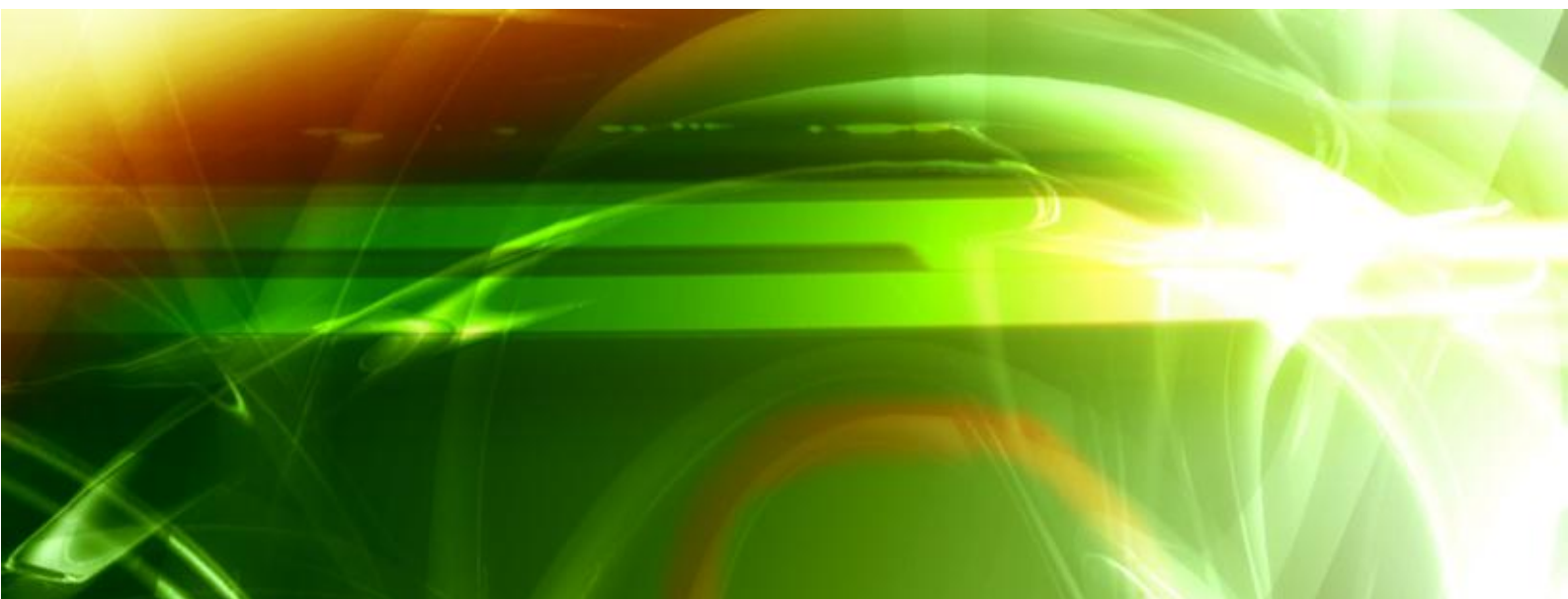


Axence

nVision



Podręcznik użytkownika

Axence nVision

Wizualizacja i zarządzanie siecią

Axence Software, Inc

nVision monitoruje serwery pocztowe i WWW, adresy URL, serwisy TCP/IP i Windows; stan i działanie aplikacji (MS SQL, Exchange, etc.); switche i routery (mapowanie portów i ruch sieciowy). Sieć jest wykrywana automatycznie i prezentowana na interaktywnych mapach. nVision automatycznie gromadzi informacje o sprzęcie i oprogramowaniu urządzeń: model, CPU, pamięć, płyta główna, napędy, karty, etc.; zainstalowane aplikacje i aktualizacje Windows. Umożliwia audyt i weryfikację użytkownika licencji. Informuje o zainstalowaniu programu lub zmianie konfiguracji. Opcjonalne agenty nVision mogą monitorować aktywność użytkowników: faktyczny czas pracy, użytkowanie aplikacji, odwiedzone strony. Agent umożliwia też zdalną kontrolę stacji użytkownika. Program zapewnia szeroki wybór alarmów i raportów: wykresy w czasie rzeczywistym i historyczne; prezentujące działanie systemu i aplikacji; dostępność serwisu i hosta; transfer i wykorzystanie interfejsu; inwentaryzację sieci i aktywność użytkowników.

Axence nVision

Copyright © 2006-2007 Axence Software, Inc. Wszelkie prawa zastrzeżone.

Całkowite ryzyko użytkowania lub wyników użytkowania tego oprogramowania i dokumentacji jest po stronie użytkownika. Żadna część tego podręcznika nie może być skopiowana w żaden sposób, elektronicznie lub mechanicznie, w jakimkolwiek celu, za wyjątkiem dozwolonym przez Umowę Licencyjną Użytkownika.

Program ten oraz dokumentacja chronione są prawem autorskim. Wszelkie prawa, włączając prawo własności programu, są zastrzeżone dla Axence Software, Inc.

Axence Software, Axence nVision i Axence NetTools są znakami towarowymi lub zarejestrowanymi znakami towarowymi firmy Axence Software, Inc. Inne produkty i marki są znakami lub zarejestrowanymi znakami towarowymi ich posiadaczy.

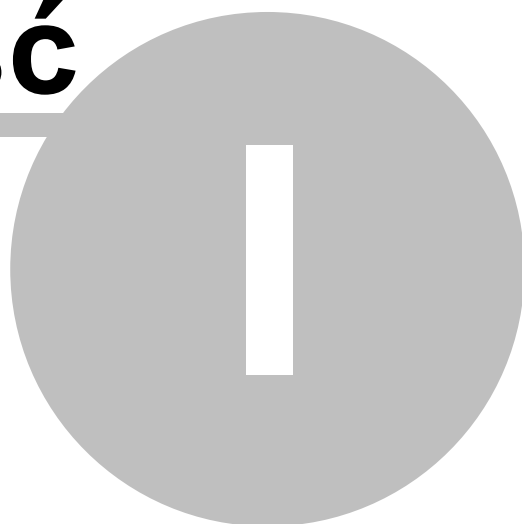
Spis treści

	0
Część I nVision	2
1 nVision	2
2 Co nowego	2
3 Wymagania systemowe	3
4 Wersje nVision i nVision Professional	4
Część II Wprowadzenie	7
1 Wprowadzenie do programu	7
2 Instalowanie nVision jako serwis	8
3 Szybki start	8
4 Układ okna	9
Część III Jak...?	11
1 Jak wykrywać urządzenia i sieci?	11
2 Jak monitorować dostępność urządzeń?	11
3 Jak wykryć problem w sieci?	11
4 Jak monitorować urządzenia i serwisy?	11
5 Jak utworzyć alarm dla serwisu?	12
6 Jak utworzyć alarm dla licznika wydajności?	12
7 Jak monitorować ruch sieciowy na interfejsach?	12
8 Jak zrobić kopię bezpieczeństwa atlasów?	13
9 Jak znaleźć urządzenie?	13
Część IV Wymagania i konfiguracja	15
1 Wprowadzenie	15
2 Wymagania	16
Liczniki Windows, inwentaryzacja, dystrybucja plików	16
Monitorowanie urządzeń SNMP	16
Inwentaryzacja	17
Monitorowanie aktywności użytkowników	18
Zdalny dostęp	19
Monitorowanie serwisów TCP na Windows XP + SP2	19
Monitorowanie i zarządzanie Windows przez WMI	19
3 Rozwiązywanie problemów	21
Nie mogę zainstalować agentów, monitorować liczników i inwentaryzować	21
Nie mogę uzyskać informacji o aktywności użytkowników i zasobach	22
Nie mogę uzyskać informacji o zasobach	22
Część V Wykrywanie i monitorowanie sieci	25
1 Wprowadzenie	25
2 Pojęcie stanu urządzenia	25
3 Skanowanie sieci	26

Wprowadzenie	26
Kreator skanowania sieci	26
Dodawanie nowego urządzenia	28
4 Monitorowanie	29
Wprowadzenie	29
Pojęcia	30
Monitorowanie serwisów	31
Wprowadzenie.....	31
Zarządzanie monitorowanymi serwisami.....	32
Monitorowanie usług Windows	33
Wprowadzenie.....	33
Monitorowanie wydajności urządzenia i systemu	33
Wprowadzenie.....	33
Typy liczników	34
Zarządzanie licznikami wydajności.....	34
Tworzenie licznika na wielu urządzeniach.....	35
Definiowanie właściwości liczników.....	35
Monitorowanie serwerów pocztowych i WWW	36
Wprowadzenie.....	36
Typy liczników	36
Definiowanie właściwości liczników.....	37
Monitorowanie routerów i switchy (MRTG)	38
Wprowadzenie.....	38
Monitorowanie portów switcha	39
Monitorowanie interfejsów sieciowych.....	39
Monitorowanie ruchu sieciowego	39
Monitorowanie aktywności użytkowników	40
Wprowadzenie.....	40
Instalowanie i odinstalowywanie agentów.....	40
5 Zasoby	42
Wprowadzenie	42
Inwentaryzacja	43
Audyt licencji i sprzętu	43
Część VI Praca z atlasami, komputerem i mapami	45
1 Wprowadzenie	45
2 Zarządzanie atlasami	45
3 Mapy	46
Wprowadzenie	46
Rodzaje map	47
Obiekty mapy	47
Zarządzanie mapami	48
Praca z mapą	49
Statyczne obiekty na mapie - właściwości	52
4 Urządzenia	54
Wprowadzenie	54
Wizualizacja urządzeń	54
Właściwości urządzeń	55
Zarządzanie urządzeniami	57
Okno informacji o urządzeniu	57
5 Style	59
Wprowadzenie	59
Definiowanie stylów	60
Zarządzanie stylami	61

Część VII Raporty	64
1 Wprowadzenie	64
2 Tworzenie raportów	64
3 Typy segmentów raportów dla urzędzeń	65
4 Typy segmentów raportów dla map	67
Część VIII Alarmowanie	71
1 Wprowadzenie	71
2 Pojęcia	71
3 Zarządzanie Alarmami	72
Wprowadzenie	72
Zarządzanie Alarmami	73
Dziedziczenie Alarmów	75
Eskalacja Alarmów	76
4 Zdarzenia	76
Wprowadzenie	76
Typy zdarzeń	76
Zarządzanie zdarzeniami	77
Definiowanie własności zdarzeń	78
Progi narastające, opadające i kończące	84
5 Akcje (Korekcyjne i Notyfikujące)	85
Wprowadzenie	85
Typy akcji	85
Zarządzanie akcjami	86
Definiowanie własności akcji	86
Konfigurowanie akcji	90
Definiowanie wiadomości alarmowych użytkownika	92
6 Wygenerowane alarmy	93
Wprowadzenie	93
Dziennik zdarzeń	94
Część IX Inne	97
1 Dystrybucja plików	97
2 Opcje	97
3 Kopia zapasowa i naprawianie bazy danych	98
Indeks	99

Część



1 nVision

1.1 nVision

Axence nVision monitoruje serwery pocztowe i WWW, adresy URL, serwisy TCP/IP i Windows; stan i działanie aplikacji (MS SQL, Exchange, etc.); switchy i routery (mapowanie portów i ruch sieciowy). Sieć jest wykrywana automatycznie i prezentowana na interaktywnych mapach. nVision automatycznie gromadzi informacje o sprzęcie i oprogramowaniu urządzeń: model, CPU, pamięć, płyta główna, napędy, karty, etc.; zainstalowane aplikacje i aktualizacje Windows. Umożliwia audyt i weryfikację użytkownika licencji. Informuje o zainstalowaniu programu lub zmianie konfiguracji.

Opcjonalne agenty nVision mogą monitorować aktywność użytkowników: faktyczny czas pracy, użytkowanie aplikacji, odwiedzane strony. Agent umożliwia też zdalną kontrolę stacji użytkownika.

Program zapewnia szeroki wybór alarmów i raportów: wykresy w czasie rzeczywistym i historyczne; prezentują działanie systemu i aplikacji; dostępność serwisu i hosta; transfer i wykorzystanie interfejsu; inwentaryzacja sieci i aktywność użytkowników.

1.2 Co nowego

Wersja 3.2 (10.10.2007)

Nowości w wersji 3.2:

- Dodatkowe optymalizacje - nVision zużywa mniej procesora, przyspieszono także ładowanie atlasu.
- Nowy skaner sieci. Zaprojektowany aby lepiej skonfigurować pierwszy skan całej sieci.
- Wiele mniej ważnych poprawek i funkcji.

Wersja 3.1 (15.09.2007)

Nowości w wersji 3.1:

- Monitor dziennika systemowego Windows (event log). Pozwala zbierać wpisy w dzienniku Windows oraz generuje alarmy w razie wykrycia określonych zdarzeń.
- Ulepszone agenty
 - Poprawione zostały wszelkie problemy ze stabilnością. Nowa wersja działa na każdym systemie, również na Windows Vista, jest bardzo stabilna i niezawodna.
 - Agent monitoruje obciążenie sieci LAN i Internet przez pracowników.
 - Agent zgłasza zmiany IP na komputerach z adresem przydzielanym przez DHCP. Powoduje to automatyczną zmianę adresu komputera w nVision oraz wygenerowanie alarmu.
- Automatyczne i cykliczne wykrywanie nowych urządzeń - nVision reskanuje wszystkie sieci za pomocą ICMP i SNMP.
- Zaawansowane wyszukiwanie w oknie głównym oraz Host info. Ułatwia zlokalizowanie komputera o określonym adresie IP/MAC/DSN, nazwie lub lokalizacji.
- Przewijanie mapy za pomocą kółeczka myszki.
- Właściwości mogą być edytowane dla wielu urządzeń na raz. Możesz łatwo ustawić właściwości takie jak: hasła, monitorowane serwisy, itp.
- Optymalizacja - nVision zużywa mniej procesora podczas monitorowania dużych sieci.
- Integracja okien audytu licencji i sprzętu oraz nowa zakładka: historia zmian na wszystkich komputerach.
- Nowy skaner sieci. Zaprojektowany aby lepiej skonfigurować pierwszy skan całej sieci.

- Podgląd dziennika zdarzeń w głównym oknie (pod mapą)
- Nowa akcja korekcyjna: zdalne uruchomienie programu
- Zdalny podgląd desktopu pokazuje wszystkie ekrany (dla komputerów z wieloma monitorami)
- Wiele mniej ważnych poprawek i funkcji.

Wersja 3.0 (15.07.2007)

Wersja 3.0 jest wzbogacona o inwentaryzację sieci oraz monitoring użytkowników/ich komputerów. Oto lista wszystkich udoskonaleń oraz nowych funkcji:

- Monitorowanie serwisów Windows; akcje korekcyjne: start/stop/restart serwisu.
- Monitorowanie routerów i switch'y:
 - Mapowanie i monitorowanie portów switch'a, prezentacja wszystkich adresów IP i MAC podłączonych komputerów i ruch sieciowy na każdym porcie.
 - Monitorowanie interfejsów sieciowych (MRTG): stan i ruch sieciowy (we/wy).
 - Monitorowanie ruchu sieciowego na wybranych urządzeniach.
- Inwentaryzacja sprzętu i oprogramowania: informacje o komputerze, zainstalowanych programach, audytowanie użytkownika licencji oraz alarmy w razie zainstalowania/odinstalowania aplikacji i zmiany konfiguracji sprzętowej komputera.
- Monitorowanie aktywności użytkowników
 - Czas aktywności (pracy)
 - Użytkowanie programów oraz raporty przedstawiające czas pracy, przeglądanie stron, konwersacji przez GG czy ICQ, grania itp.
 - Lista stron przeglądanych przez użytkowników.
- Zdalna kontrola stacji użytkownika (zgodna z VNC).
- Dystrybucja plików z możliwością uruchomienia programu na zdalnej konsoli.
- Akcje korekcyjne: zdalny restart systemu, start/stop/restart serwisów Windows.
- Program zamyka się o wiele szybciej.
- Wiele mniej ważnych poprawek i funkcji.

Wersja 2.1 (31.01.2007)

Wersja 2.1 wprowadziła raporty. Oto lista wszystkich udoskonaleń oraz nowych funkcji:

- Raporty - zaawansowane raporty, które można drukować a ich treść w pełni dostosowywać do potrzeb.
- Edytor serwisów: z możliwością utworzenia indywidualnych ustawień serwisów TCP/IP.
- Nowe akcje notyfikacyjne: SMS przez urządzenie GSM, wiadomości Syslog.

1.3 Wymagania systemowe

System operacyjny

- Windows 2000/2003/Vista, Windows XP aż do SP1
- Windows XP + SP2 - na tym systemie mogą wystąpić pewne problemy, ze względu na limit stosu TCP/IP wprowadzony przez Microsoft. Przejdź do rozdziału [Monitorowanie serwisów TCP na Windows XP + SP2](#) aby uzyskać więcej informacji.
- Wymagane prawa administratora (zobacz poniższą notę)

Sprzęt

- Procesor 1.5 GHz lub lepszy
- Przynajmniej 256 MB RAM.
- Wymagana szybkość procesora oraz zajętość pamięci mogą wzrosnąć podczas monitorowania dużej sieci posiadającej więcej niż 50 urządzeń a także w przypadku jednoczesnego wyświetlania wielu map.
- Video: 1024x768 lub więcej, true color
- Karta sieciowa podłączona do sieci LAN/WAN

Prawa Administratora

Aby program działał poprawnie wymagane są prawa administratora. W innym przypadku nVision nie może wysyłać danych ICMP - ta funkcja jest całkowicie zablokowana dla użytkowników bez praw administratora.

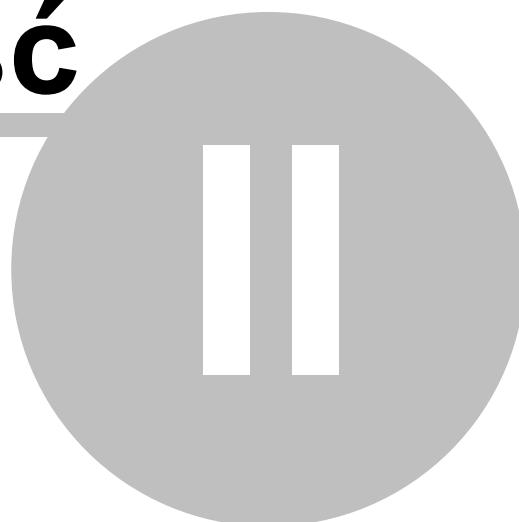
1.4 Wersje nVision i nVision Professional

Poniższa tabela zawiera porównanie wersji nVision i nVision Professional.

Funkcja	nVision	nVision Professional
Monitorowanie sieci		
Serwisy	✓	✓
Serwery pocztowe i WWW	✓	✓
Serwisy Windows	✓	✓
Router i switche (MRTG)	✓	✓
Działanie Windows i urządzeń SNMP	✓	✓
MS SQL, Exchange, IIS i inne aplikacje	✓	✓
Alarmowanie i raporty		
Alarmy	✓	✓
Powiadomienia i akcje korekcyjne	✓	✓
Raporty	✓	✓
Monitorowanie aktywności użytkowników i zdalny dostęp		
Monitorowanie aktywności (czas pracy, używane aplikacje)		✓
Lista odwiedzanych stron		✓
Zdalny dostęp do komputerów Windows		✓
Zdalne agenty		✓
Inwentaryzacja sieci		
Inwentaryzacja oprogramowania	✓	✓
Inwentaryzacja sprzętu	✓	✓
Zdarzenia w przypadku zmiany konfiguracji	✓	✓
Inwentaryzacja za pomocą agentów (bez WMI; optymalizacja dla dużych sieci)		✓

Inne		
Zawiera NetTools Professional	✓	✓

Część



2 Wprowadzenie

2.1 Wprowadzenie do programu

Rozdział ten krótko opisuje funkcjonalność programu Axence nVision.

Wykrywanie i wizualizacja sieci

- Skanowanie sieci - program ma bardzo zaawansowany skaner, pozwalający wykryć urządzenia w twojej sieci, jak również w sieciach podłączonych przez routery znajdujące się w Twojej sieci. Wykrywa typ urządzenia oraz serwisy na nich działające.
- Wykryte sieci prezentowane są na graficznych mapach, prezentujących stan każdego urządzenia. Można szybko wykryć nie działające urządzenia oraz inne problemy z wydajnością. Można np. zobaczyć ostatni czas odpowiedzi lub czas od jakiego urządzenie nie działa.

Monitorowanie i wizualizacja wydajności

- nVision ciągle monitoruje wszystkie urządzenia i serwisy na nich działające. Można także monitorować liczniki SNMP i Windows. Ułatwia to śledzenie stanu urządzeń oraz proaktywne reagowanie na wszelkie problemy z wydajnością, zanim spowodują one jakąś awarię. Można monitorować nie tylko czas odpowiedzi serwisów, ale także krytyczne informacje systemowe, jak zużycie procesora, transfery sieciowe, liczba użytkowników oraz parametry działania serwerów SQL i Exchange.
- Każdy monitorowany parametr może być przedstawiony na wykresie. Wykresy te mogą pokazywać zadany okres, aby móc sprawdzić każdą pojedynczą wartość (na wykresie 10-minutowym) lub pełny wykres miesięczny. Wykresy można przesuwac, ułatwiając szybki dostęp do danych historycznych.

Alarmowanie i zdarzenia

- Dzięki alarmowaniu możesz być powiadomiony w razie jakichkolwiek problemów z twoją siecią. Gdy urządzenie przestanie odpowiadać, kiedy serwis działa wolno lub gdy pewne aplikacje mają problemy nVision może wysłać powiadomienie, pokazać informacje na ekranie a także uruchomić akcję korekcyjną.
- Można zdefiniować wiele typów zdarzeń, kiedy alarm powinien być wygenerowany oraz wiele typów akcji wykonywanych przy każdym zdarzeniu. Alarmy można definiować jednocześnie dla wszystkich urządzeń (poziom atlas) lub dla każdego oddzielnie.
- Każdy wygenerowany alarm jest zapisywany do bazy danych, w celu analizy wydajności urządzeń i całej sieci. Daje to możliwość uzyskania raportów o najbardziej problematycznych urządzeniach, najczęstszych problemach, itp.

Zasoby sieciowe

nVision automatycznie zbiera informacje o sprzęcie i oprogramowaniu:

- Szczegóły konfiguracji sprzętowej: model, CPU, pamięć p³yta g³ówna, dyski, karty, itp.
- Zainstalowane aplikacje i aktualizacje Windows. Pozwala to na weryfikację i audyt używanych licencji.

Monitorowanie aktywnosci uzytkownikow

Opcjonalne agenty nVision monitoruj¹ aktywność użytkowników na komputerach z systemem Windows:

- Czas pracy oraz czas aktywności/nieaktywności
- Użycie z aplikacji pogrupowane wg typu aktywności (praca, gry, czat, przeglądanie stron, itp.)
- Wielkość ruchu sieciowego dla sieci LAN i Internet
- Przeglądane strony WWW

Agent pozwala także przejść zdalnie kontrolę nad stacją (funkcja zgodna z VNC).

2.2 Instalowanie nVision jako serwis

Aby zainstalować nVision jako serwis, należy zaznaczyć opcję **Instaluj jako serwis** na początkowym ekranie instalatora (opcja ta nie jest dostępna w wersji testowej). Należy także podać nazwę użytkownika oraz hasło konta na którym będzie działał serwis nVision. Musi to być konto z uprawnieniami administratora.

Aby uruchomić nVision należy użyć okna zarządzania serwisami (Service management) lub wykonać komendę konsoli: net start "Axence nVision".

Po uruchomieniu, program wyświetli ikonkę w zasobniku systemowym. Aby okno programu zostało wyświetlone, należy kliknąć na tą ikonkę.

UWAGA: Jeżeli program nVision jest uruchomiony nie można uruchomić go ponownie (przez uruchomienie nvision.exe).

nVision i Remote Desktop

Jeżeli do komputera z programem nVision uzyskujesz dostęp przez Remote Desktop, należy uruchomić go z parametrem: mstsc.exe /console. W innym przypadku ikona nVision nie będzie widoczna i dostęp do programu nie będzie możliwy.

2.3 Szybki start

Rozdział ten opisuje działania konieczne, aby szybko rozpocząć pracę z programem.

Tworzenie pierwszego atlasu

Przy pierwszym uruchomieniu program wyświetla okno pozwalające na utworzenie nowego atlasu. Atlas to zestaw map twojej sieci. Aby używać nVision konieczne jest utworzenie przynajmniej jednego atlasu. W większości przypadków będzie to atlas twojej sieci lokalnej.

Aby utworzyć pierwszy atlas:

1. Kliknij przycisk **Nowy atlas**.
Pojawi się okno kreatora atlasu. Kreator ten pomoże w wykryciu twojej sieci, wszystkich urządzeń oraz utworzeniu map.
2. Wpisz nazwę atlasu oraz twój e-mail.
3. Wpisz adres IP urządzenia w sieci, która będzie skanowana. Program automatycznie podpowiada lokalny adres, który pozostaw nie zmieniony, jeśli chcesz skanować sieć lokalną.
4. Kliknij przycisk **Zakończ**. Spowoduje to wykrycie sieci, utworzenie map i rozpoczęcie monitorowania urządzeń.
Aby dowiedzieć się więcej o opcjach kreatora, przejdź do rozdziału [Wykrywanie sieci](#).

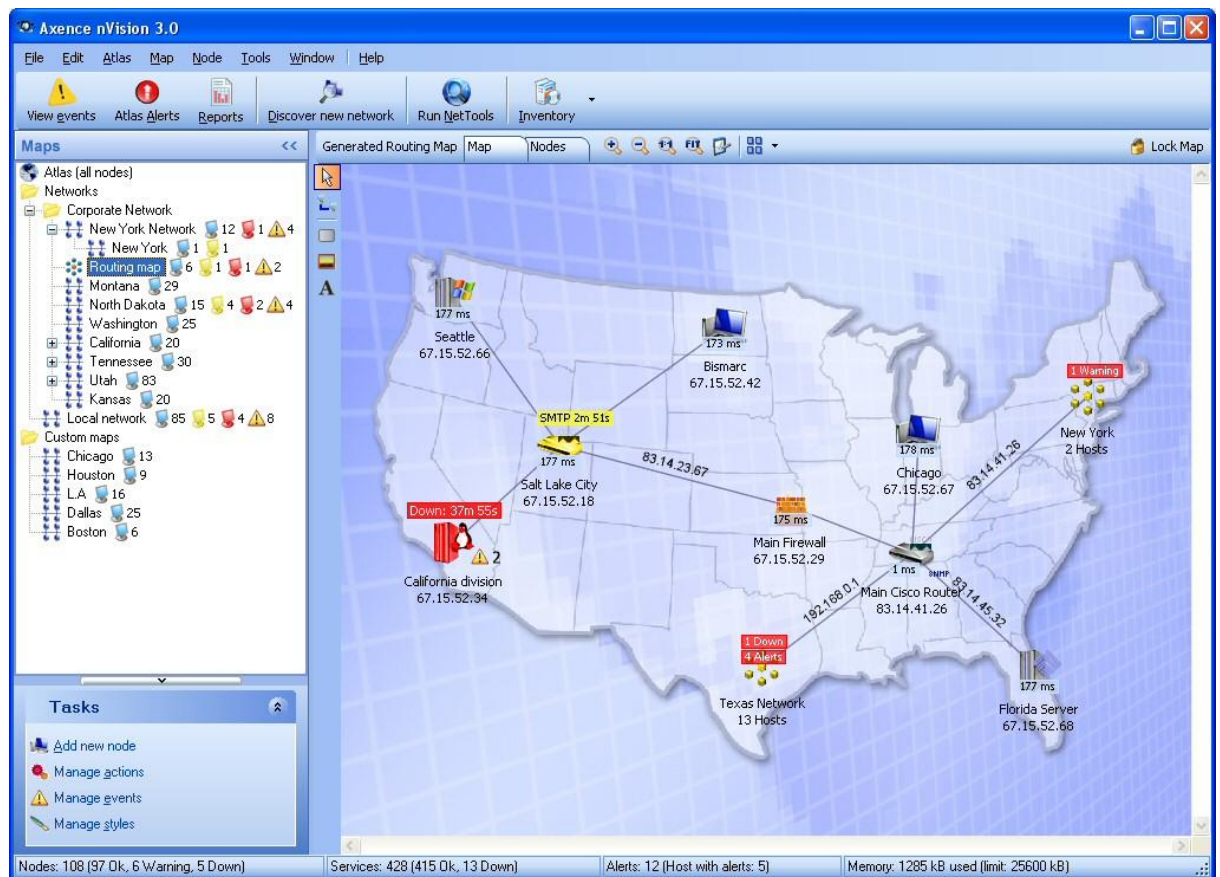
Alarmy

Po utworzeniu atlas posiada kilka predefiniowanych alarmów, takich jak: Urządzenie nie działa i Serwis nie działa.

Jeśli chcesz utworzyć nowe alarmy, przejdź do rozdziału [Wprowadzenie](#) w części Alarmowanie.

2.4 Układ okna

Układ okna nVision jest intuicyjny i prosty w użyciu.



Drzewo atlasu

Drzewo atlasu, zlokalizowane w górnej, lewej części okna, przedstawia listę wszystkich dostępnych map. Aby dowiedzieć się więcej o mapach, przejdź do rozdziału [Mapy - Wprowadzenie](#). Po wybraniu mapy w drzewie, jest ona prezentowana po prawej stronie.

Mapa

Ta część prezentuje mapę wybraną w drzewie atlasu.

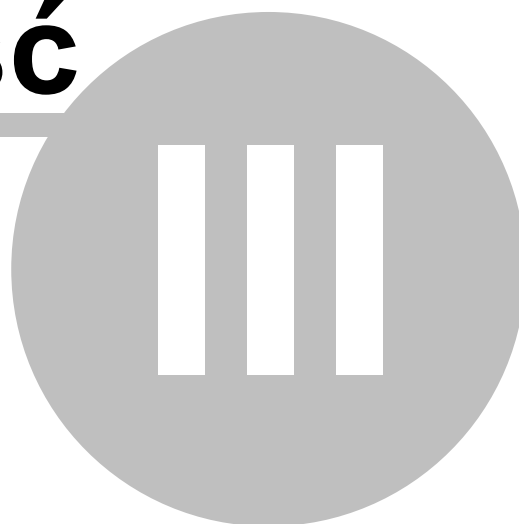
Dziennik zdarzeń

Pasek dziennika zdarzeń pozwala szybko sprawdzić ostatnie alarmy.

Zadania

Okno zadań, znajdujące się na dole, po lewej stronie, pozwala wykonywać najczęstsze zadania. Można ukryć okno klikając na pasku podziału.

Część



3 Jak...?

3.1 Jak wykrywać urządzenia i sieci?

Wykrywanie nowej sieci

W celu wykrycia wszystkich sieci oraz urządzeń możesz użyć skanera sieciowego nVision. Wykryje on wszystkie urządzenia oraz serwisy działające na nich. Aby uzyskać szczegółową informację na temat wykrywania sieci, przeczytaj rozdział [Wykrywanie sieci - Wprowadzenie](#).

Wykrywanie urządzeń w istniejącej sieci

Aby szybko wykryć nowe urządzenia we wszystkich sieciach, możesz użyć tego samego mechanizmu jak do wykrywania nowych sieci - zobacz rozdział [Wykrywanie sieci - Wprowadzenie](#). nVision może też wykryć urządzenia automatycznie przez wybranie **Wykryj nowe urządzenia** z menu kontekstowego mapy. Proces ten może być wykonywany okresowo.

1. Wybierz mapę, na której chcesz włączyć automatyczne wykrywanie.
2. Otwórz okno właściwości mapy i wybierz zakładkę **Wykrywanie automatyczne**, która pozwala skonfigurować uruchomienie procesu wykrywania. Zakładka ta pokazuje też aktualny stan i postęp w belce statusu.
3. Zaznacz opcję **Wykrywaj nowe urządzenia**
4. Skonfiguruj częstotliwość czasu wykrywania
5. Możesz też uruchomić wykrywanie klikając na przycisku **Wykryj teraz**.

3.2 Jak monitorować dostępność urządzeń?

nVision automatycznie monitoruje dostępność wszystkich urządzeń, więc nie są potrzebne żadne dodatkowe działania po skanowaniu sieci. Dostępność urządzeń będzie domyślnie monitorowana.

3.3 Jak wykryć problem w sieci?

Można na dwa sposoby rozwiązywać problemy z sieciami.

Wizualizacja sieci

Po pierwsze, możesz zlokalizować problematyczne urządzenia za pomocą graficznych map. nVision wyświetla kilka informacji obok każdej ikony, takich jak czas odpowiedzi, czas kiedy urządzenie lub określony serwis nie działa. Wskazuje także liczbę wygenerowanych alarmów. Można więc łatwo wykryć problemy, przeglądając mapy.

Łatwo można też określić liczbę urządzeń działających/niedziałających/z ostrzeżeniem w każdej mapie drzewa atlasu. W ten sposób można szybko zauważyć wszelkie zmiany.

Alarmowanie

Alarmowanie to ogólny sposób na zapisywanie zdarzeń, powiadamianie administratora oraz wykonywanie akcji korekcyjnych. Można zdefiniować różnego rodzaju alarmy, które będą wygenerowane po wykryciu problemu i wyśle do Ciebie powiadomienie przez email, ICQ, SMS, itp.




3.4 Jak monitorować urządzenia i serwisy?

Po wykryciu urządzeń w sieci nVision automatycznie wykrywa wszelkie serwisy na nich działające. Aby więc rozpocząć monitorowanie urządzeń i ich serwisów, nie ma potrzeby wykonywania żadnych dodatkowych działań poza wykrywaniem sieci. Można jednak manualnie, lub przez wywołanie narzędzia wykrywania serwisów dodać nowy serwis. Aby uzyskać więcej informacji o serwisach przejdź do rozdziału [Zarządzanie urządzeniami](#).

Lista monitorowanych serwisów wraz z wykresami reprezentującymi czas odpowiedzi i % utraconych pakietów/łączności, dostępna jest w oknie [Stan urządzeń](#).




3.5 Jak utworzyć alarm dla serwisu?

Aby zostać powiadomionym w razie problemów z serwisem konieczne jest utworzenie alarmu. Rozdział ten opisuje kolejne kroki niezbędne do wykonania tej czynności.

1. Aby otworzyć okno alarmów, kliknij ikonę  znajdującą się w głównym pasku narzędziowym.
2. Utwórz nowy alarm klikając ikonę  znajdującą się w głównym pasku narzędziowym. Otworzy się okno właściwości alarmu. Za pomocą tego okna można utworzyć zdarzenie inicjujące alarm oraz dodać akcje do wykonania w razie wygenerowania alarmu.
3. Kliknij przycisk znajdujący się po prawej stronie pola zdarzenia. Pozwoli to utworzyć nowe zdarzenie.
Dla serwisów wybierz typ zdarzenia: **Serwis nie działa** lub **Wydajność serwisu**. Utwórz zdarzenie zgodnie z informacją w rozdziale [właściwości zdarzeń](#).
4. Kliknij ikonę  i zdefiniuj akcję, która będzie wykonana gdy alarm zostanie wygenerowany. Możesz wybrać akcję istniejącą lub utworzyć nową. Aby stworzyć nową akcję kliknij przycisk znajdujący się po prawej stronie pola wyboru akcji. Utwórz akcję zgodnie z informacjami dostępnymi w rozdziale [właściwości akcji](#).

3.6 Jak utworzyć alarm dla licznika wydajności?


Rozdział ten opisuje sposób utworzenia alarmu na wypadek przekroczenia przez licznik wydajności dopuszczalnego zakresu. Np. alarm, który powiadomi, gdy kolejka pocztowa serwera MS Exchange będzie zbyt długa. Taki licznik wydajnościowy musi być utworzony na każdym serwerze, na którym działa Exchange - następnie tworzymy zdarzenie, które zainicjuje alarm. nVision zapewnia możliwość łatwego utworzenia alarmu i licznika na każdym komputerze, na którym uruchomiony jest MS Exchange.

1. Aby otworzyć okno alarmów, kliknij ikonę  znajdującą się w głównym pasku narzędziowym.
2. Utwórz nowy alarm klikając ikonę  znajdującą się w głównym pasku narzędziowym. Otworzy się okno właściwości alarmu. Za pomocą tego okna można utworzyć zdarzenie inicjujące alarm oraz dodać akcje do wykonania w razie wygenerowania alarmu.
3. Kliknij przycisk znajdujący się po prawej stronie pola zdarzenia. Pozwoli to utworzyć nowe zdarzenie.
Dla liczników wybierz typ zdarzenia: **Test serwisu** lub **Liczniki**. Utwórz zdarzenie zgodnie z informacją w rozdziale [właściwości zdarzeń](#).
4. Kliknij ikonę  i zdefiniuj akcję, która będzie wykonana gdy alarm zostanie wygenerowany. Możesz wybrać akcję istniejącą lub utworzyć nową. Aby stworzyć nową akcję, kliknij przycisk znajdujący się po prawej stronie pola wyboru akcji. Utwórz akcję zgodnie z informacjami dostępnymi w rozdziale [właściwości akcji](#).

3.7 Jak monitorować ruch sieciowy na interfejsach?

nVision automatycznie monitoruje interfejsy sieciowe na wszystkich urządzeniach SNMP. Tabela interfejsów znajduje się w oknie **Informacje o urządzeniu** na zakładce **Ogólne**. Przedstawia stan interfejsów oraz umożliwia zdefiniowanie alarmu na wypadek zmiany ich stanu.

Aby monitorować ruch sieciowy na interfejsach

1. Wybierz ikonę urządzenia i otwórz okno w konfiguracji urządzenia.
2. Sprawdź, czy urządzenie to jest zarządzane przez SNMP i czy pole wspólnoty jest właściwie ustawione.
3. Otwórz okno Informacji o urządzeniu i sprawdź, czy wszystkie interfejsy wyświetlone są z ikoną  (na zakładce **Ogólne**). Jeżeli nie, przejdź na zakładkę **SNMP** i sprawdź czy pokazuje ona informacje. Jeżeli tak, należy poczekać aż nVision zgromadzi za pomocą SNMP informacje o interfejsach. Jeżeli na zakładce **SNMP** nie pokazują się informacje, prawdopodobnie nie zdefiniowano wspólnoty SNMP.
4. Z paska bocznego zadania wybierz **Konfiguruj monitorowanie ruchu sieciowego** (z prawej strony okna) i zaznacz wszystkie interfejsy, na których chcesz monitorować ruch sieciowy.
5. Możesz także kliknąć prawym klawiszem myszki na interfejsie, który chcesz monitorować i wybrać z menu kontekstowego **Monitoruj ruch sieciowy (MRTG)**.
6. Na zakładce **Liczniki wydajności** zostaną utworzone liczniki SNMP dla każdego interfejsu (dla ruchu przychodzącego i wychodzącego).

3.8 Jak zrobić kopię bezpieczeństwa atlasów?

Informacja o wszystkich atlasach znajduje się w katalogu Atlases. Program nVision jest zawsze zgodny wstecz, a więc wersja aktualna może korzystać ze starszej wersji bazy danych atlasów. Automatycznie wykonywana jest aktualizacja bazy, co oznacza, że po takiej operacji poprzednia wersja programu nie będzie mogła już być uruchomiona.

Aby zrobić kopie bezpieczeństwa oraz naprawić bazy atlasów, użyj programu dbRepair. Można go uruchomić wybierając z menu Start **Kopia i naprawa bazy danych**. Upewnij się wcześniej, że nVision nie jest uruchomione.

1. Uruchom dbRepair z menu Start.
2. Wylacz opcje **Kopia zapasowa** jeśli chcesz wykonać tylko naprawę bazy.
3. Kliknij przycisk **Napraw**. Kopia bezpieczeństwa zostanie utworzona w katalogu Atlases\Backup a następnie uruchomi się proces naprawy bazy.

Aby uzyskać informacje na temat odzyskiwania danych z kopii, przejdź do rozdziału XXX.

3.9 Jak znaleźć urządzenie?

Możesz łatwo znaleźć urządzenie przez wyszukiwarkę znajdującą się na głównym pasku narzędziowym oraz w oknie **Informacje o urządzeniu**. Poniżej znajduje się lista właściwości branych pod uwagę przy wyszukiwaniu:

- Nazwa
- Adresy IP, DNS and MAC każdego interfejsu
- Lokalizacja
- System
- Info1 i Info2

Część

IV

4 Wymagania i konfiguracja

4.1 Wprowadzenie

Planowanie monitorowania

Aby z powodzeniem monitorować wszystkie urządzenia w Twojej sieci, przed uruchomieniem skanera sieci nVision, musisz wykonać określone kroki. Oto lista wszystkich czynności, które należy przeprowadzić, aby w pełni wykorzystywać wszystkie funkcje nVision:

- Prawidłowe skonfigurowanie urządzeń SNMP
- Uruchomienie WMI na wszystkich komputerach Windows. Uruchamianie WMI jest szczegółowo opisane w rozdziale [Monitorowanie Windows przez WMI](#).
- Skonfigurowanie danych logowania systemu dla wszystkich urządzeń
- Otwarcie określonych portów na komputerach zdalnych, i na tym gdzie uruchomione jest nVision
- Zainstalowanie agenta nVision na wszystkich komputerach.

Warto również przeczytać o [ograniczeniach przy nVision uruchomionym na Windows XP + SP2](#).

Konfiguracja danych logowania

Zarówno SNMP i WMI wymagają danych logowania w celu poprawnego monitorowania. Domyślne dane logowania dla Windows (WMI) oraz wspólnoty SNMP można podać w oknie zarządzania danymi logowania (dane te nazywają się domyślnymi danymi logowania Windows i SNMP). Dane te będą domyślnie ustawione we właściwościach urządzenia.

Wymagania przy monitorowaniu różnych aspektów sieci

Rozdziały poniżej szczegółowo opisują wszelkie wymagania:

 [Wymagania przy monitorowaniu urządzeń SNMP](#)

 [Wymagania przy inwentaryzacji](#)

 [Wymagania przy monitorowaniu liczników Windows, inwentaryzacji za pomocą WMI i dystrybucji plików](#)

 [Wymagania przy monitorowaniu aktywności użytkowników](#)

 [Wymagania przy zdalnym dostępie](#)

Tabela poniżej zawiera wszystkie porty, które muszą być otwarte na zaporze zdalnego urządzenia:

Protokół lub monitorowanie	Porty, które muszą być otwarte
Monitorowanie serwisów TCP/IP	W zależności od monitorowanego serwisu. Na przykład: HTTP wymaga dostępności portu TCP 80.
Monitorowanie liczników Windows Zasoby (przez WMI) Dystrybucja plików	TCP 135,139,445,593
Monitorowanie aktywności użytkowników Zasoby (przez agenty)	TCP 4433 na zdalnym urządzeniu (zalecane)
Zdalny dostęp	TCP 37659

Następujący port musi być otwarty na zaporze komputera, na którym jest uruchomiona konsola nVision:

Protokół lub monitorowanie**Porty, które muszą być otwarte**

Monitorowanie aktywności użytkowników TCP 4434 na komputerze z uruchomionym nVision

Powiązane tematy

 [Instalacja agentów nVision](#)

4.2 Wymagania

4.2.1 Liczniki Windows, inwentaryzacja, dystrybucja plików

Planowanie monitorowania

Do monitorowania liczników Windows, gromadzenia informacji o zasobach przez WMI i dystrybucji plików, nVision używa protokołu WMI.

Wymagania

Aby połączyć się ze zdalnym komputerem przez protokół WMI, nVision musi posiadać jego dane logowania (nazwę użytkownika/hasło). Należy je ustawić we właściwościach urządzenia w zakładce **Dane logowania**.

Monitorowanie	Używany protokół	Wymagania
Liczniki wydajności Windows	WMI	<ul style="list-style-type: none"> Właściwie ustawione dane logowania. WMI udostępnione na zdalnym komputerze. Aby się dowiedzieć, jak uruchomić WMI, przejdź do rozdziału Monitorowanie i zarządzanie Windows przez WMI.
Dystrybucja plików		
Zasoby (przez WMI)		

Poza powyższymi wymaganiami, zaporę na zdalnym komputerze musi być właściwie skonfigurowana. Poniższa tabela przedstawia porty, które muszą być otwarte:

Protokół lub monitor**Porty, które muszą być otwarte**

WMI

TCP 135,139,445,593

Jeśli w dalszym ciągu masz z tym problemy, aby je zdiagnozować, przejdź do rozdziału [Nie mogę zainstalować agentów, monitorować liczników, inwentaryzować](#).

4.2.2 Monitorowanie urządzeń SNMP

Planowanie monitorowania

Aby właściwie monitorować wszystkie urządzenia w sieci, konieczne jest wykonanie kilku niezbędnych kroków - zanim skaner sieciowy zostanie uruchomiony. Przede wszystkim należy odpowiednio skonfigurować urządzenia SNMP (najważniejsze jest ustawienie właściwego adresu IP i wspólnoty SNMP). Aby dowiedzieć się więcej o konfiguracji urządzeń SNMP, skorzystaj z odpowiedniej dokumentacji urządzenia.

Konfiguracja danych logowania

Aby monitorować SNMP należy podać wspólnotę SNMP. Wspólnotę możesz określić w oknie właściwości urządzenia w zakładce **Dane logowania**.

Wymagania przy monitorowaniu urządzeń SNMP

Monitorowanie	Używany protokół	Wymagania
Liczniki wydajności SNMP	SNMP	<ul style="list-style-type: none"> • Właściwie ustawione dane logowania. • Urządzenie skonfigurowalne jako zarządzalne przez SNMP.
Porty i interfejsy na switch'ach i router'ach		<ul style="list-style-type: none"> • Przynajmniej jeden interfejs zaznaczony jako wspierający SNMP.
Ruch sieciowy		<ul style="list-style-type: none"> • SNMP właściwie skonfigurowane na zdalnym urządzeniu. • Dostępność określonych OID-ów i tabel SNMP na urządzeniu.

Poza powyższymi wymaganiami, zaporą na zdalnym komputerze musi być właściwie skonfigurowana. Poniższa tabela przedstawia porty, które muszą być otwarte:

Protokół lub monitor	Porty, które muszą być otwarte
SNMP	UDP 161,162

4.2.3 Inwentaryzacja

Planowanie inwentaryzacji

Do inwentaryzacji sieci nVision wykorzystuje protokół WMI lub agenty nVision. Każda z tych metod ma inne wymagania.

Wymagania przy inwentaryzacji przez WMI

Aby połączyć się ze zdalnym komputerem przez protokół WMI, nVision musi mieć jego dane logowania (nazwa użytkownika /hasło). Musisz je ustawić we właściwościach urządzenia w zakładce **Dane logowania**.

Monitorowanie	Używany protokół	Wymagania
Liczniki wydajności Windows	WMI	<ul style="list-style-type: none"> • Właściwie ustawione dane logowania. • WMI udostępnione na zdalnym komputerze. Aby się dowiedzieć, jak uruchomić WMI, przejdź do rozdziału Monitorowanie i zarządzanie Windows przez WMI.
Dystrybucja plików		
Zasoby (przez WMI)		

Poza powyższymi wymaganiami, zaporą na zdalnym komputerze musi być właściwie skonfigurowana. Poniższa tabela przedstawia porty, które muszą być otwarte:

Protokół lub monitor	Porty, które muszą być otwarte
WMI	TCP 135,139,445,593

Jeśli w dalszym ciągu masz problemy, aby je zdiagnozować, przejdź do rozdziału [Nie mogę zainstalować agentów, monitorować liczników, inwentaryzować](#).

Wymagania przy inwentaryzacji przez agenty

Aby przeprowadzać inwentaryzację za pomocą agentów, należy je zainstalować na każdym zdalnym komputerze. Instrukcje dotyczące instalowania agentów znajdują się w rozdziale [Instalacja agentów](#).

Moniotorowanie	Uzywany protokół	Wymagania
Zasoby (przez agenty)	HTTP	<ul style="list-style-type: none"> Agent zainstalowany na zdalnym komputerze. Otwarty port 4434 (TCP) na komputerze z nVision. Otwarty port TCP 4433 na zdalnym komputerze (zalecane).

Poza powyższymi wymaganiami, zaporę na zdalnym komputerze musi być właściwie skonfigurowana. Poniższa tabela przedstawia porty, które muszą być otwarte:

Protokół lub monitor	Porty, które muszą być otwarte
Agenty	<ul style="list-style-type: none"> Otwarty port TCP 4433 na zdalnym komputerze (zalecane). Otwarty port 4434 (TCP) na komputerze z nVision.
Zdalny dostęp	<ul style="list-style-type: none"> Otwarty port TCP 37659 na zdalnym komputerze

Agenty i nVision otwierają wymagane porty w zaporze Windows automatycznie. Jeśli jednak masz jeszcze jakąś inną zaporę, musisz otworzyć je ręcznie.

4.2.4 Monitorowanie aktywności użytkowników

Planowanie monitorowania

Do monitorowania aktywności użytkowników nVision wykorzystuje agenty.

Wymagania przy monitorowaniu aktywności użytkowników

Aby monitorować aktywność użytkowników, musisz zainstalować agenta nVision na każdym komputerze. Instrukcje dotyczące instalowania agentów znajdują się w rozdziale [Instalacja agentów](#).

Monitorowanie	Uzywany protokół	Wymagania
Aktywność użytkowników	HTTP	<ul style="list-style-type: none"> Agent zainstalowany na zdalnym komputerze. Otwarty port TCP 4434 na komputerze z nVision. Otwarty port TCP 4433 na zdalnym komputerze (zalecane).

Poza powyższymi wymaganiami, zaporę na zdalnym komputerze musi być właściwie skonfigurowana. Poniższa tabela przedstawia porty, które muszą być otwarte:

Protokół lub monitor	Porty, które muszą być otwarte
Agenty	<ul style="list-style-type: none"> Agent zainstalowany na zdalnym komputerze. Otwarty port TCP 4434 na komputerze z nVision.
Zdalny dostęp	<ul style="list-style-type: none"> Otwarty port TCP 37659 na zdalnym komputerze.

Agenty i nVision otwierają wymagane porty w zaporze Windows automatycznie. Jeśli jednak masz jeszcze jakąś inną zaporę, musisz otworzyć je ręcznie.

4.2.5 Zdalny dostęp

Planowanie monitorowania

Aby zapewnić zdalny dostęp do komputerów, nVision wykorzystuje agenty.

Wymagania przy zdalnym dostępie

Aby uzyskać zdalny dostęp do komputerów, musisz zainstalować na nich agenty. Instrukcje dotyczące instalowania agentów znajdują się w rozdziale [Instalacja agentów](#).

Monitorowanie	Używany protokół	Wymagania
Zdalny dostęp	HTTP	<ul style="list-style-type: none"> Agent zainstalowany na zdalnym komputerze. Otwarty port TCP 37659 na zdalnym komputerze.

Poza powyższymi wymaganiami, zaporę na zdalnym komputerze musi być właściwie skonfigurowana. Poniższa tabela przedstawia port, który musi być dostępny:

Protokół lub monitor	Porty, które muszą być otwarte
Zdalny dostęp	<ul style="list-style-type: none"> Otwarty port TCP 37659 na zdalnym komputerze.

Agent otwiera wymagany port w zaporze Windows automatycznie. Jeśli jednak masz jeszcze jakąś inną zaporę, musisz otworzyć go ręcznie.

4.2.6 Monitorowanie serwisów TCP na Windows XP + SP2

Microsoft wprowadził znaczącą zmianę w Windows XP Service Pack 2, która może powodować poważne problemy podczas monitorowania serwisów TCP. Stos TCP/IP posiada limit na liczbę jednocześnie półotwartych wychodzących połączeń TCP (do 10). Po osiągnięciu limitu, kolejne próby połączenia umieszczane są w kolejce i obsługiwane w stałym tempie. Podczas normalnej pracy, kiedy aplikacje łączą się z dostępnymi serwerami i poprawnymi adresami IP, limit ten nie ma znaczenia. Kiedy zostanie przekroczony, zdarzenie ID 4226 pojawia się systemowym dzienniku zdarzeń.

Kiedy taka sytuacja ma miejsce (przekroczenie limitu), większość albo nawet wszystkie serwisy TCP przestają się w ogóle monitorować. Wynika to z faktu, iż wszystkie zadania są wstawiane do kolejki systemowej i nie są wysyłane do monitorowanych serwisów.

W razie monitorowania wielu serwisów TCP, należy:

1. Zainstalować nVision na Windows 2000, 2003 Server or Windows XP without SP2.
2. Jeśli program jest zainstalowany na Windows XP z SP2, należy usunąć limit za pomocą łatki dostępnej na stronie: <http://www.lvllord.de/> Program ten umożliwia zwiększenie limitu.

4.2.7 Monitorowanie i zarządzanie Windows przez WMI

Udostępnianie monitorowania liczników Windows

Protokół WMI (używany przez WinTools, zbieranie informacji o zasobach i monitorowanie liczników wydajności Windows) jest dostępny na Windows 2000 i 2003 Server. Jednak aby uzyskać informacje z komputerów Windows XP Professional i Vista należy wykonać kilka czynności. Aby je przyspieszyć przygotowaliśmy program (WMIEnable.exe), który automatycznie wykona niezbędne operacje. Aby udostępnić WMI, należy uruchomić ten program na zdalnym komputerze. Można uruchomić go ze skryptu logowania, co zapewni dostępność WMI na wszystkich Windows XP. **If you are using any third party firewall on the remote node, then you also need to open the following ports: TCP 135, 139, 445, 593.**

Aby używać WinTools lub odczytać zasoby z Windows XP Home należy pamiętać, że system zdalny musi mieć dokładnie te same dane logowania (nazwę użytkownika i hasło) co użytkownik zalogowany na komputerze gdzie działa NetTools i nVision.

WMIEnable

Program ten udostępnia WMI na Windows XP Professional i Vista. Poniżej znajduje się lista operacji wykonywanych przez program:

1. DCOM jest w³¹czony przez ustawienie klucza rejestru [HKEY_LOCAL_MACHINE\Software\Microsoft\OLE\EnableDCOM] na wartoœæ "Y".
2. Zdalny UAC na Windows Vista jest w³¹czony przez ustawienie klucza rejestru [HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy] na wartoœæ 1.
3. Porty WMI (TCP 135,139,445,593) s¹ otwierane na zaporze Windows przez wykonanie komendy: netsh firewall set service RemoteAdmin
4. Dostêp do WMI na Windows Vista jest udostêpniany przez dodanie wyjątku zapory dla "Windows Management Instrumentation (WMI)".
5. Model autoryzacji jest ustawiany na "Local user authorize as themselves" przez ustawienie wartoœci klucza rejestru [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\forceguest] na wartoœæ 0.

Zwykle restart systemu nie jest konieczny a WMI b¹dzie dostêpne zaraz po wykonaniu programu, mo¿na jednak wymusiæ restart systemu przez uruchomienie programu z parametrem **/restart**. Program nie dokona restartu jeœli ustawienie parametrów systemu siê nie powiedzi¹.

Jeœli WMI dalej nie dzia³a

Jeœli WMI nie dzia³a pomimo uruchomienia programu WMIEnable, nale¿y sprawdziæ

1. Uruchom Local Security Settings (secpol.msc /s) wybierz Local Policies -> User Rights Assignment -> Access this computer from network. Sprawdź czy wszystkie w³¹czone grupy/u¿ytkownicy s¹ dodani. Przynajmniej grupa Administrators lub Administrator powinni byæ dodani.
2. Sprawdź czy WMI dzia³a przez wywo³anie komendy : **"wbemtest"**. WMI dzia³a jeœli program ten dzia³a poprawnie.
3. Sprawdź, czy nastêpuj¹ce serwisy s¹ uruchomione:
COM+ Event System
Remote Access Auto Connection Manager
Remote Access Connection Manager
Remote Procedure Call (RPC)
Remote Procedure Call (RPC) Locator
Remote Registry
Server
Windows Management Instrumentation
Windows Management Instrumentation Driver Extensions
WMI Performance Adapter
Workstation

Wycieki pamieci przez stara wersjeRpcrt4.dll

W razie monitorowania liczników wydajności Windows, należy upewnić się, że zainstalowana jest najnowsza wersja pliku Rpcrt4.dll. Wszystkie poprzednie wersje powodują poważne wycieki pamięci w systemie, co może doprowadzić do awarii systemu. Problem ten jest opisany przez Microsoft na stronie <http://support.microsoft.com/?kbid=911262>
Plik Rpcrt4.dll powinien być w poni¿szej wersji (lub wy¿szej):

System	Wersja	Rozmiar pliku
Windows 2003	5.2.3790.2900	582,144
Windows XP	5.1.2600.2810	643,072

4.3 Rozwiązywanie problemów

4.3.1 Nie mogę zainstalować agentów, monitorować liczników i inwentaryzować

Rozdział ten wyjaśnia, dlaczego nie jesteś w stanie:

- Zainstalować agentów nVision
- Inwentaryzować zasobów (przez WMI)
- Monitorować liczniki Windows
- Dystrybuować plików
- Używać narzędzi WinTools (dostępne w NetTools)

i co zrobić, aby wykonać powyższe zadania.

Dlaczego nVision tego nie wykonuje

Wszystkie wymienione zadania są wykonywane za pomocą protokołu WMI. Musi on więc być uruchomiony i dostępny na zdalnym komputerze. Musisz upewnić się, że serwisy WMI są uruchomione, model autoryzacji jest prawidłowo ustawiony i że wszystkie wymagane porty są otwarte w zaporze. Kluczowe jest także skonfigurowanie danych logowania urządzenia (nazwa użytkownika i hasło).

WMI (wykorzystywane przy inwentaryzacji, przez narzędzia WinTools oraz przy monitorowaniu liczników wydajności) jest domyślnie w pełni udostępnione na Windows 2000 i 2003 Server. Ale na komputerach z Windows XP Professional lub Vista jest zablokowane przez zaporę i niewłaściwy model autoryzacji. Aby zautomatyzować wykonanie tych zadań, przygotowaliśmy specjalny program (WMIEnable.exe), który wykonuje wszystkie konieczne operacje. Aby dowiedzieć się więcej o WMIEnable.exe, przejdź do rozdziału [Monitorowanie Windows przez WMI](#).

Jak wykonać te zadania

Oto lista kroków, które musisz wykonać, aby uruchomić WMI:

- 1. Uruchom WMIEnable.exe na zdalnym urządzeniu.**

Znajduje się on w katalogu programu i należy go skopiować na zdalny komputer. Program ten wykonuje następujące czynności:

 - Włącza DCOM
 - Włącza Zdalny UAC na Windows Vista
 - Ustawia model autoryzacji na "Local user authorize as themselves"
 - Konfiguruje zaporę Windows tak, aby otworzyć wszystkie porty WMI.
- 2. Otwórz porty WMI, jeśli jest to konieczne**

Jeśli używasz jakiegokolwiek dodatkowej zapory na zdalnym komputerze, musisz otworzyć następujące porty: TCP 135, 139, 445, 593.
- 3. Konfiguruje dane logowania.**

Przejdź do okna właściwości urządzenia i otwórz zakładkę **Dane logowania**. Wybierz istniejące już dane logowania systemu, lub wybierz <Dostosuj>, aby wprowadzić nowe dane logowania. Teraz możesz przetestować dane logowania i łączność WMI - kliknij małą strzałkę na przycisku znajdującym się obok pola rozwijanej listy (pola combo) danych logowania systemu i wybierz z menu **Testuj dane logowania**. Program będzie próbował połączyć się ze zdalnym komputerem przez WMI i poinformuje, jaki jest tego rezultat.

Jesli w dalszym ciagu funkcje nie dzialaja

Przejdź do rozdziału [Monitorowanie Windows przez WMI](#), aby dowiedzieć się, jak ustalić przyczynę problemów.

Jesli potrzebujesz jedynie zainstalowac agenty lub nie chcesz uruchamiac WMI

Jesli jedynie chcesz zainstalowac agenty i nie chcesz uruchamiac WMI, musisz zainstalowac agenty recznie. aby uzyskac wiecej informacji, przejdź do rozdziału [Instalowanie agentów](#).

4.3.2 Nie mogę uzyskać informacji o aktywności użytkowników i zasobach

Rozdział ten wyjaśnia, dlaczego nie jesteś w stanie:

- Uzyskać od agentów informacji o aktywności użytkowników
- Uzyskać informacji o zasobach (przez agenty)
- Uzyskać podglądu pulpitu użytkownika
- Zdalnie kontrolować komputerów

i co zrobić, aby wykonać powyższe zadania.

Dlaczego nVision tego nie wykonuje

Wszystkie powyższe zadania są wykonywane przy pomocy połączeń TCP pomiędzy konsolą nVision i agentem na zdalnym komputerze. Musisz więc upewnić się, że odpowiednie porty są otwarte po obu stronach. nVision i agenty otwierają te porty na zaporze Windows, ale jeśli korzystasz z jakiegось innej zapory, musisz sam je otworzyć.

Jesli wykonujesz inwentaryzacje przez WMI, aby rozwiaczac problem, przejdź do rozdziału [Nie moge zainstalowac agentów, monitorowac liczników i inwentaryzowac](#).

Jak wykonac te zadania

Oto lista portów, które należy otworzyć, aby umożliwić wykonywanie zadań agentom:

- 1. Otwarty port 4434 (TCP) na komputerze z nVision**
Port ten jest odpowiedzialny za przyjmowanie wszystkich danych przysyłanych przez agenta (dane o aktywności użytkowników, o zasobach, zrzuty z pulpitu)
- 2. Otwarty port 4433 (TCP) na zdalnym komputerze**
Poprzez ten port, agenty otrzymują wszystkie zapytania od nVision. Jeđli jest on zamknięty, nVision będzie co prawda otrzymywało dane o aktywności użytkownika, ale nie będzie w stanie zarządać tych danych - jeđli potrzebujesz ich szybciej i jeđli chcesz przesłać zrzut ekranowy pulpitu.
- 3. Otwarty port 37659 (TCP) na zdalnym komputerze**
Port ten jest wykorzystywany przy zdalnym dostępie. Port ten może być zamknięty, jeśli nie korzystasz ze zdalnej kontroli komputerów.

4.3.3 Nie mogę uzyskać informacji o zasobach

Rozdział ten wyjaśnia, dlaczego nie jesteś w stanie uzyskać informacji o zasobach i co zrobić, aby to wykonać.

Dlaczego nVision tego nie wykonuje

nVision może gromadzić informacje o zasobach przez agenty lub protokół WMI. Na początku musisz

wybrać metode, która jest dla najbardziej odpowiednia: agenty muszą być zainstalowane na wszystkich komputerach - wymaga to więc więcej pracy (ale zapewnia więcej funkcji oraz większe bezpieczeństwo); WMI jest udostępniane na każdym komputerze Windows, ale obniża bezpieczeństwo systemu i musi być włączone na Windows XP.

Jak inwentaryzować przez agenty

Aby inwentaryzować sieć za pomocą agentów, musisz zainstalować je na wszystkich komputerach. Należy także otworzyć odpowiednie porty: port TCP 4434 na komputerze z uruchomionym nVision (koniecznie) i porty TCP 4433 oraz 37659 na każdym zdalnym komputerze (zalecane). Jeśli będziesz miał z tym jakikolwiek problem, przejdź do rozdziału [Nie mogę uzyskać informacji o aktywności użytkowników i zasobach](#), aby uzyskać więcej informacji o konfigurowaniu agentów.

Instrukcje dotyczące instalowania agentów znajdują się w rozdziale [Instalacja agentów](#).

Jak inwentaryzować przez WMI

Zadanie to jest wykonywane przez protokół WMI. Musi on więc być uruchomiony i dostępny na każdym zdalnym urządzeniu. Należy upewnić się, że wszystkie serwisy WMI są uruchomione, model autoryzacji jest odpowiednio ustawiony i że wszystkie wymagane porty są otwarte na zaporze. Należy również skonfigurować dane logowania (nazwę użytkownika i hasło) każdego komputera.

Aby dowiedzieć się więcej, przejdź do rozdziału [Nie mogę zainstalować agentów, monitorować liczników i inwentaryzować](#). Wyясnia on, w jaki sposób uruchomić i skonfigurować WMI na zdalnych komputerach.

Część

V

5 Wykrywanie i monitorowanie sieci

5.1 Wprowadzenie

Wymagania i planowanie

Przed rozpoczęciem monitorowania sieci, należy zapoznać się z rozdziałem [Wymagania i planowanie](#). Opisuje on sposób przygotowania urządzeń oraz sieci, tak aby uzyskać wszelkie konieczne informacje.

Wykrywanie sieci

nVision posiada wbudowany, zaawansowany skaner sieciowy który nie tylko wykrywa wszystkie urządzenia w sieci, ale także routery przez które "przechodzi" wykrywając wszystkie sąsiednie sieci. Wykrywa wszystkie urządzenia oraz serwisy na nich działające, takie jak: HTTP, FTP, poczta, serwery bazodanowe, itp.

Do atlasu można dodać dowolną liczbę sieci. Po dodaniu sieci, jest ona skanowana, a więc w pierwszej kolejności należy użyć kreatora skanera sieci, aby zdefiniować opcje wykrywania.

Po ukończeniu procesu skanowania, program utworzy mapę sieci, lub ich zestaw dla wszystkich wykrytych sieci IP. Sieci zostaną utworzone jako drzewo, które pokazuje zależności pomiędzy nimi.

Aby dowiedzieć się więcej o procesie skanowania, przejdź do rozdziału [Wykrywanie sieci - Wprowadzenie](#).

Monitorowanie urządzeń

nVision może monitorować serwisy sieciowe, liczniki systemowe i SNMP. Nie tylko monitoruje, ale zapisuje wszelkie informacje i pozwala przeglądać historyczne dane w celu raportowania.

Aby uzyskać więcej informacji, przejdź do rozdziału [Monitorowanie - Wprowadzenie](#).

Stan urządzenia

Stan urządzenia to bardzo ważne pojęcie, której poświęcony został osobny rozdział: [Pojęcie stanu urządzenia](#). Absolutnie wskazane jest zapoznanie się z tym rozdziałem, aby całkowicie zrozumieć jak nVision prezentuje stan urządzenia.

5.2 Pojęcie stanu urządzenia

Rozdział ten opisuje pojęcie stanu urządzenia - jest ono bardzo ważne, dlatego poświęcony jest mu cały rozdział. Powinieneś go przeczytać, nawet jeśli znasz już inne programy do monitorowania sieci.

Stan urządzenia jako wartość wyliczona

Odmienne niż w przypadku innych produktów, stan urządzenia w nVision może być zmieniony przez zdarzenia. Można zdefiniować warunki, w których urządzenie uzyska stan <Nieznany>, <Działa>, <Nie działa> lub <Ostrzeżenie>. Stan urządzenia zmienia się też w zależności od stanu monitorowanych serwisów.

Automatyczna zmiana stanu

Stan urządzenia początkowo ustawiony jest na <Nieznany>. Zmienia się, gdy nVision rozpoczyna monitorowanie serwisów. Gdy tylko pierwszy serwis zostanie sprawdzony i działa, stan zmieni się na <Działa>. Stan <Ostrzeżenie> oznacza, że istnieją serwisy, które nie działają, ale przynajmniej jeden serwis działa. Stan zmienia się na <Nie działa> jeśli żaden serwis nie działa.

Zmiana stanu przez zdarzenia

Bardzo ważne jest, aby zrozumieć, że nVision określa stan urządzenia także na podstawie aktualnie wygenerowanych alarmów. W tym celu można zdefiniować pole **Zmien stan urządzenia na** w każdym zdarzeniu. Kiedy alarm dla danego zdarzenia jest wygenerowany, wtedy stan urządzenia może zmienić się zgodnie ze zdefiniowaną wartością.

W polu tym można zdefiniować trzy wartości: <Bez zmiany>, <Ostrzeżenie> oraz <Nie działa>. Stan <Nie działa> ma najwyższy priorytet, co oznacza, że jeśli choć jedno zdarzenie ma taki stan, wtedy stan urządzenia również zmieni się na <Nie działa> (niezależnie od stanu monitorowanych serwisów). Jeśli wygenerowanych jest kilka zdarzeń o stanie <Ostrzeżenie> i <Nie działa> wtedy stan urządzenia będzie także <Nie działa>. Jeśli wygenerowane były tylko zdarzenia o stanie <Ostrzeżenie> wtedy stan urządzenia też zmieni się na <Ostrzeżenie> (chyba, że stan już jest <Nie działa> ze względu na niedziałające serwisy - wtedy stan pozostanie <Nie działa>).

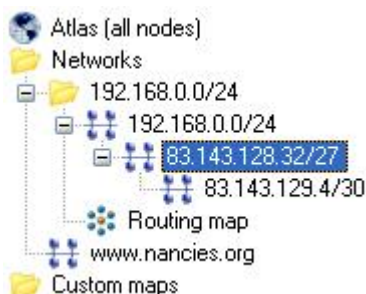
5.3 Skanowanie sieci

5.3.1 Wprowadzenie

Do atlasu można dodać dowolną liczbę sieci. Aby dodać sieć należy skorzystać ze skanera sieciowego, który wykryje wszystkie urządzenia.

1. Kliknij przycisk **Wykryj nowa sieć**. Otworzy się kreator skanera sieci. Kreator ten pomoże wykryć sieć, wszystkie urządzenia oraz utworzyć mapy sieci.
2. Przejdź przez kolejne kroki kreatora. Informacje dotyczące dostępnych w nim opcji znajdują się w rozdziale [Kreator wykrywania sieci](#).

Po zakończeniu procesu skanowania program utworzy mapę wykrytej sieci lub zestaw takich. Sieci będą utworzone jako drzewo pokazujące zależności pomiędzy nimi - sieci utworzone pod określoną mapą są przyłączone właśnie do niej. Prezentuje to poniższy przykład:



Jak można zauważyć sieć 83.143.128.32 jest utworzona pod siecią 192.168.0.0. Oznacza to, że sieci te połączone są przez router. nVision wykrywa wszystkie routery oraz podłączone sieci, co pozwala zobaczyć strukturę logiczną sieci.

5.3.2 Kreator skanowania sieci

Kreator skanowania sieci pozwala zdefiniować opcje konieczne do przeprowadzenia właściwego skanowania sieci. Uruchamiany jest jeśli chcemy dodać nową sieć i podczas tworzenia atlasu.

Kreator skanowania sieci zawiera kilka planów pozwalających zdefiniować opcje.

Podczas tworzenia atlasu

Kiedy tworzony jest atlas, kreator wyświetla dodatkową planszę, gdzie podaje się nazwę atlasu i kilka innych informacji.

Właściwość	Opis
Nazwa atlasu	Nazwa atlasu (zestawu map sieci)

Wlasciwosc	Opis
Utwórz atlas dla swojej sieci	Opcja zalecana: pozwoli wyskanowac twoja siec, utworzyc mapy i rozpoczac monitorowanie.
Utwórz pusty atlas	Wybranie tej opcji spowoduje utworzenie pustego atlasu i jest wskazane tylko dla zaawansowanych uzytkownikow. Nie wlaczaj jej jezeli uruchomiles program po raz pierwszy.
E-mail	Adres e-mail posluzy do stworzenia predefiniowanej akcji alarmowej.

Opcje skanowania nowej sieci

Pozwala zdefiniowac jaka siec i w jaki sposob bedzie skanowana.

Wlasciwosc	Opis
Adres	Podaj adres IP/DNS komputera znajdujacego sie w sieci, która ma byc skanowana. Program domyslnie podpowiada lokalny adres, który nalezy pozostawic, jesli skanujemy siec lokalna.
Maska	Maska sieciowa. W wiekszosci przypadków nie ma koniecznosci zmiany domyslnej maski o wartosci "255.255.255.0". Zmiany moze spowodowac bardzo dlugi czas skanowania.
Mala siec	Wybierz jesli chcesz skanowac tylko wybrana siec.
Siec z podsieciami	Wybierz ta opcje, jesli w twojej sieci jest router i chcesz takze wyskanowac sasiednie sieci, znajdujace sie za routerem. nVision moze skanowac nie tylko podana siec, ale potrafi tez "przechodzic" routery znajdujace sie w tej sieci, aby wyskanowac wszystkie podlaczone sieci. Funkcja ta wymaga udostepnionego na routerze protokolu SNMP oraz podania wspólnoty SNMP. Program odczyta tabele routingu i zacznie skanowac wszystkie sieci podlaczone przez ten router.
Limituj skan do	Pozwala okreslic limit hopów (routerów) podczas skanowania.
Tylko prywatne adresy	Wlacz ta opcje jesli masz duza siec z wieloma routerami a wszystkie adresy IP pochodza z puli adresów prywatnych. Program przejdzie przez wszystkie routery i wyskanuje wszystkie sieci wylaczajac te, które maja publiczne adresy IP.
Uzyj skanowania dokladnego	Wlacz ta opcje jesli podczas skanowania wystepuja jakies problemy i nie wszystkie urzadzenia sa wykrywane. Zwieksza to zarówno liczbe zadan i limit czasu odpowiedzi, moze jednak znacząco wydłużyc proces skanowania.
Nie zezwalaj na krótkie maski sieciowe	Wlacz, aby zapobiec uzyciu przez skaner maski sieciowej krótszej niz 255.255.255.0. Konfiguracja na niektórych routerach moze spowodowac, ze skaner bedzie próbował skanowac siec z krótką maską - np. 255.255.0.0 - co spowoduje wyjątkowo dlugi czas skanowania.
Ustaw dane logowania	Pozwala skonfigurowac dane logowania dla Windows i SNMP, tak aby siec byla wlasciwie wyskanowana.

Dane logowania

Plansza ta jest dostepna tylko podczas tworzenia atlasu (pierwszy skan sieci).

Wlasciwosc	Opis
Uzytkownik	Domyślna nazwa użytkownika, do logowania do komputerów Windows. Wprowadź najczęściej używane dane logowania – nVision będzie używać ich do monitorowania.
Haslo	Haslo domyslne.
Wspólnota SNMP do odczytu	Wprowadz wszystkie wspólnoty SNMP do odczytu jakie uzywasz w sieci. Jest to konieczne, aby poprawnie wyskanowac routery.

Opcje monitorowania

Wlasciwosc	Opis
Monitoruj ruch sieciowy na interfejsach	Jesli wlaczone - nVision odczyta informacje SNMP o interfejsach sieciowych i skonfiguruje monitorowanie ruchu na nich. Liczniki ruchu sieciowego dostepne beda na zakładce Liczniki wydajnosci w oknie Informacje o urzadzeniu.
Tylko jesli znaleziono wiecej niz jeden interfejs	Zaznacz, aby monitorowac ruch tylko na routerach. Nie bedzie on monitorowany na urzadzeniach z jednym interfejsem.
Monitoruj podstawowe parametry systemowe	Wlacz, aby nVision automatycznie tworzylo liczniki wydajnosci monitorujace CPU, pamiec i miejsce na dysku.
Tylko na routerach, serwerach i waznych/krytycznych urzadzeniach	Parametry systemowe beda monitorowane tylko na najwazniejszych urzadzeniach.
Inwentaryzuj zasoby	Wlacz jesli chcesz aby nVision inwentaryzowalo sprzet i oprogramowanie.
Monitoruj aktywnosc uzytkowników	Wlacz aby monitorowac aktywnosc uzytkowników za pomoca agentów nVision.
Konfiguruj wykrywane serwisy i czas monitorowania	Mozesz skonfigurowac opcje skanowania i monitorowania serwisów. Nie jest to wazne dla skanowania sieci, determinuje jednak jak beda monitorowane wykryte urzadzenia.
Okresowy wykrywaj nowe urzadzenia	Jesli opcja jest wlaczona, nVision bedzie automatycznie i cyklicznie skanowac sieci i wykrywac nowe urzadzenia. Proces ten moze byc skonfigurowany po utworzeniu map - w oknie wlasciwosci mapy.

Zadania koncowe

Kliknij przycisk **Zakonc**. Rozpocznie to proces skanowania, który bedzie mozna sledzic. Proces ten mozna w dowolnej chwili przerwac. W takim przypadku mozna dodac sieci i urzadzenia juz wykryte.

Po zakonczeniu skanowania, pokaze sie okno okreslajace liczbe wykrytych sieci/urzadzen. Kliknij OK, aby zamknac skaner i dodac do atlasu wykryte sieci i urzadzenia.

5.3.3 Dodawanie nowego urzadzenia

Opis dodawania nowego urzadzenia znajduje sie w rozdziale [Zarzadzanie urzadzeniami](#).

5.4 Monitorowanie

5.4.1 Wprowadzenie

Co może być monitorowane

nVision może monitorować:

- **Stan urządzenia**
Monitorowany jest dla każdego urządzenia i pozwala uzyskać raporty na temat dostępności urządzeń w czasie.
- **Serwisy**
 - Dostępność: jeśli serwis przestanie odpowiadać nVision pokazuje taką informację na mapie i może wygenerować alarm.
 - Wydajność: czas odpowiedzi i procent utraconych pakietów. Można monitorować dowolny serwis TCP/UDP. nVision posiada dużą listę predefiniowanych serwisów takich jak MS SQL Server, Oracle, Notes/Domino, itp.
- **Serwery pocztowe i WWW**
Specjalne testy serwisów: nVision posiada kilka wbudowanych próbników, które mogą sprawdzać wydajność wysokopoziomowych funkcji pewnych serwisów). Są to następujące próbniki:
 - Czas ładowania strony - mierzy czas załadowania określonej strony.
 - Zmiana treści strony - sprawdza czy zawartość strony nie uległa zmianie.
 - Czas logowania do POP3 - mierzy czas potrzebny na zalogowanie się do serwera POP3 i sprawdzenia listy dostępnych emaili.
 - Czas wysłania przez SMTP - mierzy czas potrzebny na wysłanie emaila przez serwer SMTP.
- **Routery i switch'e (MRTG)**
 - Interfejsy sieciowe: stan i we/wy ruch sieciowy.
 - Porty switch'a: informacja o stanie portu, adres MAC oraz IP komputerów podłączonych do dowolnego portu oraz ilość przetransmitowanych danych.
 - Ruch sieciowy urządzenia: ruch sieciowy generowany przez urządzenie (monitorowanie przez RMON za pomocą SNMP)
- **Liczniki wydajności**
 - SNMP: można monitorować dowolny licznik SNMP, który zwraca wartość liczbowa.
 - Windows: nVision może monitorować liczniki systemu Windows co pozwala monitorować wydajność systemu oraz aplikacji na nim działających. W ten sposób można monitorować liczniki serwisów takich jak serwery MS SQL, Exchange, itp.
- **Aktywność użytkowników**
 - Obciążenie sieci
 - Czas aktywności
 - Przeglądane strony WWW
 - Użycie aplikacji

Wizualizacja

nVision prezentuje wszystkie monitorowane parametry (zarówno serwisy jak i liczniki) na przejrzystych wykresach. Pokazują one nie tylko raporty zmian wartości w czasie, ale także pozwalają śledzić je w czasie rzeczywistym.

Wydajność monitorowania

nVision zostało przygotowane z myślą o monitorowaniu dużych sieci posiadających 5 000 urządzeń, zakładając, że dla każdego z nich monitorujemy 5-10 serwisów/liczników. W rzeczywistości nie ma

potrzeby, aby monitorować tyle parametrów na każdym urządzeniu, możliwe jest więc monitorowanie ok 10 000 urz¹ dzeń. Przy tej liczbie monitorowanych urz¹ dzeń, konieczny jest szybki procesor i przynajmniej 512 MB RAM.

Czas monitorowania

Ustawienie czasu monitorowania we właściwościach urządzenie nie oznacza, że serwisy i liczniki będą monitorowane dokładnie co zadany okres. Jeśli nVision monitoruje dużą sieć z wieloma urządzeniami, okres monitorowania może się wydłużyć, ponieważ nVision może wysłać tylko określoną liczbę zapytań na sekundę. Jeśli program uruchomiony jest na Windows XP z Support Pack 2 dodatkowo limitowane są zadania TCP do 10 na sekundę. nVision może wysłać więcej, ale w takim przypadku będą one kolejgowane przez system. Sytuacja taka może prowadzić do utraconych pakietów/zapytań.

W związku z tym, czas monitorowania jest najkrótszym możliwym czasem w jakim serwisy i liczniki mogą być monitorowane. Jeśli urządzeń jest dużo, czas ten może się też znacząco wydłużyć.

Jak dane z monitorowania są przetwarzane

nVision początkowo gromadzi dane z monitorowania w pamięci. Informacja ta zbierana jest w formie kolejnych próbek zapisywanych w momencie każdego sprawdzenia. Można zobaczyć wszystkie próbki tylko na wykresie 15-minutowym. Jeśli zebrane dane przekrocza limit zajętości pamięci, najstarsza próbka jest usuwana za każdym razem, gdy dodawana jest nowa. Aby zwiększyć liczbę próbek, jakie mogą być zgromadzone w pamięci, zwiększ opcję **Maksymalna zajętość pamięci przez dane z monitorowania**. Przejdź do rozdziału [Opcje](#) aby uzyskać więcej informacji.

Dane z monitorowania zapisywane są do bazy jako 1-minutowe średnie wartości. Dlatego przeglądając wykresy dla dłuższych okresów, dane prezentowane są co najwyżej z rozdzielczością 1-minutową. nVision nie zapisuje wszystkich próbek, ze względu na możliwość monitorowania dużych sieci. W takich sieciach, z dużą liczbą urządzeń, ilość danych gromadzonych codziennie jest znaczna i nie byłoby możliwe ich szybkie przetwarzanie.

5.4.2 Pojęcia

Skaner serwisów i monitor

Po znalezieniu wszystkich urządzeń w sieci nVision wykrywa serwisy na nich działające. Skanowane są tylko wybrane serwisy. Aby uzyskać więcej informacji na temat wyboru skanowanych serwisów, przejdź do rozdziału [Opcje programu](#).

Skaner serwisów nie tylko sprawdza, czy odpowiedni port jest otwarty. Wysyła określone zapytanie i sprawdza, czy odpowiedź odpowiada zdefiniowanemu kryteriom. Jeśli tak, serwis jest dodawany do urządzenia i nVision rozpoczyna jego monitorowanie.

Monitor serwisów używa tej samej metody co skaner: wysyła zapytanie przez TCP/UDP i zapamiętuje czas odpowiedzi oraz procent zapytań (pakietów) utraconych. Sprawdza też, czy otrzymana odpowiedź pasuje do ustalonych kryteriów.

Monitor liczników

nVision pozwala monitorować kilka typów liczników wydajności. Poniższa tabela przedstawia dostępne liczniki:

Typ licznika	Opis
Stan urządzenia	Prezentuje stan urządzenia dla każdej minuty. Pozwala raportować dostępność urządzenia.

Typ licznika	Opis
SNMP	Liczniki SNMP udostępniane są przez protokół SNMP dostępne na routerach i większości serwerów. Pozwalają na monitorowanie takich informacji jak transfery sieciowe, liczba użytkowników, obciążenie CPU, itp.
Windows	nVision może monitorować dowolne liczniki Windows, włączając w to te podawane przez aplikacje nie systemowe, jak serwery MS SQL i Exchange.
Czas ładowania strony	Mierzy czas załadowania określonej strony WWW.
Zmiana strony	Określa zmianę określonej strony WWW.
Czas logowania POP3	Sprawdza czas potrzebny do zalogowania się do serwera POP3 i sprawdzenia listy dostępnych e-maili.
Czas wysłania SMTP	Mierzy czas konieczny do wysłania e-maila.

Monitorowanie informacji SNMP

nVision stale monitoruje kilka wartości SNMP takich jak "System name", "Location" oraz "Up time". Informacja ta jest dostępna w oknie **Informacje o urządzeniu**.

Stan urządzenia

Odmiennie niż w innych, podobnych produktach, stan urządzenia w nVision jest wartością wyliczoną, a nie zakodowaną na stałe. Można więc zdefiniować warunki w których urządzenie ma stan <Nie działa> oraz <Ostrzeżenie>. Aby uzyskać więcej informacji, zapoznaj się z rozdziałem [Pojęcie stanu urządzenia](#).

5.4.3 Monitorowanie serwisów

5.4.3.1 Wprowadzenie

Jak serwisy są wykrywane i monitorowane

nVision monitoruje serwisy UDP/TCP bazując na predefiniowanych regułach. Nie tylko sprawdza czy określony port jest otwarty, ale wysyła zadanie i czeka na odpowiedź. Potem odpowiedź ta jest sprawdzana pod kątem zgodności z określonymi regułami. Tylko takie zadania, gdzie odpowiedź jest poprawna, uznawane są jako świadczące o działaniu serwisu. Ten sam mechanizm wykorzystywany jest do wykrywania serwisów działających na urządzeniach. Zapewni to, że serwisy nie są omyłkowo wykrywane, gdy jakiś serwis działa na porcie przeznaczonym dla innego serwisu. Przykładowo, jeśli FTP będzie działał na porcie 80, nie zostanie wykryty serwis HTTP, jako że odpowiedź nie jest właściwa jako serwisu HTTP.

Serwis nie działa

Gdy serwis nie działa, otrzymuje stan <Nie działa>. Można to zobaczyć jako czerwoną ikonkę w tabeli serwisów dostępnej na zakładce **Serwisy** w oknie **Informacje o urządzeniu**.

Serwis wiodący

Dla każdego urządzenia jest zawsze zdefiniowany jeden serwis wiodący. Serwis ten jest oznaczony pogrubioną czcionką w tabeli serwisów w oknie **Informacje o urządzeniu**. Serwis wiodący jest najważniejszym serwisem urządzenia. Czas odpowiedzi tego serwisu może być prezentowany na ikonie urządzenia. Także czas odpowiedzi oraz procent utraconych zadań mogą być wizualizowane w wykresach wydajności (po lewej stronie ikony).

5.4.3.2 Zarządzanie monitorowanymi serwisami



Rozdział ten opisuje zarządzanie monitorowanymi serwisami.

Otwieranie okna Informacje o urządzeniu na zakładce Serwisy

Za pomocą tego okna można przeglądać, tworzyć, modyfikować i usuwać monitorowane serwisy. Okno nie tylko prezentuje wszystkie serwisy, ale także pokazuje wykresy czasu odpowiedzi w czasie. Wykresy te mogą przedstawiać informacje w czasie rzeczywistym.


1. Kliknij podwójnie na ikonie urządzenia lub wybierz **Informacje o urządzeniu** z menu kontekstowego.
2. Wybierz zakładkę Serwisy.

Dodawanie nowych serwisów do monitora lub modyfikowanie istniejącego

1. Otwórz okno **Informacje o urządzeniu** na zakładce **Serwisy**.
2. Kliknij ikonę  (zlokalizowana po prawej stronie pod tabelą serwisów) aby dodać nowy serwis lub wybierz istniejący serwis i kliknij ikonę  aby zmodyfikować jego właściwości. Otworzy się okno **Właściwości serwisu**.
3. Skonfiguruj opcje. Poniższa tabela opisuje ich znaczenie.

Właściwość	Opis
Serwis do monitorowania	
Nazwa	Wybierz serwis, który chcesz monitorować. Pole to nie może być zmienione podczas edycji istniejącego serwisu. Aby rozpocząć monitorowanie innego serwisu, należy go stworzyć.
Na interfejsie/IP	Wybierz adres na którym serwis ma być monitorowany.
Parametry monitorowania	
Czas monitorowania	Wybierz Auto aby nVision samo zarządzało czasem monitorowania tak, aby zapewnić jak najczęstsze sprawdzenia (zależnie od liczby monitorowanych urządzeń). Jeśli chcesz ustawić określoną wartość, wybierz Ustaw i wpisz tę wartość w polu edycji.
Zadania	Jest to liczba zadań wysyłanych podczas każdego sprawdzenia. Dla serwisów TCP wartość ta powinna być ustawiona na 1, ponieważ protokół ten ma własne mechanizmy chroniące przed utratą zadania (serwisy TCP same powtarzają utracone zadania, więc zwykle podawanie większej wartości nie miałoby sensu). Dla serwisów bazujących na ICMP i UDP warto podać 2-3 aby zagwarantować, iż przypadkowa utrata pakietów nie uruchomi fałszywego alarmu.
Limit czasu	Czas oczekiwania na odpowiedź. Jeśli nie zostanie otrzymana w tym czasie, zadanie jest uznawane za utracone. Dla serwisów ICMP i UDP wartość 1000 - 2000 ms będzie zwykle odpowiednia. Dla serwisów TCP, ze względu na ich właściwości, należy podać zdecydowanie wyższą wartość w przedziale 15 000 - 30 000 ms.

Usuwanie serwisu

1. Otwórz okno **Informacje o urządzeniu** na zakładce **Serwisy**.
2. Wybierz serwis.
3. Kliknij ikonę  aby usunąć serwis.

Ponowne wykrywanie serwisów urządzenia

1. Wybierz ikonę urządzenia.
2. Wybierz **Monitorowanie | Wykryj serwisy** z menu kontekstowego. nVision rozpocznie skanowanie nowych serwisów na wszystkich interfejsach/adresach urządzenia. Po zakończeniu, nowe serwisy zostaną dodane do listy i rozpocznie się ich monitorowanie.

Wybór serwisu wiodącego

Aby uzyskać informacje na temat serwisu wiodącego, przejdź do rozdziału [Monitorowanie serwisów - Wprowadzenie](#).

1. Otwórz okno **Informacje o urządzeniu** na zakładce **Serwisy**.
4. Wybierz serwis i wybierz **Ustaw jako wiodący** z menu kontekstowego. Serwis wiodący jest wskazywany pogrubioną czcionką.

5.4.4 Monitorowanie usług Windows

5.4.4.1 Wprowadzenie

nVision może monitorować serwisy Windows. W razie wystąpienia problemów z serwisem (np. serwis przestaje działać), można skonfigurować akcję alarmową, która uruchomi lub zrestartuje serwis. Monitorowanie serwisów jest wykonywane przez WMI, konieczne jest więc właściwe skonfigurowanie danych logowania w oknie właściwości urządzenia. WMI musi też być udostępnione na zdalnym urządzeniu. Aby uzyskać więcej informacji, przejdź do rozdziału [Wymagania i planowanie](#).

Aby włączyć monitorowanie serwisów Windows

1. Otwórz okno właściwości urządzenia.
2. Wybierz zakładkę **Monitorowanie**.
3. Włącz opcję **Monitoruj serwisy Windows**

Po włączeniu monitorowania serwisów Windows, można zobaczyć listę serwisów działających na zdalnym komputerze klikając przycisk **Serwisy Windows**, zlokalizowany na dole okna **Informacje o urządzeniu**.

5.4.5 Monitorowanie wydajności urządzenia i systemu

5.4.5.1 Wprowadzenie

nVision może monitorować kilka typów liczników wydajności i stan urządzenia.

Stan urządzenia

Jest to wbudowany licznik, monitorujący i zapisujący stan urządzenia. Licznik ten zapisywany jest co

minute, aby można było śledzić dostępność urządzenia w czasie.

Liczniki Windows i SNMP

nVision może monitorować liczniki Windows za pomocą WMI oraz liczniki SNMP. Liczniki te mogą być użyte do monitorowania wydajności systemu Windows, wydajności aplikacji (MS Exchange, IIS, SQL, itp.), switch'ów i routerów (ruch sieciowy, błędy, itp.).

Testy serwisów (monitorowanie serwerów pocztowych i WWW)

Jest to grupa liczników zaprojektowana do monitorowania serwerów pocztowych i WWW. Aby uzyskać więcej informacji, przejdź do rozdziału [Monitorowanie serwera pocztowego i WWW](#).

5.4.5.2 Typy liczników

Istnieje kilka grup liczników. Poniższa tabela opisuje grupy Dostępność urządzenia oraz Liczniki. Aby uzyskać więcej informacji o grupie Test serwisu, przejdź do rozdziału [Monitorowanie serwera pocztowego i WWW](#).

Dostępność urządzenia	
Stan urządzenia	Licznik ten zapisuje stan urządzenia dla celów raportowych. Jest to licznik wbudowany i nie może być usunięty.
Liczniki	
Liczniki SNMP	Mozna mierzyć dowolny licznik SNMP o wartości numerycznej. Program może też odczytać całą kolumnę tabeli i zapisać min/max/srednia/sume wartości komórek.
Licznik Windows	Mozna mierzyć dowolny licznik Windows o wartości numerycznej. Windows udostępnia liczniki systemowe i aplikacyjne. Pozwala to monitorować system oraz programy takie jak SQL Server i Exchange Server.

Liczniki określone dla urządzenia

Niektóre liczniki posiadają pełną informację konieczną do ich sprawdzenia, włączając w to adres urządzenia. Takie liczniki nazywamy Określonymi dla urządzenia. W ogólności wszystkie liczniki typu Testy serwisu są określone dla urządzenia. Na przykład, licznik **Czas ładowania strony**.

5.4.5.3 Zarządzanie licznikami wydajności



Rozdział ten opisuje zarządzanie licznikami wydajności.

Otwarcie okna Informacje o urządzeniu na zakładce Liczniki wydajności

W tym oknie można zobaczyć, zmodyfikować, tworzyć i usuwać liczniki. Liczniki nie tylko widoczne są w tabeli, ale także można przeglądać ich wartość w czasie na wykresie.

1. Kliknij podwójnie na ikonie urządzenia lub wybierz **Informacje o urządzeniu** z menu kontekstowego.
2. Wybierz zakładkę **Liczniki wydajności**.


Utworzenie nowego licznika lub modyfikacja istniejącego

1. Otwórz okno **Informacje o urządzeniu** na zakładce **Liczniki wydajności**.
2. Kliknij ikonę  (zlokalizowana po prawej stronie pod tabelą liczników) aby dodać nowy licznik lub wybierz istniejący licznik i kliknij ikonę  aby zmodyfikować jego właściwości. Otworzy się okno **Właściwości licznika**.
3. Jeśli tworzysz nowy licznik, wybierz jego typ z listy i kliknij przycisk **Dalej**. Aby dowiedzieć się

wiecej o typach liczników, przejdź do rozdziału [Typy liczników](#).

4. Skonfiguruj opcje licznika (zależnie od typu licznika jaki wybrales). Szczegóły opcji opisane sa w rozdziale [Definiowanie właściwości liczników](#).
5. Kliknij przycisk **Zakończ**.

Usuwanie licznika

1. Otwórz okno **Informacje o urządzeniu** na zakładce **Liczniki wydajności**.
2. Wybierz licznik, który chcesz usunąć.
3. Kliknij ikonę  aby usunąć licznik.

5.4.5.4 Tworzenie licznika na wielu urządzeniach


W wielu przypadkach konieczne jest stworzenie tego samego licznika na wielu urządzeniach. Można to zrobić używając funkcji automatycznego tworzenia liczników. Pozwala ona na stworzenie tego samego licznika Windows lub SNMP na wielu urządzeniach. Liczniki mogą być stworzone tylko na tych urządzeniach, które wspierają dany licznik - program sprawdzi, czy jest on dostępny na zdalnym urządzeniu.

1. Wybierz **Narzędzia | Utwórz licznik dla grupy urządzeń** z głównego menu. Otworzy się **Kreator definicji licznika**.
2. Wybierz **Windows** lub **SNMP**.
3. Wybierz liczniki i podaj czas monitorowania.
4. Wybierz **Wszystkie** aby utworzyć licznik na wszystkich urządzeniach lub **Wybrane** aby zaznaczyć urządzenia. Aby zaznaczyć kilka urządzeń, użyj Ctrl + klik i Shift + klik.
5. Jeśli chcesz, aby program sprawdził, czy licznik jest dostępny na poszczególnych urządzeniach, włącz **Utwórz tylko jeśli urządzenie wspiera licznik**. Dzięki temu można szybko utworzyć wiele liczników tylko na urządzeniach, które je udostępniają.

5.4.5.5 Definiowanie właściwości liczników

Rozdział ten opisuje właściwości poszczególnych typów liczników w grupie **Liczniki**.


Próg Windows

Właściwość	Opis
Nazwa	Nazwa ta będzie wyświetlona w tabeli.
Licznik	Licznik, który ma być monitorowany. Aby wybrać licznik, kliknij ikonę  i wybierz właściwą klasę, licznik i instancję. Może być konieczne ustawienie danych logowania, aby nVision mógł połączyć się ze zdalnym komputerem i pobrać listę liczników.
Interwał monitorowania	Jeśli wybierzesz Auto nVision będzie zarządzać czasem monitorowania, tak aby zapewnić odpowiednio częste sprawdzenia (zależnie od liczby monitorowanych urządzeń). Jeśli chcesz ustawić określoną wartość, wybierz Ustaw i wpisz ją w polu edycji.

Uwagi

- Program nVision będzie próbował zalogować się do zdalnego komputera za pomocą danych logowania podanych we właściwościach urządzenia.
- Liczniki Windows nie są monitorowane jeśli urządzenie ma stan <Nie działa>.

Próg SNMP

Właściwość	Opis
Nazwa	Nazwa ta będzie wyświetlona w tabeli.
Wybierz licznik SNMP	Licznik, który ma być monitorowany. Aby wybrać licznik, kliknij ikonę  i wybierz właściwą właściwość licznika SNMP. Można wybrać odczyt całej kolumny tabeli i zapis wartości min/max/sredniej/sumy wartości komórek. Może być konieczne ustawienie Wspólnoty SNMP do odczytu, aby nVision mógł połączyć się ze zdalnym urządzeniem i pobrać dane.
Podaj OID licznika SNMP	Licznik, który ma być monitorowany. Jeśli podasz wartość samodzielnie, jesteś odpowiedzialny za wprowadzenie poprawnej wartości. Jeśli OID nie jest poprawny, nie będzie odczytana żadna wartość.
Absolutna	Program zapisze odczytaną wartość.
Srednia na sek., jednostka	Bazując na kolejno odczytanych wartościach, nVision wyliczy szybkość zmiany na sekundę i zapisze tę wartość. Jest to właściwa opcja jeśli monitorujesz liczbę bajtów wysłanych/odebranych i chcesz monitorować obciążenie łącza. Możesz też wybrać jednostki w jakich wartość będzie zapisana.
Interwał monitorowania	Jeśli wybierzesz Auto nVision będzie zarządzać czasem monitorowania, tak aby zapewnić odpowiednio częste sprawdzenia (zależnie od liczby monitorowanych urządzeń). Jeśli chcesz ustawić określoną wartość, wybierz Ustaw i wpisz ją w polu edycji.

Uwagi

- Program nVision będzie próbował połączyć się do zdalnego komputera korzystając ze wspólnoty SNMP do odczytu podanej we właściwościach urządzenia.
- Liczniki Windows nie są monitorowane jeśli urządzenie ma stan <Nie działa>.

5.4.6 Monitorowanie serwerów pocztowych i WWW

5.4.6.1 Wprowadzenie

nVision posiada kilka specjalnych liczników do monitorowania serwerów pocztowych i WWW. Liczniki te nie tylko podłączają się do serwera, ale także wykonują pewne testy, aby sprawdzić, czy serwer funkcjonuje poprawnie: określenie czasu załadowania strony i jej zawartości, sprawdzenie listy przychodzących e-maili i wysłanie testowego emaila. Aby wykonać takie testy, należy utworzyć odpowiedni licznik w zakładce **Liczniki wydajności** okna **Informacje o urządzeniu**. Aby dowiedzieć się więcej o tych licznikach i operacjach testowych, przejdź do rozdziału [Typy liczników](#) topic. Aby uzyskać informacje o tworzeniu liczników przejdź do rozdziału [Zarządzanie licznikami wydajności](#).

5.4.6.2 Typy liczników

Poniższa lista opisuje wyłącznie grupę Test serwisu odpowiedzialną za monitorowanie serwerów pocztowych i WWW. Aby uzyskać informacje o innych grupach (Dostępność urządzenia i Liczniki)

przejdź do rozdziału [Monitorowanie wydajności urządzenia i systemu](#).

Test serwisu

Czas ładowania strony	Mierzy czas załadowania określonej strony.
Zmiana strony	Sprawdza zmiany zawartości strony.
Czas zalogowania POP3	Mierzy czas konieczny do zalogowania się do serwera pocztowego.
Czas wysłania emaila	Mierzy czas konieczny do wysłania testowego emaila.

Liczniki określone dla urządzenia

Niektóre liczniki posiadają pełną informację konieczną do ich sprawdzenia, włączając w to adres urządzenia. Takie liczniki nazywamy Określonymi dla urządzenia. W ogólności wszystkie liczniki typu Testy serwisu są określone dla urządzenia. Na przykład, licznik **Czas ładowania strony**.

5.4.6.3 Definiowanie właściwości liczników

Rozdział ten opisuje właściwości poszczególnych typów liczników w grupie **Test serwisu**.


Czas ładowania strony

Licznik ten mierzy czas załadowania określonej strony.

Właściwość	Opis
Adres	Adres strony, która będzie sprawdzana.
Interwał monitorowania	Jeśli wybierzesz Auto nVision będzie zarządzać czasem monitorowania, tak aby zapewnić odpowiednio częste sprawdzenia (zależnie od liczby monitorowanych urządzeń). Jeśli chcesz ustawić określoną wartość, wybierz Ustaw i wpisz ją w polu edycji.

Zmiana zawartości strony

Licznik ten określa procent zmiany zawartości strony.

Właściwość	Opis
Adres	Adres strony, która będzie sprawdzana.
Plik HTML do porównania	Kliknij przycisk  i wybierz plik, który będzie porównywany. Możesz też kliknąć przycisk Pobierz strone teraz - aktualna strona zostanie pobrana i zapisana jako plik do porównania (wzorzec).
Interwał monitorowania	Jeśli wybierzesz Auto nVision będzie zarządzać czasem monitorowania, tak aby zapewnić odpowiednio częste sprawdzenia (zależnie od liczby monitorowanych urządzeń). Jeśli chcesz ustawić określoną wartość, wybierz Ustaw i wpisz ją w polu edycji.

Czas logowania POP3

Licznik ten monitoruje czas potrzebny do zalogowania się do serwera POP3 i sprawdzenia listy dostępnych emaili.

Wlasciwosc	Opis
Adres serwera POP3	Adres serwera pocztowego
Uzytkownik	Nazwa uzytkownika konieczna do zalogowania
Haslo	Haslo konieczne do zalogowania
Interwal monitorowania	Jesli wybierzesz Auto nVision bedzie zarzadzac czasem monitorowania, tak aby zapewnic odpowiednio czeste sprawdzenia (zaleznie od liczby monitorowanych urzadzen). Jesli chcesz ustawic okreslona wartosc, wybierz Ustaw i wpisz ja w polu edycji.

Czas wyslania emaila

Licznik ten mierzy czas konieczny do wyslania testowego emaila.

Wlasciwosc	Opis
Adres serwera SMTP	Adres serwera pocztowego.
Wymagana autoryzacja	Wlacz ta opcje, jesli twój serwer wymaga autoryzacji do wyslania emaila.
Uzytkownik	Nazwa uzytkownika konieczna do zalogowania
Haslo	Haslo konieczne do zalogowania
Wyslij email do	Adres na który email testowy zostanie wyslany. Zmierzony bedzie czas calej operacji.
Adres zwrotny	Jesli adres ten nie jest wlasciwie ustawiony, lub pusty, wiekszosc serwerów pocztowych odrzuci email. Podaj adres, który bedzie zaakceptowany przez serwer (najprawdopodobniej twój adres email).
Interwal monitorowania	Jesli wybierzesz Auto nVision bedzie zarzadzac czasem monitorowania, tak aby zapewnic odpowiednio czeste sprawdzenia (zaleznie od liczby monitorowanych urzadzen). Jesli chcesz ustawic okreslona wartosc, wybierz Ustaw i wpisz ja w polu edycji.

5.4.7 Monitorowanie routerów i switchy (MRTG)

5.4.7.1 Wprowadzenie





Dzięki nVision można monitorować za pomocą SNMP następujące elementy sieci:

- Interfejsy: status i aktualny ruch sieciowy. Można także skonfigurować monitorowanie ruchu na wejściu/wyjściu każdego interfejsu. Takie informacje są potem prezentowane w zakładce **Liczniki wydajności**, można także zobaczyć wykresy prezentujące ruch sieciowy.
- Porty switcha: nVision automatycznie odczytuje informacje SNMP dotyczące portów switcha, jeśli tylko jest to możliwe. Gdy taka informacja jest dostępna, zobaczysz zakładkę **Mapowanie portów** w oknie **Informacje o urządzeniu**. Zakładka ta zawiera informacje o statusie każdego portu, adresach MAC i IP komputerów podłączonych do każdego portu, a także ich całkowity/aktualny ruch sieciowy na wejściu/wyjściu.
- Ruch sieciowy: niektóre switchy i routery zbierają informacje o ruchu sieciowym generowanym przez każde urządzenie. Takie dane są dostępne w tabelach RMON. nVision automatyzuje proces monitorowania ruchu sieciowego generowanego przez dane urządzenie.

To wszystko umożliwi szeroko zakrojone monitorowanie infrastruktury sieciowej, statusu switchów, routerów i ruchu sieciowego.

5.4.7.2 Monitorowanie portów switcha

nVision automatycznie odczytuje z informacji o portach dla każdego switcha zarządzalnego przez SNMP. Należy jednak odpowiednio ustawić wspólnotę SNMP we właściwościach urządzenia. Kiedy takie informacje SNMP są dostępne, zobaczysz dodatkową zakładkę w oknie **Informacje o urządzeniu: Mapowanie portów**. Zakładka ta prezentuje w formie graficznej wszystkie porty switcha. Tabela poniżej przedstawia znaczenie poszczególnych symboli graficznych:

Ikona	Opis
	Port jest aktywny, ale nic nie jest do niego podłączone.
	Port jest aktywny i jest do niego podłączona wtyczka.
	Port jest nieaktywny (uszkodzony) i nic nie jest do niego podłączone.
	Port jest nieaktywny (uszkodzony) i jest do niego podłączona wtyczka.

Zakładka ta może nie być dostępna na początku (po przeskanowaniu sieci). Pokaze się ona automatycznie, gdy tylko nVision odczyta informacje z SNMP, co może zająć jakiś czas. Jeśli zakładka nie pojawia się przez dłuższy czas, upewnij się, że SNMP jest dostępne na tym urządzeniu i że prawidłowo skonfigurowałeś wspólnotę SNMP we właściwościach urządzenia.

5.4.7.3 Monitorowanie interfejsów sieciowych

nVision automatycznie odczytuje informacje o interfejsie dla każdego urządzenia zarządzalnego przez SNMP. Należy jednak odpowiednio ustawić wspólnotę SNMP we właściwościach urządzenia. Kiedy te dane są już dostępne, tabela interfejsu jest zaktualizowana w oknie **Informacje o urządzeniu** w zakładce **Ogólne**. Zobaczysz tam status interfejsu i aktualny ruch sieciowy.

Domyslnie nVision przechowuje jedynie wielkość aktualnego ruchu sieciowego. Można jednak skonfigurować nVision tak, aby zapisywał informacje o ruchu sieciowym do historii tak, że będzie można uzyskać wykresy i raporty prezentujące ruch sieciowy w danym okresie czasu. Taka funkcja jest często nazywana MRTG (Multi Router Traffic Grapher). Można jej używać na routerze, aby monitorować ruch sieciowy na swoich połączeniach WAN. Funkcja umożliwia także alarmowanie, jeśli łącze będzie przeciążone.

Uruchamianie monitorowania ruchu na interfejsie sieciowym

1. Otwórz okno **Informacje o urządzeniu**.
2. Wybierz **Konfiguruj monitorowanie ruchu na interfejsie sieciowym** z menu przycisku **Zadania** (znajdującego się na dole okna).
3. Zaznacz wszystkie interfejsy, na których chciałbyś monitorować ruch sieciowy. Kreator utworzy dwa liczniki monitorujące SNMP dla każdego interfejsu (dla ruchu wejściowego i wyjściowego). Liczniki te będą dostępne w zakładce **Liczniki wydajności**.

5.4.7.4 Monitorowanie ruchu sieciowego

Niektóre switchy i routery zbierają informacje o ruchu sieciowym generowanym przez każde urządzenie. Dane te znajdują się w tabelach RMON SNMP. nVision automatyzuje proces monitorowania ruchu sieciowego generowanego przez dane urządzenie.

Monitorowanie ruchu sieciowego urządzenia

1. Otwórz okno **Informacje o urządzeniu**.

- Przejdź do zakładki **Mapowanie portów**. Jeśli taka zakładka nie jest dostępna, oznacza to, że nie ma takich danych dla danego urządzenia. Aby uzyskać więcej informacji, przejdź do rozdziału [Monitorowanie portów switcha](#).
- Wybierz wiersz, który zawiera informacje o urządzeniu, które chciałbyś monitorować. Wybierz **Monitoruj ruch sieciowy urządzenia** z menu kontekstowego. Utworzy to dwa liczniki monitorujące SNMP (dla ruchu sieciowego na wejściu/wyjściu). Liczniki te będą się znajdować w zakładce **Liczniki wydajnościowe**.

5.4.8 Monitorowanie aktywności użytkowników

5.4.8.1 Wprowadzenie

Axence nVision Professional jest wyposażony w agenty, przeznaczone do monitorowania aktywności użytkowników pracujących na komputerach z systemem Windows oraz przeprowadzania inwentaryzacji sprzętu i oprogramowania. nVision gromadzi następujące informacje:

- Faktyczny czas aktywności (pracy). Nieaktywność to czas, w którym użytkownik nie naciska klawiszy i nie porusza myszką.
- Czas użytkowania programów - informacje są pogrupowane dla łatwiejszej analizy aktywności użytkowników.
- Lista odwiedzanych stron. Aby otrzymać dane, agent analizuje informację sieciową niskiego poziomu, a więc funkcja ta działa dla wszystkich przeglądarek i innych programów pobierających strony internetowe.
- Zasoby sprzętu i oprogramowania.

Agenty automatycznie przesyłają informacje o aktywności użytkownika co 3 godziny, a o stanie zasobów - co 12 godzin.

Wymagania związane z monitorowaniem aktywności użytkowników

Aby gromadzić informacje o aktywności użytkowników, należy zainstalować agenta nVision na zdalnym urządzeniu (co także umożliwi wykonywanie inwentaryzacji). Należy otworzyć port TCP 4434 na komputerze, na którym jest uruchomiony nVision. Aby uzyskać więcej informacji, przejdź do rozdziału [Wymagania i planowanie](#).

Należy zauważyć, że cała komunikacja pomiędzy agentami i nVision wymaga autoryzacji i żadne dane nie zostaną przekazane, jeśli agenty i nVision nie będą odpowiednio skonfigurowane.

Informacje o aktywności użytkownika

- Otwórz okno **Informacje o urządzeniu**.
- Przejdź do zakładki **Aktywność użytkownika**.
- Wybierz zakładkę, którą chciałbyś zobaczyć:
 - Informacje ogólne**
 - Użytkowanie programów**
 - Lista odwiedzanych stron**
- Wybierz okres czasu, z którego dane chcesz zobaczyć.

Komputery z przypisanymi adresami DHCP

Jeśli komputer ma nowy adres IP przypisany przez DHCP, będzie on zaktualizowany w bazie danych nVision przy połączeniu agenta z nVision. Nie trzeba więc robić tego ręcznie.

5.4.8.2 Instalowanie i odinstalowywanie agentów

Możesz zainstalować agenta ręcznie poprzez uruchomienie `nvagentinstall.exe` na zdalnym komputerze lub korzystając z kreatora, który automatycznie zainstaluje agenty na wielu komputerach za jednym razem. Należy pamiętać, że przed rozpoczęciem pracy z kreatorem, WMI musi być

udostępnione na zdalnych komputerach i że dane logowania muszą być odpowiednio skonfigurowane. Aby uzyskać więcej informacji, przejdź do rozdziału [Wymagania i planowanie](#).

Instalowanie agentów za pomocą kreatora

1. Wybierz w menu **Narzędzia | Zainstaluj agenta nVision**.
2. Wybierz opcję **Wszystkie**, aby zainstalować agenty na wszystkich komputerach lub zaznacz **Wybrane**. Umożliwi Ci to wybranie tych komputerów, na których chcesz zainstalować agenty. Przed rozpoczęciem instalacji, możesz skonfigurować dane logowania Windows programu, wymagane do połączenia ze zdalnymi komputerami. Kliknij **Ustaw domyślne dane logowania**.
3. Kliknij przycisk **Instaluj**. Rozpocznie to proces instalacji. Zobaczysz status instalacji na każdym komputerze, aby można było powtórzyć proces instalacji na tych, na których się ona nie powiodła.

Instalowanie ręczne

Automatyczna instalacja może się nie powieść, jeśli nie jest dostępne WMI. Aby dowiedzieć się więcej, przejdź do rozdziału [Rozwiązywanie problemu instalacji agentów](#). W takim przypadku, należy ręcznie zainstalować agenta na każdym komputerze. Aby zainstalować agenta, uruchom na komputerze `nvagentinstall.exe` (plik ten znajduje się w podkatalogu Agents programu nVision). Tabela poniżej przedstawia wszystkie parametry instalatora.

Parameter	Description
<code>/nVisionOn:x.x.x.x</code>	Parametr ten definiuje adres IP komputera, na którym zainstalowany jest nVision. Wszystkie dane będą automatycznie przesyłane na ten adres.
<code>/ShowIcon</code>	Jeśli widoczna jest ta opcja, ikona agenta będzie się pokazywała na pasku zadań.
<code>/SendData:x</code>	Agenty przesyłają dane co 3 godziny. Dzięki tej opcji możesz zmienić tę liczbę godzin.
<code>/Password:x</code>	Definiuje hasło wymagane do autoryzowania komunikacji z nVision. Takie samo hasło musi być ustawione w opcjach nVision (w innym wypadku nVision nie będzie w stanie odczytać żadnych informacji z agentów).
<code>/Silent</code>	Instalacja nie wymaga żadnych działań użytkownika, ale okno instalacji jest widoczne.
<code>/VerySilent</code>	Instalacja nie wymaga żadnych działań użytkownika, okno instalacji nie pokazuje się.
<code>/KeepFiles</code>	Opcja ta chroni pliki z danymi przed usunięciem po przesłaniu ich do nVision. Służy to głównie uniknięciu problemów z konfiguracją.
<code>/EnableWMI</code>	Wykonuje wszystkie zadania aplikacji WMIEnable. Aby uzyskać więcej informacji, przejdź do rozdziału Monitorowanie systemu Windows przez WMI .
<code>/OneInstall</code>	Instalator nie będzie próbował nic zainstalować, jeśli agent jest już zainstalowany. Opcja ta jest przydatna przy instalowaniu agenta ze skryptu logowania - zapobiega powtórny instalacjom.
<code>/NoUserMonitoring</code>	Wyłącza monitorowanie aktywności użytkowników. Przy zastosowaniu tej opcji agent przekazuje jedynie informacje o zasobach.

Parameter	Description
/SendScreenshot:x /SendScreenshot	Agent będzie automatycznie przysyłał zrzuty ekranowe pulpitu (domyślnie co 3 godziny). Można także zmienić domyślne ustawienia odstępu czasowego.
/NoRemoteAccess	Wyłącza funkcję zdalnego dostępu.

Instalowanie ze skryptu logowania

Skopiuj plik `nvagentinstall.exe` znajdujący się w katalogu "agentów" do katalogu dostępnego dla wszystkich użytkowników i dodaj następującą linię do skryptu logowania:

```
nvagentinstall.exe /VerySilent /OneInstall /nVisionOn:x.x.x.x
```

Podaj IP komputera, na którym jest zainstalowany nVision jako parametr `x.x.x.x`. Agent będzie zainstalowany automatycznie, nie jest przy tym wymagana żadna czynność użytkownika.

Zainstalowany agent automatycznie nawiąże łączność z nVision. Jeśli komputer nie był obecny na żadnej mapie, jego ikona będzie automatycznie utworzona.

Zmiana adresu IP komputera z zainstalowanym nVision

Po zmianie adresu IP komputera, na którym jest zainstalowany nVision, nie trzeba rekonfigurować agentów. Program będzie próbował połączyć się z każdym agentem i zaktualizować informacje. Może to jednak się nie udać, gdy port agenta (TCP 4434) w komputerze nie jest dostępny (przez wbudowany lub zewnętrzny firewall).

Instalowanie nowej wersji agenta

Agent posiada mechanizm automatycznej aktualizacji. Przy każdym połączeniu z nVision sprawdza on, czy nie ma dostępnej nowej wersji agenta. Jeśli jest dostępna nowa wersja (np. po zainstalowaniu nowej wersji nVision), agent automatycznie ją pobierze i ponownie się uruchomi.

Pobieranie instalatora agentów z nVision

Przy ręcznym instalowaniu agentów, można skorzystać z następującego linku, aby pobrać instalator agentów na zdalny komputer: <http://x.x.x.x:4434/?nVisionAgentReqType=5>, gdzie `x.x.x.x` jest adresem IP komputera, na którym nVision jest zainstalowany i uruchomiony.

Odinstalowywanie agentów

Aby zdalnie odinstalować agenty, należy wybrać z menu zadań w oknie **Informacje o urządzeniu** opcję **Odinstaluj agenta nVision**. Można także odinstalować agenta ręcznie, uruchamiając plik `unins000.exe` znajdujący się w katalogu agenta.

5.5 Zasoby

5.5.1 Wprowadzenie

Axence nVision Professional automatycznie gromadzi informacje o konfiguracji sprzętowej każdego komputera Windows oraz zainstalowanego na nim oprogramowania. Zadanie to jest wykonywane przez WMI lub przez opcjonalnego agenta nVision. W ten sposób można wybrać rozwiązanie najlepsze dla danej konfiguracji sieci. Wykonywanie inwentaryzacji przez WMI odbywa się bez udziału agentów, jednak może zmniejszyć bezpieczeństwo komputera poprzez udostępnienie WMI. Inwentaryzacja za pomocą agentów nie wpływa na bezpieczeństwo, ale wymaga zainstalowania agentów na każdym komputerze.

Inwentaryzacja wykonywana przez WMI

Aby wykonać inwentaryzację bez agentów, należy odpowiednio skonfigurować domyślne dane logowania w opcjach programu w oknie właściwości komputera. WMI musi być także dostępne na zdalnych komputerach. Aby uzyskać więcej informacji, przejdź do rozdziału [Wymagania inwentaryzacji](#).

Inwentaryzacja wykonywana przez agenty

Mozna także zainstalować agenty nVision na zdalnych komputerach, co umożliwi nVision wykonanie inwentaryzacji. Aby uzyskać więcej informacji, przejdź do rozdziału [Instalowanie agentów](#).

Zakładka Zasoby

Informacje o zasobach można znaleźć w zakładce **Zasoby** w oknie **Informacje o urządzeniu**. Na samym początku dane te mogą być niedostępne (po przeskanowaniu sieci). Pojawia się one automatycznie, gdy tylko nVision odczyta informacje, co może chwilę potrwać. Jeśli dane nie pokazują się po dłuższym czasie, należy się upewnić, czy dane logowania są prawidłowo skonfigurowane w opcjach programu lub we właściwościach urządzenia, oraz że WMI jest dostępne na zdalnych komputerach.

5.5.2 Inwentaryzacja

nVision gromadzi informacje o zasobach automatycznie - nie jest wymagana dodatkowa konfiguracja. Zadanie to jest wykonywane co 12 godzin dla każdego komputera.

Jeśli chcesz pobrać informacje dla danego urządzenia lub urządzeń szybciej, wybierz **Monitorowanie | Inwentaryzuj zasoby urządzenia** z menu kontekstowego komputera. Można także przeprowadzać inwentaryzację dla całej mapy (wszystkich komputerów) poprzez wybranie **Inwentaryzuj** z menu kontekstowego w drzewie mapy.

5.5.3 Audyt licencji i sprzętu

Audyt licencji i informacje o zasobach sprzętowych

Okno audytu licencji i sprzętu, dostępne po wybraniu z menu **Narzędzia | Audyt inwentaryzacyjny**, prezentuje listę aplikacji, komputerów, na których są one zainstalowane i liczbę wykorzystywanych licencji.

Kolejna zakładka pokazuje dane o ogólnej konfiguracji wszystkich komputerów. Na trzeciej zakładce znajduje się historia wszystkich zmian konfiguracji.

Powiadamianie o zmianach oprogramowania i sprzętu

nVision posiada specjalnie zdefiniowane alarmy, które mogą być wykorzystywane do powiadamiania o wszelkich zmianach na wszystkich komputerach: zainstalowanie/odinstalowanie programu, zmiana/usunięcie elementu sprzętowego. Aby otrzymywać powiadomienia, należy dodać do alarmów akcję powiadamiania.

Część

VI

6 Praca z atlasami, komputerem i mapami

6.1 Wprowadzenie

Atlas

Atlas to zbiór map prezentujących monitorowane urządzenia wraz ze zdefiniowanymi alarmami, zdarzeniami, stylami wizualizacji etc. nVision może pracować na wielu atlasach, można więc korzystać z wielu atlasów z różnymi sieciami i/lub różną konfiguracją (opcje monitorowania, alarmy etc.). Należy jednak pamiętać, że w danym momencie można mieć otwarty tylko jeden atlas. Aby rozpocząć pracę z innym atlasem lub stworzyć nowy, należy uprzednio zamknąć atlas już otwarty. Aby uzyskać więcej informacji, przejdź do rozdziału [Zarządzanie atlasami](#).

Drzewo atlasu

Drzewo atlasu przedstawia wszystkie dostępne mapy. Dostępnych jest wiele rodzajów map, które są szczegółowo opisane w rozdziale [Rodzaje map](#). Drzewo atlasu umożliwia wybór mapy, która jest przedstawiona po prawej stronie, ustawienie właściwości danej mapy etc. Można zmieniać kolejność map w drzewie (Aby uzyskać więcej informacji, przejdź do rozdziału [Zarządzanie mapami](#)).

Mapy

Mapa to graficzny obraz sieci lub jej części. Mapy wizualizują urządzenia tworzące sieć. Jest wiele rodzajów map. Aby uzyskać więcej informacji, przejdź do rozdziału [Rodzaje map](#).

Style

Wszystkie obiekty na mapie (oprócz tekstu) używają mechanizmu stylów. Styl decyduje o sposobie prezentacji obiektów. Definiuje on np. kolory, czcionki, ramki etc. Aby zmienić wygląd obiektu, podczas definiowania jego właściwości, należy wybrać preferowany styl. Aby uzyskać więcej informacji o stylach, przejdź do rozdziałów [Style - Wprowadzenie](#) i [Mapy - Wprowadzenie](#).

Urządzenia

Urządzenie oznacza jakikolwiek rodzaj sprzętu fizycznego podłączonego do sieci. Może ono posiadać wiele adresów IP, a nVision może monitorować wszystkie serwisy na nim uruchomione na jakimkolwiek z jego adresów. Oznacza to, że urządzenie z wieloma adresami IP, takie jak routery lub serwery sieciowe, mogą być przedstawione w nVision jako jedna ikona (obiekt) i wszystkie ich interfejsy, adresy i serwisy będą monitorowane.

6.2 Zarządzanie atlasami

Zarządzając atlasami, należy pamiętać, że w danym momencie można mieć otwarty tylko jeden atlas. Aby rozpocząć pracę z innym atlasem lub stworzyć nowy, należy uprzednio zamknąć atlas już otwarty.


Otwieranie okna zarządzania atlasem

W tym oknie możesz wylistować, stworzyć lub usunąć atlasy. Aby je otworzyć, wykonaj jedną z następujących czynności:


- Wybierz **Plik | Otwórz atlas** z głównego menu.

- Otwórz okno zarządzania akcjami i kliknij ikonę  .

Tworzenie nowego atlasu

- Wykonaj jedna z czynności poniżej:
 - Otwórz okno zarządzania akcjami i kliknij ikonę .
 - Wybierz **Plik | Nowy atlas** z głównego menu.
- Otwórz się okno tworzenia atlasu. Wprowadź nazwę nowego atlasu.
- Teraz masz dwie możliwości - wybierz, czy chcesz stworzyć pusty atlas, czy utworzyć atlas dla Twojej sieci.
- Kliknij przycisk **Zakończ** lub **Dalej**. Jeśli wybrales utworzenie atlasu dla danej sieci, w kontynuacji zadania pomoże Ci teraz kreator skanera sieci. Aby uzyskać więcej informacji, przejdź do rozdziału [Kreator wykrywania sieci](#).

Usuwanie istniejącego atlasu

- Otwórz okno zarządzania atlasem
- Wybierz istniejący atlas i kliknij ikonę .

Definiowanie właściwości atlasu (nazwa, style, alarmy)

- Otwórz atlas.
- Wybierz z menu **Atlas | Właściwości**.
- Ustaw właściwości atlasu zgodnie z opisem w tabeli poniżej.
- Mozesz także utworzyć okno zarządzania alarmami dla danego atlasu - kliknij link znajdujący się pod napisem **Polityka alarmowania** znajdujący się na dole okna.

Właściwości	Opis
Nazwa	Nazwa atlasu
Domyslny style map	– określają sposób wizualizacji map i urządzeń. Aby uzyskać więcej informacji o stylach, przejdź do rozdziału Style: Wprowadzenie .
Wizualizacja obiektu	Domyslny styl wizualizacji ikony.
Styl kształtu	Domyslny styl kształtu.
Styl linii	Domyslny styl linii.

6.3 Mapy

6.3.1 Wprowadzenie

Mapa to graficzny obraz sieci lub jej części. Mapy przedstawiają ikony, połączenia pomiędzy nimi i trzy grupy obiektów statycznych: kształty, obrazki i tekst. Pełna lista obiektów jest opisana w rozdziale [Obiekty na mapie](#).

Dostępne są trzy rodzaje map: sieci IP, routingu i użytkownika - zagadnienie szerzej opisane w rozdziale [Rodzaje map](#).

Style

Wszystkie obiekty na mapie (oprócz tekstu) używają mechanizmu stylów. Styl decyduje o sposobie prezentacji obiektów. Definiuje on np. kolory, czcionki, ramki etc. Aby zmienić wygląd obiektów, podczas definiowania właściwości obiektów, należy wybrać preferowany styl.

Wszystkie nowe obiekty są tworzone w stylu domyślnym. Styl domyślny oznacza, że obiekty będą wykorzystywały domyślny styl mapy. Ustawionym domyślnym stylem mapy może być dowolny wybrany styl lub domyślny styl atlasu. Atlas ma zawsze ustawiony styl domyślny. Przy pierwszym uruchomieniu programu, wszystkie obiekty użyją domyślnych stylów atlasu. Style te mogą być później zmienione. Aby uzyskać więcej informacji o stylach, przejdź do rozdziału [Zarządzanie stylami](#).

6.3.2 Rodzaje map

W nVision dostępne są 3 rodzaje map. Rozdział ten przedstawia charakterystykę każdego z nich.

Rodzaj mapy	Opis	Możliwe operacje
Mapa sieci	Mapa stworzona przez program jako reprezentacja wykrytej sieci IP. nVision może regularnie skanować taką sieć i dodawać nowe urządzenia.	<ul style="list-style-type: none"> Mozna zmienić nazwę mapy, ale nawet po takiej zmianie mapa w dalszym ciągu przedstawia tę samą sieć. Usuwanie - usunięcie mapy sieci spowoduje także usunięcie wszystkich urządzeń należących do danej sieci. Wszystkie inne operacje są dostępne bez ograniczeń.
Mapa routingu	Mapa pokazuje logiczną strukturę wykrytych sieci. nVision może skanować sieć wraz z wszystkimi sąsiadującymi sieciami. W celu pokazania, w jaki sposób sieci są połączone ze sobą, tworzy mapę routingu. Przedstawia ona wszystkie wykryte sieci i routery łączące te sieci ze sobą. Można także zobaczyć łączące interfejsy jako opisy linii. nVision może cyklicznie reskanować wszystkie sieci i w przypadku jakiegokolwiek zmiany w ich logicznej topologii, przedstawić takie modyfikacje na mapie.	<ul style="list-style-type: none"> Wszystkie operacje są dostępne bez ograniczeń - można modyfikować i usuwać mapę routingu, jednak po usunięciu mapa będzie odtworzona przez program po ponownym przeskanowaniu sieci.
Mapa użytkownika	Jest to mapa stworzona przez użytkownika. Przedstawia wszelkie urządzenia skopiowane lub przeniesione z jakiegokolwiek innej mapy.	<ul style="list-style-type: none"> Wszystkie operacje są dostępne bez ograniczeń.

6.3.3 Obiekty mapy

Mapa może zawierać ikony, połączenia pomiędzy nimi i trzy rodzaje obiektów statycznych: kształty, obrazki i teksty. Oto pełna lista obiektów na mapie:

Obiekty mapy	Opis
Ikony	Urządzenia są przedstawiane jako ikony. Ikony pokazują stan urządzenia - aby dowiedzieć się więcej o wizualizacji stanu urządzeń, przejdź do rozdziału Wizualizacja urządzenia .

Obiekty mapy	Opis
Linie	Ikony mogą być połączone ze sobą, w celu zobrazowania logicznych lub fizycznych połączeń pomiędzy urządzeniami.
Kształty	Obiekty w tle, wykorzystywane do grupowania ikon.
Obrazy	Podobne do kształtów, ale przedstawiają zawartość określonego pliku graficznego.
Teksty	Teksty można umieszczać w dowolnych miejscach mapy.

Hierarchia obiektów

Obiekty mają swoją hierarchię na mapie. Oznacza to, że pewne obiekty są rysowane na innych. Przykładowo, ikony są zawsze rysowane na innych rodzajach obiektów. Jednak hierarchię obiektów jednego rodzaju można zmienić. Można przenieść dane obiekty do przodu lub do tyłu, co zmienia sposób rysowania obiektów nachodzących na siebie.

6.3.4 Zarządzanie mapami

Rozdział ten opisuje wszystkie aspekty związane z zarządzaniem mapami.

Tworzenie nowej mapy

1. W drzewie atlasu wybierz mapę lub katalog, pod którym chcesz utworzyć nową mapę. Możesz wybrać grupę Map Użytkownika.
2. Wybierz **Nowe | Mapa** z menu kontekstowego.

Uwaga

- Nowe mapy mogą być utworzone jedynie w grupie Map Użytkownika.

Edytowanie właściwości mapy

1. Wybierz mapę
2. Wybierz **Właściwości** z menu kontekstowego.
3. Ustaw właściwości mapy zgodnie z opisem w tabeli poniżej.
4. Możesz także otworzyć okno zarządzania alarmami dla tej mapy - kliknij link pod nazwą **Polityka alarmowania**, znajdujący się na dole okna.

Właściwość	Opis
Nazwa	Nazwa mapy
Siec	Siec, którą przedstawia mapa sieci (aby dowiedzieć się, czym jest mapa sieci, przejdź do rozdziału Rodzaje map). Jest to pole tylko do odczytu.
Domyslnie style map - decydują o sposobie wizualizacji map i urządzeń. Aby dowiedzieć się więcej o stylach, przejdź do rozdziału: Style - Wprowadzenie .	
Wizualizacja urządzeń	Domyslny styl wizualizacji ikon.
Styl kształtów	Domyslny styl kształtów.
Styl linii	Domyslny styl linii.

Usuwanie mapy

1. Wybierz mapę.
2. Wybierz **Usun** z menu kontekstowego.

Zmienianie kolejności map

Mozna zmieniać kolejność, według której mapy użytkownika są ułożone w drzewie atlasu. Kolejność map sieci nie może być zmieniana. Aby zmieniać kolejność map, przeciągnij i upuść wybraną mapę w drzewku atlasu.

6.3.5 Praca z mapą


Rozdział ten opisuje wszystkie narzędzia potrzebne do pracy z mapami.

Narzędzia

Narzędzia są dostępne na pasku narzędziowym mapy, znajdującym się zazwyczaj po lewej stronie okna mapy (pasek narzędziowy mapy może być przesunięty na dowolny brzeg map). Narzędzia pozwalają wybierać obiekty na mapie, łączyć ikony i tworzyć obiekty tła, takie jak kształty, obrazki i teksty.


Narzędzie - zaznaczenie

Zaznaczenie jest narzędziem domyślnym. Pozwala wybierać obiekty na mapie, przesuwać je, porządkować i wykonywać inne określone akcje, takie jak otwieranie okna stanu urządzenia czy właściwości.

Aby użyć narzędzia wyboru, kliknij ikonę  na pasku narzędziowym mapy. Narzędzie to będzie aktywne do czasu wybrania innego narzędzia.


Narzędzie - łączenie ikon

Narzędzie to umożliwia łączenie ikon - np. narysowanie graficznych połączeń pomiędzy ikonami urządzeń na mapie.

1. Aby korzystać z narzędzia łączenia ikon, kliknij ikonę  na pasku narzędziowym mapy. Narzędzie to będzie aktywne do czasu wybrania innego narzędzia.
2. Aby połączyć dwie ikony, po prostu kliknij je kolejno, czyli:
 - Kliknij jedną z ikon, które chcesz połączyć. Pojawi się linia łącząca, wskazując, że teraz możesz kliknąć następną ikonę, którą chcesz połączyć.
 - Kliknij kolejną ikonę. W ten sposób pomiędzy tymi dwoma ikonami pojawi się połączenie.
3. Teraz możesz powtórzyć kroki 2-3, aby łączyć kolejne pary ikon.


Narzędzia - tworzenie kształtów

Narzędzie to umożliwia tworzenie różnych kształtów na mapie (graficznych obiektów w tle - prostokątów, elips, etc.).

1. Kliknij ikonę  na pasku narzędziowym mapy. Narzędzie jest aktywne do momentu utworzenia kształtu. Później aktywne będzie narzędzie wyboru.
2. Kliknij i przytrzymaj lewym przyciskiem myszy miejsce, w którym chcesz otrzymać lewy górny róg danego kształtu, a następnie przeciągnij do miejsca, w którym ma być jego prawy dolny róg. Pusc przycisk.


Narzędzia - tworzenie obrazów

Narzędzie to umożliwia tworzenie obrazów na mapie. Po utworzeniu obrazu, należy go ustawić, otwierając okno właściwości i wybierając plik, który powinien być pokazany.

1. Kliknij ikonę  na pasku narzędziowym mapy. Narzędzie jest aktywne do momentu utworzenia obrazu. Później aktywne będzie narzędzie wyboru.
2. Kliknij i przytrzymaj lewym przyciskiem myszy miejsce, w którym chcesz otrzymać lewy górny róg obrazu, a następnie przeciągnij do miejsca, w którym ma być jego prawy dolny róg. Pusc przycisk.
3. Pokazuje się okno właściwości obrazu. Należy wybrać plik graficzny i [ustawić opcje](#), aby we właściwy sposób utworzyć obraz.

Narzędzia - tworzenie tekstów

Narzędzie to umożliwia tworzenie tekstów na mapie. Po utworzeniu tekstu, należy go zdefiniować, wybierając czcionkę oraz wprowadzając tekst, który ma zostać pokazany.

1. Kliknij ikonę  na pasku narzędziowym mapy. Narzędzie jest aktywne do momentu utworzenia tekstu. Później aktywne będzie narzędzie wyboru.
2. Kliknij w miejscu, w którym chcesz wprowadzić tekst.
3. Pokazuje się okno właściwości tekstu. Teraz należy wprowadzić tekst i [ustawić opcje](#), aby we właściwy sposób utworzyć tekst.

Praca na obiektach na mapie

Kopiowanie obiektów na inną mapę

1. Wybierz obiekt lub obiekty.
2. Wybierz **Skopiuj do...** z menu kontekstowego. Otworzy się okno wyboru mapy.
3. Wybierz mapę, na którą chcesz skopiować wybrany(e) obiekt(y).

Usuwanie obiektów

1. wybierz obiekt lub obiekty.
2. Wybierz **Usun** z menu kontekstowego.

Zmianianie kolejności obiektów (przesuwanie ich na wierzch / na spód)

Mozesz zmienić kolejność obiektów tego samego rodzaju - sposób, w jaki są narysowane i w jaki

zachodza na siebie. Kolejność obiektów różnego rodzaju jest stała (Aby uzyskać więcej informacji, przejdź do rozdziału [Obiekty na mapie](#)).

- Aby wyświetlić obiekt z przodu, na jakimkolwiek innym obiekcie, wybierz **Pozycja | Na wierzchu** z menu kontekstowego.
- Aby przesunąć dany obiekt pod pozostałe obiekty, wybierz **Pozycja | Na spodzie** z menu kontekstowego.


Inne operacje

Automatyczny układ mapy

Są dwa sposoby, aby automatycznie ułożyć mapę: za pomocą funkcji układu mapy i za pomocą asystenta układu mapy.


Układ mapy

Funkcje te najlepiej stosować przy mapie sieci lub mapie użytkownika, szczególnie, gdy urządzenia nie są ze sobą połączone. Układa ona ikony w kilka rzędów.


1. Kliknij ikonę , znajdująca się na pasku narzędziowym mapy i wybierz z menu **Układ mapy**.
2. Określ, jak ma być mapa ułożona i kliknij OK.

Asystent układu mapy

Aby prawidłowo ustawić układ mapy routingu (lub jakiegokolwiek innej mapy, na której wszystkie urządzenia są połączone liniami), ikony nie mogą być ułożone rzędami, gdyż spowodowałoby to nieczytelność mapy - połączenia ikon nakładaliby się na siebie. Dlatego należy użyć Asystenta układu mapy, który ułoży całą mapę tak, aby uniknąć przecinania się połączeń i aby była ona tak czytelna, jak to jest tylko możliwe.

1. Kliknij strzałką ikonę , znajdująca się na pasku narzędziowym mapy i wybierz z menu opcję **Asystent układu mapy**.
2. Asystent zostanie włączony i zacznie układać mapę. Można ingerować w proces układania, aby dostosować go do własnych potrzeb. Można przesuwać ikony i dodawać/usuwać połączenia pomiędzy nimi.

Powiększanie - zmienianie skali mapy

Można dostosować skalę, w której jest prezentowana mapa. Domyślna skala to 100% i można ją ustawić w każdej chwili, klikając ikonę .

Powiększanie

Aby powiększyć mapę, kliknij ikonę .


Pomniejszanie

Aby pomniejszyć mapę, kliknij ikonę .


Skala 1:1

Aby pokazać mapę w skali 1:1 (bez zmiany powiększenia), kliknij ikonę .

Dostosowanie do wielkości mapy

Aby skala mapy była automatycznie dostosowana do wielkości mapy, kliknij ikonę . nVision pokaze całą mapę w największej możliwej skali.

Blokowanie mapy

Gdy układanie mapy jest już zakończone i chcesz mieć pewność, że nic nie zostanie zmienione przez pomyłkę, możesz zablokować mapę, klikając ikonę . Na zablokowanej mapie nie można przesuwać obiektów, ani zmieniać ich rozmiarów, w dalszym ciągu można jednak edytować właściwości urządzeń.

6.3.6 Statyczne obiekty na mapie - właściwości

Rozdział ten poświęcony jest właściwościom statycznych obiektów na mapie. Aby uzyskać więcej informacji o obiektach na mapie, przejdź do rozdziału [Obiekty na mapie](#), a jeśli chcesz się dowiedzieć więcej o tworzeniu obiektów, przejdź do rozdziału [Praca z mapą](#).

Linie

Ikonki mogą być ze sobą połączone liniami, aby pokazać logiczne i fizyczne połączenia między urządzeniami.

1. Kliknij dwukrotnie w linię lub wybierz **Właściwości** z jej menu kontekstowego.
2. Ustaw właściwości zgodnie z opisem w tabeli poniżej.

Właściwość	Opis
Opis	Opis, który będzie pokazany nad linią łączącą.
Styl	Styl, w którym będzie narysowana linia. Aby uzyskać więcej informacji o stylach, przejdź do rozdziału Style - Wprowadzenie .

Kształt

Obiekt w tle, używany do grupowania ikon.


1. Kliknij dwukrotnie w kształt lub wybierz **Właściwości** z jego menu kontekstowego.
2. Ustaw właściwości zgodnie z opisem w tabeli poniżej.

Właściwość	Opis
Tekst	Tekst, który pojawi się na kształcie.
Styl	Styl, w którym będzie narysowany kształt. Aby uzyskać więcej informacji o stylach, przejdź do rozdziału Style - Wprowadzenie .

Obraz

Podobny do kształtu, ale jego treścią jest plik graficzny.

1. Kliknij dwukrotnie w obraz lub wybierz **Właściwości** z jego menu kontekstowego.
2. Ustaw właściwości zgodnie z opisem w tabeli poniżej.

Wlasciwosc	Opis
Nazwa pliku	Nazwa pliku graficznego. Wprowadz ja lub wybierz, klikajac ikone  .
Widok	Decyduje o rozmiarze obrazu: <ul style="list-style-type: none"> • Normalny - Rozmiar obrazu nie jest zmieniony, ale przy próbach zmniejszenia, widoczna pozostaje jedynie jego czesc (jesli obraz jest wiekszy od obiektu, bedzie on przycięty). • Rozciagniecie - Obraz bedzie dopasowany tak, aby odpowiadal rozmiarowi obiektu.. • Sasiadujaco - kopie obrazu w skali 1:1 będą wyświetlane sąsiadująco na całym obszarze.
Rozmiar rzeczywisty	Obraz widoczny w calosci, bez mozliwosci zmiany jego rozmiaru.
Stala proporcja	Podczas zmiany rozmiaru obrazu, współczynnik proporcji jest zachowany.
Transparentnosc	Zastosuj, jesli obraz ma warstwe przezroczystosci.
Przezroczystosc	Decyduje o stopniu przezroczystości całego obrazu.

Tekst

Tekst, który można umieścić w dowolnym miejscu na mapie.


1. Kliknij dwukrotnie w tekst lub wybierz **Wlasciwosci** z jego menu kontekstowego.
2. Ustaw wlasciwosci zgodnie z opisem w tabeli ponizej.

Wlasciwosc	Opis
Tekst	Tekst na mapie.
Nazwa czcionki	Czcionka tekstu.
Rozmiar	Rozmiar czcionki.
Kolor czcionki	Kolor tekstu.
Pochylenie	Pochylenie tekstu.
Cien	Cieniowanie tekstu.

Tlo

1. Wybierz **Tlo** z menu kontekstowego.
2. Wybierz rodzaj tła i ustaw jego wlasciwosci zgodnie z opisem w tabeli ponizej.

Wlasciwosc	Opis
Gradient	Wybierz kolor poczatkowy i koncowy oraz kierunek wypelnienia.
Kolor wypelnienia	Wybierz kolor.
Mapa	Wybierz mape, która bedzie pokazana w tle.
Tekstura	Wybierz teksture.

Wlasciwosc	Opis
Obraz	<p>Wprowadz nazwe pliku graficznego lub wybierz go, klikajac ikone . Ustaw tryb polozenia obrazu:</p> <ul style="list-style-type: none"> • Normalny - Obraz znajduje sie w lewym gornym rogu. • Do srodka - Obraz polozony centralne, na srodku mapy. • Rozciagniecie - Obraz bedzie dopasowany tak, aby odpowiadal rozmiarowi mapy. • Sasiadujaco - kopie obrazu w skali 1:1 będą wyświetlane sąsiadująco na całej mapie.

6.4 Urządzenia

6.4.1 Wprowadzenie

Urządzenia są przedstawione na mapie za pomocą ikon. To samo urządzenie może być pokazane jako ikona na nieograniczonej liczbie map.

Wlasciwosci urzadzenia i informacje o urzadzeniu



Istnieją dwa główne okna dotyczące urządzenia: właściwości urządzenia i informacje o urządzeniu. W oknie właściwości urządzenia można ustawić jego właściwości, opcje monitorowania i alarmowania. Okno informacji o urządzeniu prezentuje wszystkie dane zgromadzone poprzez monitorowanie. Znajdują się tam informacje i wykresy oparte na danych SNMP (dla urządzeń zarządzalnych przez SNMP), dotyczące serwisów i liczników wydajności.

6.4.2 Wizualizacja urządzeń

Ikony prezentują wiele informacji dotyczących stanu urządzeń. Dane te pomagają dokonać szybkiej oceny stanu całej sieci i znaleźć problematyczne urządzenia.

Przykład ikon komputera

Ikona komputera prezentuje szeroki zakres informacji, co prezentują poniższe przykłady:

	<ul style="list-style-type: none"> • Typ komputera: Windows XP • Czas odpowiedzi podstawowego serwisu (zwykle PING) to 10ms • Status komputera <Ostrzeżenie> (żółta ikona) ze względu na niedziałający od 4min 1s serwis HTTP • Czas odpowiedzi i procent utraconych pakietów dla podstawowego serwisu są wyświetlone na wykresie • Ten komputer jest zarządzalny przez SNMP
	<ul style="list-style-type: none"> • Typ komputera: serwer Linux • Status komputera <Nie działa> (czerwona ikona) od 1 dnia 2h • Aktualnie otwarte są (niezakończone) 3 alarmy.

Opcje wizualizacji

Poniższa tabela wyszczególnia wszystkie informacje, jakie mogą być przedstawione graficznie za pomocą ikony urządzenia.

Nazwa	Opis
Ikona z podpisem, status urządzenia: Działa	Podstawowa forma ikony. Przedstawia rodzaj urządzenia i nazwę lub adres urządzenia w podpisie.
Stan urządzenia: Nie działa	Ikona jest zaznaczona na czerwono, a czas niedziałania urządzenia jest określony na górze ikony. Aby uzyskać więcej informacji o stanie urządzenia, przejdź do rozdziału Zdarzenia - Wprowadzenie .
Status urządzenia: Ostrzeżenie	Ikona jest zaznaczona na żółto. Oznacza to, że co najmniej jeden serwis nie działa lub zainicjowano alarm ostrzegawczy na tym urządzeniu. Aby uzyskać więcej informacji o stanie urządzenia, przejdź do rozdziału Zdarzenia - Wprowadzenie .
Serwis(y) nie odpowiada (ja)	Na górze ikony wyświetla się nazwa problematycznego serwisu oraz czas trwania usterki.
Czas odpowiedzi wybranego serwisu	Na dole ikony wyświetlony jest ostatni lub średni czas odpowiedzi wybranego serwisu. Zwykle jest to średni czas odpowiedzi PING. Tło napisu zmienia kolor w zależności od wydajności serwisu.
Wykres wydajności	Mozna zobaczyć maksymalnie 6 słupków wydajności, które przedstawiają czas odpowiedzi serwisu lub liczniki wydajności.
Alarmy	Ikona ta znajduje się po prawej stronie ikony urządzenia: wskazuje niepotwierdzone alarmy zainicjowane na danym urządzeniu.
Zarządzalność przez SNMP	Ikona ta znajduje się po prawej stronie ikony urządzenia i wskazuje, że jest ono zarządzalne przez SNMP.

6.4.3 Właściwości urządzeń

Zmiana właściwości urządzenia:

1. Zaznacz urządzenie i wybierz **Właściwości** z menu kontekstowego.
2. Edytuj właściwości zgodnie z opisem poniżej.

Ogólne

Właściwość	Opis
Nazwa	Nazwa urządzenia
Rodzaj	Rodzaj urządzenia - nVision decyduje o rodzaju urządzenia poprzez SNMP, można to także zmienić manualnie.
Serwer	Wskazuje, czy urządzenie jest serwerem.
Router	Wskazuje, czy urządzenie jest routerem.
Znaczenie	Znaczenie - ważność urządzenia. Pozwala ustawić alarmy globalne tak, aby inicjowane były tylko dla urządzeń uznanych za ważne i (np. serwery) a ignorowane w przypadku stacji roboczych.
Urządzenie zarządzalne przez SNMP	Wskazuje, czy urządzenie jest zarządzalne przez SNMP.

Własciwosc	Opis
Wspólnota do odczytu	Wspólnota SNMP - rodzaj hasła używanego do odczytywania i ustawiania informacji SNMP na urządzeniu.
Wspólnota do zapisu	j.w.
Info1	Informacja zdefiniowana przez użytkownika.
Info2	Informacja zdefiniowana przez użytkownika.
Styl wizualizacji	Styl, w jakim urządzenie będzie przedstawione na mapie. Aby uzyskać więcej informacji o stylach, przejdź do rozdziału Style - Wprowadzenie .

Monitorowanie

Własciwosc	Opis
Monitoruj	Włączenie tej opcji zezwala na monitorowanie urządzenia: serwisów, liczników i SNMP.
Zapisz historie monitorowania	Włączenie tej opcji sprawia, że wszystkie dane z monitorowania będą zapisane w bazie danych. Można wyłączyć tę opcję, aby zachować więcej miejsca na dysku. Nawet jeśli opcja jest wyłączona, dane są gromadzone w pamięci, więc można zobaczyć pewną ilość ostatnich wyników.
Monitoruj serwisy Windows	Zaznacz, aby monitorować serwisy Windows stosując WMI. Aby uzyskać więcej informacji, przejdź do rozdziału Monitorowanie serwisów Windows .
Auto (Czas monitorowania)	nVision automatycznie ustali optymalny czas monitorowania na podstawie liczby urządzeń i monitorowanych serwisów/liczników. Będzie starał się monitorować je tak często, jak to możliwe.
Ustaw (Czas monitorowania)	Można ustawić minimalny czas monitorowania. nVision może zwiększyć ten czas, jeśli będzie to konieczne. Aby uzyskać więcej informacji, przejdź do rozdziału Monitorowanie - Wprowadzenie .
Monitoruj, jeśli to urządzenie działa	Urządzenie będzie monitorowane tylko wtedy, gdy jego urządzenie nadrzędne (wybrane w tym polu) ma status <Działa>. W tym polu można wybrać router, aby urządzenia znajdujące się za nim, nie były monitorowane, gdy przestanie on działać.
Monitorowane serwisy	Lista serwisów monitorowanych na danym urządzeniu.

Dane logowania

Własciwosc	Opis
Nazwa użytkownika	Nazwa użytkownika używana do zalogowania się na różnych serwerach (Windows, NetWare, Linux).
Hasło	Hasło

6.4.4 Zarządzanie urządzeniami

Rozdział ten opisuje różne aspekty zarządzania urządzeniami i ich serwisami.

Ustawianie właściwości urządzeń

1. Wybierz **Właściwości** z menu kontekstowego ikony.
2. Ustaw właściwości urządzenia zgodnie z opisem w rozdziale [Właściwości urządzeń](#).

Dodawanie urządzeń

1. Wybierz **Urządzenie | Nowe** z głównego menu.
2. Wprowadź adres DNS lub IP urządzenia.
3. Można także ustawić rodzaj urządzenia i opcje znaczenia.

Usuwanie ikon urządzeń

1. Wybierz **Usun** z menu kontekstowego ikony.
2. Potwierdź usunięcie. Podczas usuwania ostatniej ikony określonego urządzenia, usunięte zostanie całe urządzenie wraz z wszystkimi jego danymi. Można więc bezpiecznie usuwać ikony z map użytkownika, jeśli ikony tych urządzeń w dalszym ciągu znajdują się na mapach sieciowych.

Pokazywanie okna informacji o urządzeniu

1. Wybierz **Informacje o urządzeniu** z menu kontekstowego ikony lub dwukrotnie kliknij ikonę.
2. Zobaczysz okno informacji o urządzeniu - opis informacji prezentowanych w tym oknie znajduje się w rozdziale [Okno informacji o urządzeniu](#).
3. Możesz zostawić to okno na pulpicie i dalej pracować z programem. Informacje przedstawione w tym oknie będą automatycznie odświeżane, aby pokazywać zmiany i stan urządzenia.
4. Można otworzyć nieograniczoną liczbę okien informacji o urządzeniu.

Zarządzanie serwisami i licznikami urządzeń

Zarządzanie serwisami

Aby uzyskać więcej informacji o serwisach, przejdź do rozdziału [Monitorowanie serwisów](#).

Zarządzanie licznikami wydajności

Aby uzyskać więcej informacji o licznikach wydajności, przejdź do rozdziału [Monitorowanie wydajności](#).

6.4.5 Okno informacji o urządzeniu

Aby zobaczyć informacje o urządzeniu, kliknij dwukrotnie ikonę urządzenia lub wybierz **Informacje o urządzeniu** z jej menu kontekstowego.

Ogólne

Tabela poniżej wyszczególnia informacje dostępne na zakładce Ogólne w oknie Informacje o urządzeniu.

Pole	Opis
Nazwa	Nazwa urządzenia.
Rodzaj	Rodzaj urządzenia - nVision określa rodzaj za pomocą SNMP, ale można także zmienić ten rodzaj ręcznie.
Stan	Aktualny stan urządzenia.
Adresy i interfejsy	Lista wszystkich adresów i interfejsów dostępnych na danym urządzeniu. Zawiera następujące informacje: <ul style="list-style-type: none"> • Stan serwisu • Adres IP i DNS • Adres MAC • Opis SNMP interfejsu. Jeśli nie ma żadnego opisu, jest to tylko adres IP, a nie interfejs. • Szybkość interfejsu.
System	Opis systemu urządzenia, odczytany przez SNMP.
Lokalizacja	Lokalizacja urządzenia, odczytana przez SNMP.
Nazwa komputera	Nazwa urządzenia, odczytana przez SNMP.
Monitorowanie	
Ostatnie sprawdzenie	Czas ostatniego sprawdzenia jakiegokolwiek serwisu.
Ostatnia odpowiedź	Czas ostatniej pomyślnej odpowiedzi od jakiegokolwiek serwisu.
Czas następnego sprawdzenia	Czas następnego sprawdzenia.
Czas monitorowania	
Czas działania	Czas działania urządzenia - całkowity i dla aktualnej sesji (suma stanu Ok i Ostrzeżenie)
Ok	Czas, gdy urządzenie miało status Ok - całkowity i dla aktualnej sesji.
Ostrzeżenie	Czas, gdy urządzenie miało status Ostrzeżenie - całkowity i dla aktualnej sesji.
Nie działa	Czas niedziałania urządzenia - całkowity i dla danej sesji.
Alarmy	
Otwarte	Liczba aktualnie otwartych (niezamkniętych) alarmów.
Ostatni	Czas ostatniego alarmu.

Serwisy

nVision może monitorować serwisy ICMP, TCP i UDP. Możesz zobaczyć wszystkie monitorowane serwisy w tabeli, dostępnej na zakładce Serwisy. Dla każdego serwisu prezentowane są informacje o czasie odpowiedzi i żądaniach wysłanych/przyjętych. Po wybraniu jednego lub więcej serwisów, zobaczysz wykres prezentujący czas odpowiedzi oraz procent utraconych zadań/pakietów (w przypadku, gdy wybrany jest jeden serwis). Dane historyczne można zobaczyć dla wielu różnych okresów (np. z ostatnich 15 minut, godziny, dnia, tygodnia, miesiąca, czy z całego roku). Aby wybrać odpowiedni okres, kliknij odpowiednią ikonę na pasku narzędzi wykresu. Aby przewijać wykres do przodu i do tyłu, użyj ikon ze strzałkami znajdujących się na pasku narzędziowym wykresu.

Aby uzyskać więcej informacji o serwisach, przejdź do rozdziału [Monitorowanie serwisów](#).

Liczniki wydajności

nVision może monitorować wiele liczników wydajności (aby uzyskać pełną listę dostępnych liczników, przejdź do rozdziału [Rodzaje liczników](#)). Możesz zobaczyć wszystkie monitorowane liczniki, wyszczególnione w tabeli dostępnej na zakładce **Liczniki wydajności**. Dla każdego licznika prezentowane są dane o ostatniej i najmniejszej/największej/średniej wartości (oprócz licznika statusu urządzenia, który nie ma min/max/średnich wartości). Po wybraniu licznika, zobaczysz wykres pokazujący jego wartość. Możesz zobaczyć dane historyczne dla wielu okresów czasu (np. z ostatnich 15 minut, godziny, dnia, tygodnia, miesiąca, czy z całego roku). Aby przewijać wykres do tyłu i do przodu, użyj ikon ze strzałkami znajdujących się na pasku narzędziowym wykresu.

Aby uzyskać więcej informacji o licznikach, przejdź do rozdziału [Monitorowanie wydajności](#).

Monitor dziennika systemowego (Event log)

Jest to lista wszystkich zainicjowanych alarmów, wraz z rejestrem akcji wykonanych dla każdego alarmu. Możesz zobaczyć alarmy posortowane według wielu pól, a także przefiltrować je tak, aby zobaczyć jedynie te, które Cię interesują.

Przeglądarka SNMP

Jeśli urządzenie jest zarządzalne przez SNMP, dostępna będzie zakładka SNMP, zawierająca przeglądarkę SNMP. Jeśli zakładka ta nie jest dostępna, otwórz okno właściwości urządzenia, włącz opcję zarządzalności przez SNMP i ustaw wspólnotę SNMP.

Mapowanie portów

Zakładka mapowanie portów przedstawia listę wszystkich urządzeń podłączonych do portu switcha. Dane te widoczne są tylko wtedy, gdy nVision jest w stanie odczytać odpowiednie informacje SNMP z urządzenia (które są dostępne głównie na switchach). Aby uzyskać więcej informacji, przejdź do rozdziału [Monitorowanie portów switcha](#).

Aktywność użytkowników

Zakładka ta prezentuje informacje zgromadzone przez agenta nVision. Przedstawia czas aktywności użytkownika, wykorzystanie aplikacji oraz listę odwiedzanych stron. Aby uzyskać więcej informacji, przejdź do rozdziału [Monitorowanie aktywności użytkowników](#).

Zasoby

Zakładka ta prezentuje wszystkie aplikacje zainstalowane na komputerach, a także informacje o sprzecie. Aby uzyskać więcej informacji, przejdź do rozdziału [Zasoby](#).

6.5 Style

6.5.1 Wprowadzenie

Style definiują sposób wizualizacji map. Rozdział ten opisuje domyślne style i sposób definiowania stylów dla różnych obiektów. Aby zapoznać się z informacjami o tworzeniu i modyfikowaniu stylów, przejdź do rozdziału [Zarządzanie stylami](#).

Style domyślne

Domyslnie style atlasu

Domyslnie style atlasu zdefiniowane są we właściwościach atlasu. Style te używane są przez wszystkie nowe utworzone obiekty oraz te, które mają styl zdefiniowany jako <domyslny> (jednak mapa zawierająca te obiekty może nadpisywać styl atlasu). Po utworzeniu mapy jej style oraz styl

wszystkich jej obiektów przyjmują wartość <domyslny>, w związku z czym zastosowane będą style zdefiniowane dla atlasu. Zmiana stylu we właściwościach atlasu spowoduje zmianę stylów takich obiektów.

Aby zmienić domyślne style atlasu, użyj okna właściwości atlasu. Jest to opisane w rozdziale [Zarządzanie atlasem](#).

Style domyślne mapy

Mapa - podobnie jak atlas - posiada swoje domyślne style. Za ich pomocą można nadpisać style globalne. Jeśli ustawimy styl <domyslny>, wtedy styl zdefiniowany dla atlasu będzie miał zastosowanie.

Styl <domyslny> w tym przypadku oznacza, iż mapa używa stylu zdefiniowanego we właściwościach atlasu. Można to traktować jako referencję do stylu atlasu. Dlatego styl <domyslny> nie może być modyfikowany lub usunięty, ponieważ tylko wskazuje na jakiś inny.

Style obiektu mapy

Styl wizualizacji urządzenia

Za pomocą stylu wizualizacji definiuje się sposób prezentacji urządzenia na mapie. Można wybrać informacje, jakie wyświetlane są na ikonach: czas niedziałania, informacja o niedziałających serwisach, czas ostatniej odpowiedzi, wskaźniki SNMP i alarmów, itp.

Styl kształtu

Styl kształtu określa wygląd obiektu kształt (obiekt tła mapy): ramki, kolory, itp.

Styl linii

Styl ten definiuje właściwości graficzne linii łączącej dwie ikony.



6.5.2 Definiowanie stylów

Rozdział ten opisuje właściwości poszczególnych typów stylów. Aby zapoznać się z informacjami o tworzeniu i modyfikowaniu stylów, przejdź do rozdziału [Zarządzanie stylami](#).

Styl wizualizacji urządzenia

Styl ten definiuje sposób prezentacji ikony urządzenia na mapie. Poniższa tabela opisuje właściwości stylu.

Właściwość	Opis
Nazwa	Nazwa stylu
Podpis ikony	Definiuje tekst znajdujący się w podpisie ikony.
Podpis przezroczysty	Podpis ikony będzie przezroczysty po włączeniu tej opcji.
Po zmianie stanu migaj	Czas migania ikony w razie zmiany stanu urządzenia. Miganie pozwala na łatwe lokalizowanie tych urządzeń, które zmieniły stan.
Czas odpowiedzi serwisu wiodącego	Opcja ta określa, czy wyświetlać czas odpowiedzi wiodącego serwisu.
Czas niedziałania urządzenia i serwisów	Po włączeniu tej opcji na ikonach urządzeń o stanie <Nie działa> będzie wyświetlony czas trwania takiego stanu. Jeśli urządzenie działa, jednak niektóre serwisy nie odpowiadają, wtedy zobaczysz informacje o tych serwisach.

Wlasciwosc	Opis
Zarządzanie przez SNMP	Jesli urzadzenie jest zarzadzalne przez SNMP, ikona  wyswietli sie po prawej stronie ikony urzadzenia.
Ostrzezenie o alarmach	Jesli urzadzenie ma niepotwierdzone alarmy, wtedy po prawej stronie wyswietli sie ikona  - wraz z liczba alarmów.
Pokaz wykres wydajnosci	Mozesz ustawic do 6 slupków obrazujacych czas odpowiedzi serwisu lub dowolny licznik.
Obrazuj wiodacy serwis	Czas odpowiedzi wiodacego serwisu bedzie prezentowany na wykresie.

Styl kształtu

Styl kształtu określa wygląd obiektu kształt (obiekt tła mapy): ramke, kolory, itp.

Wlasciwosc	Opis
Nazwa	Nazwa stylu
Typ	Typ kształtu. Dostępne są 4 typy: prostokąt, prostokąt zaokrąglony, elipsa i gwiazda.
Czcionka	Nazwa czcionki napisu.
Kolor i rozmiar czcionki	Kolor i rozmiar czcionki napisu.
Tło	<ul style="list-style-type: none"> Jednolite - tło kształtu ma wybrany kolor. Gradient - tło to przejście tonalne o określonych kolorach i kierunku.
Ramka	<ul style="list-style-type: none"> Kolor - kolor ramki. Grubość - grubość ramki.
Przezroczystość	Określa przezroczystość kształtu.
Cień	Definiuje rozmiar cienia. Wartość 0 oznacza brak cienia.

Styl linii

Styl ten definiuje właściwości graficzne linii łączącej dwie ikony.

Wlasciwosc	Opis
Nazwa	Nazwa stylu
Grubość	Grubość linii
Kolor	Kolor linii
Typ	<ul style="list-style-type: none"> Prosta - linia prosta Lamana - linia lamana


6.5.3 Zarządzanie stylami

Wszystkie obiekty na mapie (oprócz tekstu) używają mechanizmu stylów. Determinują one wygląd obiektu. Na przykład określają kolor, czcionkę, ramki, itp. Aby zmienić wygląd obiektu należy zmienić jego styl w oknie właściwości.


Okno zarządzania stylami

1. Aby otworzyć okno zarządzania stylami, wykonaj jedno z poniższych:
 - Wybierz **Narzędzia | Zarządzaj stylami** z głównego menu.
 - Można też otworzyć okno zarządzania podczas edycji właściwości obiektu za pomocą przycisku znajdującego się obok pola wyboru stylu. Kliknij strzałkę znajdującą się na przycisku i wybierz z menu **Zarządzaj stylami**.
2. Wybierz typ stylów jakimi chcesz zarządzać (urządzenie, kształt lub linia) w pasku nawigacyjnym po prawej stronie.


Tworzenie nowego stylu

1. Otwórz okno zarządzania stylami
2. Kliknij ikonę .
3. Zdefiniuj styl zgodnie z informacją dostępną w rozdziale [Definiowanie stylów](#).

Edycja stylów

1. Otwórz okno zarządzania stylami
2. Zaznacz styl i kliknij ikonę .
3. Zmieniaj właściwości stylu zgodnie z informacją dostępną w rozdziale [Definiowanie stylów](#).

Usuwanie stylu

1. Otwórz okno zarządzania stylami.
2. Zaznacz styl i kliknij ikonę .

Część

VII

7 Raporty

7.1 Wprowadzenie

Axence nVision posiada zaawansowany system raportowania, pozwalający na tworzenie drukowalnych raportów, dostarczających najważniejsze informacje o każdym urządzeniu lub mapie. Program dostarcza także narzędzie służące do tworzenia własnych raportów: więcej informacji znajdziesz w dziale [Tworzenie raportów](#).

Otwieranie okna zarządzania raportami

Kliknij przycisk **Raporty**, znajdujący się na głównym pasku narzędzi - zostanie otwarte okno zarządzania raportami, w którym możesz przeglądać, drukować oraz tworzyć nowe raporty.

Przeglądanie i drukowanie raportów

Aby przygotować raport dla urządzenia albo mapy:

1. Wybierz typ raportu: dla mapy lub urządzenia. Dla obu typów zdefiniowane są różne raporty.
2. Wybierz urządzenie albo mapę (w zależności od wcześniej wybranego typu raportu).
3. Wybierz raport z panelu znajdującego się po lewej stronie.
4. Wybierz przedział czasu, dla którego chcesz wygenerować raport.
5. Kliknij przycisk **Przygotuj i wyświetl raport**. Ten przycisk jest widoczny tylko, gdy dany raport nie był nigdy wcześniej przygotowany. Gdy raport zostanie raz przygotowany, zostanie automatycznie wyświetlony za każdym razem, gdy wybierzesz go ponownie - z wyjątkiem sytuacji, w której dane mogły ulec dezaktualizacji (np. raport dla danych z dnia dzisiejszego).
6. Po utworzeniu raportu możesz go wydrukować klikając przycisk **Drukuj** znajdujący się na pasku narzędzi raportu.

7.2 Tworzenie raportów

Axence nVision pozwala w bardzo prosty sposób tworzyć nowe raporty. Tworzenie raportów oparte jest o wybór i konfigurację predefiniowanych segmentów. Segmenty to kolektory danych, które gromadzą dane zebrane przez nVision i przetwarzają je tak, aby można je było wyświetlić w tabeli lub na wykresie.

Aby utworzyć własny raport:

1. Otwórz okno zarządzania raportami.
2. Wybierz pozycje **Urządzenie** albo **Mapa**, określające typ raportu jaki chcesz utworzyć.
3. Wybierz kategorię, do której ma należeć nowo utworzony raport.
4. Kliknij przycisk **Utwórz nowy raport**.
5. Wpisz nazwę i opis raportu.
6. Dodaj segment klikając przycisk z zielonym plusem na pasku narzędzi po lewej stronie.
7. Wpisz nazwę segmentu oraz wybierz jego typ. Więcej informacji znajdziesz w rozdziałach [Typy segmentów dla urządzeń](#) lub [Typy segmentów dla map](#).
8. Wybierz odpowiednie opcje, opisane w rozdziałach [Typy segmentów dla urządzeń](#) lub [Typy segmentów dla map](#).
9. Wpisz krótki i długi opis, które znajdują się odpowiednio nad i pod segmentem.

7.3 Typy segmentów raportów dla urzędzeń

Rozdział ten opisuje typy segmentów raportów dla urzędzeń oraz ich właściwości (jeśli jest to potrzebne). Większości segmentów nie trzeba konfigurować.

Wykres wydajności serwisu

Segment wydajności serwisu przedstawia czas odpowiedzi i procent utraconych pakietów dla wybranego lub wszystkich serwisów.

Własność	Opis
Generuj dla wybranego serwisu	Segment zostanie utworzony tylko dla wybranego serwisu. Jeśli urządzenie, dla którego generujemy raport nie posiada tego serwisu, segment nie zostanie wygenerowany.
Generuj dla wszystkich serwisów	Segment zostanie wygenerowany dla wszystkich serwisów, które posiada dane urządzenie.
Przedstaw jako	Określa w jaki sposób segment zostanie przedstawiony: <ul style="list-style-type: none"> Wykres wydajności serwisu (domyślnie) - wyspecjalizowany wykres który przedstawia czas odpowiedzi oraz procent utraconych pakietów na jednym wykresie. Wykres liniowy Tabela

Nagłówek raportu

Nagłówek ze szczegółami raportu. Powinien być pierwszym segmentem każdego raportu.

Historia stanu urządzenia

Tabela prezentująca historię zmian stanu urządzenia w zadanym przedziale czasowym.

Najczęstsze zdarzenia

Lista zdarzeń posortowana według ilości wystąpień.

Własność	Opis
Ogranicz listę do X pierwszych zdarzeń	Włącz tę opcję jeśli chcesz ograniczyć listę zdarzeń pokazanych w raporcie.
Przedstaw jako	Określa w jaki sposób segment zostanie przedstawiony: <ul style="list-style-type: none"> Wykres słupkowy poziomy Wykres słupkowy pionowy Wykres kołowy Tabela

Serwisy - informacje ogólne

Lista przedstawiająca wszystkie serwisy danego urządzenia wraz z najważniejszymi informacjami dotyczącymi ich wydajności.

Liczniki wydajności

Lista przedstawiająca wszystkie liczniki wydajności danego urządzenia.

Dziennik zdarzeń

Lista przedstawiająca wszystkie wpisy dziennika zdarzeń dla zadanego przedziału czasowego.

Wykres licznika wydajności

Przedstawia wykres wartości licznika wydajności dla zadanego przedziału czasowego.

Własność	Opis
Licznik wydajności	Wykres zostanie utworzony dla wybranego licznika wydajności. Jeśli dane urządzenie nie posiada takiego licznika, segment nie zostanie utworzony.
Przedstaw jako	Określa w jaki sposób segment zostanie przedstawiony: <ul style="list-style-type: none"> Wykres liniowy Wykres warstwowy Wykres słupkowy pionowy Tabela

Czas urządzenia w stanie "działa"/"nie działa"

Czasy wyrażone w procentach, w których host znajdował się w stanie "działa" albo "nie działa".

Własność	Opis
Przedstaw jako	Określa w jaki sposób segment zostanie przedstawiony: <ul style="list-style-type: none"> Wykres słupkowy poziomy Wykres słupkowy pionowy Wykres kołowy Tabela

Strony WWW

Lista przeglądanych stron WWW przez użytkowników na danym komputerze.

Zainstalowane programy

Lista zainstalowanych programów na danym komputerze.

Własność	Opis
Pokaz	Określa czy mają zostać przedstawione tylko zainstalowane programy, czy także aktualizacje Windows.

Własność	Opis
Przedstaw jako	Mozna wybrać tylko tabele.

Używane programy

Lista używanych programów przez użytkowników na danym komputerze.

Używane grupy programów

Lista używanych programów na danym komputerze pogrupowana według ich funkcjonalności.

7.4 Typy segmentów raportów dla map

Ten temat opisuje typy segmentów raportów dla map oraz ich właściwości (jeśli jest to potrzebne).

Najlepsze/najgorsze urządzenia według wydajności serwisów

Lista urządzeń z najdłuższymi lub najkrótszymi czasami odpowiedzi.

Własność	Opis
Serwis	Wybierz serwis, na podstawie którego urządzenia będą porównywane. Jeśli któreś urządzenie nie posiada danego serwisu, nie będzie brane pod uwagę przy porównywaniu.
Sortuj według procentu utraconych pakietów	Wyniki zostaną posortowane według procentu utraconych pakietów zamiast czasu odpowiedzi.
Pokaz najlepsze urządzenia	Zaznacz tę opcję, jeśli chcesz zobaczyć najlepsze urządzenia (z najkrótszym czasem odpowiedzi lub z najmniejszym procentem utraconych pakietów).
Pokaz najgorsze urządzenia	Zaznacz tę opcję, jeśli chcesz zobaczyć najgorsze urządzenia.
Ogranicz listę	Zaznacz tę opcję, jeśli chcesz ograniczyć liczbę prezentowanych urządzeń.
Przedstaw jako	Określa sposób w jaki segment zostanie przedstawiony: <ul style="list-style-type: none">• Wykres słupkowy poziomy• Wykres słupkowy pionowy• Tabela

Nagłówek raportu

Nagłówek ze szczegółami raportu. Powinien być pierwszym segmentem każdego raportu.

Historia stanu urządzeń

Tabela prezentująca historię zmian stanu wszystkich urządzeń należących do danej mapy w zadanym przedziale czasowym.

Najlepsze/najgorsze urządzenia względem ilości zdarzeń

Lista przedstawiająca najbardziej lub najmniej problematyczne urządzenia względem ilości alarmów, które zostały na nich wygenerowane.

Własność	Opis
Generuj dla wszystkich zdarzeń	Porównuje urządzenia względem ilości wystąpień wszystkich zdarzeń
Generuj dla wybranego zdarzenia	Porównuje urządzenia względem ilości wystąpień wybranego zdarzenia
Pokaż najlepsze urządzenia	Zaznacz tę opcję, jeśli chcesz zobaczyć najlepsze urządzenia (z najmniejszą ilością zdarzeń)
Pokaż najgorsze urządzenia	Zaznacz tę opcję, jeśli chcesz zobaczyć najgorsze urządzenia
Ogranicz listę	Włącz tę opcję, jeśli chcesz ograniczyć ilość prezentowanych urządzeń.
Przedstaw jako	Określa sposób w jaki segment zostanie przedstawiony: <ul style="list-style-type: none"> Wykres słupkowy poziomy Wykres słupkowy pionowy Tabela

Najczęstsze zdarzenia

Lista zdarzeń posortowana według ilości ich wystąpień.

Własność	Opis
Ogranicz listę do X pierwszych zdarzeń	Włącz tę opcję, jeśli chcesz ograniczyć listę zdarzeń pokazanych w raporcie.
Przedstaw jako	Określa w jaki sposób segment zostanie przedstawiony: <ul style="list-style-type: none"> Wykres słupkowy poziomy Wykres słupkowy pionowy Wykres kołowy Tabela

Dziennik zdarzeń

Lista przedstawiająca wszystkie wpisy dziennika zdarzeń dla zadanego przedziału czasowego.

Najlepsze/najgorsze urządzenia według liczników wydajności

Lista urządzeń, które są najbardziej/najmniej wydajne względem licznika wydajności.

Własność	Opis
Licznik wydajności	Wybierz licznik wydajności, na podstawie którego urządzenia będą porównywane. Jeśli dane urządzenie nie posiada wybranego licznika wydajności, nie będzie brane pod uwagę przy porównywaniu.
Pokaż najlepsze urządzenia	Zaznacz tę opcję, jeśli chcesz zobaczyć listę najlepszych urządzeń (z najmniejszą wartością licznika wydajności).

Wlasnosc	Opis
Pokaz najgorsze urzadzenia	Zaznacz ta opcje, jesli chcesz zobaczyc liste najgorszych urzadzen
Ogranicz liste	Wlacz ta opcje, jesli chcesz ograniczyc ilosc urzadzen przedstawianych w zestawieniu
Przedstaw jako	Okresla sposob w jaki segment zostanie przedstawiony: <ul style="list-style-type: none">• Wykres slupkowy poziomy• Wykres slupkowy pionowy• Tabela

Zainstalowane programy

Lista wszystkich programów zainstalowanych na komputerach znajdujących się na wybranej mapie.

Wlasnosc	Opis
Pokaz	Okresla czy maja zostac przedstawione tylko zainstalowane programy, czy takze aktualizacje Windows.
Przedstaw jako	Mozna wybrac tylko tabele.

Uzywane programy

Lista uzywanych programów przez uzytkowników na danym komputerze.

Uzywane grupy programów

Lista uzywanych programów na danym komputerze pogrupowana wedlug ich funkcjonalnosc.

Część



8 Alarmowanie

8.1 Wprowadzenie

Rozdział ten opisuje zasady korzystania z mechanizmu alarmowania dostępnego w nVision. Dzięki niemu, możesz być np. informowany w przypadku jakichkolwiek problemów w Twojej sieci. Jeśli jakieś urządzenie przestanie odpowiadać, czas odpowiedzi któregoś z monitorowanych serwisów znacząco wzrośnie lub gdy jakaś aplikacja przestanie działać prawidłowo, nVision może wysłać Ci wiadomość, wyświetlić informacje na ekranie, lub rozpocząć którąś ze zdefiniowanych przez Ciebie akcji korekcyjnych.

Jak to działa?

Po pierwsze, musisz zdefiniować pewien zbiór zdarzeń, który Cię interesuje. Przykładem takiego zdarzenia jest sytuacja, w której urządzenie sieciowe przestaje odpowiadać. nVision stale monitoruje wszystkie urządzenia w celu wykrycia, czy na którymś z nich miało miejsce jakieś zdarzenie. W podanym przykładzie, zdarzenie będzie zainicjowane, gdy wszystkie serwisy działające na urządzeniu przestaną odpowiadać.

Zdefiniowanie samego zdarzenia nie wystarcza jednak do jego pełnej obsługi. Należy także zdefiniować zbiór akcji, które mogą zostać wykonane, gdy zajdzie któreś ze zdarzeń. Po zdefiniowaniu tych zdarzeń oraz akcji, możemy rozpocząć definicję alarmów. Alarm określa jakie akcje mają zostać wykonane gdy zajdzie konkretne zdarzenie.

Wszystkie wygenerowane alarmy są zapisywane w bazie danych, aby umożliwić ich późniejszą analizę i przygotowanie raportów na ich podstawie. Jeśli chcesz zbierać takie informacje, ale nie chcesz aby żadna akcja była wykonana w wypadku konkretnych zdarzeń, musisz zdefiniować dla nich alarmy, ale nie przypisywać żadnych akcji. nVision takie zdarzenia zapisze tylko w bazie danych.

Podsumowując proces tworzenia alarmu:

1. Utwórz zdarzenie. Wystąpienie takiego zdarzenia zainicjuje alarm. Przykłady zdarzeń: urządzenie nie odpowiada, problem z wydajnością serwisu, czas załadowania strony WWW przekroczy wartość graniczną, itp.
2. Zdefiniuj akcje informujące oraz korekcyjne, które mają być wykonane gdy zdarzenie będzie miało miejsce. Przykłady akcji: wysłanie wiadomości e-mail lub ICQ, uruchomienie zewnętrznej aplikacji, zrestartowanie usługi Windows. Ten krok nie jest konieczny - możesz zdefiniować alarm bez żadnych akcji.
3. Utwórz alarm. Alarm określa jakie akcje i kiedy mają zostać wykonane gdy konkretne zdarzenie będzie miało miejsce. Każdy alarm jest zapisywany do bazy danych programu, nawet jeśli nie zostały do niego przypisane żadne akcje.

8.2 Pojęcia

Rozdział ten poświęcony jest ogólnym założeniom systemu alarmowania w nVision.

Zdarzenia

nVision stale monitoruje Twoją sieć, wszystkie urządzenia oraz serwisy - może więc wykryć sytuację, w której konkretny serwis zacznie odpowiadać wolniej lub wcale. Wykryje też, kiedy całe urządzenie przestaje odpowiadać. Dla takich właśnie sytuacji możesz zdefiniować zdarzenie. Każde zdarzenie ma swój czas rozpoczęcia oraz zakończenia, na przykład: w przypadku zdarzenia **urządzenie nie odpowiada** zostanie ono zakończone, gdy urządzenie zacznie odpowiadać. Dlatego dzięki nVision wiesz nie tylko kiedy pewne zdarzenie się zaczęło, ale także kiedy się zakończyło. W **dzienniku zdarzeń** możesz zobaczyć listę wszystkich zdarzeń, które się jeszcze nie zakończyły. Dla celów tego podręcznika będziemy nazywać je zdarzeniami otwartymi.

Mozesz także zdefiniować własne zdarzenia: założmy, że posiadasz serwer MSSQL, który chcesz monitorować. W takim przypadku nie wystarczy sprawdzać jak szybko reaguje on na proste zapytanie, najprawdopodobniej będziesz chciał także monitorować kilka liczników wydajności, opisujących aktualny stan serwera, by móc zareagować zanim jakkolwiek krytyczna sytuacja będzie miała miejsce. Na przykład kiedy licznik wydajności określający ilość wolnej pamięci zacznie przyjmować niskie wartości ze względu na degradację wydajności pamięci cache. Alarm oparty na takim zdarzeniu może zostać wygenerowany zanim wystąpi jakkolwiek błąd, którego skutki są nieodwracalne, co pozwoli Ci szybko naprawić problem i uniknąć utraty danych.

Wszystkie występujące zdarzenia są zapisywane w dzienniku zdarzeń nVision. Dzięki temu możesz analizować wydajność swojej sieci, tworząc na przykład raporty przedstawiające najbardziej problematyczne urządzenia, lub najczęściej występujące zdarzenia.

Stan urządzenia

W przeciwieństwie do konkurencyjnych programów, stan urządzenia jest w nVision wartością wyliczana, nie zdefiniowana na sztywno. Można więc definiować warunki, kiedy uznajemy urządzenie jako działające, nie działające lub w stanie ostrzeżenia. Aby uzyskać więcej informacji przejdź do rozdziału [Stan urządzenia - koncepcje](#).

Akcje

Mozna zdefiniować dwa podstawowe typy akcji: informacyjne oraz korekcyjne. Jeśli jakies zdarzenie miało miejsce, nVision korzystając z mechanizmu akcji powiadamia administratora o problemie lub uruchamia zewnętrzny program, aby go naprawić. Dlatego zanim zaczniesz definiować alarmy, musisz utworzyć zbiór akcji, które będą używane do powiadamiania Ciebie.

Mozna zdefiniować np. akcje: wysłanie wiadomości e-mail, ICQ lub SMS, odegranie dźwięku, wyświetlenie wiadomości lub uruchomienie zewnętrznego programu. Kompletna lista dostępnych akcji znajduje się w rozdziale [Typy Akcji](#).

Alarmy

Alarm określa zachowanie programu w wypadku jakichkolwiek problemów w sieci. Na początku wybiera się, kiedy alarm powinien zostać wygenerowany poprzez przypisanie mu odpowiedniego zdarzenia. Następnie należy określić dla jakiego obiektu alarm ma być zdefiniowany - można definiować alarmy dla całego atlasu, mapy lub konkretnego urządzenia. Alarmy są generowane jeśli zdarzenie wystąpiło na urządzeniu należącym do obiektu, na którym alarm jest zdefiniowany (np. atlas, mapa lub mapa pochodna).

8.3 Zarządzanie Alarmami

8.3.1 Wprowadzenie

Zarządzanie alarmami wymaga wcześniejszego zapoznania się z kilkoma koncepcjami. Musisz wiedzieć czym są zdarzenia i akcje. Zanim zaczniesz zarządzać alarmami, przeczytaj rozdział [Pojęcia](#), w którym powyższe kwestie są opisane.

Wymagania wstępne

Aby rozpocząć zarządzanie alarmami musisz wcześniej zdefiniować zbiór zdarzeń. W nVision zdarzenia określają w jakich sytuacjach alarmy mają zostać zainicjowane. Na przykład: po zainstalowaniu programu istnieje predefiniowane zdarzenie "Urządzenie nie działa". Opisuje ono zdarzenie, gdy urządzenie przestaje odpowiadać. Należy zdefiniować zdarzenia dla wszelkich problematycznych sytuacji, które chcesz wykrywać.

Po zdefiniowaniu zdarzenia należy zdefiniować akcje informujące. Akcje określają co nVision ma zrobić, kiedy pewne zdarzenie będzie miało miejsce. Na przykład akcja może określać, w jaki sposób poinformować Cię za pomocą wiadomości e-mail. Można jednak definiować alarmy bez akcji - takie rozwiązanie może być przydatne, jeśli chcesz zachować informację o zdarzeniu do późniejszej analizy, ale nie potrzebujesz być o nim poinformowany.

Po wykonaniu powyższych kroków, możesz rozpocząć zarządzanie alarmami. Kolejne rozdziały opisują wszystkie dostępne funkcje tego mechanizmu.

Gdzie można definiować alarmy

Alarmy można definiować na kilku poziomach atlasu. Przede wszystkim, istnieje możliwość zdefiniowania globalnych alarmów dla całego atlasu. Takie alarmy są dziedziczone przez wszystkie urządzenia w atlasie, co oznacza, że warunki wystąpienia takiego alarmu są sprawdzane na każdym urządzeniu (jeśli dane urządzenie spełnia kryteria zdefiniowane w alarmie, na przykład alarm zdefiniowany tylko dla ważnych urządzeń nie zostanie wygenerowany na urządzeniu ze znaczeniem ustawionym na "niskie").

Alarmy mogą być także zdefiniowane dla każdej mapy - w takiej sytuacji, alarmy są dziedziczone przez wszystkie urządzenia znajdujące się na danej mapie lub na którejkolwiek z map podrzędnych. I w końcu, alarmy mogą być także definiowane dla każdego urządzenia.

Istnieje więc kilka sposobów definiowania alarmu pozwalających na utworzenie odpowiedniej polityki alarmowania bazującej na znaczeniu urządzeń, sieci, serwisów itp. Należy pamiętać, że alarmy są dziedziczone z obiektów nadrzędnych do podrzędnych. Aby uzyskać więcej informacji na temat przejdź do rozdziału [Alarmy Dziedziczone](#).

8.3.2 Zarządzanie Alarmami





Aby skonfigurować program tak, aby informował Cię o jakichkolwiek problemach użyj okna zarządzania alertami. W tym i kolejnych rozdziałach znajdziesz informacje o tym, jak zarządzać alarmami.


Otwieranie okna zarządzania alarmami

Za pomocą tego okna możesz przeglądać, modyfikować, tworzyć nowe oraz usuwać alarmy. Aby otworzyć okno zarządzania alarmami wykonaj następujące czynności.

1. Wybierz obiekt, którego alarmami chcesz zarządzać. Może być to urządzenie, mapa lub atlas. Jeśli wybrales atlas lub mapę, alarmy definiowane na nich wpływają także na urządzenia należące do tego obiektu. Aby uzyskać więcej informacji na ten temat przejdź do rozdziału [Alarmy Dziedziczone](#).
2. Wybierz **Konfiguruj Alarmy** z menu kontekstowego.

Tworzenie nowych alarmów lub modyfikacja istniejących

1. Otwórz okno zarządzania alarmami dla obiektu, na których chcesz utworzyć alarm.
2. Kliknij przycisk  aby utworzyć nowy alarm lub wybierz istniejący alarm i kliknij przycisk .
3. W polu **Dla zdarzenia** wybierz zdarzenie, dla którego chcesz zdefiniować alarm. Jeśli zdarzenie, które Cię interesuje nie jest jeszcze zdefiniowane, możesz je utworzyć klikając przycisk **Nowy**  po prawej stronie. Aby uzyskać więcej informacji o zarządzaniu zdarzeniami, przejdź do rozdziału [Zarządzanie zdarzeniami](#).
4. Pole **Uruchom akcje** pozwala Ci dodawać akcje, które zostaną uruchomione w razie alarmu. Aby dodać akcje kliknij ikonę  znajdująca się po lewej stronie listy akcji. Zostanie wyświetlone okno **Akcja**, w której możesz określić następujące własności akcji:

Wlasnosc	Opis
Uruchom akcje	Wybierz akcje, która ma być uruchomiona. Jeśli akcja nie została jeszcze zdefiniowana, możesz ją utworzyć klikając przycisk Nowa  po prawej stronie. Aby uzyskać więcej informacji na ten temat, przejdź do rozdziału Zarządzanie Akcjami .
Grupa "Kiedy"	
Wraz z rozpoczęciem alarmu	Domyslna opcja, która uruchamia akcje jak tylko alarm zostanie zainicjowany.
Po	Wybierz opcje "Po" i wpisz liczbę minut jaka program ma przeczekać z uruchomieniem akcji. Pamiętaj, że jeśli alarm zostanie zakończony przed tym czasem, akcja nie zostanie uruchomiona.
Po zakończeniu alarmu	Niekiedy potrzebujemy być poinformowani gdy pewna problematyczna sytuacja się zakończy. Można wykorzystywać te opcje jeśli chcesz być na przykład poinformowany gdy ważne urządzenie zacznie znowu odpowiadać.
Ograniczenie czasowe	W tym polu możesz zdefiniować ograniczenie czasu, w którym akcja może być wykonana. Bardzo często występuje sytuacja, w której inaczej chcesz być informowany w godzinach pracy, a inaczej gdy jesteś poza biurem. Na przykład: nVision może wysłać Ci tylko e-maila, gdy jesteś w biurze, ale gdy jesteś poza nim, możesz chcieć dostać wiadomość SMS.
Powtórz akcje co	Pozwala ustawić akcję, która będzie wykonywana cyklicznie aż do czasu zakończenia alarmu. Wpisz liczbę minut, określającą co ile chcesz aby akcja była wykonywana.

- Ostatni krok pozwala ograniczyć alarm do wybranych typów urządzeń i ich znaczenia. Metoda ta jest przydatna jeśli chcesz skonfigurować globalny alarm dla całego atlasu, ale nie chcesz by był on generowany dla mniej ważnych urządzeń - administratorzy najczęściej nie potrzebują wiedzieć o tym, że zwykła stacja robocza została wylączona, ale chcą wiedzieć, że przestał działać serwer.
 - Wybierz typ urządzenia w polu "Typ"
 - Zaznacz wszystkie odpowiednie pola znajdujące się obok napisu "Znaczenie" aby ograniczyć alarm tylko do urządzeń z ustawionym odpowiednim znaczeniem.
- Upewnij się, że pole "Alarm włączony" jest zaznaczone. Jeśli tak nie jest - alarm nie będzie aktywny.

Uwaga

- Zmiana ustawień dziedziczonych alarmów może wpłynąć na inne urządzenia, dlatego zachowaj ostrożność zmieniając je.

Usuwanie alarmu

- Otwórz okno zarządzania alarmami dla obiektu, na którym chcesz usunąć alarm.
- Zaznacz alarm na liście.
- Kliknij przycisk **Usun alarm** znajdujący się na pasku narzędzi. Pamiętaj, że nie możesz usunąć alarmu, który jest dziedziczony (taki alarm można usunąć tylko z poziomu, na którym został zdefiniowany).

Wylaczanie lub włączanie alarmu


1. Otwórz okno zarządzania alarmami dla obiektu, na którym chcesz wyłączyć lub włączyć alarm.
2. Zaznacz alarm na liście i kliknij przycisk **Edytuj alarm**.
3. Aby wyłączyć alarm, wyłącz opcję **Alarm włączony**. Aby włączyć alarm upewnij się, że to pole jest zaznaczone.

Blokowanie alarmów dziedzicznych

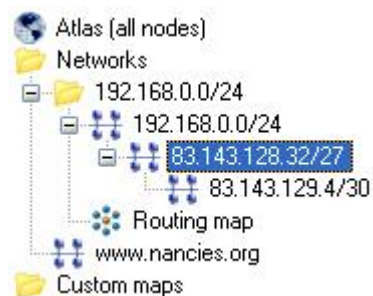
1. Otwórz okno zarządzania alarmami dla obiektu, na którym chcesz zablokować dziedziczenie alarmów.
2. Włącz opcję **Zablokuj dziedziczenie alarmów** jeśli nie chcesz aby dziedziczone alarmy były generowane dla danego obiektu. Jeśli ta opcja jest aktualnie włączona, a chcesz korzystać z dziedziczenia alarmów, wyłącz ją.

8.3.3 Dziedziczenie Alarmów

Poprzednie rozdziały omawiały sposoby definiowania alarmu: możliwość zdefiniowania dla całego atlasu, dla mapy oraz dla pojedynczego urządzenia. Jeśli alarm został zdefiniowany globalnie dla całego atlasu, wtedy będzie on dotyczył także każdej mapy oraz każdego urządzenia, które spełnia kryterium typu urządzenia (wykluczając te obiekty, które mają wyłączoną opcję dziedziczenia alarmów). Przejdź do rozdziału [Zarządzanie Alarmami](#) aby uzyskać więcej informacji na ten temat). Alarmy dziedziczone to takie alarmy, które są zdefiniowane gdzie indziej, lecz są widoczne na aktualnie wybranym urządzeniu lub mapie.

W analogiczny sposób, alarmy zdefiniowane dla mapy są dziedziczone przez wszystkie mapy podrzędne. Mapy podrzędne to te mapy, które w drzewie atlasu występują pod daną mapą. Gałęzie drzewa z mapami podrzędnymi można związać lub rozwijać używając ikony  znajdującej się obok nazwy mapy.

Przykład drzewa atlasu:



W powyższym przykładzie mapa 192.168.0.0/24 posiada dwie mapy podrzędne: 83.143.128.32/27 oraz 83.143.129.4/30. Alarmy zdefiniowane dla mapy 192.168.0.0/24 będą także wpływać na listę alarmów tych dwóch map podrzędnych. Istnieje jednak możliwość zablokowania dziedziczenia alarmów.

Blokowanie alarmów dziedzicznych

Jeśli nie chcesz aby żadne alarmy zdefiniowane na wyższym poziomie były dziedziczone dla danego obiektu, możesz je zablokować. Można to zrobić niezależnie dla każdej mapy i urządzenia.

1. Otwórz okno zarządzania alarmami dla mapy albo urządzenia.
2. Włącz opcję **Zablokuj dziedziczenie alarmów**, jeśli nie chcesz aby dziedziczone alarmy były generowane dla danego obiektu. Jeśli to pole jest zaznaczone, a chcesz korzystać z funkcji dziedziczenia alarmów, wyłącz je.

8.3.4 Eskalacja Alarmów

Dla szczególnie ważnych zdarzeń można użyć mechanizmu eskalacji alarmów. Polega on na wykonaniu kilku akcji dla zdarzenia w predefiniowanym okresie czasu. Na przykład: pierwsza akcja może zostać uruchomiona wraz z rozpoczęciem alarmu, następna po 30 minutach i być wykonywana cyklicznie co godzinę aż do zakończenia alarmu. Gdy alarm się zakończy kolejna akcja może zostać uruchomiona.

Dzięki temu mechanizmowi można być pewnym, że o krytycznej sytuacji administrator zostanie szybko poinformowany, a w wypadku, gdy nie będzie on w stanie poradzić sobie z nią, po jakimś czasie zostanie o niej poinformowana inna osoba, która może się nią zająć.

Aby uzyskać więcej informacji na temat konfiguracji akcji, tak aby były uruchamiane w innym czasie, lub by powtarzały się cyklicznie, przejdź do rozdziału [Zarządzanie Akcjami](#).

8.4 Zdarzenia

8.4.1 Wprowadzenie

Aby zarządzać zdarzeniami należy wcześniej zapoznać się z koncepcją zdarzeń, która jest omówiona w rozdziale [Koncepcje](#).

Przed rozpoczęciem konfiguracji alarmów, należy wcześniej zdefiniować wszystkie zdarzenia, które chcemy monitorować. Program będzie monitorował wszystkie urządzenia ze zdefiniowanym konkretnym alarmem, w celu wykrycia wystąpienia zdarzenia. Gdy zdarzenie zostanie wykryte nVision wykonuje następujące operacje:

1. Inicjuje wszystkie alarmy bazujące na danym zdarzeniu. To pociąga za sobą wykonanie wszystkich akcji przypisanych danemu alarmowi. Należy pamiętać, że akcje, które mają być uruchomione po pewnym czasie, mogą nigdy nie zostać wykonane - taka sytuacja ma miejsce, gdy alarm zostanie zakończony przed jej wykonaniem. Akcje uruchamiane wraz z rozpoczęciem alarmu lub wraz z jego zakończeniem będą wykonane zawsze (chyba, że program został zamknięty).
2. Zdarzenie jest zapisane w dzienniku zdarzeń. To pozwala na przyszłą analizę wydajności urządzeń i sieci oraz pozwala przygotować raporty. Więcej informacji na temat przeglądania wygenerowanych alarmów znajduje się w rozdziale [Przeglądanie Dziennika Zdarzeń](#).

Gdy problematyczna sytuacja się kończy, alarm także się kończy i uruchamiane są wszystkie akcje, skonfigurowane do wykonania po zakończeniu alarmu.

Ważność

Każde zdarzenie ma zdefiniowaną swoją wagę, która służy tylko do celów informacyjnych. Podczas notyfikacji o zdarzeniu, które miało miejsce, dostępna będzie także informacja o jego wadze, pozwalając Ci reagować szybciej na bardziej istotne sytuacje.

Stan hosta

W przeciwieństwie do konkurencyjnych programów, stan urządzenia jest w nVision wartością wyliczaną, nie zdefiniowaną na sztywno. Można więc definiować warunki, kiedy uznajemy dane urządzenie jako działające, nie działające lub w stanie ostrzeżenia. Aby uzyskać więcej informacji przejdź do rozdziału [Stan urządzenia - koncepcje](#).

8.4.2 Typy zdarzeń

Można wyróżnić kilka głównych grup zdarzeń. Ich opis znajduje się w poniższej liście:

Zdarzenie	Opis
Dostępność urządzenia lub serwisu	
Urządzenie nie działa	Zadanie z serwisów danego urządzenia nie działa
Serwis nie działa	Serwis danego urządzenia (np. FTP, HTTP) nie odpowiada
Problem wydajności serwisu	Zdarzenie generowane, gdy serwis odpowiada wolniej niż powinien, lub ilość utraconych pakietów jest zbyt duża.
Interfejs nie działa	Zdarzenie generowane, gdy któryś z interfejsów urządzenia przestaje działać
Zmiana stanu urządzenia	Zdarzenie może zostać wygenerowane dla każdej zmiany stanu urządzenia - także gdy urządzenie przechodzi ze stanu <Nie działa> na <Działa>.
Testy serwisu	
Czas załadowania strony zbyt długi	Za pomocą tego zdarzenia możesz sprawdzać czas ładowania strony WWW.
Zmiana zawartości strony	Pozwala wykrywać zmiany treści stron WWW (wynikające np. z włamań hackerów)
Czas logowania POP3 zbyt długi	Zdarzenie generowane, gdy występują trudności z zalogowaniem się na serwer mailowy.
Czas wysłania wiadomości e-mail zbyt długi	Zdarzenie generowane, gdy występują problemy z wysyłaniem wiadomości e-mail.
Liczniki wydajności	
Próg SNMP	Można sprawdzać wartość określonego licznika wydajności - zdarzenie jest inicjowane jeśli wartość jest zbyt wysoka (ponad zdefiniowany próg) lub zmniejszy się.
Próg Windows	Podobnie jak wyżej – dla liczników wydajności aplikacji i systemu Windows. Pozwala to na monitorowanie stanu aplikacji takich jak Serwer SQL lub Serwer Exchange.
Windows	
Zmiana stanu usługi Windows	Zdarzenie inicjowane, gdy nVision wykryje zmianę stanu usługi Windows. Pozwala ono na monitorowanie ważnych usług na zdalnych komputerach i daje możliwość np. ich zrestartowania w wypadku jakichkolwiek problemów.
Zasoby sprzętowe	Zdarzenie informujące o jakichkolwiek zmianach sprzętowych na komputerach z włączoną opcją zbierania informacji o zasobach.
Zasoby oprogramowania	Zdarzenie informujące o instalacji/deinstalacji jakiegokolwiek programu.

8.4.3 Zarządzanie zdarzeniami

Aby poprawnie skonfigurować system alarmowania w nVision, należy wcześniej zdefiniować wszelkie problematyczne sytuacje, podczas których alarm ma zostać wygenerowany.

Otwieranie okna zarządzania zdarzeniami

Korzystając z tego okna można przeglądać, modyfikować, tworzyć nowe oraz usuwać zdarzenia. Aby otworzyć okno zarządzania zdarzeniami, wybierz **Alarmy | Zarządzaj zdarzeniami** z menu głównego programu.

Tworzenie nowego zdarzenia

1. Otwórz okno zarządzania zdarzeniami.
2. Kliknij przycisk **Dodaj zdarzenie** znajdujący się na pasku zadań - zostanie otwarty **Kreator definicji zdarzenia**.
3. Wpisz nazwę zdarzenia, które chcesz utworzyć w polu **Nazwa zdarzenia**.
4. Wybierz stan urządzenia dla tego zdarzenia korzystając z pola **Stan urządzenia** - determinuje ono stan, w jakim urządzenie się znajdzie, gdy zdarzenie zostanie zainicjowane. Aby uzyskać więcej informacji na ten temat przejdź do rozdziału [Zdarzenia - wprowadzenie](#).
5. Wybierz istotność zdarzenia korzystając z pola **Istotność** - służy ono tylko do celów informacyjnych.
6. Wybierz z listy typ zdarzenia. Aby uzyskać więcej informacji na temat typów zdarzeń, przejdź do rozdziału [Typy zdarzeń](#).
7. Kliknij przycisk **Dalej**.
8. Następnie skonfiguruj właściwości zdarzenia (w zależności od typu zdarzenia wybranego przez Ciebie). Więcej informacji na ten temat znajdziesz w rozdziale [Definiowanie właściwości zdarzeń](#).
9. Kliknij przycisk **Zakończ**.

Modyfikowanie istniejącego zdarzenia

1. Otwórz okno zarządzania zdarzeniami.
2. Wybierz istniejące zdarzenie z kliknij przycisk **Edytuj zdarzenie**. Zostanie uruchomiony **Kreator definicji zdarzenia**.
3. Następnie skonfiguruj właściwości zdarzenia (w zależności od typu zdarzenia wybranego przez Ciebie). Więcej informacji na ten temat znajdziesz w rozdziale [Definiowanie właściwości zdarzeń](#).
4. Kliknij przycisk **Zakończ**.

8.4.4 Definiowanie właściwości zdarzeń

Ten rozdział opisuje definiowanie właściwości różnych typów zdarzeń.

Dostępność urządzenia lub serwisu

Urządzenie nie działa

To zdarzenie jest generowane, gdy każdy serwis urządzenia przestanie odpowiadać. Należy zdecydować, kiedy nVision ma uznać urządzenie za nie działające – po określonej liczbie minut albo sprawdzeń z brakiem odpowiedzi. Sprawdzanie wystąpienia tego zdarzenia będzie wykonywane na każdym urządzeniu, które posiada co najmniej jeden serwis.

Własność	Opis
Określona liczba sprawdzeń	Wybierz te opcje, jeśli chcesz aby zdarzenie było generowane gdy urządzenie nie odpowiedziało na określoną liczbę sprawdzeń. Wpisz liczbę nieudanych sprawdzeń, po których urządzenie zostanie uznane za nie działające.

Wlasnosc	Opis
Okreslona liczba minut	Wybierz te opcje, jesli chcesz aby zdarzenie bylo generowane gdy wszystkie serwisu urzadzenia nie odpowiedzialy przez okreslona liczbe minut. Okres ten jest liczony od ostatniego pomyslnego sprawdzenia - gdy wybierzesz zbyt maly czas, mozesz otrzymac falszywe alarmy. Wpisz liczbe minut, po których urządzenie zostanie uznane za nie działające.

Serwis nie dziala

To zdarzenie jest generowane, gdy określony serwis urządzenia przestanie odpowiadać. Należy zdecydować, kiedy nVision ma uznać serwis za niedziałający – po określonej liczbie minut albo sprawdzeń z brakiem odpowiedzi..

Wlasnosc	Opis
Serwis	Wybierz serwis, który chcesz monitorowac. Zdarzenie bedzie sprawdzane na kazdym urzadzeniu, które posiada dany serwis.
Okreslona liczba sprawdzen	Wybierz te opcje, jesli chcesz aby zdarzenie bylo generowane, gdy serwis nie odpowiedzial na okreslona liczbe sprawdzen. Wpisz liczba nieudanych sprawdzen, po których serwis zostanie uznany za nie działający.
Okreslona liczba minut	Wybierz te opcje, jesli chcesz aby zdarzenie bylo generowane, gdy serwis nie odpowiedzial przez okreslona liczbe minut. Okres ten jest liczony od ostatniego pomyslnego sprawdzenia serwisu - gdy wybierzesz zbyt maly czas sprawdzania, mozesz otrzymac falszywe alarmy. Wpisz liczbe minut, po których serwis zostanie uznany za nie działający.

Problem wydajnosci serwisu

To zdarzenie jest generowane, jesli jakis serwis zacznie dzialac wolniej, lub zbyt duza ilosc pakietów jest utracona.

Wlasnosc	Opis
Serwis	Wybierz serwis, który chcesz monitorowac. Zdarzenie bedzie sprawdzane na kazdym urzadzeniu, które posiada dany serwis.
Sprawdz ostatnie	Liczba ostatnich minut, które chcesz sprawdzac.
Generuj zdarzenie, gdy	Wybierz przynajmniej jeden z warunków opisanych ponizej. Jesli wybierzesz obydwa, zdarzenie zostanie zainicjowane, jesli co najmniej jeden warunek zostanie spelniony.

Własność	Opis
Sredni/Kazdy czas odpowiedzi	<p>Wybierz Sredni czas odpowiedzi, jesli chcesz aby zdarzenie bylo generowane gdy serwis zacznie dzialac wolniej.</p> <ul style="list-style-type: none"> nVision sprawdza domyslnie srednia wartosc. Mozesz wybrac jednak metode sprawdzania kazdej wartosci klikajac napis (link) Sredni. Napis zamieni sie na Kazdy wskazujac, ze kazda próbka (sprawdzenie) bedzie sprawdzana oddzielnie. Wpisz wartosc proggu czasu odpowiedzi w milisekundach. Zdarzenie zostanie wygenerowane, jesli czas odpowiedzi bedzie wiekszy niz podana wartosc. Wpisz wartosc proggu konczacego w nastepnym polu. Aby uzyskac wiecej informacji na temat progów przejdź do rozdziału Progi narastajace, opadajace i konczace.
Procent utraconych pakietów	<p>Wybierz Procent utraconych pakietów, jesli chcesz aby zdarzenie bylo generowane gdy procent utraconych pakietów dla danego serwisu bedzie zbyt duzy.</p> <ul style="list-style-type: none"> Wpisz wartosc proggu. Zdarzenie zostanie wygenerowane, gdy procent utraconych pakietów bedzie wiekszy niz podana wartosc. Wpisz wartosc proggu konczacego w nastepnych polu.

Zmiana stanu urzadzenia

Zdarzenie to moze zostac wygenerowane dla kazdej zmiany stanu urzadzenia, nawet jesli urzadzenie przechodzi ze stanu <Nie dziala> na <Dziala>. Zdarzenie sprawdzane na kazdym urzadzeniu.

Własność	Opis
Generuj zdarzenie, gdy	Wybierz stan, dla którego chcesz, aby nVision generowało zdarzenie. Zdarzenie moze zostac wygenerowane jesli stan urzadzenia zmieni sie na <Dziala>, <Ostrzezenie> lub <Nie dziala>. Wybierz odpowiednia opcje.

Test wydajności konkretnego serwisu

Czas załadowania strony zbyt dlugi

Za pomoca tego zdarzenia mozesz testowac czas załadowania Twojej strony WWW. Zdarzenie to bedzie sprawdzane na kazdym urzadzeniu, które monitoruje czas załadowania dowolnej strony WWW (posiada zdefiniowany licznik wydajności tego typu).

Własność	Opis
Sprawdz ostatnie	Liczba ostatnich minut, które chcesz sprawdzac

Własność	Opis
Generuj zdarzenie, gdy	<ul style="list-style-type: none"> nVision sprawdza domyślnie średnią wartość. Możesz wybrać jednak metodę sprawdzania każdej wartości klikając napis (link) Sredni. Napis zamieni się na Kazdy wskazując, że każda próbka (sprawdzenie) będzie sprawdzana oddzielnie. Wpisz wartość progu czasu ładowania strony w milisekundach. Zdarzenie zostanie wygenerowane, gdy czas załadowania strony będzie większy niż podana wartość.
Zakończ zdarzenie, gdy	Wpisz wartość progu kończącego w następnym polu. Aby uzyskać więcej informacji na temat progów, przejdź do rozdziału Progi narastające, opadające i kończące .

Zmiana zawartości strony WWW

Pozwala zapobiegać przypadkowym zmianom treści stron (np. dokonanych przez hakera). Zostanie zainicjowane gdy tylko próbnik wykryje, że procent zmiany treści strony wzrósł powyżej progu. Zdarzenie to będzie sprawdzane na każdym urządzeniu, które posiada zdefiniowany licznik wydajności tego typu.

Własność	Opis
Sprawdź ostatnie	Liczba ostatnich minut, które chcesz sprawdzać
Średni stopień zmiany treści >	<ul style="list-style-type: none"> nVision sprawdza domyślnie średnią wartość. Możesz wybrać jednak metodę sprawdzania każdej wartości klikając napis (link) Średnia. Napis zamieni się na Każda wskazując, że każda próbka (sprawdzenie) będzie sprawdzana oddzielnie. Wpisz wartość progu czasu ładowania strony w milisekundach. Zdarzenie zostanie wygenerowane, gdy czas załadowania strony będzie większy niż podana wartość.
Zakończ zdarzenie, gdy	Zdarzenie zakończy się, gdy treść powróci do oryginału i procent zmiany spadnie poniżej progu kończącego.

Czas logowania POP3 zbyt długi

Zdarzenie to jest generowane gdy występują problemy z logowaniem się do serwera pocztowego. Sprawdzanie warunków zajścia tego zdarzenia będzie wykonywane na każdym urządzeniu, które monitoruje czas logowania do dowolnego serwera POP3 (posiada zdefiniowany licznik wydajności tego typu).

Własność	Opis
Sprawdź ostatnie	Liczba ostatnich minut, które chcesz sprawdzać.

Wlasnosc	Opis
Sredni czas logowania do serwera POP3	<ul style="list-style-type: none"> nVision sprawdza domyslnie srednia wartosc. Mozesz wybrac jednak metode sprawdzania kazdej wartosci klikajac napis (link) Sredni. Napis zamieni sie na Kazdy wskazujac, ze kazda próbka (sprawdzenie) bedzie sprawdzana oddzielnie. Wpisz wartosc progu czasu logowania do serwera POP3 w milisekundach. Zdarzenie zostanie wygenerowane, gdy czas zaladowania strony bedzie wiekszy niz podana wartosc.
Zakonczone zdarzenie gdy	Wpisz wartosc progu konczacego w nastepnym polu. Aby uzyskac wiecej informacji na temat progów przejdź do rozdziału Progi narastajace, opadajace i konczace .

Czas wyslania wiadomosci e-mail zbyt dlugi

Zdarzenie to jest generowane, gdy wystepuja problemy z wysylaniem wiadomosci e-mail. Sprawdzanie warunków zajscia tego zdarzenie bedzie wykonywane na kazdym urzadzeniu, które monitoruje czas wyslania wiadomosci e-mail do dowolnego serwera (posiada zdefiniowany licznik wydajnosci tego typu).

Wlasnosc	Opis
Sprawdz ostatnie	Liczba ostatnich minut, które chcesz sprawdzac.
Sredni czas wyslania wiadomosci e-mail	<ul style="list-style-type: none"> nVision sprawdza domyslnie srednia wartosc. Mozesz wybrac jednak metode sprawdzania kazdej wartosci klikajac napis (link) Sredni. Napis zamieni sie na Kazdy wskazujac, ze kazda próbka (sprawdzenie) bedzie sprawdzana oddzielnie. Wpisz wartosc progu czasu logowania do serwera POP3 w milisekundach. Zdarzenie zostanie wygenerowane, gdy czas zaladowania strony bedzie wiekszy niz podana wartosc.
Zakonczone zdarzenie gdy	Wpisz wartosc progu konczacego w nastepnym polu. Aby uzyskac wiecej informacji na temat progów przejdź do rozdziału Progi narastajace, opadajace i konczace .

Liczniki wydajnosci

Próg licznika wydajnosci SNMP

Wlasnosc	Opis
Licznik wydajnosci	Wybierz licznik wydajnosci SNMP, który ma byc sprawdzany. Należy pamietac, ze dany licznik wydajnosci bedzie sprawdzany tylko, jesli istnieje na monitorowanym urzadzeniu. Dlatego aby sprawdzanie zdarzenia dzialalo poprawnie musisz zdefiniowac dany licznik wydajnosci na odpowiednich urzadzeniach.
Sprawdz ostatnie	Liczba ostatnich minut, które chcesz sprawdzac.

Wlasnosc	Opis
Srednia wartosc	<ul style="list-style-type: none"> nVision sprawdza domyslnie srednia wartosc. Mozesz wybrac jednak metode sprawdzania kazdej wartosci klikajac napis (link) Sredni. Napis zamieni sie na Kazdy wskazujac, ze kazda próbka (sprawdzenie) bedzie sprawdzana oddzielnie. Wpisz wartosc progu czasu logowanie do serwera POP3 w milisekundach. Zdarzenie zostanie wygenerowane, gdy czas zaladowania strony bedzie wiekszy niz podana wartosc.
Zakonczone zdarzenie gdy	Wpisz wartosc progu konczacego w nastepnym polu. Aby uzyskac wiecej informacji na temat progów przejdź do rozdziału Progi narastajace, opadajace i konczace .

Uwaga

- Należy mieć na uwadze, że ustawienie długiego okresu czasu sprawdzania może spowolnić działanie programu. Licznik wydajności, który jest sprawdzany bardzo często, dostarcza wiele próbek, których analiza zużywa zasoby procesora. Nie należy ustawiać okresu sprawdzania na więcej niż 10 minut dla urządzeń, które są sprawdzane częściej niż co 10 sekund.

Próg licznika wydajności Windows

Wlasnosc	Opis
Licznik wydajności	Wybierz licznik wydajności Windows, który ma być sprawdzany. Należy pamiętać, że dany licznik wydajności będzie sprawdzany tylko, istnieje na monitorowanym urządzeniu. Dlatego, aby sprawdzanie zdarzenia działało poprawnie musisz zdefiniować dany licznik wydajności na odpowiednich urządzeniach .
Sprawdź ostatnie	Liczba ostatnich minut, które chcesz sprawdzać.
Srednia wartosc	<ul style="list-style-type: none"> nVision sprawdza domyslnie srednia wartosc. Mozesz wybrac jednak metode sprawdzania kazdej wartosci klikajac napis (link) Sredni. Napis zamieni sie na Kazdy wskazujac, ze kazda próbka (sprawdzenie) bedzie sprawdzana oddzielnie. Wpisz wartosc progu czasu logowanie do serwera POP3 w milisekundach. Zdarzenie zostanie wygenerowane, gdy czas zaladowania strony bedzie wiekszy niz podana wartosc.
Zakonczone zdarzenie gdy	Wpisz wartosc progu konczacego w nastepnym polu. Aby uzyskac wiecej informacji na temat progów przejdź do rozdziału Progi narastajace, opadajace i konczace .

Uwaga

- Należy mieć na uwadze, że ustawienie długiego okresu czasu sprawdzania może spowolnić działanie programu. Licznik wydajności, który jest sprawdzany bardzo często, dostarcza wiele próbek, których analiza zużywa zasoby procesora. Nie należy ustawiać okresu sprawdzania na więcej niż 10 minut dla urządzeń, które są sprawdzane częściej niż co 10 sekund.

Windows

Zmiana stanu usługi Windows

Wlasnosc	Opis
Generuj zdarzenie, gdy	Wybierz odpowiedni ¹ opcjê okreœlaj ¹ c ¹ , kiedy zdarzenie ma byæ generowane.
Wszystkie serwisy	Wybierz, jeœli chcesz aby zdarzenie by³o generowane dla wszystkich serwisów Windows.
Wybrane serwisy	Wybierz, jeœli chcesz aby zdarzenie by³o generowane dla wybranych serwisów Windows. Kliknij ikonê z zielonym plusem i wybierz us³ugê, która chcesz monitorowaæ

Inwentaryzacja oprogramowania

Wlasnosc	Opis
Generuj zdarzenie gdy	Wybierz odpowiednia opcje, okreslajaca kiedy zdarzenie ma byc generowane.

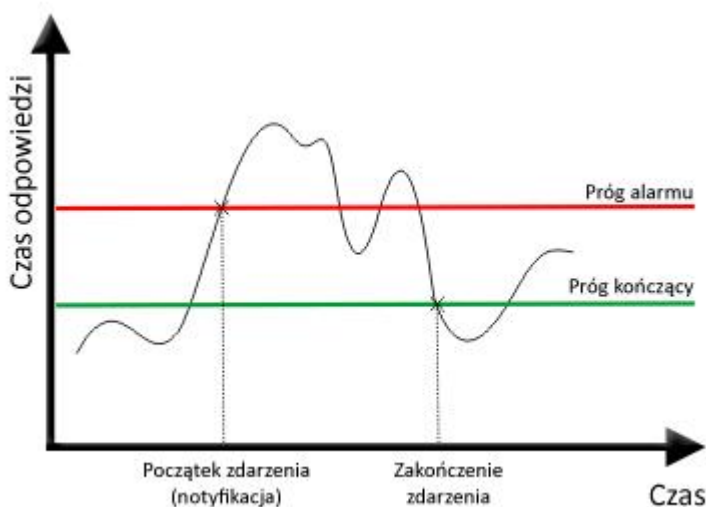
Inwentaryzacja sprzetu

To zdarzenie nie posiada zadnych wlasnosci - jest generowane za kazdym razem gdy jakokolwiek zmiana konfiguracji sprzetowej urzadzenia zostanie wykryta.

8.4.5 Progi narastaj±ce, opadaj±ce i koñcz±ce

Dla wiêkszoœci zdarzen definiowana jest wartosc progu, która wskazuje kiedy zdarzenie ma zostac wygenerowane. Na przyklad - dla serwisu okreœla on jak wolno serwis moze odpowiadac zanim zdarzenie zostanie wygenerowane.

Istnieja jednak zdarzenia, dla których nalezy zdefiniowac takze próg "koñcz±cy". Jego znaczenie jest istotne - zapobiega on generowaniu zdarzenia za kazdym razem, gdy warunek zdarzenia jest spe³niony. Powodowalo by to sytuacjê, w której alarm by³by generowany co kilka minut. Mierzona wartosc musi najpierw spasc ponizej progu koñcz±cego zanim nastêpny alarm zostanie wygenerowany.



Czerwona linia pokazuje próg alarmu - kiedy czas odpowiedzi (lub procent utraconych pakietów)

serwisu lub wartość licznika wydajności przekroczy ten próg, alarm zostanie wygenerowany. Następny alarm zostanie jednak dopiero wygenerowany gdy dana wartość spadnie poniżej progu kończącego. Ten mechanizm zapobiega cyklicznemu generowaniu alarmu dla jednego zdarzenia.

Progi narastające i opadające

Próg opisany powyżej jest nazywany progiem narastającym, ponieważ generuje on alarm gdy mierzona wartość go przekroczy. Istnieje także możliwość zdefiniowania zdarzenia, które określa sytuację, w której mierzona wartość powinna znajdować się powyżej progu. Wtedy alarm jest generowany gdy owa wartość spadnie poniżej progu alarmu, dlatego ten typ progu nazywany jest progiem opadającym.

Uwaga

- Próg kończący nie może mieć większej wartości niż próg alarmu dla progów narastających i mniejszej dla progów opadających.

8.5 Akcje (Korekcyjne i Notyfikujące)

8.5.1 Wprowadzenie

W większości przypadków gdy definiujesz zdarzenie, chcesz zostać poinformowany o jego wystąpieniu, lub chcesz aby zostały wykonane czynności naprawcze mające rozwiązać niepożądaną sytuację. nVision pozwala na tworzenie obydwu typów akcji: notyfikacyjnych i korekcyjnych. Dlatego też przed definicją alarmu należy utworzyć zbiór akcji, które mają być wykonane gdy alarm zostanie wygenerowany.

Mozna zdefiniować takie akcje jak: wysłanie wiadomości e-mail, ICQ lub SMS, odegranie dźwięku, wyświetlenie okna dialogowego, uruchomienie zewnętrznego programu. Pełna lista dostępnych akcji znajduje się w rozdziale [Typy akcji](#).

8.5.2 Typy akcji

Istnieje kilka ogólnych grup akcji. Poniższa lista opisuje je:

Akcja	Opis
Notyfikacja desktopowa	
Okno alarmowe	Małe okienko informujące o alarmie zostanie pokazane na zdefiniowanej pozycji. Okno to nie przeszkadza w wykonywaniu aktualnych zadań na komputerze.
Odegranie dźwięku	nVision odegra zdefiniowany dźwięk.
Synteza mowy	nVision korzystając z syntezy mowy odczyta treść alarmu.
Wysyłanie wiadomości	
E-mail	Wysłana zostanie wiadomość e-mail zawierająca informacje o alarmie.
ICQ	Wysłana zostanie wiadomość ICQ zawierająca informacje o alarmie.
SMS przez GSM	Wysłanie wiadomości SMS przy pomocy podłączonego telefonu lub modemu GSM.
Wiadomość SysLog	Wiadomość SysLog zostanie wysłana do zdefiniowanego serwera SysLog.
Program lub skrypt	

Akcja	Opis
Uruchom program lokalnie	Uruchamia zewnętrzny program na lokalnym komputerze.
Uruchom program zdalnie	Uruchamia program na zdalnym komputerze z systemem Windows
Inne	
Zapis do pliku	Informacja o alarmie jest zapisywana do pliku.
Windows	
Uruchomienie/zatrzymanie usługi Windows	Kontroluje usługi na zdalnym lub lokalnym komputerze z systemem Windows.
Wylacz/zrestartuj komputer	Wylacza lub restartuje zdalnie komputer z systemem Windows.
Wpis do Dziennika Zdarzen Windows	Tworzy wpis do Dziennika Zdarzen Windows na lokalnym lub zdalnym komputerze z systemem Windows.

8.5.3 Zarządzanie akcjami



Aby skonfigurować nVision tak, aby notyfikowało o wygenerowanych zdarzeniach, należy wcześniej zdefiniować wszelkie możliwe sposoby notyfikacji, z jakich chcemy korzystać. Niniejszy rozdział dostarcza więcej informacji na temat zarządzania akcjami.

Otwieranie okna zarządzania akcjami

Za pomocą tego okna możesz przeglądać, modyfikować, tworzyć nowe oraz usuwać akcje. Aby otworzyć to okno, wybierz **Narzędzia | Zarządzaj akcjami** z menu głównego programu.

Tworzenie nowej akcji lub modyfikowanie istniejącej

1. Otwórz okno zarządzania akcjami.

2. Kliknij przycisk  aby utworzyć nową akcję lub wybierz istniejącą i kliknij przycisk . Zostanie otwarte **Kreator definicji akcji**.
3. Jeśli tworzysz nową akcję, wpisz jej nazwę w polu **Nazwa akcji** i wybierz jej typ z listy znajdującej się poniżej tego pola. Kliknij przycisk **Dalej**. Aby dowiedzieć się więcej na temat typów akcji, przejdź do rozdziału [Typy akcji](#).
4. Skonfiguruj właściwości akcji (w zależności od typu akcji, który wybrałeś). Aby uzyskać więcej informacji na ten temat przejdź do rozdziału [Definiowanie własności akcji](#).
5. W tym momencie może się okazać niezbędne skonfigurowanie danej akcji. Taka konfiguracja jest niezbędna do poprawnego działania niektórych akcji (np. adres serwera SMTP dla wiadomości e-mail, lub port COM, do którego jest podłączony modem GSM). Konfigurowanie akcji jest omówione w rozdziale [Konfigurowanie akcji](#).
6. Jeśli wszystkie opcje są zdefiniowane, możesz przetestować działanie akcji korzystając z przycisku **Testuj** - wykona on akcję tak, abyś mógł sprawdzić, czy wszystko zostało poprawnie ustawione.
7. Kliknij przycisk **Zakończ**.

8.5.4 Definiowanie własności akcji

Ten rozdział omawia definiowanie własności oraz różne typy akcji.

Notyfikacja desktopowa


Okno alarmowe

Małe okienko informujące o alarmie zostanie pokazane na zdefiniowanej pozycji. Okno to nie przeszkadza w wykonywaniu aktualnych zadań na komputerze.

Własność	Opis
Wiadomość	Pozwala wybrać format wiadomości, jaka zostanie pokazana w oknie alarmowym.
Automatyczna	Wybierz, jeśli chcesz wyświetlić wiadomość o alarmie o domyślnej treści.
Użytkownika	Wybierz te opcje, jeśli chcesz utworzyć własną treść wiadomości. Więcej informacji na ten temat znajdziesz w rozdziale Definiowanie wiadomości alarmowych użytkownika .

Odegranie dźwięku

Program odegra zdefiniowany dźwięk.

Własność	Opis
Predefiniowany dźwięk nVision	Wybierz jeden z predefiniowanych dźwięków nVision.
Dźwięk systemowy Windows	Wybierz jeden z predefiniowanych dźwięków systemowych Windows.
Wybierz plik	Kliknij przycisk  i wybierz plik dźwiękowy, który chcesz odegrać.

Synteza mowy

nVision korzystając z syntezatora mowy odczyta treść alarmu.

Własność	Opis
Wiadomość	Pozwala wybrać format wiadomości, jaka zostanie odczytana przez syntezator mowy.
Automatyczna	Wybierz, jeśli chcesz odegrać wiadomość o alarmie o domyślnej treści.
Użytkownika	Wybierz te opcje, jeśli chcesz utworzyć własną treść wiadomości. Więcej informacji na ten temat znajdziesz w rozdziale Definiowanie wiadomości alarmowych użytkownika .

Wysyłanie wiadomości

Wysyłanie wiadomości e-mail

nVision wyśle wiadomość e-mail z informacjami o alarmie.

Wlasnosc	Opis
Wyslij e-mail do	Adres e-mail, na jaki ma zostac wyslana wiadomosc. Mozesz podac kilka adresow email, rozdzielajac je przecinkami, srednikami, lub spacjami.
Temat	Temat wiadomosci e-mail. W temacie mozesz uzyc zmiennych opisanych w rozdziale Definiowanie wiadomosci alarmowych uzytkownika .
Tresc wiadomosci	Pozwala wybrac tresc wiadomosci, ktora zostanie uzyta do wygenerowania wiadomosci alarmowej.
HTML	Domyslana tresc wiadomosci.
Krótki tekst	Krótki tekst z podstawowymi informacjami o alarmie.
Długi tekst	Tekst z kompletnymi informacjami o alarmie.
XML	Format XML. Mozna go wykorzystac do zbudowania wlasnych zewnetrznych programow obslugujacych alarmy. Twój program moze otrzymac wiadomosc w formacie XML, zinterpretowac ja i wykonac dodatkowe zadania.
Uzytkownika	Wybierz te opcje, jesli chcesz utworzyc wlasna tresc wiadomosci. Wiecej informacji na ten temat znajdziesz w rozdziale Definiowanie wiadomosci alarmowych uzytkownika .

Wiadomosc ICQ

nVision wysle wiadomosc ICQ z informacjami o alarmie.

Wlasnosc	Opis
Numer ICQ	Numer konta ICQ, na jaki zostanie wyslana wiadomosc o alarmie.
Treść wiadomosci.	Pozwala wybrac format wiadomosci, który zostanie uzyty do wygenerowania wiadomosci alarmowej.
HTML	Domyslana tresc wiadomosci.
Krótki tekst	Krótki tekst z podstawowymi informacjami o alarmie.
Długi tekst	Tekst z kompletnymi informacjami o alarmie.
XML	Format XML. Mozna go wykorzystac do zbudowania wlasnych zewnetrznych programow obslugujacych alarmy. Twój program moze otrzymac wiadomosc w formacie XML, zinterpretowac ja i wykonac dodatkowe zadania.
Uzytkownika	Wybierz te opcje, jesli chcesz utworzyc wlasna tresc wiadomosci. Wiecej informacji na ten temat znajdziesz w rozdziale Definiowanie wiadomosci alarmowych uzytkownika .

SMS przez GSM

Wyslanie wiadomosci SMS przy pomocy podlaczonego telefonu lub modemu GSM.

Wlasnosc	Opis
Numer telefonu	Numer telefonu, na jaki ma zostac wyslana wiadomosc SMS. Musi sie zaczynac prefiksem z kodem kraju (+48 dla Polski).
Wiadomosc alarmowa	Wybierz te opcje, jesli chcesz aby wiadomosc zostala wyswietlona od razu na ekranie telefonu komórkowego.
Automatyczna	Domyslana tresc wiadomosci
Uzytkownika	Wybierz te opcje, jesli chcesz utworzyc wlasna tresc wiadomosci. Wiecej informacji na ten temat znajdziesz w rozdziale Definiowanie wiadomosci alarmowych uzytkownika .

Wiadomosc SysLog


Wiadomosc SysLog zostanie wyslana do zdefiniowanego serwera SysLog.

Wlasnosc	Opis
Adres zdalnego komputera	Adres serwera SysLog.
Port zdalnego komputera	Port na jakim dziala serwis SysLog.
Wiadomosc	Zdefiniuj tresc wiadomosci w polu edycji. Wiecej informacji na temat definiowania wiadomosci znajdziesz w rozdziale Definiowanie wiadomosci alarmowych uzytkownika .

Program lub skrypt

Uruchom program lokalnie


Uruchamia zewnetrzny program na lokalnym komputerze.

Wlasnosc	Opis
Uruchom program	Kliknij przycisk  i wybierz program, który ma zostac uruchomiony.
Z parametrami	Wpisz parametry uruchomienia programu. Mozesz uzyć zmiennych opisanych w rozdziale Definiowanie wiadomosci alarmowych uzytkownika .

Inne

Zapis do pliku

Zapisuje informacje o alarmie do pliku.

Wlasnosc	Opis
Zapis do pliku	Kliknij przycisk  i wybierz plik, w którym wiadomosc alarmowa ma zostac zapisana.
Tresc wiadomosci	Pozwala wybrac tresc wiadomosci, która zostanie użyta do wygenerowania wiadomości alarmowej.

Wlasnosc	Opis
HTML	Domyslna tresc wiadomosci
Krótki tekst	Krótki tekst z podstawowymi informacjami o alarmie.
Długi tekst	Tekst z kompletnymi informacjami o alarmie.
XML	Format XML. Mozna go wykorzystac do zbudowania wlasnych zewnetrznych programów obsługujących alarmy. Twój program moze odczytac plik w formacie XML, zinterpretowac ja i wykonac dodatkowe zadania.
Uzytkownika	Wybierz te opcje, jesli chcesz utworzyc wlasny format wiadomosci. Wiecej informacji na ten temat znajdziesz w rozdziale Definiowanie wiadomosci alarmowych uzytkownika .

Windows

Uruchom/zatrzymaj usluge Windows

Kontroluje uslugi na zdalnym lub lokalnym komputerze z systemem Windows.

Wlasnosc	Opis
Usluga Windows, która wygenerowala alarm	Zaznacz te opcje, jesli chcesz aby akcja byla wykonana na komputerze i usłudze, która wygenerowala alarm.
Wybrana usługa Windows	Zaznacz te opcje, jesli chcesz aby akcja byla wykonana na wybranym komputerze i usłudze Windows.
Komputer	Wybierz komputer, na którym ma byc wykonana akcja.
Usluga	Wybierz usluge Windows.
Akcja	Wybierz akcje jaka ma zostac wykonana: mozesz uruchomic, zatrzymac, spauzowac lub wznowic usluge Windows.

Wylacz/zrestartuj komputer

Wylacza lub restartuje zdalnie komputer z systemem Windows.

Wlasnosc	Opis
Komputer, który wygenerowal alarm	Zaznacz te opcje, jesli chcesz aby akcja byla wykonana na komputerze, który wygenerowal alarm.
Wybrany komputer	Zaznacz te opcje, jesli chcesz aby akcja byla wykonana na wybranym komputerze.
Zrestartuj	Restartuje komputer
Wylacz	Wylacza komputer

8.5.5 Konfigurowanie akcji

Wikszosc akcji wymaga ich poprawnego skonfigurowania, zanim nVision bedzie w stanie je wykonac. Na przyklad: adres serwera SMTP dla wiadomosci email, lub port COM, do którego jest podlaczony modem GSM. Ten rozdzial omawia konfiguracje kazdego typu akcji (niektóre akcji nie posiadaja opcji).

Akcja może być konfigurowana w opcjach programu, lub podczas tworzenia nowej akcji lub modyfikacji istniejącej.

Notyfikacja desktopowa

Okno alarmowe

Małe okienko informujące o alarmie zostanie pokazane na zdefiniowanej pozycji. Okno to nie przeszkadza w wykonywaniu aktualnych zadań na komputerze.

Własność	Opis
Pozycja	Określa pozycję na pulpicie, na której pojawi się okno alarmowe.
Czas wyświetlania	Określa czas, jak długo okno ma być wyświetlane.

Synteza mowy

nVision korzystając z syntezy mowy odczyta treść alarmu.

Własność	Opis
Silnik syntezy mowy	Silnik syntezy mowy, z którego chcesz skorzystać.
Tempo czytania	Tempo czytania

Wysyłanie wiadomości

Wiadomość email

nVision wyśle wiadomość email z informacjami alarmu.

Własność	Opis
Adres zwrotny	Jeśli adres nie zostanie poprawnie ustawiony, większość serwerów pocztowych może odrzucić taką wiadomość. Wpisz adres e-mail, o którym wiesz, że na pewno zostanie zaakceptowany przez serwer pocztowy (najczęściej Twój własny adres).
Użyj zewnętrznego serwera SMTP	nVision posiada własny wbudowany serwer SMTP, ale możesz użyć zewnętrznego, jeśli chcesz. Włącz tę opcję i określ poniższe właściwości.
Adres	Adres zewnętrznego serwera pocztowego.
Port	Numer portu, na jakim serwer pocztowy jest uruchomiony.
Wymaga autoryzacji	Jeśli zewnętrzny serwer pocztowy wymaga autoryzacji, zaznacz tę opcję i wpisz nazwę użytkownika i hasło w odpowiednich polach.
Nazwa użytkownika	Nazwa użytkownika wymagana do zalogowania się.
Hasło	Hasło wymagane do zalogowania się.

Wiadomość ICQ

nVision wysle wiadomosc ICQ z informacjami alarmie.

Wlasnosc	Opis
Serwer ICQ	Adres serwera ICQ.
Port	Numer portu, na którym dziala serwer ICQ.
UIN	UIN, z którego nVision skorzysta aby wyslac wiadomosc.
Haslo	Haslo wymagane do zalogowania sie.

8.5.6 Definiowanie wiadomości alarmowych użytkownika


Podczas definiowania akcji notyfikujących o alarmach, można skorzystać z mechanizmu wiadomości użytkownika, aby dostosować do własnych potrzeb treść wiadomości, jaka zostanie wysłana/zapisana. nVision pozwala na użycie kilku nazw zmiennych, które zostaną zamienione w odpowiednią wartość podczas tworzenia wiadomości alarmowej. Ten rozdział opisuje owe zmienne i sposób korzystania z nich.

Zmienne

Nazwa zmiennej	Opis
\$Host.Name	Nazwa urządzenia, dla którego alarm został wygenerowany.
\$Host.Type	Typ urządzenia. Aby uzyskać więcej informacji na ten temat przejdź do rozdziału Wlasciwosci urzadzenia .
\$Host.Importance	Znaczenie urządzenia. Zobacz: Wlasciwosci urzadzenia .
\$Host.Status	Stan urządzenia. Określa stan urządzenia w momencie, w którym alarm jest generowany. W przypadku akcji uruchamianych z opóźnieniem, stan urządzenia może być inny niż podczas generowania alarmu.
\$Host.Info1	Pole urządzenia Info1 . Zobacz: Wlasciwosci urzadzenia .
\$Host.Info2	Pole urządzenia Info2. Zobacz: Wlasciwosci urzadzenia .
\$Host.ParentHost	Urządzenie nadrzędne. Zobacz: Wlasciwosci urzadzenia .
\$Host.SNMPManagable	Informacja, czy dane urządzenie jest zarządzalne przez SNMP. Zobacz: Wlasciwosci urzadzenia .
\$Host.SNMPSystem	Opis systemu urządzenia odczytany przez SNMP. Zobacz: Wlasciwosci urzadzenia .
\$Host.SNMPLocation	Lokalizacja urządzenia odczytana przez SNMP. Zobacz: Wlasciwosci urzadzenia .
\$Host.SNMPName	Nazwa urządzenia odczytana przez SNMP. Zobacz: Wlasciwosci urzadzenia .
\$Alert.Name	Nazwa alarmu - nazwa zdarzenia, które zostało wygenerowane na urządzeniu.
\$Alert.Description	Krótki opis zdarzenia.
\$Alert.Type	Typ zdarzenia. Przejdź do rozdziału Typy zdarzen aby uzyskać więcej informacji.
\$Alert.Severity	Ważność zdarzenia, które wygenerowało alarm.
\$Alert.StartTime	Czas wygenerowania alarmu.
\$Alert.Duration	Czas trwania alarmu.

Nazwa zmiennej	Opis
\$Alert.Resolution	Stan rozwiązania alarmu.
\$Alert.Owner	Właściciel alarmu.

Jak korzystać ze zmiennych

Gdy program pozwala na zdefiniowanie wiadomości użytkownika, wtedy można skorzystać ze zmiennych. Wystarczy wpisać nazwę zmiennej w polu tekstowym wiadomości, lub skorzystać z przycisku . Po kliknięciu tego przycisku zostanie wyświetlona lista zmiennych - po wybraniu jednej, zostanie automatycznie wklejona do pola tekstowego.

8.6 Wygenerowane alarmy

8.6.1 Wprowadzenie

Jak nVision przetwarza alarmy

W większości programów służących do monitorowania sieci komputerowych można tylko zdefiniować kiedy alarm ma zostać wygenerowany, ale nie ma możliwości otrzymania potem informacji o czasie trwania takiego alarmu. Nie ma także możliwości zdefiniowania akcji, które mają zostać wykonane, gdy warunki alarmu przestaną być spełnione. W nVision każdy wygenerowany alarm ma swój czas rozpoczęcia i czas zakończenia. Gdy warunki zdarzenia określającego alarm zachodzą, nVision generuje alarm. Następnie nVision cyklicznie sprawdza, czy dane warunki są ciągle spełnione i kończy alarm, gdy już nie są. Oznacza to, że można uzyskać informacje o czasie rozpoczęcia i zakończenia alarmu, wraz z jego czasem trwania.

Gdy alarm zostaje wygenerowany, nazywany jest wtedy alarmem otwartym i stan takiego alarmu jest ustawiany na <Otwarty>. Pozostaje otwarty tak długo, jak długo warunki zdarzenia są spełnione, lub gdy warunki zakończenia nie zostały jeszcze spełnione. Gdy wszystkie warunki potrzebne do zakończenia alarmu są spełnione, nVision zamyka alarm i zmienia jego stan na <Zamknięty>, wskazując tym samym, że nie tylko alarm został zakończony, ale także, że zdarzenie, które go uruchomiło nie ma już miejsca.

Jak nVision uruchamia akcje

Gdy alarm zostaje wygenerowany, wszystkie akcje, które są związane z nim (i ustawione do natychmiastowego uruchomienia) są uruchamiane. Wszystkie akcje, ustalone jako opóźnione będą wykonane tylko wtedy jeśli alarm pozostanie otwarty. Gdy alarm jest zamykany, uruchamiane są wszystkie akcje przypisane do zamknięcia alarmu. Można także zaniechać uruchamiania pozostałych akcji zmieniając stan Rozwiązania alarmu.

Każdy alarm jest generowany z Rozwiązaniem ustawionym na <Nowy>. Jeśli chcesz zaznaczyć, że zostałeś już poinformowany o danym alarmie i nie chcesz być informowany dalej, musisz potwierdzić alarm. Aby to zrobić należy ustawić w Dzienniku Zdarzeń nVision Rozwiązanie alarmu na <Potwierdzony>. Podobnie: jeśli problem, który spowodował wygenerowanie alarmu, został już naprawiony, możesz ustawić Rozwiązanie alarmu na <Rozwiązany>. Podsumowując: zmiana stanu Rozwiązania alarmu zapobiega dalszemu wykonywaniu akcji alarmu.

Dziennik zdarzeń

Wszystkie wygenerowane alarmy są zapisywane przez nVision i dostępne w Dzienniku Zdarzeń. Dziennik Zdarzeń prezentuje wszystkie wygenerowane alarmy, ich stan, a także wszystkie akcje przypisane do danego alarmu. Pozwala także zmieniać stan Rozwiązania alarmu.

8.6.2 Dziennik zdarzeń

Wszystkie wygenerowane alarmy są zapisywane przez nVision i dostępne w Dzienniku Zdarzeń. Dziennik Zdarzeń prezentuje wszystkie wygenerowane alarmy, ich stan, a także wszystkie akcje przypisane do danego alarmu. Pozwala także zmieniać stan Rozwiązania alarmu, oraz sortować i filtrować listę alarmów, aby ułatwić ich przeglądanie.

Ikony użyte w tabeli Alarmy i Akcje

Tabela Alarmy





















Ikona	Opis
Stan - określa stan alarmu	
	Alarm otwarty
	Alarm zamknięty (zakończony)
Rozwiązanie - pozwala administratorowi zarządzać alarmami	
	Nowy alarm
	Alarm, który został potwierdzony przez administratora i którego akcje nie będą już wykonywane
	Alarm, który został już rozwiązany przez administratora i którego akcje nie będą już wykonywane
Typ zdarzenia - typ zdarzenia, które wygenerowało alarm	
	Dostępność urządzenia lub usługi
	Test wydajności konkretnego serwisu
	Licznik wydajności
Ważność zdarzenia - ważność zdarzenia, które wygenerowało alarm	
	Niska ważność
	Normalna ważność
	Wysoka ważność
	Krytyczna ważność
Stan urządzenia	
	Działa
	Ostrzeżenie
	Nie działa

Tabela akcji

Ikona	Opis
Typ - typ akcji	
	Notyfikacja desktopowa
	Wiadomość
	Program lub skrypt

Ikona	Opis
	Inne
Stan - określa stan wykonania akcji	
	Jeszcze nie wykonana
	Akcja aktualnie wykonywana
	Pomyślnie wykonana
	Błąd wykonania (w kolumnie Info znajduje się opis błędu)

Otwieranie Dziennika Zdarzeń

Mozesz wyświetlić zdarzenia dla konkretnego urządzenia lub dla całego atlasu. Aby wyświetlić Dziennik Zdarzeń dla atlasu wybierz z menu głównego **Atlas | Alarmy | Wyświetl**. Aby wyświetlić Dziennik Zdarzeń dla pojedynczego urządzenia wybierz z menu kontekstowego ikony urządzenia **Alarmy | Wyświetl**, lub przejdź do zakładki Dziennik Zdarzeń w oknie **Informacje o urządzeniu**.

Odblokowywanie Alarmów (zmiana stanu Rozwiązania alarmów)

Aby odblokować alarm, musisz zmienić stan jego Rozwiązania na <Potwierdzony> lub <Rozwiązany>.

1. Zaznacz alarm lub wiele alarmów.
2. Wybierz **Potwierdź** lub **Rozwiąż** z menu kontekstowego.



Aby uzyskać więcej informacji na temat zmiany stanu Rozwiązania alarmów przejdź do rozdziału [Wprowadzenie](#).

Sortowanie i filtrowanie

- Możesz sortować obie tabele względem konkretnej kolumny klikając jej nagłówek.
- Możesz filtrować zdarzenia przez stan lub stan rozwiązania. Aby wyświetlić tylko te alarmy, które mają określony stan/stan rozwiązania wybierz odpowiednią wartość z pola **Filtruj**.

Zmiana przedziału czasowego

Mozesz przeglądać alarmy dla jednego dnia, tygodnia lub miesiąca. Aby wybrać przedział czasowy, skorzystaj z paska narzędzi. Aby przeglądać archiwalne wpisy w Dzienniku Zdarzeń skorzystaj ze

strzałek   znajdujących się na pasku narzędzi. Podczas przeglądania zawsze będzie wyświetlony aktualny przedział czasowy.

Część

IX

9 Inne

9.1 Dystrybucja plików

nVision pozwala na zdalna dystrybucje plików do komputerów z systemem Windows. Wykonywane jest to za pomoca usługi WMI, dlatego musisz odpowiednio skonfigurowac dane logowania we właściwościach urządzenia. Dodatkowo usługa WMI musi zostac włączona na wszystkich zdalnych komputerach. Aby uzyskac wiecej informacji przejdź do rozdziału [Wymagania i planowanie](#).

Dystrybucja plików

1. Wybierz **Narzedzia | Dystrybucja plików** z menu głównego.
2. Wybierz plik, który chcesz dystrybuowac.
3. Wybrany plik moze byc plikiem wykonywalnym (np. plik instalacyjny). Istnieje mozliwosc uruchomienia takiego pliku po jego skopiowaniu na zdalny komputer. Mozesz za pomoca tego mechanizmu dystrybuowac programy lub aktualizacje (również tzw. łatki). Sprecyzuj ustawienia uruchomienia w polu **Parametry** i włącz opcje **Uruchom plik po skopiowaniu**.
4. Wybierz **Wszystkie**, aby dystrybuowac plik do wszystkich komputerów lub **Wybrane** gdy chcesz wybrac ich okreslona grupe.
5. Kliknij przycisk **Dystrybuuj**. Zobaczysz okno przedstawiajace stan dystrybucji oraz pozwalajace na weryfikacje jej powodzenia.

9.2 Opcje

Aby zmienic opcje programu

1. Wybierz **Narzedzia | Opcje** z menu głównego.
2. Wybierz odpowiednia zakladke.
3. Edytuj opcje zgodnie z ponizszymi instrukcjami.

Ogólne

Wlasnosc	Opis
Maksymalne zuzycie pamieci przez dane monitorowania	Okresla maksymalna pamiec, jaka moze zostac przeznaczona na dane monitorowania. Ta pamiec jest wykorzystana dla pamieci podrecznej monitorowania. Jesli zalezy Ci na szybszym dostepnie do takich danych i jesli chcesz aby wykresy byly wyswietlane z wieksza rozdzielczoscia, mozesz zwiekszyc ta wartosc. Uwaga: próbki w pamieci sa zapisywane z dokladnoscia monitorowania, lecz próbki na dysku sa zapisywane z rozdzielczoscia 1-minutowa.

Monitorowanie

Wlasnosc	Opis
Uslugi	Lista serwisów, które nVision spróbuje wykryc na kazdym urzadzeniu. Jesli chcesz aby jakis serwis byl wykrywany automatycznie przez program, dodaj go do tej listy.
Inteligentne monitorowanie	Mechanizm monitorowania, który daje gwarancje, ze kazde urzadzenie bedzie monitorowane tak czesto jak to mozliwe. Jest to szczególnie istotne dla duzych sieci, w których znajduja sie setki urzadzen.

Wlasnosc	Opis
Usun alarmy i dane monitorowania	Wszystkie alarmy i dane monitorowania starsze niz okreslona liczba dni beda usuniete z dysku po zamknieciu programu.
Inwentaryzuj urzadzenia z systemem Windows	Ta opcja jest domyslnie wlaczona i pozwala na automatyczna inwentaryzacje sprzetu i oprogramowania za pomoca uslugi WMI i agentów.
Monitoruj aktywnosc uzytkowników	Ta opcja jest domyslnie wlaczona i pozwala na automatycznie monitorowanie aktywnosci uzytkowników za pomoca agentów.
Nie usuwaj danych agentów	Wlacz ta opcje, jesli chcesz monitorowac dane dotyczace aktywnosci uzytkowników z wiecej niz jednej instalacji nVision. Sprawi to, ze agenty nVision beda utrzymywac dane dzienne na dysku. Domyslnie dane te kasowane sa tuz po odczytaniu ich przez nVision.

Akcje

Niektóre akcje wymagaja konfiguracji, aby dzialaly poprawnie (np. wyslanie wiadomosci ICQ wymaga podania danych konta ICQ potrzebnych do zalogowania na serwer). Aby uzyskac wiecej informacji przejdź do rozdzialu [Konfigurowanie akcji](#).

Aktywnosc uzytkowników

Dotyczy tylko wersji Professional

Wlasnosc	Opis
Uzytkownik traktowany jako nieaktywny po	Okresla liczbe minut, po jakiej agent nVision zaczyna zliczac czas nieaktywnosci uzytkownika. Czas ten jest mierzony od ostatniego ruchu myszka lub wcisniecia dowolnego klawisza klawiatury.
Ogranicz poziom odwiedzonych stron do	Okresla maksymalny poziom odwiedzonych stron przez uzytkowników.
Programy	Pozwala definiowac grupy programów. Mozna tworzyć, modyfikowac i usuwac grupy.

9.3 Kopia zapasowa i naprawianie bazy danych

Aby utworzyc kopie zapasowa i naprawic baze danych programu, uzyj narzedzia dbRepair. Mozesz to zrobic wybierajac **Kopia zapasowa i naprawianie bazy danych** z menu Start. Upewnij sie, ze nVision nie dziala podczas pracy tego programu.

1. Wybierz dbRepair z menu Start.
2. Wylacz opcje **Utwórz kopie zapasowa** jesli chcesz wykonac tylko naprawienie bazy.
3. Kliknij przycisk **Napraw**. Spowoduje to utworzenie (jesli zostala wybrana odpowiednia opcja) bazy danych w katalogu Atlases\Backup i rozpocznie proces naprawiania.

Indeks

- A -

- Agent 40
- Akcje
 - Definiowanie własności 86
 - Konfiguracja 90
 - Typy 85
 - Wiadomości alarmowe użytkownika 92
 - Wprowadzenie 85
 - Zarządzanie 86
- Alarmy
 - Dziedziczenie 75
 - Dziennik zdarzeń 94
 - Eskalacja 76
 - Filtrowanie dziedziczonych alarmów 73
 - Kiedy licznik jest powyżej/poniżej progu 12
 - Kiedy serwis jest wolny lub nie działający 12
 - Pojęcia 71
 - Wprowadzenie 71
 - Wprowadzenie do zarządzania alarmami 72
 - Wygenerowane alarmy - wprowadzenie 93
 - Wyłączanie 73
 - Zarządzanie 73
- Atlas
 - Wprowadzenie 45
 - Zarządzanie 45
- Audyt licencji 43

- B -

- Blokowanie mapy 49

- C -

- Co nowego 2

- D -

- DHCP 40
- Dodawanie nowego urządzenia 28
- Dostępność urządzeń 11
- Dystrybucja 97
- Dystrybucja plików 97
 - Rozwiązywanie problemów 21
 - Wymagania 16
- Dziedziczenie alarmów 75

- I -

- Informacje o urządzeniu 57
- Instalacja agenta 40
- Instalacja jako usługa Windows 8
- Instalowanie agentów
 - Rozwiązywanie problemów 21
- Inventaryzacja
 - Rozwiązywanie problemów 21, 22
 - Wymagania 15, 16
- Inwentaryzacja
 - Audyt 43
 - Audyt licencji 43
 - Wprowadzenie 42
 - Wymagania 17, 42
 - Zbieranie danych 43
- Inwentaryzacja programów 42
- Inwentaryzacja sprzętu 42

- K -

- Komputery z adresem przypisanym przez DHCP 40
- Kopia 13
- Kopia bezpieczeństwa Atlasu 13
- Kopia zapasowa bazy danych 98
- Kopia zapasowa atlasów 98
- Kreator wykrywania sieci 26

- L -

- Licznik wydajności
 - Tworzenie licznika na wielu urządzeniach 35
 - Typy 34
- Liczniki 33
 - Włączanie monitorowania na Windows XP 19
- Liczniki wydajności
 - Definiowanie właściwości 35
 - Wprowadzenie 33
 - Wymagania 15, 16

- M -

- Mapy 45
 - Blokowanie 49
 - Hierarchia obiektów 49
 - Narzędzia 49
 - Obiekty 47
 - Praca z 49

- Mapy 45
 - Tworzenie obiektów 49
 - Typy 47
 - Układ 49
 - Właściwości obiektów statycznych 52
 - Wprowadzenie 46
 - Zarządzanie 48
 - Monitorowanie
 - Adresów URL 36
 - Aktywności użytkowników 40
 - Czasu ładowania stron 36
 - Interfejsów sieciowych 38
 - Komputery z adresem przypisanym przez DHCP 40
 - Pojęcia 30
 - Routerów 38
 - Ruch sieciowy 12
 - Ruchu sieciowego 38
 - Serwerów pocztowych 36
 - Serwerów POP3 36
 - Serwerów SMTP 36
 - Serwerów WWW 36
 - Serwisy 31
 - Serwisy TCP/IP 31
 - Switch'y 38
 - Treści stron 36
 - Usługi Windows 33
 - Wprowadzenie 29
 - Wydajność systemu i urządzeń 33
 - Wymagania i planowanie 15
 - Monitorowanie aktywności użytkowników
 - Czas aktywności 40
 - Instalacja agenta 40
 - Przeglądane strony 40
 - Rozwiązywanie problemów 22
 - Użycie łącza 40
 - Używane aplikacje 40
 - Wymagania 15, 18, 40
 - Monitorowanie routerów i switch'ów
 - Wymagania 15
 - Monitorowanie routerów i switch'y
 - Interfejsy sieciowe 39
 - Porty switch'a 39
 - Ruch sieciowy 39
 - Wprowadzenie 38
 - Monitorowanie serwerów pocztowych i WWW
 - Definiowanie właściwości licznika 37
 - Typy liczników (testów) 36
 - Wprowadzenie 36
 - Monitorowanie serwisów
 - Limit TPC na Windows XP z SP2 19
 - Wprowadzenie 31
 - Zarządzanie 32
 - Monitorowanie sieci 25
 - Stan urządzenia 25
 - Monitorowanie SNMP
 - Wymagania 16
 - Monitorowanie urządzeń 11
 - Monitorowanie Windows
 - Rozwiązywanie problemów 21
 - Monitorowanie wydajności
 - Tworzenie licznika na wielu urządzeniach 35
 - Typy liczników 34
 - Właściwości licznika 35
 - Wprowadzenie 33
 - Zarządzanie 34
- N -**
- Naprawianie bazy danych 98
 - Naprawianie bazy danych atlasów 98
 - nVision
 - Co to jest 2
 - Szybki start 8
 - Układ okna 9
 - Wprowadzenie 7
 - Wymagania systemowe 3
- O -**
- Opcje 97
- P -**
- Problem sieciowy - lokalizowanie 11
 - Professional 4
 - Progi 84
- R -**
- Raporty
 - Tworzenie nowych raportów 64
 - Typy segmentów raportów dla map 67
 - Typy segmentów raportów dla urządzeń 65
 - Wprowadzenie 64
- S -**
- Skanowanie portów 11
 - Skanowanie serwisów 11
 - Skanowanie sieci 11
 - Skanowanie trojanów 11

Skanowanie urządzenia 11
Stan urządzenia 25
Style
 Definiowanie 60
 Wprowadzenie 59
 Zarządzanie 61
Szukanie 13
Szukanie urządzenia 13
Szybki start 8

- U -

Układ mapy
 Asystent układu 49
 Tworzenie 49
Układ okna 9
Urządzenia 45
 Okno Informacje o urządzeniu 57
 Wizualizacja 54
 Właściwości 55
 Wprowadzenie 54
 Zarządzanie 57

- W -

Wersje 4
WMI - problem 19
Wprowadzenie 7
Wstęp 2
Wykrywanie sieci 25
 Kreator wykrywania sieci 26
 Wprowadzenie 26
Wymagania 3
Wymagania i planowanie monitorowania 15
Wymagania systemowe 3

- Z -

Zdalny dostęp
 Wymagania 19
Zdarzenia
 Definiowanie własności 78
 Progi 84
 Progi narastające, opadające i kończące 84
 Typy 76
 Wprowadzenie 76
 Zarządzanie 77