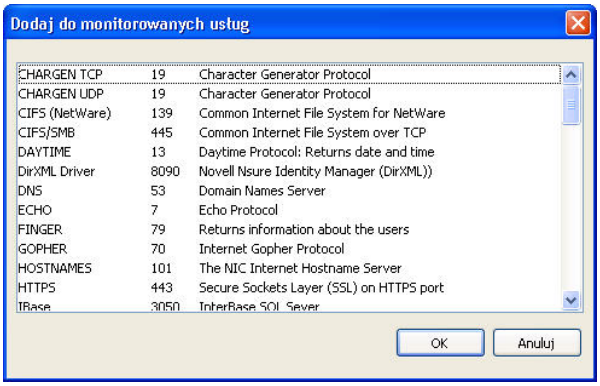


Rys. 25 Ekran Usługi sieciowe

26. Kliknij ikonę ***Dodaj***, aby dodać usługi sieciowe do wyświetlanej listy usług, które zostaną przeszukane w każdym węźle i ewentualnie poddane monitorowaniu.

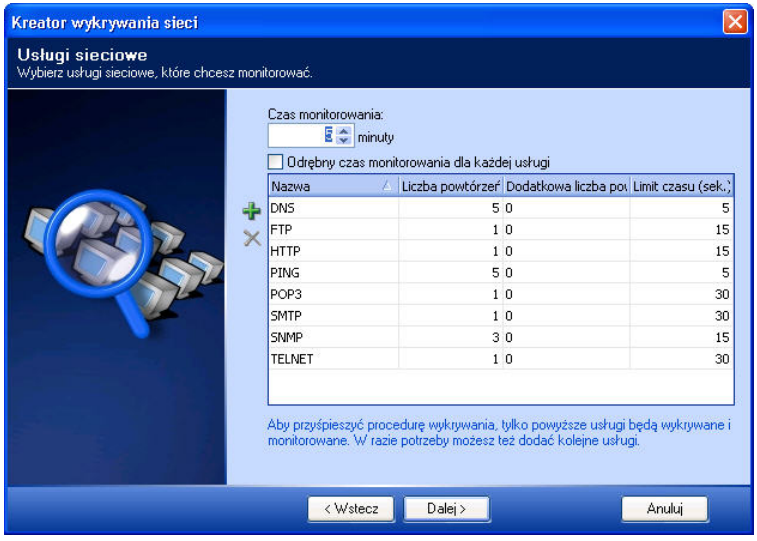
Otworzy się okno **Dodaj do monitorowanych usług**.

27. Aby wybrać więcej niż jedną usługę sieciową, przytrzymując klawisz **CTRL** kliknij każdą żądaną usługę sieciową. Zostaną one podświetlone, jak widać na Rys. 26.



Rys. 26 Okno Dodaj do monitorowanych usług

28. Kliknij **OK**.
Okno **Dodaj do monitorowanych usług** zostanie zamknięte, a wybrane usługi sieciowe dodane do listy na ekranie kreatora, jak widać na Rys. 27.

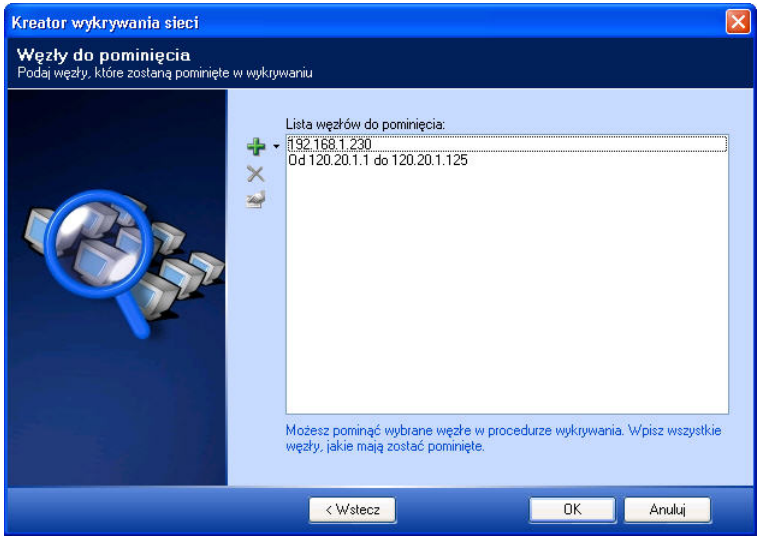


Rys. 27 Ekran Usługi sieciowe po dodaniu usług do listy

Uwaga

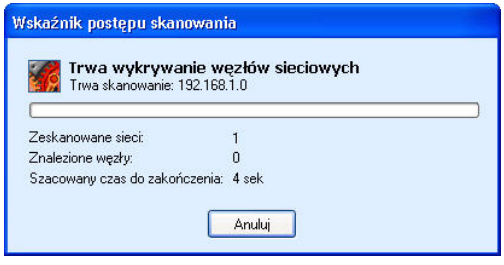
Im większa liczba usług sieciowych zostanie dodana do listy, tym dłużej Kreator wykrywania sieci *będzie skanował i tworzył mapy sieci. Należy mieć to na względzie szczególnie w dużych sieciach, zawierających setki węzłów. Dlatego też zalecane jest umieszczanie na liście wyłącznie niezbędnych usług. Warto pamiętać, że później podczas używania programu można w dowolnej chwili dodać do monitorowania kolejne usługi.*

29. Aby zmienić czas monitorowania, wpisz nową wartość w polu **Czas monitorowania**.
30. Aby określić osobny czas monitorowania dla każdej usługi sieciowej na liście, zaznacz pole wyboru o nazwie **Pozwól ustawić oddzielny czas dla każdej usługi**.
    Na liście zostanie umieszczona nowa kolumna o nazwie *Czas monitorowania*. Możliwa jest zmiana każdego czasu monitorowania określonego dla danej usługi sieciowej.
    W tym celu należy kliknąć aktualną wartość czasu monitorowania i wpisać nową wartość.
31. Kliknij **Dalej**.
    Otworzy się okno **Węzły do pominięcia**, jak widać na Rys. 28.



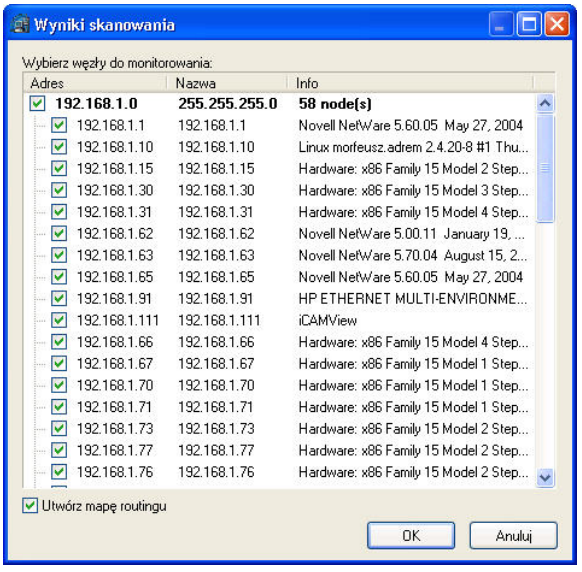
Rys. 28 Ekran Węzły do pominięcia

32. Kliknij ikonę **Dodaj**, w celu dodania adresu IP węzła, który ma zostać ominięty z procesu wykrywania. Możesz również określić zakres adresów IP węzłów, które mają zostać ominięte.
33. Kliknij **OK**, aby zamknąć kreatora *Wykrywanie sieci*.
    NetCrunch przystąpi do wykrywania sieci lokalnej używając parametrów wybranych w poprzednich punktach. Otworzy się okno **Wskaźnik postępu skanowania**, przedstawione na Rys. 29.



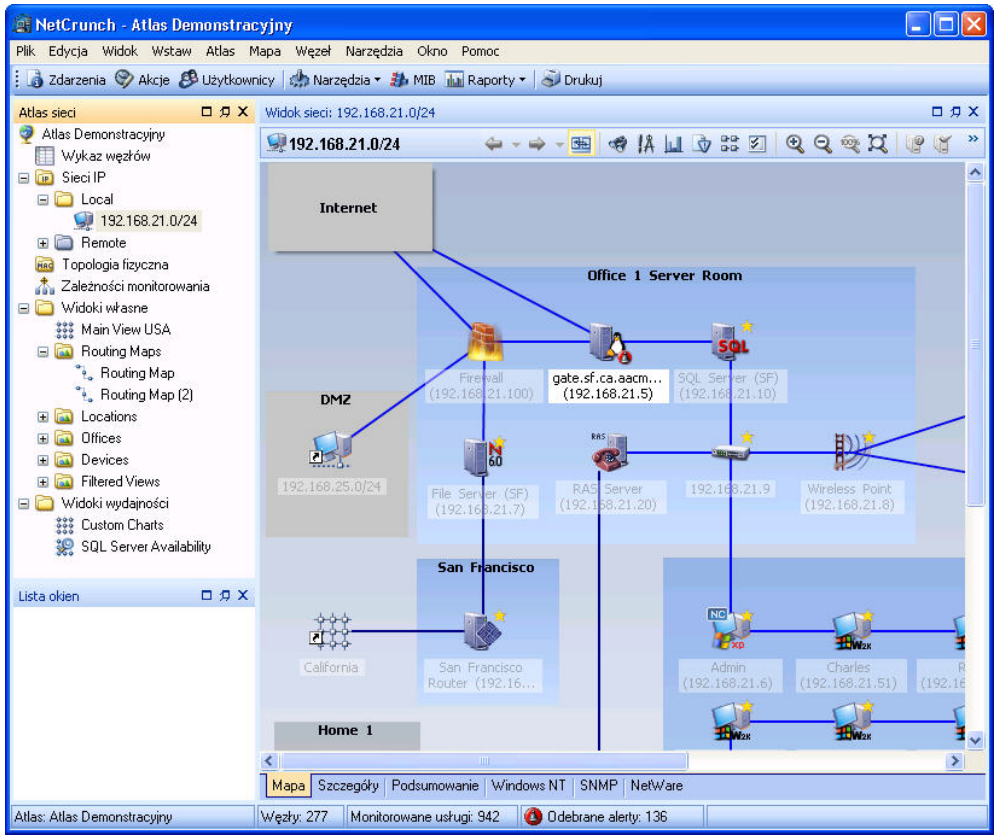
Rys. 29 Okno postępu skanowania

34. Gdy program zakończy skanowanie sieci (może to potrwać od kilku sekund do kilkudziesięciu minut w zależności od liczby węzłów w danej sieci), pojawi się okno **Wyniki skanowania**, przedstawione na Rys. 30.W oknie tym pojawią się wszystkie węzły, które spełniły kryteria określone w *Kreatorze wykrywania sieci*.



Rys. 30 Okno wyników skanowania

35. Odznacz pole wyboru przy węzłach, które nie mają zostać umieszczone w nowym atlasie, a następnie kliknij przycisk **OK**.
Wówczas wyświetli się nowy atlas zawierający wszystkie nowo wykryte mapy sieci i węzły, jak widać na Rys. 31.



Rys. 31 Ekran nowego Atlasu sieci

Uwaga

Więcej informacji na temat używania funkcji i kreatorów w NetCrunchu zawiera ***Podręcznik użytkownika*** *programu.*

Dostosowywanie interfejsu użytkownika

Interfejs użytkownika w NetCrunchu może być na wiele sposobów dostosowywany do własnych potrzeb użytkownika. NetCrunch dopuszcza modyfikowanie układu okien programu i tabel wyświetlanych na stronach widoków sieci.

Dostosowywanie układu okien

Okna programu można personalizować poprzez zmianę ich położenia przy użyciu opcji dokowania (czyli przyłączania) i oddokowywania (odłączania). Utworzone w ten sposób układy okien można zapisywać
w pliku w celu późniejszego użycia. Uściślając, program umożliwia otwieranie znajdujących się w nim paneli jako osobnych okien. Dokowaniu/oddokowywaniu podlegają następujące okna programu:

Atlas sieci	Organizuje wszystkie mapy atlasu w trzech sekcjach drzewa: *Sieci IP* (mapy logiczne), *Segmenty fizyczne* (mapy fizyczne) oraz *Widoki własne* (utworzone przez użytkownika).
Dziennik zdarzeń	Wyświetla/umożliwia zarządzanie zdarzeniami przetwarzanymi przez program.
Lista okien	Wyświetla listę aktualnie otwartych okien programu nie będących oknem głównym programu.
Ruch monitorowania	Wyświetla aktualne informacje o stanie monitorowania i umożliwia ustawianie limitów ruchu monitorowania w podsieciach.
Widok sieci	Wyświetla widoki sieci na graficznych mapach lub w formie tabel.
Wyszukaj	Wyświetla wyniki operacji **Znajdź węzeł**.
Zadania	Wyświetla listę najczęściej używanych zadań programu w celu szybkiego do nich dostępu.

Więcej informacji o oknach programu zawiera sekcja *Opis/charakterystyka programu* na stronie 11.

Oddokowywanie okien

Z głównego obszaru dokowania (a więc nadrzędnego okna, do którego można dokować [dołączać] dowolne okna programu), a także z innych obszarów dokowania można bardzo łatwo oddokowywać (usuwać) okna programu, takie jak Atlas sieci, Widok sieci lub Lista okien. A tym celu należy kliknąć ikonę ***Oddokuj,*** która powinna być widoczna w prawym górnym rogu okna pod warunkiem, że została włączona opcja **Włącz dokowanie**. Aby oddokować okno programu z aktualnie wyświetlanego obszaru dokowania, można również prawym przyciskiem myszy kliknąć pasek tytułowy okna i w menu podręcznym wskazać pozycję **Oddokuj**.

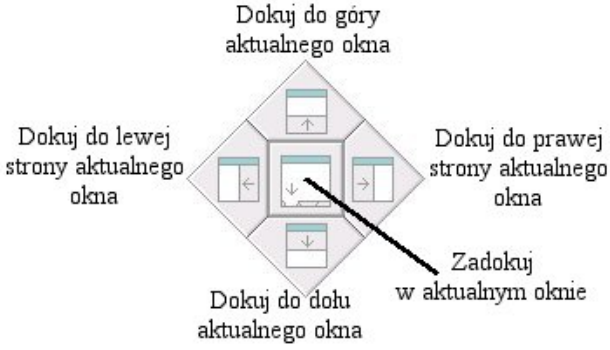
Uwaga

Przed dokowanie/oddokowaniem okien, należy upewnić się, że została włączona opcja dokowania w programie; w tym celu w menu ***Widok*** *kliknij na pozycję* ***Włącz dokowanie****.*

Dokowanie okna

Niezadokowane widoczne okno może zostać zadokowane w dowolnym obszarze dokowania w programie. Odbywa się to poprzez przeciągnięcie paska tytułu wybranego okna na obszar innego okna i upuszczenie go tam. Podczas przeciągania niezadokowanego okna na obszar dokowania innego okna chwilowo wyświetlana jest podręczna ilustracja ułatwiająca dokowanie (odbywa się to dla każdego zadokowanego okna, nad którym znajdzie się kursor myszki).

Rys. 32 pokazuje obszary podręcznej ilustracji, w których można upuścić przeciągany pasek tytułowy dokowanego okna, a także opisuje skutki upuszczenia w nich pasków okien.



Rys. 32 Akcje dostępne w ilustracji podręcznej

Upuszczanie okna w obszarach podręcznej ilustracji pozwala umieścić okno w następujących pozycjach:

- W górnej części zadokowanego okna na obszarze dokowania,
- W dolnej części zadokowanego okna na obszarze dokowania,
- Po lewej stronie zadokowanego okna na obszarze dokowania,
- Po prawej stronie zadokowanego okna na obszarze dokowania,
- W centralnej części (u góry) zadokowanego okna na obszarze dokowania (aby ułatwić nawigację między dawnymi a nowo utworzonymi zadokowanymi oknami, pojawią się specjalne karty).

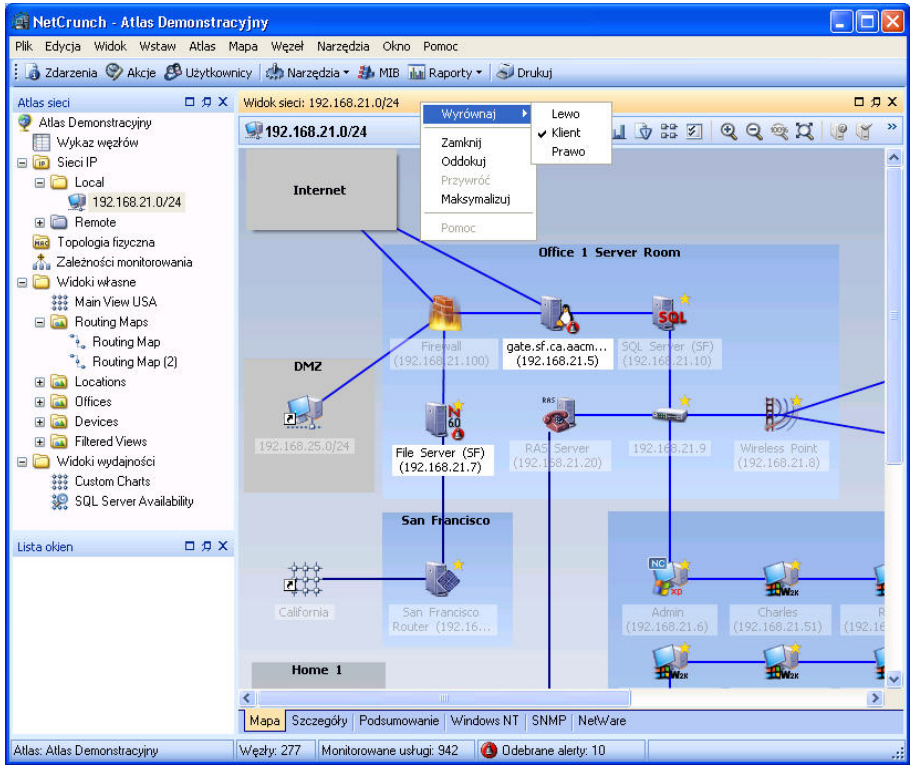
Uwaga

Aby zmienić położenie okna programu, które poprzednio zostało zadokowane centralnie na obszarze dokowania, przeciągnij kartę (zakładkę) z nazwą okna zamiast pasku tytułowego sekcji (który jest niewidoczny).

Zmiana położenia zadokowanych okien programu

Po umocowaniu odpowiednich okien w obszarze dokowania, można w łatwy sposób zmienić ich położenie w stosunku do innych okien. Możliwe są następujące zmiany pozycji okna (kliknij jego pasek tytułowy, aby wybrać odpowiednią opcję, jak widać na Rys. 33):

Góra	Okno zostanie przesunięte w górę obszaru dokowania w stosunku do innych okien,
Dół	Okno zostanie przesunięte w dół obszaru dokowania w stosunku do innych okien,
Lewo	Okno zostanie przesunięte w lewą stronę obszaru dokowania w stosunku do innych okien,
Prawo	Okno zostanie przesunięte w prawą stronę obszaru dokowania w stosunku do innych okien,
Klient	Okno pozostanie tam, gdzie było i zmieni rozmiar w zależności od tego, czy użytkownik zwiększa czy zmniejsza obszar dokowania.



Rys. 33 Wybór nowej pozycji okna Widok sieci

Modyfikacja rozmiaru okna

Rozmiar okien programu widocznych na obszarze dokowania może być modyfikowany stosownie według potrzeb użytkownika. W tym celu należy przeciągnąć obramowanie okna,

zwiększając lub zmniejszając jego obszar w stosunku do innych okien umocowanych w obszarze dokowania.

Przeglądanie wszystkich aktualnie otwartych okien

Po opanowaniu umiejętności otwierania nowych okien programu i dokowania/oddokowywania ich na wielu obszarach dokowania, przydatne okaże się szybkie nawigowanie do okna, które jest schowane za innymi oknami. Należy wówczas wybrać odpowiednią opcję z pozycji **Okno** w menu i użyć okna **Lista okien**. Okno to wyszczególnia aktualnie otwarte okna programu, które mogą być widoczne lub ukryte.

Aranżacja układu okien w trybie wielomonitorowym

Tworzenie kilku obszarów dokowania okazuje się przydatne podczas korzystania z trybu wielomonitorowego na komputerze, na których został uruchomiony NetCrunch. Przykładowo, w taki wypadku główny obszar dokowania może mieścić okno **Atlas sieci** i **Widok sieci** na jednym monitorze, jednocześnie wyświetlając inne okna **Widoku sieci** na drugim monitorze (w powiększeniu) lub nawet na projektorze. Jeśli na komputerze tym istnieje więcej monitorów, można oczywiście tworzyć kolejne obszary dokowania skupiające wybrane okna programu.

Zapisywanie układów okien w programie

Po zamknięciu programu aktywny układ okien jest automatycznie zapamiętywany, dzięki czemu podczas następnego uruchomienia programu pokazany zostanie identyczny układ. Ponadto istnieje możliwość zapisywania w pliku układów okien programu, dzięki czemu można je odzyskać w przyszłości. Aby zapisać lub odtworzyć zapisane układy okien, należy wybrać odpowiednie polecenie z menu **Widok**.

Synchronizowanie okien z Atlasem sieci

Domyślnie widok wyświetlany w oknie **Widok sieci** jest zsynchronizowany z atlasem sieci. Oznacza to, że przy wyborze różnych widoków sieci w oknie **Atlas sieci**, okno **Widok sieci** automatycznie wyświetli swoją zawartość.

Opcja ta jest natomiast wyłączona w przypadku otwierania okna **Widok sieci** w nowym, osobnym oknie. Dzieje się tak, ponieważ otwarcie nowego widoku sieci w osobnym oknie zazwyczaj oznacza, że użytkownik chce zachować jego zawartość za zawsze dla celów monitorowania i alertowania. Okno takie może później zostać zsynchronizowane z atlasem sieci. W tym celu wystarczy nacisnąć ikonę ***Synchronizuj*** w pasku narzędzi okna **Widok sieci**.

Operację tą można również przeprowadzić w oknie **Dziennik zdarzeń**, bez względu na to, czy okno to jest zadokowane czy oddokowane w stosunku do innych okien. Zawartość Dziennika zdarzeń można tak zsynchronizować, aby wyświetlały się jedynie elementy należące do wybranej mapy w oknie **Atlas sieci**. W tym celu kliknij ikonę ***Synchronizuj*** w pasku narzędzi Dziennika zdarzeń.

Możliwe jest dokowanie/oddokowywanie kilku okien map i dziennika zdarzeń na innych obszarach dokowania (głównych i dodatkowych). Niezmiennie jednak główne okno programu będzie zawierać główny, globalny pasek narzędzi.

Dostosowywanie tabel

Kliknięcie na karty *Szczegóły*, *Windows NT*, *SNMP* lub *NetWare* w oknie **Widok sieci** powoduje wyświetlenie przydatnych informacji dotyczących rodzajów widoków sieci. Program pozwala dostosowywać zawartość tabel.

Dostosowywanie kolumn

Możliwe jest chwilowe usuwanie lub dodawanie kolumn do tabeli. W tym celu należy kliknąć ikonę ***Dostosuj kolumny***, co spowoduje otwarcie okna dialogowego **Dostosowanie**. Należy wówczas przeciągnąć kolumnę z tego okna do innego nagłówka tabeli. Aby usunąć widoczne w tabeli kolumny, przeciągnij jej nagłówek do okna dialogowego **Dostosowanie**.

Przechowywanie informacji

Sortowanie informacji w tabeli obywa się poprzez kliknięcie odpowiedniego nagłówka kolumny, który posłuży za punkt odniesienia sortowania. Jednokrotne kliknięcie go sortuje pola kolumny w porządku alfabetycznym, rozpoczynającym się w pierwszej komórce. Ponowne kliknięcie nagłówka tabeli wprowadzi sortowanie w odwrotnym porządku alfabetycznym.

Grupowanie informacji w sekcje

Aby podzielić informacje tabeli na sekcje w oparciu o nagłówek kolumny, kliknij na skierowaną w dół strzałkę znajdującą się koło ikony ***Grupuj wg*** znajdującej się na pasku narzędzi Widok sieci. Wybierz nagłówek kolumny, na podstawie którego odbędzie się grupowanie. Zawartość tabeli zostanie natychmiast zreorganizowana w odpowiednie sekcje.

Filtrowanie informacji

Można także filtrować wyświetlane w tabeli informacje na podstawie kryteriów użytkownika. W tym celu należy kliknąć skierowaną w dół strzałkę umieszczoną w nagłówku danej kolumny i wybrać elementy do wyświetlenia. Aby zdefiniować własne filtry, kliknij przycisk **Dostosuj** i w oknie **Konstruktor filtra** utwórz własne reguły, używając wyrażeń powszechnie używanych w języku polskim. Aby usunąć aktualnie stosowane w tabeli filtry, kliknij ikonę ***Zamknij*** umieszczoną w lewym dolnym roku okna **Widok sieci**.

Indeks