Zeszyty Naukowe WWSI, No 22, Vol. 14 2020, s. 39-63
DOI: 10.26348/znwwsi.22.39

Implementacja systemu informatycznego do monitorowania infrastruktury sieciowej

Dariusz Chaładyniak[*], Piotr Pindral[**]

Warszawska Wyższa Szkoła Informatyki

Abstrakt

Artykuł dotyczy monitorowania współczesnych sieci komputerowych. Działanie to umożliwia natychmiastową reakcję na różne nieprawidłowości w funkcjonowaniu infrastruktury teleinformatycznej czy naruszenia zasad bezpieczeństwa. Systemy monitoringu są obecnie wdrażane w każdej organizacji, niezależnie od jej wielkości czy profilu działania.

Monitorowanie sieci jest niezbędnym wymogiem zwłaszcza w firmach, w których praca opiera się głównie na systemach informatycznych. Wiele firm wdraża tego typu rozwiązania w celu zminimalizowania problemów z infrastrukturą teleinformatyczną oraz poprawy wydajności sieci komputerowych i produktywności pracowników.

W artykule przedstawiono proces implementacji jednego z najpopularniejszych systemów monitorowania współczesnych sieci komputerowych Nagios Core w wersji 4.4.5.

Słowa kluczowe **–** sieci komputerowe, monitorowanie, systemy bezpieczeństwa, systemy informatyczne

[*] E-mail: dchalad@wwsi.edu.pl
[**] E-mail: p_pindral@poczta.wwsi.edu.pl

Zgłoszono do druku 19 czerwca 2020 r.

1 Wprowadzenie do systemów monitoringu sieci teleinformatycznych

System monitoringu sieci to narzędzie, które monitoruje wewnętrzną infrastrukturę teleinformatyczną w celu wykrycia potencjalnych problemów. Taki system jest w stanie na bieżąco identyfikować dużą liczbę konkretnych problemów, które mogą mieć wpływ na ogólną wydajność infrastruktury sieciowej. Kiedy zostanie wykryta nieścisłość, system monitoringu sieci zaalarmuje administratora, zanim nieprawidłowość stanie się problemem krytycznym.

Proces monitorowania sieci opiera się na systemie, który może posiadać wiele różnych konfiguracji obejmujących zarówno rozwiązania sprzętowe, jak i oprogramowanie. Takie rozwiązanie pozwala nadzorować funkcje praktycznie każdego rodzaju sieci, w tym sieci lokalnej, rozległej czy VPN.

Narzędzia do monitorowania umożliwiają nadzór nad systemami o różnorodnych funkcjach i urządzeniach. Zaliczają się do nich między innymi: serwery, komputery o różnych systemach operacyjnych czy urządzenia sieciowe takie jak routery, przełączniki, zapory ogniowe czy urządzenia mobilne. Taki system usprawnia identyfikację problemów sieciowych, mierzenie wydajności oraz stanu technicznego sieci. Oprogramowanie zapewnia ochronę przed wewnętrznymi naruszeniami bezpieczeństwa, spełniając określone standardy.

Monitoring sieci pomaga również kontrolować przepustowość podczas wykonywania codziennych operacji sieciowych.

Wypada również wspomnieć, że rozwiązanie monitoringu sieci wyraźnie różni się od systemu wykrywania włamań. System monitorowania sieci pomaga między innymi śledzić stan sieci, usług, sprzętu, aktualizacje oprogramowania, wykorzystanie przepustowości czy zawodność infrastruktury sieciowej. System wykrywania włamań koncentruje się wyłącznie na bezpieczeństwie. Jest specjalnie zaprojektowany w celu wykrycia naruszenia sieci przez nieautoryzowanego użytkownika, wykorzystując różne metody identyfikacji próby włamania.

Rozwiązania monitoringu sieci zostały zaprojektowane w celu ułatwienia zarządzania siecią. Umożliwiają monitorowanie kilku oddalonych od siebie placówek firmy z jednej scentralizowanej lokalizacji. Znacząco ułatwia to nadzorowanie w stosunku do przestarzałych systemów rozmieszczonych w wielu lokalizacjach, co sprawiało, że monitoring sieci był czasochłonnym zadaniem.

System monitorowania sieci może również pomóc w planowaniu rozbudowy infrastruktury. W trakcie monitorowania, narzędzie będzie generować raporty i gromadzić krytyczne dane. Takie informacje są automatycznie wysyłane do przechowywania w bazie danych. W momencie przepływu danych przez serwery sieciowe i inne komponenty, monitorowanie sieci śledzi ten sam rodzaj aktywności. Następnie system generuje wyniki działań przeprowadzonych podczas procesu monitorowania. Monitorowanie obejmuje wydajność serwera, przełącznika, routera, wykorzystanie przepustowości oraz wydajność aplikacji.

Monitorowanie sieci jest również używane do badania całego ruchu przechodzącego przez sieć. Wówczas proces monitorowania skupia się na zasobach, z których najczęściej korzystają pracownicy tj. smartfony, serwery, routery, drukarki, przełączniki oraz komputery.

Oprogramowanie monitoringu usprawnia również zarządzanie siecią za pomocą zautomatyzowanych narzędzi, które ułatwiają pracę administratorom. Zaliczają się do nich takie, które śledzą urządzenia dodane lub usunięte z sieci, czy też takie, które miały zmiany konfiguracji. Oszczędzają czas i zapisują dokładne wyniki. Urządzenia są klasyfikowane według typu, usługi, adresu IP, fizycznej lokalizacji oraz są identyfikowane poprzez automatyczne wykrywanie.

Automatyczne narzędzia zapewniające segmentację i kategoryzację mogą pomóc w określeniu, które komponenty sprzętowe są nieużywane lub nie działają z maksymalną wydajnością. Pomaga to zidentyfikować problemy zarządzania zasobami.

System monitoringu infrastruktury sieciowej pomaga zrozumieć dowolne środowisko IT, bez względu na jego złożoność. Administrator wybiera, co chciałby monitorować, a system wspomaga go generując szczegółowy raport. Raporty mogą być dostosowane ze względu na zapotrzebowanie na różne postaci danych. Pomagają administratorom sieci rozwiązać problemy z utraconymi wiadomościami e-mail, zerwanymi połączeniami sieciowymi, identyfikują przeciążone urządzenia, zanim spowodują awarię sieci. Szczegółowe raporty mogą pomóc w identyfikacji zduplikowanych, niepotrzebnych zasobów. Przyniesie to oszczędności finansowe, zmniejszy opóźnienia w przesyłaniu danych i wykryje wszelki wewnętrzny ruch, który stanowi potencjalne zagrożenie bezpieczeństwa oraz zidentyfikuje wąskie gardła w ruchu sieciowym.

Systemy monitorowania infrastruktury teleinformatycznej można wdrożyć jako oprogramowanie układowe (system operacyjny) lub oprogramowanie narzędziowe. Mogą być wdrażane lokalnie lub na zewnętrznym hostingu. Takie oprogramowanie można skonfigurować jako proste lub złożone rozwiązania monitoringu, w celu dostosowania ich do konkretnych wymagań biznesowych.

Rynek oprogramowania do monitorowania sieci jest zróżnicowany. Poza prostymi rozwiązaniami, istnieją kompleksowe, oferujące te najbardziej przydatne narzędzia. W ich skład wchodzą te, które wykonują zarówno wspólne jak i złożone testy, raporty i szczegółowo opisują konkretne problemy oraz systemy graficzne, które obrazowo podsumowują stan sieci, a także określone dane dotyczące każdego urządzenia i całej sieci. Wiele organizacji zleca monitorowanie sieci zewnętrznym firmom, które oferują zewnętrzne usługi monitorowania sieci dwadzieścia cztery godziny na dobę siedem dni w tygodniu, ściśle monitorując kluczowe elementy infrastruktury sieciowej.

Monitorowanie sieci teleinformatycznej dostarcza informacje krytyczne, wymagane do przeprowadzenia przyszłych aktualizacji, zmniejszenia kosztów, zwiększenia wydajności pracy, najlepszego wykorzystania zasobów oraz zapewnienia wysokiej dostępności aplikacji. System monitorowania informuje, jeśli określona usługa, urządzenie lub aplikacja nie spełnia poziomu wydajności, który został wcześniej skonfigurowany. Systemy monitoringu sieci teleinformatycznej w złożonych sieciach są niezastąpione. Koszty związane z zatrzymaniem pracy organizacji mogą znacznie przewyższyć koszty wdrożenia narzędzia monitorowania sieci, które z reguły zapobiega problemom krytycznym.

2 Porównanie systemów monitoringu sieci teleinformatycznych

Istnieje wiele narzędzi, które zapewniają monitorowanie sieci. Szczególnie wyróżniają się tutaj dwa rozwiązania: Nagios oraz Zabbix, które zostały porównane w tabeli 1.

Tabela 1. Porównanie Nagios Core oraz Zabbix [1]

Kategoria	Nagios Core	Zabbix
Pulpit nawigacyjny i interfejs użytkownika	Pulpit nawigacyjny zawiera podstawowe informacje, takie jak stan urządzeń i usług.	Pulpit nawigacyjny można dostosowywać pod własne wymagania.
Konfiguracja	Konfigurację przeprowadza się w plikach tekstowych.	Konfigurację przeprowadza się w interfejsie WWW lub w plikach tekstowych.
Wizualizacja (wykresy)	Domyślnie nie posiada wykresów. Można jednak pobrać wtyczkę NagVis, która ma wbudowane wykresy.	Posiada wbudowane własne wykresy.
Interfejs WWW	Posiada wbudowany interfejs WWW umożliwiający wykonywanie podstawowych czynności, takich jak kontrolowanie kondycji sieci oraz generowanie raportów.	Posiada wbudowany interfejs WWW pozwalający skonfigurować środowisko monitorowania za pomocą interfejsu użytkownika.
Automatyczne wykrywanie	Automatyczne wykrywanie urządzeń, umożliwia pobranie wtyczki NagiosQL.	Brak.
Obsługa protokołów	HTTP, FTP, SMTP, SNMP, POP3, SSH, MySQL.	HTTP, FTP, SMTP, SNMP, POP3, SSH, MySQL.
Alerty i powiadomienia	Posiada wbudowany system alertów i powiadomień, przez e-mail oraz SMS.	Posiada wbudowany system alertów i powiadomień, przez e-mail oraz SMS.
Szablony monitorowania	Brak.	FTP, HTTP, HTTPS, IMAP, LDAP, MySQL, NNTP, SSH, SMTP, POP, Telnet.
Wtyczki	Dużo dodatkowych wtyczek.	Brak.
Społeczność	67 000 użytkowników.	80 000 użytkowników.
Cena	Darmowy, z możliwością wykupienia rozszerzonej wersji Nagios XI.	Darmowy.

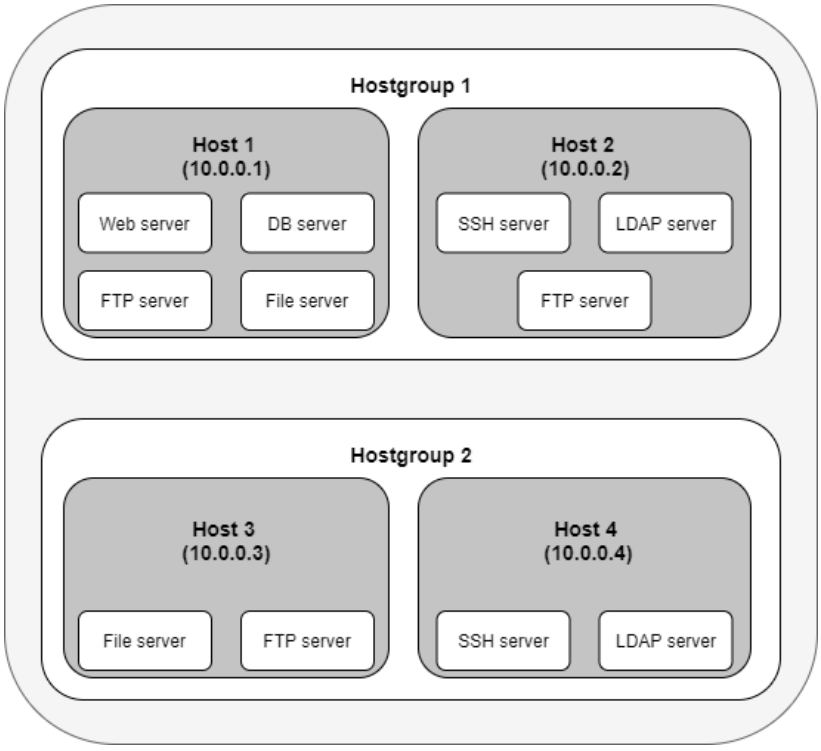
3 Charakterystyka oprogramowania Nagios Core

Nagios jest narzędziem służącym do monitorowania systemów. Oznacza to, że ma wgląd w urządzenia sieciowe, komputery oraz działające na nich usługi. Sprawdza czy działają poprawnie według ustalonych zasad. Głównym założeniem systemu

monitoringu jest jak najszybsze zdiagnozowanie nieprawidłowości związanej z działaniem usługi czy sprzętu. Monitorowanie systemu w Nagios Core obejmuje dwie kategorie obiektów:

1. Hosty – fizyczne urządzenia lub maszyny wirtualne, np. serwery, routery, drukarki, stacje robocze;
2. Usługi – konkretne funkcjonalności np. Serwer SSH może być określony i monitorowany jako usługa.

Każda usługa jest powiązana z hostem, na którym działa. W dodatku, maszyny mogą być przydzielone do grupy hostów (patrz rysunek 1).



Rysunek 1. Przykładowe grupy hostów [1].

Główną zaletą oprogramowania Nagios Core jest mało skomplikowana identyfikacja statusu danego obiektu: Ok, Warning, Critical oraz Unknown. Podejście opierające się na trzech stanach działania pozwala administratorom, którzy ustalają ich limity,

skupić się na ostrzeżeniach oraz stanach krytycznych. Jest to sprawdzona koncepcja, znacznie bardziej wydajna niż analizowanie wykresów pracy danej usługi. Administratorzy systemów zwykle ignorują niektóre rzeczy, jak np. stopniowo malejące miejsce na dysku. Posiadanie ściśle określonych limitów jest o wiele korzystniejsze, ponieważ administrator zawsze wychwytuje problem, niezależnie od tego, czy zmienia się on z ostrzeżenia na błąd krytyczny w ciągu piętnastu minut, czy siedmiu dni. To właśnie robi Nagios – zamienia każdy odczyt z wartości liczbowych (zużycie miejsca na dysku czy obciążenie procesora) na jeden z trzech możliwych stanów działania usługi. Kontrola opiera się pluginach (wtyczkach), więc jeżeli mamy do monitorowania usługę, do której nie udostępniono wtyczki, możemy napisać prosty kod, który będzie ją obsługiwał.

Istnieje wiele powodów, dla których należy się upewnić, że wszystkie nasze zasoby działają jak trzeba. Są to między innymi:

- Zwiększenie jakości świadczenia usług – jeżeli zespół IT może szybciej zauważać nieprawidłowości używając narzędzia monitoringu, zwiększa się jego szybkość reakcji na incydenty. Czasami potrzeba kilku godzin, a nawet dni, aby wykryć problemy. Niestety w tym czasie wielu użytkowników spotyka się z danym błędem. Nagios zapewnia natychmiastowe poinformowanie administratora o zaprzestaniu prawidłowego działania jakiejkolwiek części systemu.
- Znacznie lepsze rozpoznawanie problemu – bardzo często, gdy użytkownicy zgłaszają administratorom awarię, ich zgłoszenie jest dalekie od tego, co jest główną przyczyną problemu. Przykładem może być zgłoszenie o niedziałającym serwerze pocztowym. Odpowiednio skonfigurowany Nagios wskaże, że serwer poczty POP3 nie działa, ponieważ usługa LDAP, od której jest zależny, ma problem.
- Elastyczność w powiadamianiu o tym, co funkcjonuje niepoprawnie – w większych firmach zespoły IT liczą wiele osób. Zazwyczaj ich obowiązki są podzielone. Nagios pozwala na grupowanie maszyn, co umożliwia przydzielenie konkretnych powiadomień do działów IT.
- Monitorowanie zasobów nie tylko ułatwia znajdywanie problemów, pomaga również ich unikać – Nagios inaczej traktuje ostrzeżenia i sytuacje krytyczne. Oznacza to, że administrator jest świadomy sytuacji, które wkrótce mogą stanowić poważne problemy. Przykładem może być kończące się miejsce na

dysku serwera pocztowego. Lepiej jest być świadomym takiej sytuacji, zanim stanie się ona problemem krytycznym.

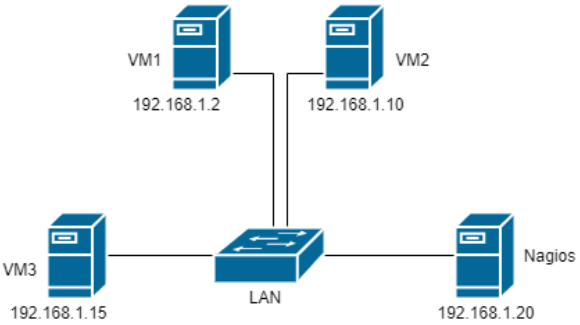
- Centralny serwer Nagios, który odbiera powiadomienia z wielu lokalizacji – monitorowanie można skonfigurować na wielu urządzeniach w różnych lokalizacjach. Następnie te maszyny przekażą wszystkie swoje wyniki do głównego serwera Nagios. Dzięki temu mamy dostęp do wszystkich informacji z jednej maszyny. Daje nam to dokładniejszy obraz infrastruktury IT i umożliwia testowanie złożonych serwerów, takich jak zapory ogniowe.
- Konfigurowanie serwera Nagios poza Intranetem firmy – administratorzy, dzięki takiemu rozwiązaniu, mogą upewnić się, że ruch z Internetu jest prawidłowo blokowany. Wystarczy sprawdzić, czy dana usługa jest dostępna z zewnętrznego adresu IP.

4 Konfiguracja środowiska dla systemu monitoringu Nagios Core

W celu przetestowania systemu monitoringu zostało przygotowane odpowiednie środowisko Hyper-V w infrastrukturze sieciowej (patrz rysunek 2). Skonfigurowano w nim kilka przykładowych usług, pracujących na serwerach z rodziny zarówno Windows Server jak i Linux (patrz tabela 2).

Tabela 2. Wykaz hostów Hyper-V z adresacją IP oraz opisem monitorowanych elementów

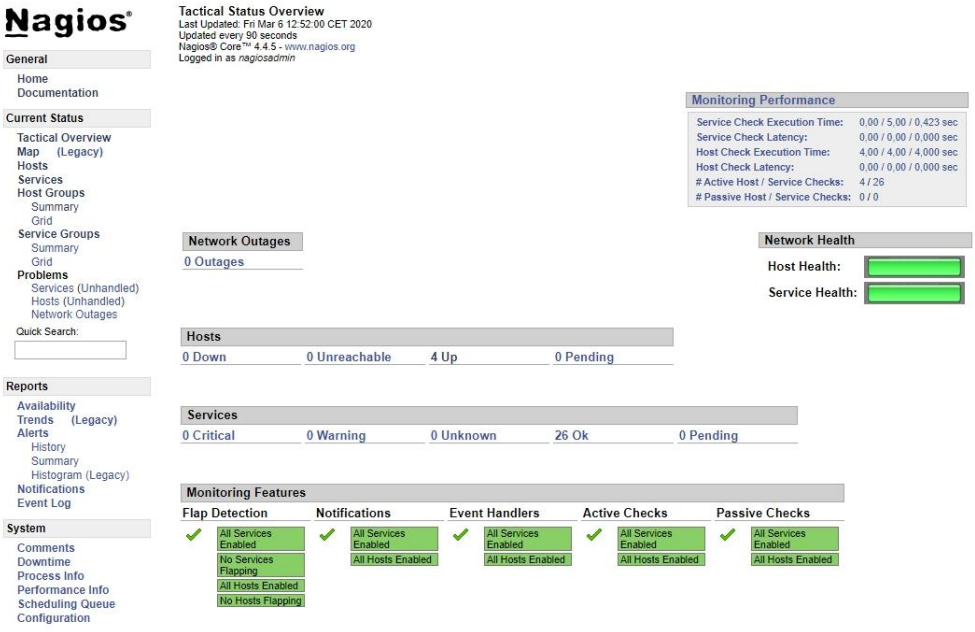
Lp.	Hostname	Opis	Adres IP	Zasoby	Usługi
1	VM1	Win Server 2016 DC DNS / DHCP	192.168.1.2	CPU, RAM, HDD	DNS, DHCP, Uptime
2	VM2	Win Server 2016 DC Serwer Plików	192.168.1.10	CPU, RAM, HDD	Serwer Plików SMB, Uptime
3	VM3	Debian 10.3.0 Serwer Czasu, WWW	192.168.1.15	CPU, RAM, HDD	NTP, Apache2, SSH
4	Nagios	Debian 10.3.0 Serwer monitoringu	192.168.1.20	CPU, RAM, HDD	Nagios Core, SSH



Rysunek 2. Schemat infrastruktury sieciowej

5 Administrowanie systemem Nagios Core

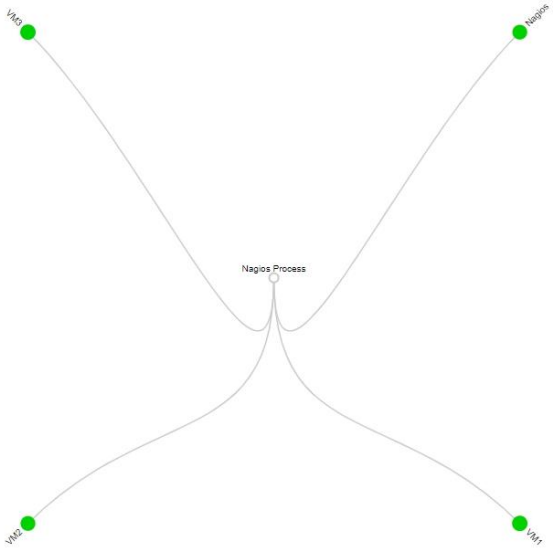
Po zalogowaniu się do systemu Nagios (http://192.168.1.20/nagios), należy przejść do zakładki ***Tactical Status Overwiew*** (patrz rysunek 3).



Rysunek 3. Zakładka ***Tactical Status Overview*** aplikacji Nagios Core

W tej zakładce administrator ma wgląd na całokształt działania systemów, sieci oraz konfiguracji. Można tu sprawdzić status zarówno hostów, jak i usług na nich działających. Ponadto widoczne są tam ustawienia powiadomień oraz odpytywania hostów.

W zakładce ***Map*** (patrz rysunek 4), widać mapę urządzeń. W przypadku pracy w dużych środowiskach teleinformatycznych na wirtualizatorach, np. Hyper-V, można podpiąć hosty pod hypervisior'y tworząc mapę, która ułatwi zidentyfikowanie problemu oraz odszukanie problematycznego hosta.



Rysunek 4. Zakładka ***Map*** interfejsu webowego Nagios Core

Hosts to zakładka, w której znajdują się wylistowane wszystkie hosty podpięte do systemu Nagios. W górnej części można zauważyć informacje zbiorcze odnośnie działania hostów (patrz rysunek 5).

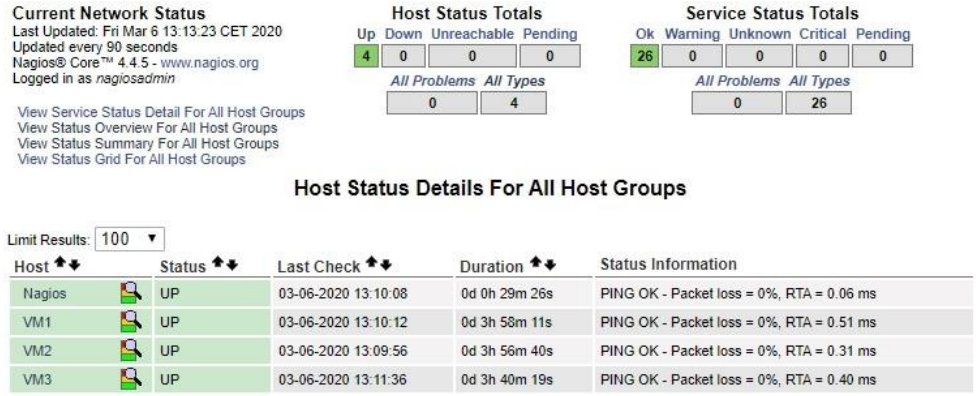
Statusy hostów:

Up – działa;

Down – nie działa;

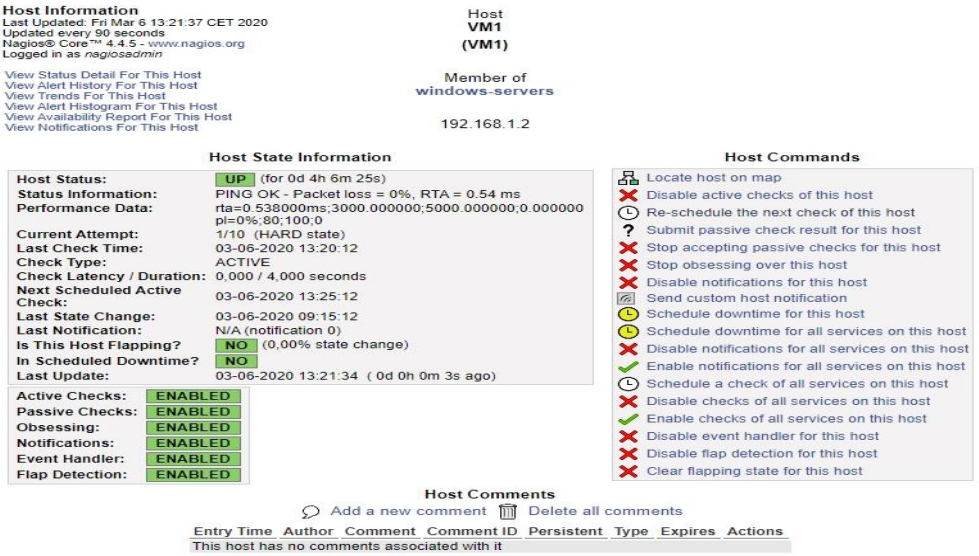
Unreachable – nieosiągalny;

Pending – w oczekiwaniu na odpowiedź hosta.



Rysunek 5. Zakładka ***Hosts*** interfejsu webowego Nagios Core.

Po kliknięciu w wybranego hosta wyświetlą się dodatkowe informacje o statusie hosta oraz ustawienia zdefiniowane dla niego. Można tu m.in. wyłączyć powiadomienia dla tego hosta, wysłać żądanie ponownego odpytania, wyłączyć odpytywanie hosta o usługi czy wyłączyć zbieranie logów. W dolnej części strony widać również miejsce na komentarze, które można dodać w celu informacji o przekonfigurowaniu hosta (rysunek 6).



Rysunek 6. Wyświetlanie informacji o hoście w interfejsie webowym Nagios Core

Services to zakładka, w której wyszczególnione są wszystkie usługi podpięte pod system Nagios Core. W górnej części widzimy informację zbiorczą odnośnie monitorowanych usług (patrz rysunek 7).

Statusy usług:

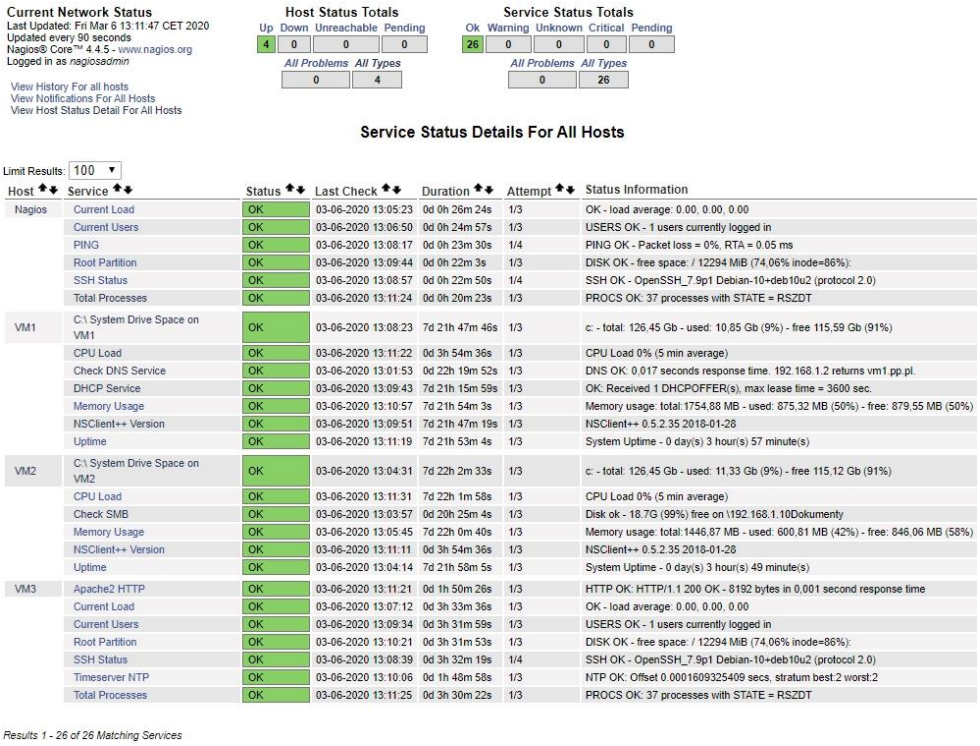
Ok – sprawna;

Warning – ostrzeżenie;

Unknown – nieznana;

Critical – problem krytyczny;

Pending – w oczekiwaniu na odpowiedź hosta.



Current Network Status
Last Updated: Fri Mar 6 13:11:47 CET 2020
Updated every 90 seconds
Nagios® Core™ 4.4.5 - www.nagios.org
Logged in as *nagiosadmin*

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
4	0	0	0

All Problems	All Types
0	4

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
26	0	0	0	0

All Problems	All Types
0	26

Service Status Details For All Hosts

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Nagios	Current Load	OK	03-06-2020 13:05:23	0d 0h 26m 24s	1/3	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	03-06-2020 13:06:50	0d 0h 24m 57s	1/3	USERS OK - 1 users currently logged in
	PING	OK	03-06-2020 13:08:17	0d 0h 23m 30s	1/4	PING OK - Packet loss = 0%, RTA = 0.05 ms
	Root Partition	OK	03-06-2020 13:09:44	0d 0h 22m 3s	1/3	DISK OK - free space: / 12294 MiB (74,06% inode=86%):
	SSH Status	OK	03-06-2020 13:08:57	0d 0h 22m 50s	1/4	SSH OK - OpenSSH_7.9p1 Debian-10+deb10u2 (protocol 2.0)
	Total Processes	OK	03-06-2020 13:11:24	0d 0h 20m 23s	1/3	PROCS OK: 37 processes with STATE = RSZDT
VM1	C:\ System Drive Space on VM1	OK	03-06-2020 13:08:23	7d 21h 47m 46s	1/3	c: - total: 126,45 Gb - used: 10,85 Gb (9%) - free 115,59 Gb (91%)
	CPU Load	OK	03-06-2020 13:11:22	0d 3h 54m 36s	1/3	CPU Load 0% (5 min average)
	Check DNS Service	OK	03-06-2020 13:01:53	0d 22h 19m 52s	1/3	DNS OK: 0,017 seconds response time. 192.168.1.2 returns vm1.pp.pl.
	DHCP Service	OK	03-06-2020 13:09:43	7d 21h 15m 59s	1/3	OK: Received 1 DHCPOFFER(s), max lease time = 3600 sec.
	Memory Usage	OK	03-06-2020 13:10:57	7d 21h 54m 3s	1/3	Memory usage: total:1754,88 MB - used: 875,32 MB (50%) - free: 879,55 MB (50%)
	NSClient++ Version	OK	03-06-2020 13:09:51	7d 21h 47m 19s	1/3	NSClient++ 0.5.2.35 2018-01-28
	Uptime	OK	03-06-2020 13:11:19	7d 21h 53m 4s	1/3	System Uptime - 0 day(s) 3 hour(s) 57 minute(s)
VM2	C:\ System Drive Space on VM2	OK	03-06-2020 13:04:31	7d 22h 2m 33s	1/3	c: - total: 126,45 Gb - used: 11,33 Gb (9%) - free 115,12 Gb (91%)
	CPU Load	OK	03-06-2020 13:11:31	7d 22h 1m 58s	1/3	CPU Load 0% (5 min average)
	Check SMB	OK	03-06-2020 13:03:57	0d 20h 25m 4s	1/3	Disk ok - 18.7G (99%) free on \\192.168.1.10Dokumenty
	Memory Usage	OK	03-06-2020 13:05:45	7d 22h 0m 40s	1/3	Memory usage: total:1446,87 MB - used: 600,81 MB (42%) - free: 846,06 MB (58%)
	NSClient++ Version	OK	03-06-2020 13:11:11	0d 3h 54m 36s	1/3	NSClient++ 0.5.2.35 2018-01-28
	Uptime	OK	03-06-2020 13:04:14	7d 21h 58m 5s	1/3	System Uptime - 0 day(s) 3 hour(s) 49 minute(s)
VM3	Apache2 HTTP	OK	03-06-2020 13:11:21	0d 1h 50m 26s	1/3	HTTP OK: HTTP/1.1 200 OK - 8192 bytes in 0,001 second response time
	Current Load	OK	03-06-2020 13:07:12	0d 3h 33m 36s	1/3	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	03-06-2020 13:09:34	0d 3h 31m 59s	1/3	USERS OK - 1 users currently logged in
	Root Partition	OK	03-06-2020 13:10:21	0d 3h 31m 53s	1/3	DISK OK - free space: / 12294 MiB (74,06% inode=86%):
	SSH Status	OK	03-06-2020 13:08:39	0d 3h 32m 19s	1/4	SSH OK - OpenSSH_7.9p1 Debian-10+deb10u2 (protocol 2.0)
	Timeserver NTP	OK	03-06-2020 13:10:06	0d 1h 48m 58s	1/3	NTP OK: Offset 0.0001609325409 secs, stratum best:2 worst:2
	Total Processes	OK	03-06-2020 13:11:25	0d 3h 30m 22s	1/3	PROCS OK: 37 processes with STATE = RSZDT

Results 1 - 26 of 26 Matching Services

Rysunek 7. Wyświetlanie usług w interfejsie webowym Nagios Core

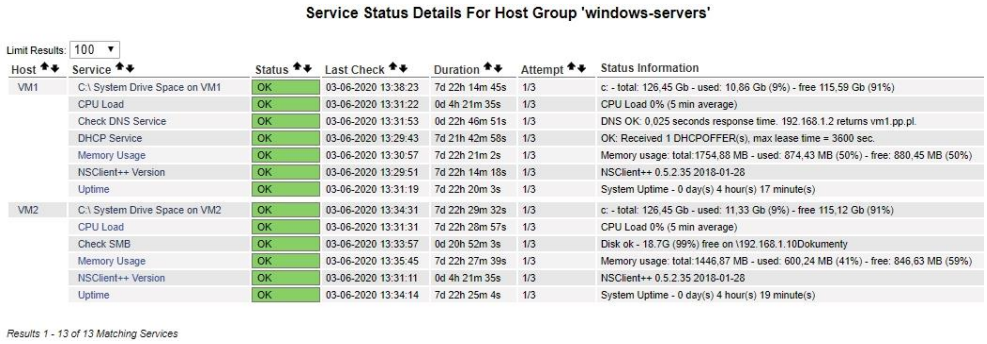
Host Groups to zakładka, w której hosty oraz usługi są podzielone na grupy urządzeń. Na rysunku 8 widać dwie grupy hostów (*linux servers*, *windows servers*) oraz ich status.

Rysunek 8. Zakładka grup hostów w interfejsie webowym Nagios Core

Grupy hostów możemy również wyświetlić w sposób, jak pokazano na rysunku 9, tzn. wybrać opcję ***Grid***.

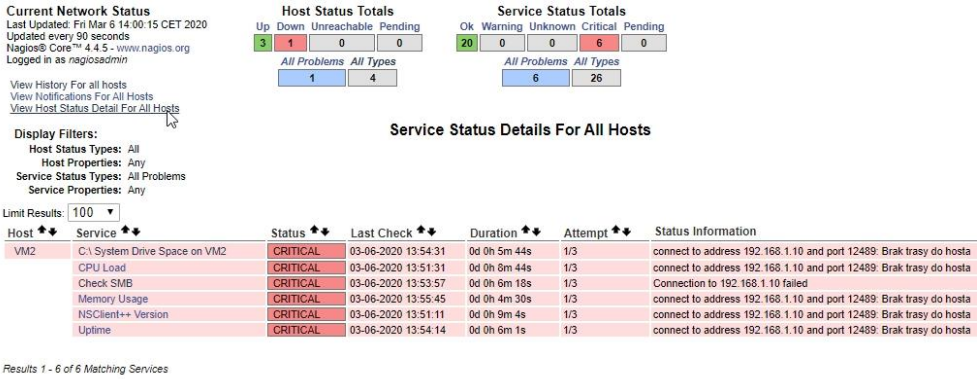
Rysunek 9. Zakładka ***Grid*** interfejsu webowego Nagios Core

Po kliknięciu w jedną z grup pokażą nam się hosty oraz usługi z wybranej grupy (patrz rysunek 10).



Rysunek 10. Wyświetlanie usług grupy hostów w interfejsie webowym Nagios Core

W zakładce ***Problems*** widzimy wszystkie aktualnie występujące problemy z hostami oraz usługami czy siecią (patrz rysunek 11).



Rysunek 11. Wyświetlanie problemów w interfejsie webowym Nagios Core

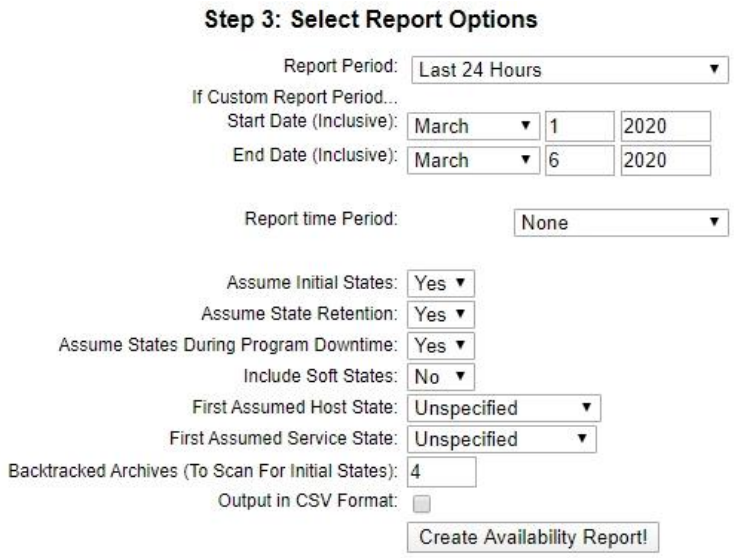
Następną grupą zakładek są raporty. W celu wygenerowania raportu dostępności (availability), wybieramy typ raportu i przechodzimy do następnego kroku (patrz rysunek 12).

Rysunek 12. Generowanie raportu w interfejsie webowym Nagios Core

Teraz należy wybrać, które hostgroupy mają być uwzględnione.

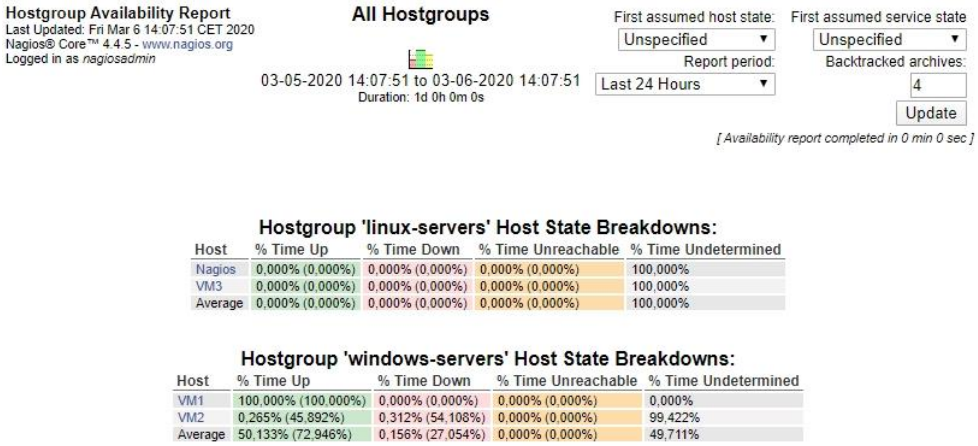
W kolejnym kroku wybieramy przedział czasowy raportu oraz opcje, na podstawie których będzie generowany raport (patrz rysunek 13).

Można również wybrać opcje stworzenia raportu do pliku CSV.



Rysunek 13. Generowanie raportu w interfejsie webowym Nagios Core

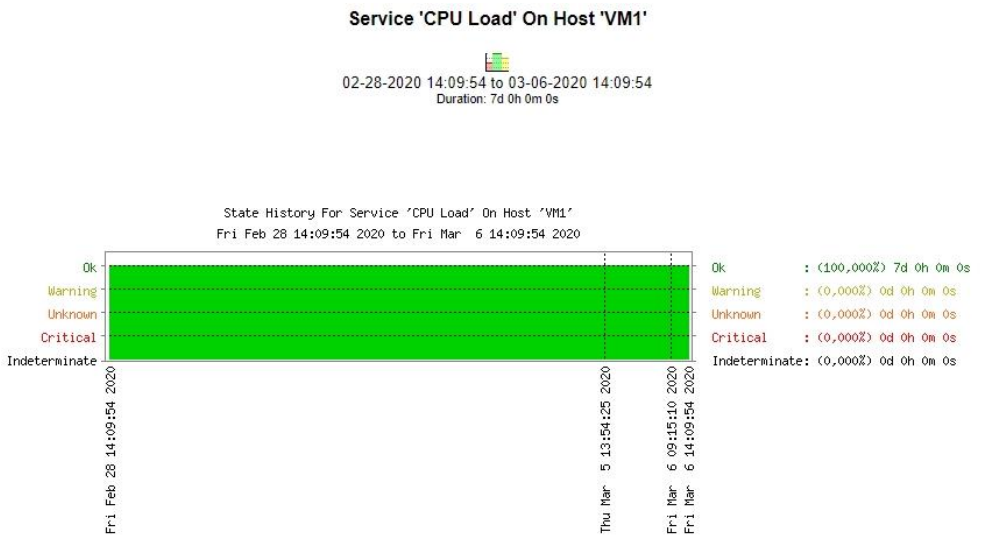
Na rysunku 14 widać przykład wygenerowanego raportu z ostatnich 24 godzin. Przedstawia on w procentach czas, w którym wybrana maszyna działała w danym statusie.



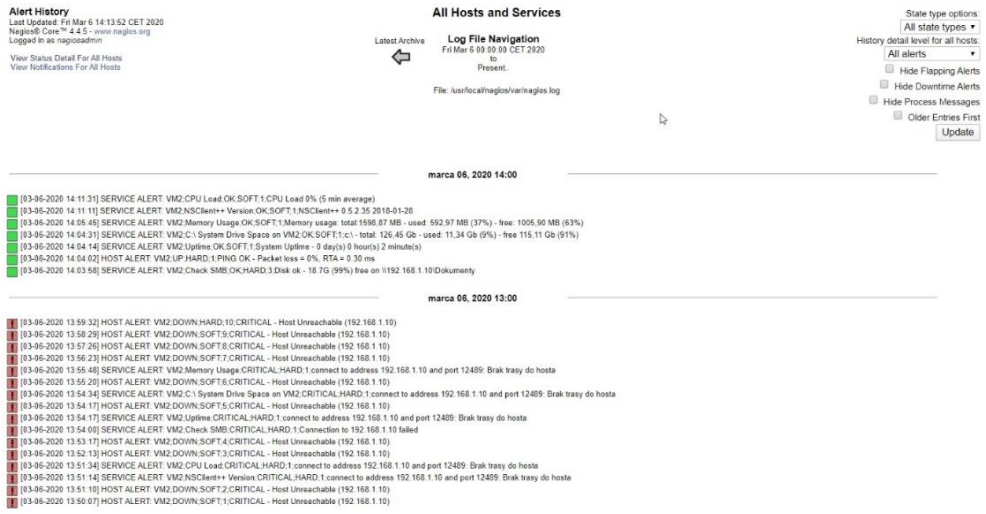
Rysunek 14. Wygenerowany raport w interfejsie webowym Nagios Core

Korzystając z raportu ***Trends*** można również stworzyć raport z działania usługi lub hosta (rysunek 15).

W zakładce ***Alerts*** można zobaczyć historię wszystkich alarmów (patrz rysunek 16). Można również użyć opcji filtrowania w celu wyszczególnienia np. statusów.

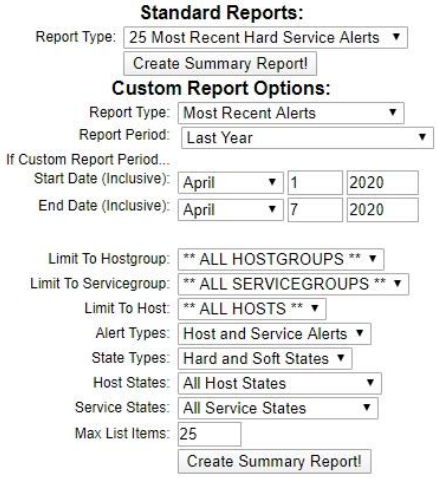


Rysunek 15. Raport ***Trends*** w interfejsie webowym Nagios Core



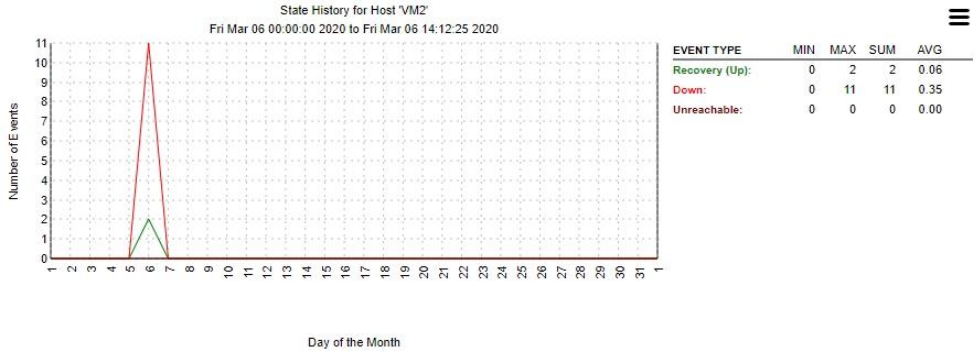
Rysunek 16. Logi z alertami w interfejsie webowym Nagios Core

Zakładka ***Alerts Summary*** umożliwia generowanie podsumowania np. rocznego ze wszystkich usług, które sprawiały najwięcej problemów (patrz rysunek 17).



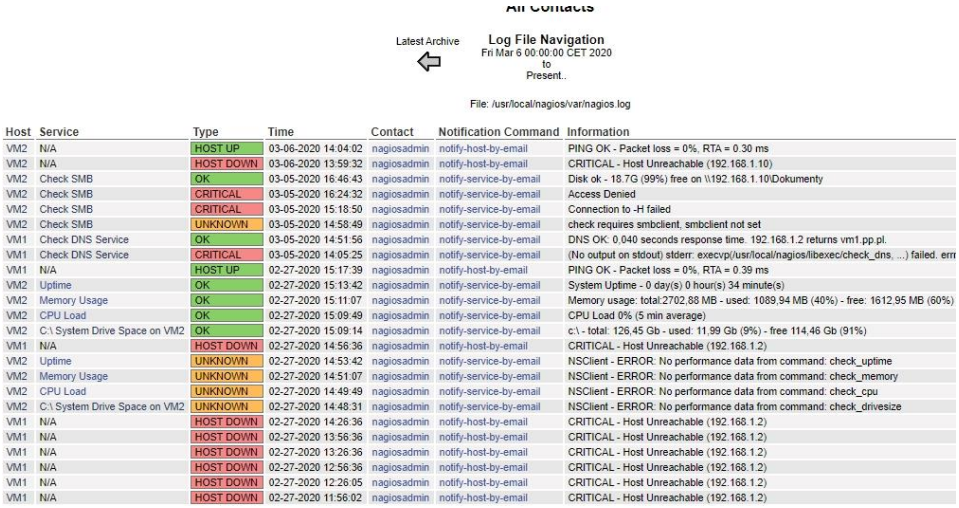
Rysunek 17. Generowanie sumarycznego logu z alertami w interfejsie webowym Nagios Core

Istnieje również opcja stworzenia wykresu z działania wybranego hosta, co widać na rysunku 18.



Rysunek 18. Wygenerowany wykres w interfejsie webowym Nagios Core

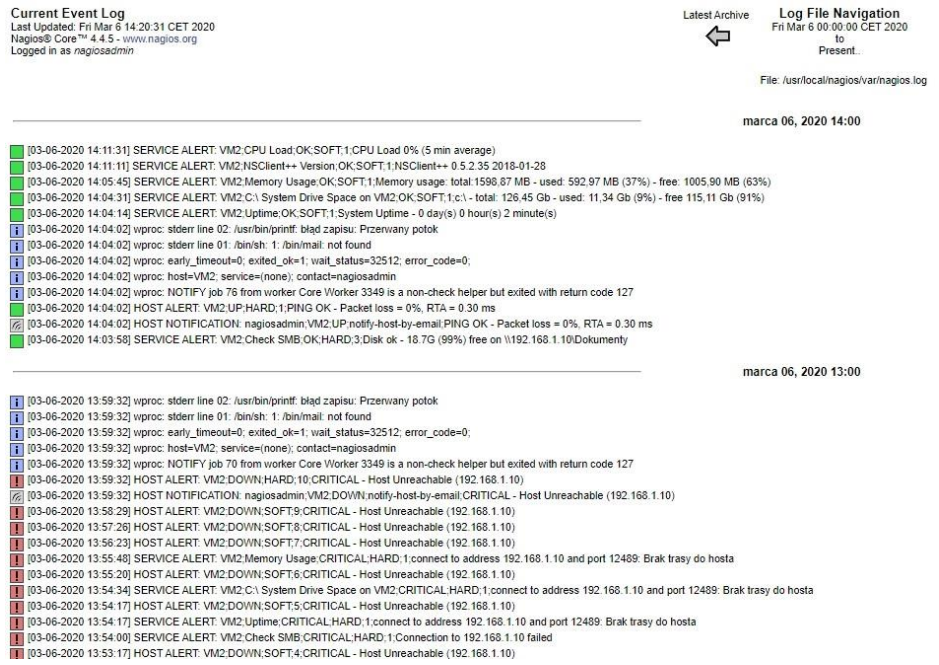
Zakładka ***Notifications*** odpowiada za wyświetlanie pliku *nagios.log*, w którym znajdują się powiadomienia usług oraz hostów (rysunek 19).



Host	Service	Type	Time	Contact	Notification Command	Information
VM2	N/A	HOST UP	03-06-2020 14:04:02	nagiosadmin	notify-host-by-email	PING OK - Packet loss = 0%, RTA = 0.30 ms
VM2	N/A	HOST DOWN	03-06-2020 13:59:32	nagiosadmin	notify-host-by-email	CRITICAL - Host Unreachable (192.168.1.10)
VM2	Check SMB	OK	03-05-2020 16:46:43	nagiosadmin	notify-service-by-email	Disk ok - 18.7G (99%) free on \\192.168.1.10\Dokumenty
VM2	Check SMB	CRITICAL	03-05-2020 16:24:32	nagiosadmin	notify-service-by-email	Access Denied
VM2	Check SMB	CRITICAL	03-05-2020 15:18:50	nagiosadmin	notify-service-by-email	Connection to -H failed
VM2	Check SMB	UNKNOWN	03-05-2020 14:58:49	nagiosadmin	notify-service-by-email	check requires smbclient, smbclient not set
VM1	Check DNS Service	OK	03-05-2020 14:51:56	nagiosadmin	notify-service-by-email	DNS OK: 0,040 seconds response time. 192.168.1.2 returns vm1.pp.pl.
VM1	Check DNS Service	CRITICAL	03-05-2020 14:05:25	nagiosadmin	notify-service-by-email	(No output on stdout) stderr: execvp(/usr/local/nagios/libexec/check_dns, ...) failed. errr
VM1	N/A	HOST UP	02-27-2020 15:17:39	nagiosadmin	notify-host-by-email	PING OK - Packet loss = 0%, RTA = 0.39 ms
VM2	Uptime	OK	02-27-2020 15:13:42	nagiosadmin	notify-service-by-email	System Uptime - 0 day(s) 0 hour(s) 34 minute(s)
VM2	Memory Usage	OK	02-27-2020 15:11:07	nagiosadmin	notify-service-by-email	Memory usage: total:2702,88 MB - used: 1089,94 MB (40%) - free: 1612,95 MB (60%)
VM2	CPU Load	OK	02-27-2020 15:09:49	nagiosadmin	notify-service-by-email	CPU Load 0% (5 min average)
VM2	C:\ System Drive Space on VM2	OK	02-27-2020 15:09:14	nagiosadmin	notify-service-by-email	c:\ - total: 126,45 Gb - used: 11,99 Gb (9%) - free 114,46 Gb (91%)
VM1	N/A	HOST DOWN	02-27-2020 14:56:36	nagiosadmin	notify-host-by-email	CRITICAL - Host Unreachable (192.168.1.2)
VM2	Uptime	UNKNOWN	02-27-2020 14:53:42	nagiosadmin	notify-service-by-email	NSClient - ERROR: No performance data from command: check_uptime
VM2	Memory Usage	UNKNOWN	02-27-2020 14:51:07	nagiosadmin	notify-service-by-email	NSClient - ERROR: No performance data from command: check_memory
VM2	CPU Load	UNKNOWN	02-27-2020 14:49:49	nagiosadmin	notify-service-by-email	NSClient - ERROR: No performance data from command: check_cpu
VM2	C:\ System Drive Space on VM2	UNKNOWN	02-27-2020 14:48:31	nagiosadmin	notify-service-by-email	NSClient - ERROR: No performance data from command: check_drivesize
VM1	N/A	HOST DOWN	02-27-2020 14:26:36	nagiosadmin	notify-host-by-email	CRITICAL - Host Unreachable (192.168.1.2)
VM1	N/A	HOST DOWN	02-27-2020 13:56:36	nagiosadmin	notify-host-by-email	CRITICAL - Host Unreachable (192.168.1.2)
VM1	N/A	HOST DOWN	02-27-2020 13:26:36	nagiosadmin	notify-host-by-email	CRITICAL - Host Unreachable (192.168.1.2)
VM1	N/A	HOST DOWN	02-27-2020 12:56:36	nagiosadmin	notify-host-by-email	CRITICAL - Host Unreachable (192.168.1.2)
VM1	N/A	HOST DOWN	02-27-2020 12:26:05	nagiosadmin	notify-host-by-email	CRITICAL - Host Unreachable (192.168.1.2)
VM1	N/A	HOST DOWN	02-27-2020 11:56:02	nagiosadmin	notify-host-by-email	CRITICAL - Host Unreachable (192.168.1.2)

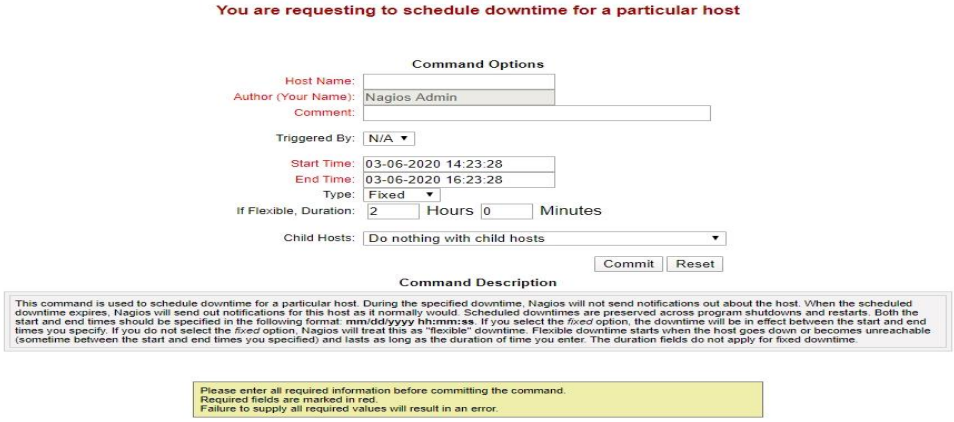
Rysunek 19. Zakładka powiadomień w interfejsie webowym Nagios Core

Zakładka ***Event Log*** wyświetla wszystkie zdarzenia, grupując je w cogodzinne grupy (rysunek 20).



Rysunek 20. Zakładka ***Event Log*** w interfejsie webowym Nagios Core

W zakładce ***Downtime*** można wygenerować planowane wyłączenie hosta lub usługi (patrz rysunek 21). Ograniczy to liczbę błędnych alertów oraz logów w systemie Nagios.

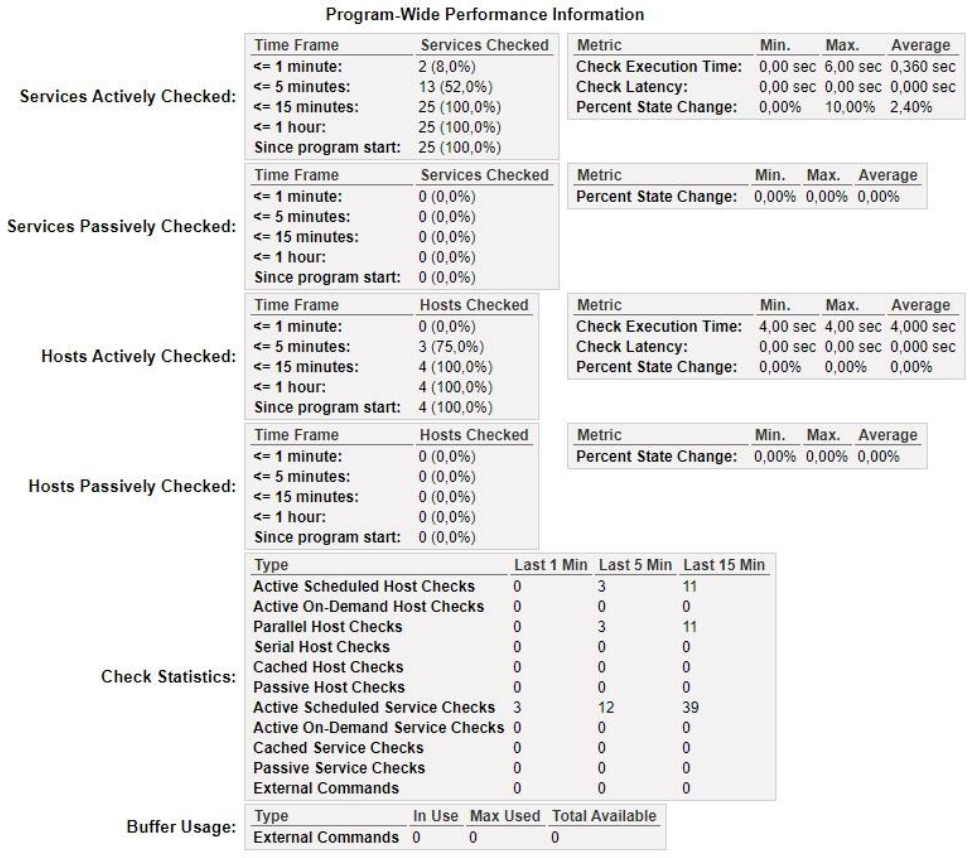


Rysunek 21. Zakładka ***Downtime*** w interfejsie webwym Nagios Core

Zakładka ***Process Info***, wyświetla informacje o zainstalowanym oprogramowaniu Nagios Core. Można z tego poziomu również wykonać podstawowe czynności m.in. restart serwera, wyłączenie powiadomień, wyłączenie odpytywania czy wyłączenie zbierania logów (patrz rysunek 22).

Rysunek 22. Zakładka ***Process Info*** w interfejsie webowym Nagios Core

W zakładce ***Performance Info*** widać aktualne statystyki działania usług oraz hostów. Można tam sprawdzić między innymi liczbę sprawdzeń usług oraz hostów w zdefiniowanych odstępach czasowych, co widać na rysunku 23.



Program-Wide Performance Information

Services Actively Checked:

Time Frame	Services Checked
<= 1 minute:	2 (8,0%)
<= 5 minutes:	13 (52,0%)
<= 15 minutes:	25 (100,0%)
<= 1 hour:	25 (100,0%)
Since program start:	25 (100,0%)

Metric	Min.	Max.	Average
Check Execution Time:	0,00 sec	6,00 sec	0,360 sec
Check Latency:	0,00 sec	0,00 sec	0,000 sec
Percent State Change:	0,00%	10,00%	2,40%

Services Passively Checked:

Time Frame	Services Checked
<= 1 minute:	0 (0,0%)
<= 5 minutes:	0 (0,0%)
<= 15 minutes:	0 (0,0%)
<= 1 hour:	0 (0,0%)
Since program start:	0 (0,0%)

Metric	Min.	Max.	Average
Percent State Change:	0,00%	0,00%	0,00%

Hosts Actively Checked:

Time Frame	Hosts Checked
<= 1 minute:	0 (0,0%)
<= 5 minutes:	3 (75,0%)
<= 15 minutes:	4 (100,0%)
<= 1 hour:	4 (100,0%)
Since program start:	4 (100,0%)

Metric	Min.	Max.	Average
Check Execution Time:	4,00 sec	4,00 sec	4,000 sec
Check Latency:	0,00 sec	0,00 sec	0,000 sec
Percent State Change:	0,00%	0,00%	0,00%

Hosts Passively Checked:

Time Frame	Hosts Checked
<= 1 minute:	0 (0,0%)
<= 5 minutes:	0 (0,0%)
<= 15 minutes:	0 (0,0%)
<= 1 hour:	0 (0,0%)
Since program start:	0 (0,0%)

Metric	Min.	Max.	Average
Percent State Change:	0,00%	0,00%	0,00%

Check Statistics:

Type	Last 1 Min	Last 5 Min	Last 15 Min
Active Scheduled Host Checks	0	3	11
Active On-Demand Host Checks	0	0	0
Parallel Host Checks	0	3	11
Serial Host Checks	0	0	0
Cached Host Checks	0	0	0
Passive Host Checks	0	0	0
Active Scheduled Service Checks	3	12	39
Active On-Demand Service Checks	0	0	0
Cached Service Checks	0	0	0
Passive Service Checks	0	0	0
External Commands	0	0	0

Buffer Usage:

Type	In Use	Max Used	Total Available
External Commands	0	0	0

Rysunek 23. Zakładka ***Performance Info*** w interfejsie webowym Nagios Core

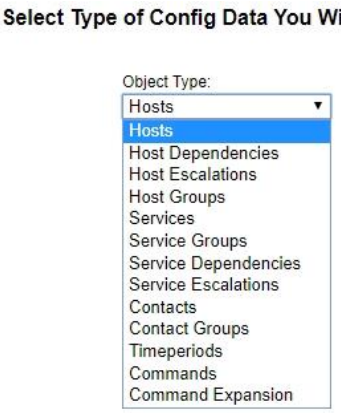
Na rysunku 24 pokazano zakładkę ***Scheduling Queue***, w której wyświetlana jest kolejka odpytywania usług. Możemy z tego poziomu usunąć z kolejki odpytywanie określonej usługi lub przełożyć ją na inny, wybrany termin.

Entries sorted by **next check time** (ascending)

Host	Service	Last Check	Next Check	Type	Active Checks	Actions
VM2	NSClient++ Version	04-07-2020 13:27:17	04-07-2020 13:37:17	Normal	ENABLED	
VM3	Timeserver NTP	04-07-2020 13:27:40	04-07-2020 13:37:40	Normal	ENABLED	
VM1		04-07-2020 13:33:10	04-07-2020 13:38:10	Normal	ENABLED	
VM1	NSClient++ Version	04-07-2020 13:28:26	04-07-2020 13:38:26	Normal	ENABLED	
VM2	Uptime	04-07-2020 13:28:49	04-07-2020 13:38:49	Normal	ENABLED	
VM3	Total Processes	04-07-2020 13:29:12	04-07-2020 13:39:12	Normal	ENABLED	
VM2		04-07-2020 13:34:25	04-07-2020 13:39:25	Normal	ENABLED	
Nagios	Total Processes	04-07-2020 13:29:35	04-07-2020 13:39:35	Normal	ENABLED	
VM1	Uptime	04-07-2020 13:29:58	04-07-2020 13:39:58	Normal	ENABLED	
VM3	Apache2 HTTP	04-07-2020 13:30:21	04-07-2020 13:40:21	Normal	ENABLED	
VM3		04-07-2020 13:35:40	04-07-2020 13:40:40	Normal	ENABLED	
VM1	C:\ System Drive Space on VM1	04-07-2020 13:31:07	04-07-2020 13:41:07	Normal	ENABLED	
VM3	SSH Status	04-07-2020 13:36:08	04-07-2020 13:41:08	Normal	ENABLED	
VM2	C:\ System Drive Space on VM2	04-07-2020 13:31:31	04-07-2020 13:41:31	Normal	ENABLED	
VM3	Current Load	04-07-2020 13:31:54	04-07-2020 13:41:54	Normal	ENABLED	
VM3	Current Users	04-07-2020 13:31:55	04-07-2020 13:41:55	Normal	ENABLED	
VM2	CPU Load	04-07-2020 13:31:55	04-07-2020 13:41:55	Normal	ENABLED	
VM1	CPU Load	04-07-2020 13:31:55	04-07-2020 13:41:55	Normal	ENABLED	
Nagios	SSH Status	04-07-2020 13:36:55	04-07-2020 13:41:55	Normal	ENABLED	
Nagios		04-07-2020 13:36:56	04-07-2020 13:41:56	Normal	ENABLED	
Nagios	Current Load	04-07-2020 13:33:27	04-07-2020 13:43:27	Normal	ENABLED	
VM1	Check DNS Service	04-07-2020 13:33:50	04-07-2020 13:43:50	Normal	ENABLED	
VM2	Check SMB	04-07-2020 13:34:13	04-07-2020 13:44:13	Normal	ENABLED	
VM3	Root Partition	04-07-2020 13:34:36	04-07-2020 13:44:36	Normal	ENABLED	
Nagios	Current Users	04-07-2020 13:34:59	04-07-2020 13:44:59	Normal	ENABLED	
VM1	DHCP Service	04-07-2020 13:35:22	04-07-2020 13:45:22	Normal	ENABLED	
VM2	Memory Usage	04-07-2020 13:35:45	04-07-2020 13:45:45	Normal	ENABLED	
Nagios	Root Partition	04-07-2020 13:36:31	04-07-2020 13:46:31	Normal	ENABLED	
VM1	Memory Usage	04-07-2020 13:36:54	04-07-2020 13:46:54	Normal	ENABLED	

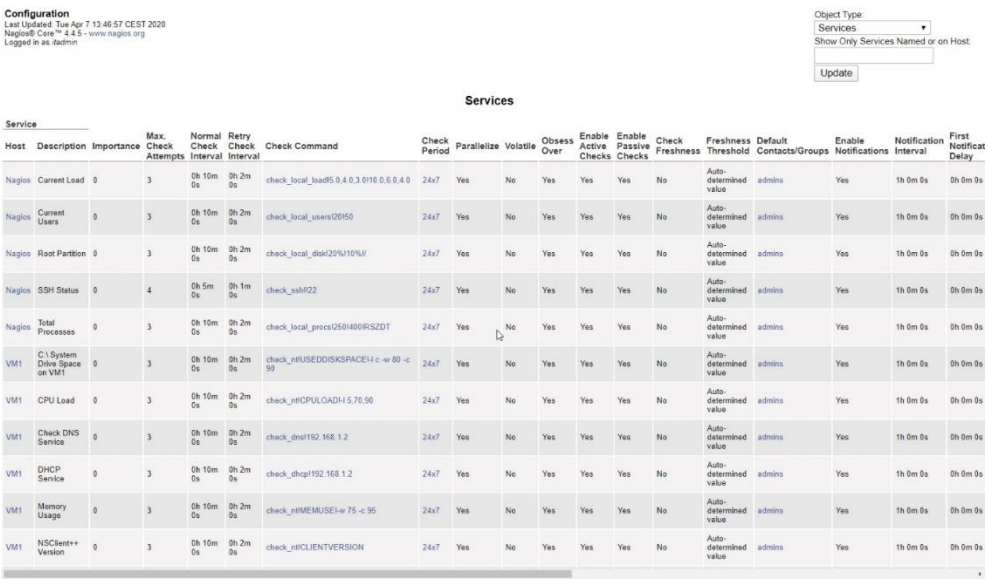
Rysunek 24. Zakładka ***Scheduling Queue*** w interfejsie webowym Nagios Core

Zakładka ***Configuration*** umożliwia podgląd ustawień plików konfiguracyjnych. Typy obiektów, które można wyświetlić, widoczne są na rysunku 25.



Rysunek 25. Zakładka ***Configuration*** w interfejsie webowym Nagios Core

Na rysunku 26 została wyświetlona konfiguracja usług, którą możemy dowolnie filtrować.



Rysunek 26. Podgląd konfiguracji usług w interfejsie webowym Nagios Core

W tym panelu można również wyświetlić plik z ustawieniami poleceń. Wyświetlają się polecenia wbudowane w system Nagios Core oraz te, które zostały dopisane (patrz rysunek 27).

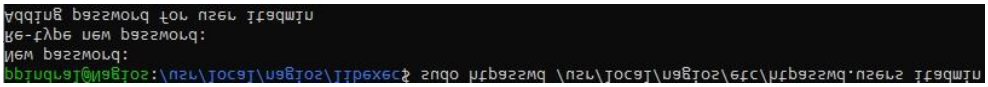
Commands

Command Name	Command Line
check-host-alive	$USER1$/check_ping -H $HOSTADDRESS$ -w 3000.0,80% -c 5000.0,100% -p 5
check_dhcp	$USER1$/check_dhcp $ARG1$
check_disk_smb	$USER1$/check_disk_smb -H $ARG1$ -s $ARG2$
check_dns	$USER1$/check_dns -H $ARG1$ -s $HOSTADDRESS$
check_ftp	$USER1$/check_ftp -H $HOSTADDRESS$ $ARG1$
check_hpjd	$USER1$/check_hpjd -H $HOSTADDRESS$ $ARG1$
check_http	$USER1$/check_http -I $HOSTADDRESS$ $ARG1$
check_imap	$USER1$/check_imap -H $HOSTADDRESS$ $ARG1$
check_local_disk	$USER1$/check_disk -w $ARG1$ -c $ARG2$ -p $ARG3$
check_local_load	$USER1$/check_load -w $ARG1$ -c $ARG2$
check_local_mrtgtraf	$USER1$/check_mrtgtraf -F $ARG1$ -a $ARG2$ -w $ARG3$ -c $ARG4$ -e $ARG5$
check_local_procs	$USER1$/check_procs -w $ARG1$ -c $ARG2$ -s $ARG3$
check_local_swap	$USER1$/check_swap -w $ARG1$ -c $ARG2$
check_local_users	$USER1$/check_users -w $ARG1$ -c $ARG2$
check_nt	$USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -s zaq1@WSX -v $ARG1$ $ARG2$
check_ntp_time	$USER1$/check_ntp_time -H $ARG1$ -w $ARG2$ -c $ARG3$
check_ping	$USER1$/check_ping -H $HOSTADDRESS$ -w $ARG1$ -c $ARG2$ -p 5
check_pop	$USER1$/check_pop -H $HOSTADDRESS$ $ARG1$
check_smtp	$USER1$/check_smtp -H $HOSTADDRESS$ $ARG1$
check_snmp	$USER1$/check_snmp -H $HOSTADDRESS$ $ARG1$
check_ssh	$USER1$/check_ssh $ARG1$ $HOSTADDRESS$
check_tcp	$USER1$/check_tcp -H $HOSTADDRESS$ -p $ARG1$ $ARG2$
check_udp	$USER1$/check_udp -H $HOSTADDRESS$ -p $ARG1$ $ARG2$
notify-host-by-email	/usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type: $NOTIFICATIONTYPE$\nHost: $HOSTNAME$\nState: $HOSTSTATE$ $NOTIFICATIONTYPE$ Host Alert: $HOSTNAME$ is $HOSTSTATE$ **" $CONTACTEMAIL$
notify-service-by-email	/usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type: $NOTIFICATIONTYPE$\n\nService: $SERVICEDESC$\nHost: $HOSTA Info:\n\n$SERVICEOUTPUT$\n" | /bin/mail -s "** $NOTIFICATIONTYPE$ Service Alert: $HOSTALIAS$/$SERVICEDESC$ is $SEF
process-host-perfdata	/usr/bin/printf "%b" "$LASTHOSTCHECK$\t$HOSTNAME$\t$HOSTSTATE$\t$HOSTATTEMPT$\t$HOSTSTATETYPE$\t$HOSTE
process-service-perfdata	/usr/bin/printf "%b" "$LASTSERVICECHECK$\t$HOSTNAME$\t$SERVICEDESC$\t$SERVICESTATE$\t$SERVICEATTEMPT$\t$SERVICESTATETY /usr/local/nagios/var/service-perfdata.out

Rysunek 27. Podgląd konfiguracji poleceń w interfejsie webowym Nagios Core

W kolejnym kroku przedstawiono proces zakładania konta *itadmin* oraz przypisywania uprawnień w systemie Nagios Core (patrz rysunek 28). Na serwerze Nagios należy wywołać polecenie:

$ sudo htpasswd /usr/local/nagios/etc/htpasswd.users itadmin.



Rysunek 28. Zakładanie konta do interfejsu webowego Nagios Core

Następnie należy edytować plik cgi.cfg:

$ sudo nano /usr/1oca1/nagios/etc/cgi.cfg.

W kolejnym kroku należy odnaleźć poniższe wpisy oraz dopisać po przecinku *itadmin*, w celu dodania pełnych uprawnień dla drugiego administratora:

authorized_f or_system_information=nagiosadmin, itadmin
authorized_for_confiquration_information=nagiosadmin, itadmin
authorized_for_system_commands=nagiosadmin, itadmin
authorized_for_all_services=nagiosadmin, itadmin
authorized_for_all_hosts=nagiosadmin, itadmin
authorized_for_a11_service_commands=nagiosadmin, itadmin
authorized_for_all_host_commands=nagiosadmin, itadmin.

Po zapisaniu pliku należy zrestartować usługę Nagios, pisząc polecenie:

$ sudo systemctl restart Nagios.

6 Podsumowanie

Monitorowanie systemów teleinformatycznych to jeden z głównych obowiązków administratorów IT. Zwiększenie gwarantowanego poziomu świadczenia usług (SLA – ang. *Service Level Agreement*), poprawa wydajności pracowników firmy, zmniejszenie strat spowodowanych przestojem w działaniu systemów to tylko kilka z wielu usprawnień, które wnosi system monitoringu. Zastosowanie takiego systemu gwarantuje jasny wgląd w wydajność oraz pracę infrastruktury sieciowej. W związku z tym, niezależnie od wielkości firmy, niezbędne jest wdrożenie takiego systemu.

Oprogramowanie Nagios Core posiada wiele zróżnicowanych metod wyświetlania danych m.in. są to logi, wykresy, diagramy. Niestety przy oprogramowaniu Nagios Core wszelkie zmiany wykonujemy na plikach tekstowych z poziomu terminala maszyny, a nie jak w przypadku niektórych systemów, gdzie służy do tego interfejs przeglądarkowy. Utrudnia to przede wszystkim najprostsze czynności administracyjne, takie jak założenie nowego użytkownika Nagios Core czy dodanie nowego sprzętu, który ma być monitorowany. Pomimo trudności z konfiguracją, system Nagios Core jest jednym z najlepszych systemów do monitorowania sieci teleinformatycznych. Posiada on wszystkie niezbędne funkcje, jest darmowy i niczym nie odbiega od konkurencji.

Oprogramowanie Nagios Core spełnia wszystkie założenia dotyczące monitoringu sieci teleinformatycznych. Odpowiednia konfiguracja tego systemu znacznie poprawia dostępność sieci, zwiększając przy tym jakość świadczonych usług.

Bibliografia

[1] W. Kocjan, *Learning Nagios 4*, Birmingham, UK: Packt Publishing Ltd., 2014.

IT system implementation for network infrastructure monitoring

Abstract

The paper concerns contemporary computer networks monitoring. This enables immediate reaction to various irregularities in the functioning of the ICT infrastructure or breaches of security rules. Currently, monitoring systems are implemented in every organization, regardless of its size or activity profile. Network monitoring is a necessary requirement, especially in companies where the work is based mainly on IT systems. Many companies implement such solutions to minimize problems with the ICT infrastructure, and to improve computer network performance and employee productivity.

The paper presents the implementation process of Nagios Core in version 4.4.5 – one of the most popular monitoring systems of modern computer networks.

Keywords: *computer networks, monitoring, security systems, information systems*