

Monitoring sieci Nagios

Wstęp

HomePage : <http://www.nagios.org/about>

Nagios – program do monitorowania sieci, urządzeń sieciowych, aplikacji oraz serwerów działający w systemach Linux i Unix rozpowszechniany na podstawie licencji GPL.

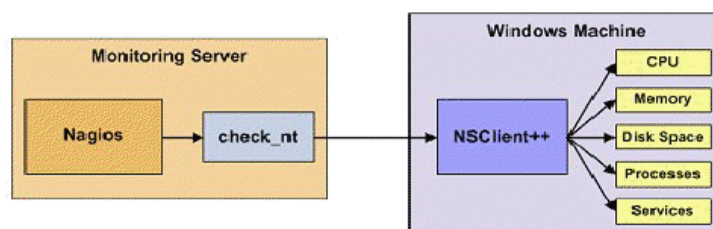
Może monitorować hosty oraz usługi według określonych ustawień, dzięki czemu jest możliwe dostosowanie go do swoich potrzeb. W razie wykrycia problemu Nagios może wysłać pocztę, info na pager lub SMS do administratora systemu z informacją o problemie.

Nagios posiada budowę modułową, czyli bazuje na wtyczkach.

Monitoring

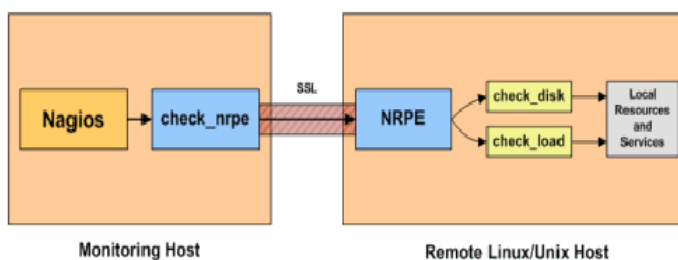
Nagios monitoruje krytyczne usługi i komponenty w infrastrukturach sieci, usługi systemowe, protokoły sieciowe, aplikacje, usługi serwerowe, infrastrukturę.

Maszyny z zainstalowanym systemem Windows



- Wymaga zainstalowania agenta na maszynie monitorowanej,
- Używamy pluginu check_nt,
- Możemy monitorować procesy działające na maszynie,
- zajętość pamięci, zajętość dysku itp.

Maszyny z zainstalowanym systemem Linuks

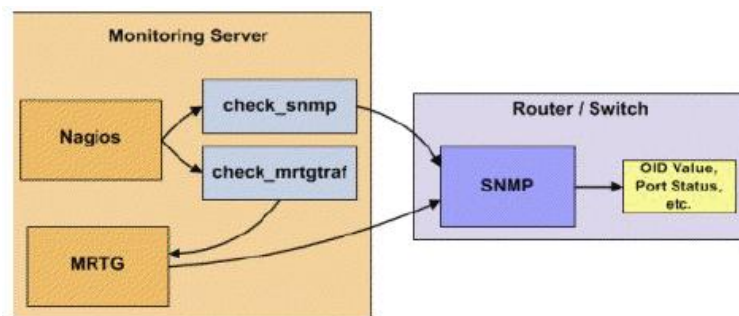


- Wymaga zainstalowanie dodatku NRPE,
- Możemy monitorować obciążenie procesora, zajętość dysku, ilość zalogowanych użytkowników, uruchomione procesy itd.

NRPE umożliwia uruchomienia wtyczek Nagiosa na zdalnych maszynach:

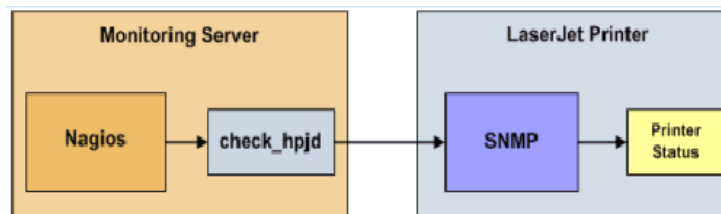
1. Maszyna monitorująca poprzez plugin `check_nrpe` łączy się z maszyną monitorowaną,
2. Na maszynie monitorowanej uruchamiany jest lokalny plugin w zależności od usługi, którą chcemy sprawdzić,
3. Rezultat wraca poprzez `check_nrpe` do maszyny monitorującej.

Router i switche



- Możemy monitorować straty pakietów (packet loss),
- Możemy monitorować opóźnienie (ping),
- Możemy sprawdzać wiadomości SNMP,
- Możemy monitorować ruch na interfejsach.

Drukarki sieciowe/Print Servers



- Monitorowane drukarki wspierają protokół JetDirect.
- Monitorujemy dostępność drukarki (ping),
- Monitorujemy zdarzenia takie jak: brak papieru, zacięcia papieru, niski poziom/brak atramentu, otwarcie pokrywy drukarki itp.,
- Używamy do tego pluginu `check_hpjd`.

Usługi sieciowe (services) takie jak:

- HTTP,
- FTP,
- SSH,
- SMTP,
- POP3,

- IMAP.

Do wszystkich tych serwisów dostępne są wtyczki monitorujące.

Możliwość definicji własnych wtyczek monitorujących hosty i usługi

- Można monitorować wszystko dla czego da się napisać wtyczkę, Dowolny język programowania C, Python, Perl, itp.
- Istnieją dwa warunki konieczne do tego, aby nasz plugin działał poprawnie:
 - Musi zakończyć się z określoną wartością - 0,1,2,3,
 - Musi zwracać co najmniej jedną linię tekstu do STDOUT,

Alarmowanie

Nagios potrafi wysyłać powiadomień o krytycznych zdarzeniach zachodzących w infrastrukturze . Alarm mogą być dostarczane za pomocą poczty elektronicznej, sms , skryptów , bipera , i wielu innych. Można określić użytkownika bądź grupę użytkowników, do Których wysyłamy komunikaty, Definiujemy filtry wysyłania powiadomień.

Metody sprawdzania

- Aktywne - Wykonywane przez Nagios w regularnych odstępach czasu (synchroniczne),
- Pasywne
 - Nadają się do sprawdzania asynchronicznych zdarzeń lub hostów (usług) znajdujących się „za firewallem”,
 - Wykonywane są przez zewnętrzne aplikacje,
 - Wyniki przesyłane są do Nagiosa w celu obróbki.

Raportowanie

Zawansowane raportowanie dowolnej części w infrastrukturze , powiadomień , alarmów, do późniejszego przeglądania.

Planowanie

Funkcje planowania zapobiegają wysyłania błędnych komunikatów w przypadku zaplanowanych konserwacji i uaktualnień systemów.

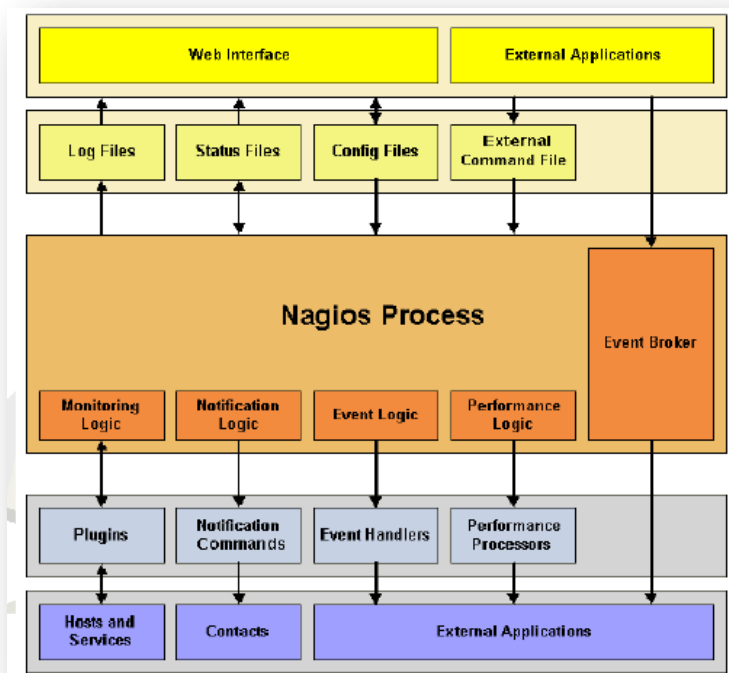
Automatyzacja

Przy wykrytych błędach lub usterkach system jest w stanie wykonać automatyczna naprawę zaplanowaną przez administratora systemu do określonego błędu.

Licencja

- Oprogramowanie Open Source
- Pełny dostęp do kodu źródłowego
- Wydany na licencji GPL

Architektura



Instalacja

Instalacja nagios3

```
apt-get install nagios3 nagios-plugins
```

Konfiguracja

Główny plik konfiguracyjny nagiosa znajduje się w : `/etc/nagios3/nagios.conf` Zawiera główne konfiguracje usługi oraz łąduje dodatkowe konfiguracje. Po każdej wprowadzonej zmianie w plikach konfiguracyjnych należy użyć komendy `/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg`, która weryfikuje i aktualizuje ustawienia nagiosa

Zewnętrzne polecenia

Aby polecenia mogły zostać wykonywane za pośrednictwem interfejsu webowego muszą zostać przeprowadzone następujące kroki, opisane są one w `/usr/share/doc/nagios3/README.Debian.[1]`

Na początku opcji `check_external_commands` w pliku konfiguracyjnym `/etc/nagios3/nagios.cfg` zostanie przyporządkowana wartość 1

Następnie muszą jeszcze zostać dostosowane uprawnienia dotyczące plików:

```
/etc/init.d/nagios3 stop  
dpkg-statoverride --update --add nagios www-data 2710 /var/lib/nagios3/rw  
dpkg-statoverride --update --add nagios nagios 751 /var/lib/nagios3  
/etc/init.d/nagios3 start
```

Katalog z plikami `cfg`, które reprezentują hosty w sieci. Przykład dla `localhost.cfg` o nazwie `zie-srv-nagios` znajduje się poniżej. Najpierw zdefiniowany jest host, który używa template o nazwie `linux-server`, a następnie zdefiniowane są określone usługi, które także mają swoje template o nazwie `generic-service` oraz `local-service`

```
define host{
use linux-server
host_name zie-srv-nagios
alias Nagios 3.0.6
address 127.0.0.1
}define service {
use generic-service
service_description Memory
host_name zie-srv-nagios
check_command check_linux_free_memory.pl!20!10
}
define service{
use local-service
host_name zie-srv-nagios
service_description PING
check_command check_ping!100.0,20%!500.0,60%
}

define service{
use generic-service
host_name zie-srv-nagios
service_description Total Processes
check_command check_procs!250!400
}
```

`commands.cfg` – do tego pliku odwołuje się każdy plik (w naszym przypadku `localhost.cfg`) w którym jest użyta komenda „`check_command`”. To właśnie tu następuje zdefiniowanie komendy. Oprócz podania nazwy komendy trzeba podać ścieżkę w której dany plugin się znajduje (`$USER1$` jest częścią działy, która jest zdefiniowana w pliku `resource.cfg`; przeważnie jest to `/usr/local/nagios/libexec`)

```
define command{
command_name check_linux_free_memory.p
command_line /usr/bin/perl $USER1$/check_linux_free_memory.pl -w $ARG1$ -c $ARG2$
}define command{
command_name check_procs
command_line $USER1$/check_procs.sh -w $ARG1$ -c $ARG2$
}
define command{
command_name check_ping
command_line $USER1$/check_ping -H $HOSTADDRESS$ -w $ARG1$ -c $ARG2$ -p 5
}
```

`templates.cfg` – zdefiniowane template dla hosta i usług (o nazwach `generic-host`, `linux-server`, `generic-service` i `local-service`)

`contacts.cfg` – określenie kto ma być informowany o problemach

timeperiod.cfg – określenie przedziałów czasowych dla których będzie działał Nagios; najlepiej jest użyć pliku przykładowego dostarczonego wraz z instalacją pakietu Nagios.

hostgroup.cfg – zdefiniowane grupy, które łatwiej można później zlokalizować i przyporządkować w Nagios

Nagios XI

Instalacja :

Źródła należy skopiować do katalogu **/tmp** , następnie uruchomić proces instalacji za pomocą komendy **./fullinstall**

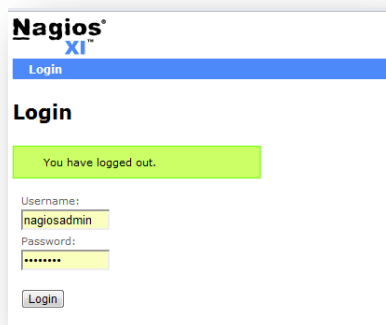
Konfiguracja

System nagios xi konfiguruje się za pomocą interfejsu webowego dostępnego pod adresem <http://localhost/> na serwerze gdzie jest zainstalowany demon nagiosa xi.

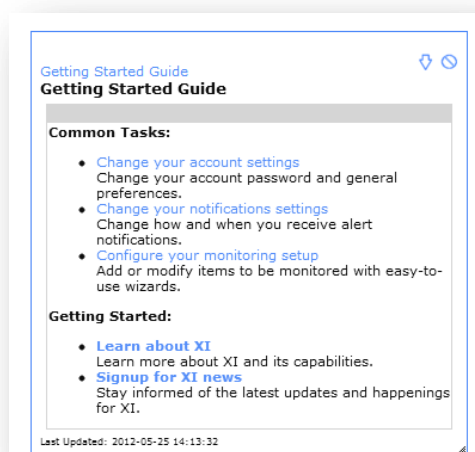
Logowanie

Login : **nagiosadmin**

Hasło: **nagios**



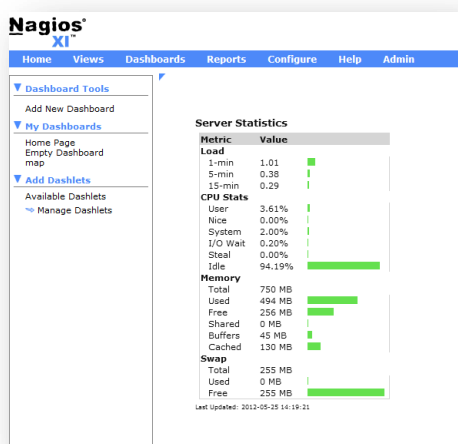
1. Ustawienie haseł - Getting Started Guide



Opis

Dashboards

Dashboard – to konfigurowalny panel umożliwiający wyświetlenie wszystkich komponentów obsługiwanych przez nagios xi, każdy dasbord można dodać bezpośrednio do widoku. W szybki sposób na dowolny dashboard można dodać wiele komponentów w przygotowanych przez producenta lub niezależnego developera.



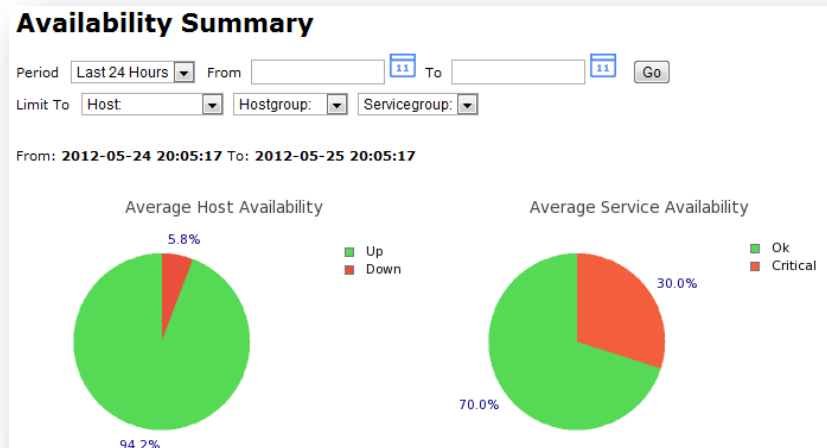
Views

Część systemu odpowiedzialna za podgląd aktualnych statystyk, komponentów i dasbordów. Domyślnie nagios co minutę wyświetla kolejną zakładkę z aktualnymi widokami. W skład podstawowych zakładek wchodzi:

- **Tactical Overview** – jest to podstawowy widok w który są zestawione wszystkie główne statystyki. Widok został specjalnie pogrupowany w cztery podstawowe grupy Network Outages, Host, Services, Monitoring Features
- **Open Problems** – widok odpowiedzialny za wyświetlenie statusów pogrupowanych ze względu na hosty, service i ważność statusu które wymagają ingerencji administratora.
- **Service Detail** – widok wyświetlający wszystkie statusy monitorowane przez nagios
- **Hostgroup Overview** – widok statusów dzielony ze względu na hosty i ich aktualny stan.

Raports

Sekcja służąca do raportowania i tworzenia zestawień informacji generowanych przez nagios. Jednymi z ważniejszych funkcjonalności z raportowania są Dostępność hostów, Najważniejsze problemy czy wszystkie logi.



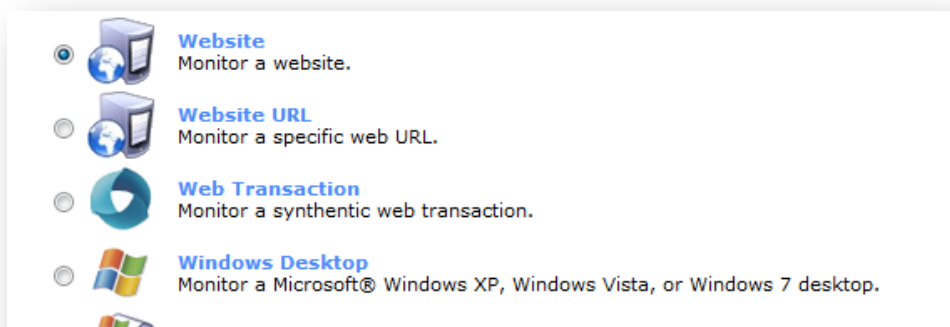
Configure

Monitoring Wizard – kreator w którym można określić krok po kroku monitorowane usługi, czynność w przypadku wystąpienia powiadomienia, rodzaje powiadomienia , itp.

Auto-Discovery Wizard Admin – pozwala na automatyczne wyszukanie i konfigurowanie monitorowanych hostów czy usług sieciowych

Dodanie monitorowania serwera WWW

1. Wybieramy usługę Website i kontynuujemy za pomocą przycisku next



2. Podajemy adres serwera WWW , podajemy dodatkowe informacje jeżeli są potrzebne do konfiguracji.
Wybieramy monitorowane usługi .

Website Services

Specify which services you'd like to monitor for the website.

☒ **HTTP**
Includes basic monitoring of the website to ensure the web server responds with a valid HTTP response.

☒ **Ping**
Monitors the website server with an ICMP "ping". Useful for watching network latency and general uptime of your web server. Not all web servers support this.

☒ **DNS Resolution**
Monitors the website DNS name to ensure it resolves to a valid IP address.

☒ **DNS IP Match**
Monitors the website DNS name to ensure it resolves to the current known IP address. Helps ensure your DNS doesn't change unexpectedly, which may mean a security breach has occurred.

☐ **Web Page Content**
Monitors the website to ensure the specified string is found in the content of the web page. A content mismatch may indicate that your website has experienced a security breach or is not functioning correctly.
Content String To Expect:

☐ **Web Page Regular Expression Match**
Monitors the website to ensure the specified regular expression is found in the content of the web page. A content mismatch may indicate that your website has experienced a security breach or is not functioning correctly.
Regular Expression To Expect:

3. Określamy czas sprawdzania monitorowania usługi.
4. Określamy powiadomienia oraz grupę docelową powiadamianych użytkowników
5. Wybieramy grupy przynależności dla tworzonego powiadomienia.
6. Dodajemy

Admin

Admin – panel administracyjny służący do zarządzania nagiosie, tworzenia użytkowników i konfiguracja podstawowych funkcji w nagiosie.

Core Config Manager – panel administracyjny umożliwiający zarządzaniem skonfigurowanego monitoringu

Nagios Core Config Manager Configuration

Service Management

☐ Check All Search: Config name filter:

Config Name	Service Name	Active	Sync Status	Actions
☐ 192.168.1.1	Ping	Yes	Synced	
☐ 192.168.1.100	Ping	Yes	Synced	
☐ 192.168.1.100	TCP Port 62078	Yes	Out of Sync	
☐ 192.168.1.101	Ping	Yes	Synced	
☐ 192.168.1.106	HTTP	Yes	Out of Sync	
☐ 192.168.1.106	NRPE	Yes	Out of Sync	
☐ 192.168.1.106	Ping	Yes	Synced	
☐ 192.168.1.106	SSH	Yes	Out of Sync	
☐ 192.168.1.106	TCP Port 3306 (mysql)	Yes	Out of Sync	
☐ 192.168.112.101	Ping	Yes	Synced	
☐ localhost	Current Load	Yes	Synced	
☐ localhost	Current Users	Yes	Synced	
☐ localhost	HTTP	Yes	Synced	
☐ localhost	PING	Yes	Synced	
☐ localhost	Root Partition	Yes	Synced	

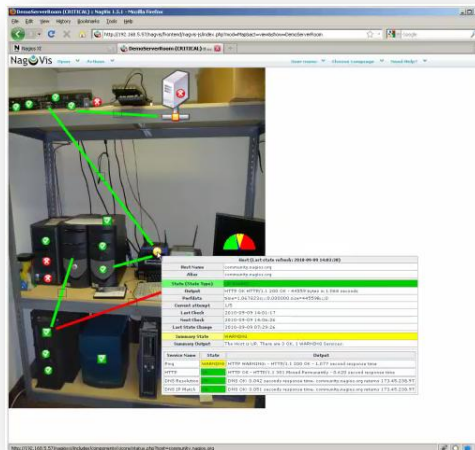
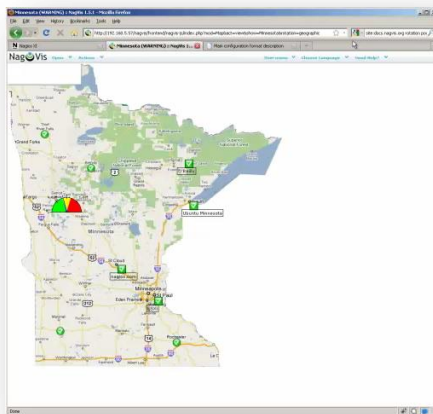
Dodatki

NRPE – rozszerzenie, które pozwala na wysyłanie statystyk z odległych hostów z systemem Linux / Unix do nagiosa. NRPE potrafi między innymi sprawdzać użycie dysku, obciążenie procesora, wykorzystywanie pamięci itp.

NSCA to rozszerzenie, które pozwala na wysyłanie usługonych stałych wyników z innych Linux / Unix hostów do demona Nagios działającego na serwerze. Jest to bardzo przydatne w [rozproszonych](#) infrastrukturach.

NDOutils to rozszerzenie, które pozwala na przechowywanie wszystkich informacji o stanie z Nagios w bazie danych MySQL. Można to posłużyć do zbudowania centralnej bazy raportowania.

Visio - Rozszerzenie nagiosa umożliwiające nakładanie aktualnych ikon statusu na wybrane zdjęcie czy mapę.



Zadania

1. Zainstaluj nagiosa w wersji z obsługą wtyczek lub nagios3
2. Dodaj monitorowanie usługi internetowej na host xxx.asl24.pl, gdzie xxx to numer twojego indeksu
3. Stwórz nowy dashboard monitorujący całą sieć lokalną za pomocą hypermapy.
4. Zainstaluj na niezależnym hoście usługę NRPE i połącz raportowanie z nagiosem stanu hosta

*zamieszczone obrazy pochodzą z Internetu i nie są mojego autorstwa,