



System monitorowania Nagios

1. Wstęp

Celem ćwiczenia jest zapoznanie się z przykładowym systemem monitorowania — Nagios <http://www.nagios.org>.

2. Nagios

Nagios jest znanym, darmowym systemem monitorowania dostępności węzłów, jednakże dzięki aktywnemu zaangażowaniu społeczności w jego rozwój, powstało wiele rozszerzeń, które uzupełniają system Nagios o nową funkcjonalność. Przykładem mogą być rozszerzenia pozwalające podłączać sensory monitorujące wydajność, uruchamiać zdalne agenty, kreślić wykresy na podstawie zebranych danych, czy prezentować topologię sieci na mapie geograficznej.

Nagios zyskał sobie uznanie dzięki prostocie użytkowania, instalacji oraz łatwemu rozszerzaniu go o nowe wtyczki monitorowania.

2.1. Architektura Nagiosa

Domyślnie architektura Nagiosa składa się z dwóch elementów: głównego serwera odpytującego oraz interfejsu graficznego Web.

Serwer co jakiś czas odpytuje pakietem ICMP dany węzeł. Jeśli węzeł nie odpowiada, Nagios ustawia status węzła na *nie działający*.

Nagios może zostać rozszerzony o kolejne sensory za pomocą prostych skryptów. Dany skrypt powinien być

2.2. Instalacja nagiosa

Nagios można zainstalować z pakietów danej dystrybucji lub ze źródeł pobranych ze strony projektu. W przypadku dystrybucji OpenSuse, nagios można zainstalować za pomocą komend:

```
zypper install nagios oraz zypper install nagios-plugins.
```

W systemie Debian oraz Ubuntu, Nagiosa instalujemy następująco:

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

W przypadku instalacji ze źródeł należy ściągnąć odpowiednie paczki źródłowe (nagios core i nagios plugins) ze strony <http://www.nagios.org/download>.

Po rozpakowaniu paczek, tradycyjnie należy wykonać komendy: `configure`, `make` oraz `make install`.

Domyślnie Nagios zainstalowany zostanie w katalogu `/usr/local/`.

2.3. Konfiguracja Nagiosa

2.3.1. Katalogi Nagios

Po instalacji z pakietów, w zależności od systemu, pliki konfiguracyjne Nagiosa powinny znajdować się w katalogu `/etc/nagios` lub `/etc/nagios3`.

W zależności od systemu, wtyczki Nagiosa, powinny znajdować się w katalogu `/usr/lib/nagios/plugins`.

2.3.2. Konfiguracja

W systemie Nagios można wyróżnić kilka obiektów konfiguracyjnych, najważniejsze z nich zostały opisane poniżej, są one wystarczające do minimalnej konfiguracji systemu Nagios.

Szablon węzła Definicja węzła z parametrem `register 0`; wykorzystywana do tworzenia szablonów konfiguracji.

Węzeł (*host*) Definicje węzłów z definicją adresu IP, hostname, aliasu, nazwy i szablonu konfiguracji.



```
define host{
    use          generic-host ; szablon
    host_name    dalek.example.com ; hostname
    alias        dalek ; alias dla nagiosa
    address      1.2.3.4 ; adres IP
}
```

Grupa węzłów (*hostgroup*) Obiekt grupujący węzły o wspólnej cesze, np. posiadające te same usługi, będące w tym samym pokoju, będące tym samym typem urządzenia, itd.

```
define hostgroup {
    hostgroup_name    debian-servers
    alias              Serwery Debian
    members            dalek, drwho, amypond
}
```

Usługa (*service*) Definicja usług działających na danym węźle, definiowana przez szablon konfiguracji, węzeł lub grupę węzłów, na którym jest udostępniana, opis, oraz komendę odpytania sensora;; przykład SSH, HTTP, MySQL, itd.

```
define service{
    use          generic-service ; szablon
    host_name    dalek;
    service_description SNMPLOAD;
    check_command snmp_load!public!7!7!7!15!15!15
}

define service {
    hostgroup_name    debian-servers
    service-description Debiany_z_HTTP
    use                generic-service
    check_command     check_http
}
```

Definicję komend (sensorów) tworzymy w Nagiosie za pomocą obiektów **command**. Każdy taki obiekt posiada nazwę oraz linię poleceń, która jest uruchamiana przez system w trakcie odpytania. Poniżej przykład sensora (komendy) dla sprawdzenia dostępności usługi HTTP. Zmienna **\$HOSTADDRESS** definiuje adres węzła zdalnego, jest automatycznie wartościowana adresem wpisanym w obiektach **host**. Przełączniki **-w** oraz **-c** odpowiednio ustawiają wartości progowe dla statusów **WARNING** oraz **CRITICAL**. To jakie parametry przyjmuje dany sensor, można sprawdzić uruchamiając go w terminalu ręcznie.

```
define command{
    command_name    check-host-alive
    command_line    /usr/lib/nagios/plugins/check_ping -H '$HOSTADDRESS$' -w 5000,100% -c
}
```

Konfiguracja interfejsu WWW systemu Nagios znajduje się w serwerze HTTP, w ćwiczeniach wykorzystany zostanie jeden z popularniejszych serwerów — Apache HTTPd. Aby skonfigurować interfejs WWW, należy odnaleźć ścieżkę do katalogu, w którym zostały zainstalowane pliki CGI GUI Nagiosa (komenda rpm, zypper, dpkg). Następnie, w pliku konfiguracyjnym serwera Apache, należy dodać odpowiednie dyrektywy Alias.

Przykład:

```
ScriptAlias /cgi-bin/nagios /usr/lib/cgi-bin/nagios
ScriptAlias /nagios/cgi-bin /usr/lib/cgi-bin/nagios
Alias /nagios/stylesheets /etc/nagios/stylesheets
Alias /nagios /usr/share/nagios/htdocs
```

W powyższym przykładzie Nagios dostępny będzie pod adresem `http://localhost/nagios/`.



2.3.3. Przygotowanie do zajęć

Ponieważ domyślnie w systemach zainstalowanych w salach laboratoryjnych Nagios skonfigurowany jest z opcją uwierzytelniania, należy wykonać następujące kroki, aby opcję tę wyłączyć:

W pliku: `/etc/nagios/cgi.cfg` należy znaleźć wpis `use_authentication` i ustawić w nim wartość 0.

W pliku: `/etc/apache2/conf.d/nagios.conf` zakomentować wszystkie linie zaczynające się na:

```
AuthName
AuthType
AuthUserFile
Require
```

Po wykonaniu czynności, należy oczywiście przeładować serwer nagios oraz apache2:

```
/etc/init.d/apache2 restart oraz
```

```
/etc/init.d/nagios restart.
```

W przypadku gdy chcemy skorzystać z opcji uwierzytelniania, nie zmieniamy nic w plikach konfiguracyjnych. Wykonujemy komendę, tworzącą użytkownika `nagiosadmin` w ramach mechanizmu uwierzytelniania HTTP Auth:

```
htpasswd2 -c /etc/nagios/htpasswd.users nagiosadmin
```

Komenda poprosi o podanie hasła, proszę wymyślić cokolwiek.

Ćwiczenia

1. Zainstaluj Nagios jeśli nie jest zainstalowany.
2. Skonfiguruj odpytywanie jednego z węzłów.
3. Skonfiguruj odpytywanie wszystkich węzłów w sali.
4. Skonfiguruj SNMP i sensor `check_snmp_load`.
5. Napisz wtyczkę monitorującą poziom entropii w systemie.