Podstawowe dane zapisywane w plikach systemu rozliczeń

- Nazwa rekordu
- Czas wykorzystania procesora (oddzielnie dla użytkowników i systemu)
- Czas działania
- Czas uaktywnienia procesów
- ID użytkownika i grupy procesów
- Wykorzystanie pamięci
- Liczba odczytanych i zapisanych znaków
- Liczba odczytanych i zapisanych bloków dyskowych
- Terminal, z którego zainicjowano proces
- Stan wskaźników procesu (łącznie ze statusem wyjścia)

Zestawienia generowane przez program *sa*

Zestawienie podstawowe

11345	414534.56re	5367.64cp	15avio	145k	login
3457	1324.45re	1243.34cp	122avio	23k	touch
34643	2007.56re	453.45cp	12avio	54k	rm
656	455.76re	345.87cp	346avio	10k	grep
43	1533.43re	436.54cp	2345avio	8k	find

Niektóre przyrostki w raportach tworzonych przez program *sa*

brak - liczba wywołań
cp, cpu- zużycie CPU (przez system i użytkownika) w minutach
re - całkowity czas działania w minutach
avio - średnia liczba operacji we/wy podczas jednego wywołania
k - średnie wykorzystanie pamięci w kB
k*sec - łączna ilość pamięci w kB * sek
tio - suma operacji we/wy podczas wszystkich wywołań
s - czas CPU dla systemu
u - czas CPU dla użytkownika

Opcje sortujące polecenia *sa*

-b - wg sumarycznego wykorzystania pamięci
-d - wg średniej liczby operacji we/wy
-D - wg sumy wszystkich operacji we/wy
-k - wg średniego wykorzystania pamięci
-K - wg łącznej zajętości pamięci liczonej w kB*sek
-n - wg liczby wywołań

```
Apr 16 13:10 2000  DAILY USAGE REPORT FOR iarsco1 Page 1

     LOGIN     CPU (MINS)       KCORE-MINS   CONNECT (MINS)      DISK      #OF  #OF   #DISK    FEE
UID  NAME     PRIME  NPRIME    PRIME  NPRIME    PRIME  NPRIME     BLOCKS    PROCS SESS  SAMPLES
--   TOTAL     2         0    96        12     21912   3400      0         413    841      0    0
0    root      1         0    74         8      1078    12       0         231    80       0    0
200  furtak    0         0    2          0      96      12       0         19     9        0    0
202  koniec    0         0    0          0      3       0        0         0      1        0    0
203  zsuski    0         0    5          2      1127    287      0         68     104      0    0
204  chudy     0         0    2          0      119     0        0         23     28       0    0
2101 c4101     0         0    0          0      370     168      0         0      12       0    0
2102 c4102     0         0    0          0      360     0        0         0      2        0    0
2103 c4103     0         0    0          0      356     0        0         0      4        0    0
2126 c4301     0         0    0          0      732     11       0         0      19       0    0
2127 c4302     0         0    0          0      680     10       0         0      23       0    0
2128 c4303     0         0    0          0      443     0        0         0      10       0    0
```

```
Apr 16 13:02 2000  DAILY COMMAND SUMMARY Page 1

                                    TOTAL COMMAND SUMMARY
COMMAND    NUMBER      TOTAL       TOTAL       TOTAL    MEAN     MEAN      HOG          CHARS      BLOCKS
NAME         CMDS    KCOREMIN    CPU-MIN    REAL-MIN  SIZE-K  CPU-MIN  FACTOR       TRNSFD       READ

TOTALS   1269149      107.13        1.88      7391.23   56.92     0.00     0.00     11512845        2436

accountG    3073       17.21        0.14         1.30  123.54     0.00     0.11       505280          44
ls        175161       11.60        0.22         1.00   51.61     0.00     0.23       373977         237
sh        119847        7.65        0.17        89.49   44.01     0.00     0.00      1086027         538
login      46095        7.07        0.14      7161.81   51.62     0.00     0.00      1662912         123
pcidossv   12292        7.02        0.23        28.67   30.45     0.00     0.01      1820616         252
telnetd    43022        6.21        0.12        72.41   51.77     0.00     0.00      1311232         201
scoadmin    6146        6.02        0.07         2.33   80.93     0.00     0.03       285824         150
html2asc   24584        1.46        0.03         0.04   58.21     0.00     0.67       109438           1
man        55314        1.34        0.05         3.93   27.45     0.00     0.01       464021         102
telnet     12292        1.23        0.04         6.62   32.64     0.00     0.01        22733           1
passwd      9219        1.19        0.02         0.70   50.99     0.00     0.03       193648         103
more       49168        1.17        0.04         6.72   26.81     0.00     0.01       119619          13
last       18438        0.97        0.04         0.24   24.24     0.00     0.16       340864          26
sendmail   82971        0.89        0.01         0.04   96.69     0.00     0.22        34668           0
```

Plik /etc/syslog.conf

podsystem_wysyłający.poziom_zagrożenia ***wyjście***

Podsystemy_wysyłające (niektóre):

kern - jądro systemu
mail - podsystem pocztowy
lpr - podsystem drukowania
daemon - demon systemowy
auth - system identyfikacji użytkownika (login, su, itp.)
cron - demon ***crond***
ftp - demon ***ftpd***
news - system wiadomości
syslog - demon ***syslogd***
user - procesy uzytkowników

Poziomy zagrożenia:

emerg - stan najwyższego zagrożenia
alert - poważne błędy wymagające natychmiastowego przeciwdziałania
crit - błędy krytyczne (np dysku)
err - błędy
warn - ostrzeżenie
notice - komunikat
info - informacja

Planowanie polityki *audytu w Windows NT*

1. **Jakie zdarzenia rejestrować ?**
   - **wykorzystanie poszczególnych plików i katalogów**
   - **logowania użytkowników**
   - **uruchomienia i zatrzymania systemu**
   - **zmiany w definicji grup i użytkowników**
   - **zmiany w polityce bezpieczeństwa**

2. **Czy rejestrować dozwolone dostępy do zasobów ?**
   - **statystyki o wykorzystaniu poszczególnych zasobów**

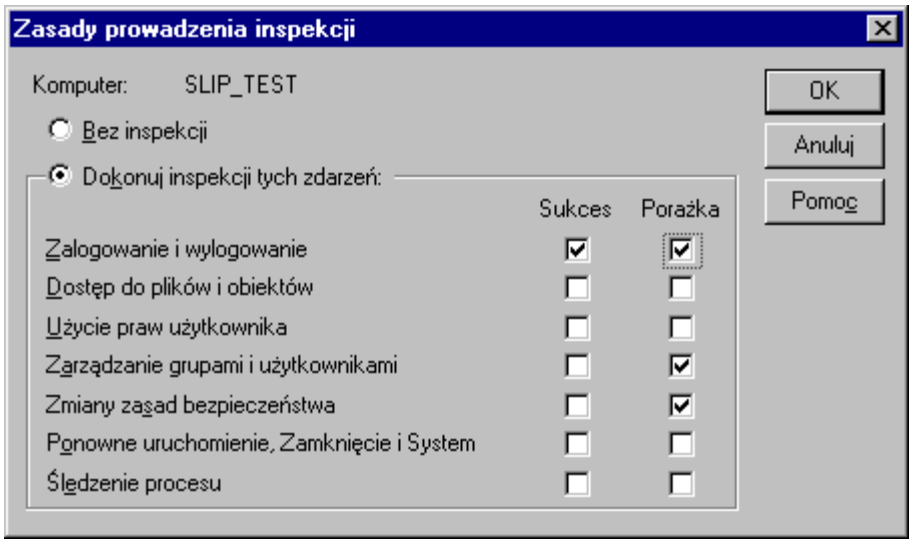
3. **Czy rejestrować niedozwolone dostępy do zasobów ?**
   - **próby złamania zabezpieczeń**

4. **Jakie trendy należy śledzić ?**
   - **plan archiwacji kronik**

Nadmierny audyt powoduje duże obciążenie systemu i duże zużycie zasobów pamięciowych

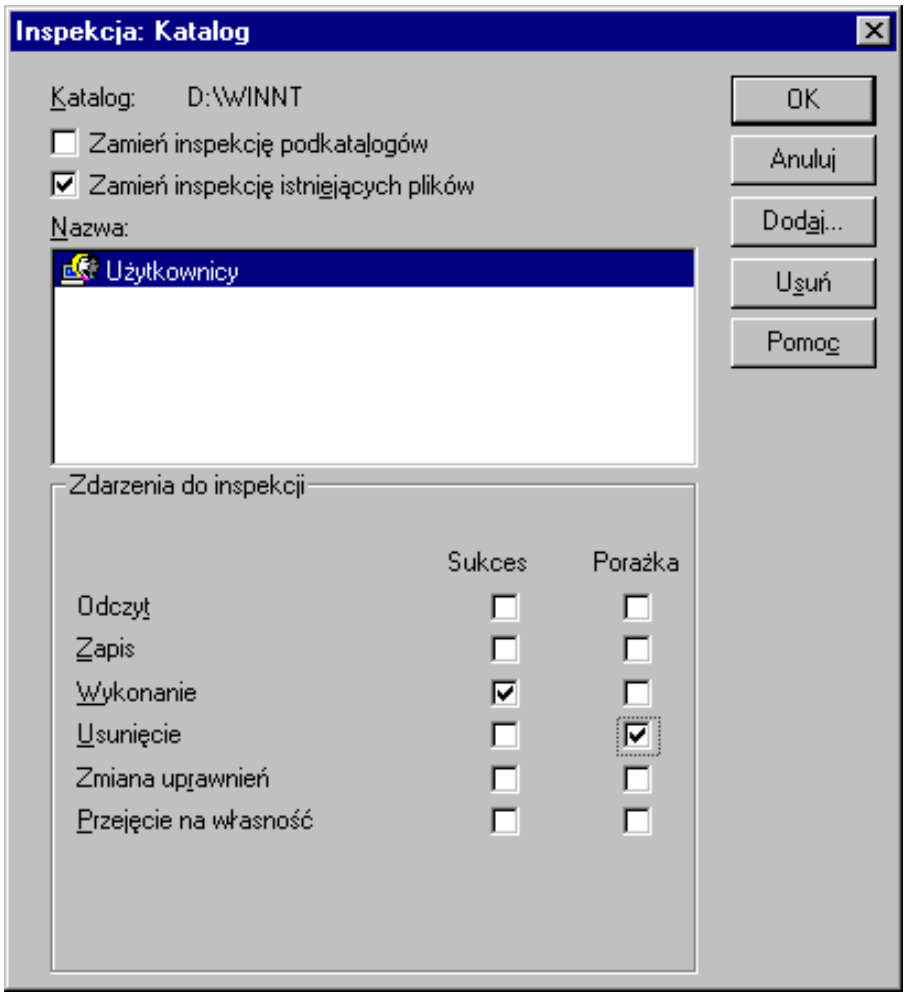
Definiowanie polityki inspekcji w Windows NT

Inspekcja zdarzeń



Definiowanie polityki inspekcji w Windows NT

Inspekcja plików i katalogów



Definiowanie polityki inspekcji w Windows NT

Inspekcja drukarek