Podstawowe narzędzia do monitorowania

Należące do systemu:

`uptime`	-	*load average*
`who -b`	-	*boot time*
`who -r`	-	*run level*
`ps`	-	lista plików w systemie

Public domain software:

`top`	-	bieżące monitorowanie najaktywniejszych procesów
`lsof`	-	lista plików otwartych przez proces

Rejestr zdarzeń: syslog

mechanizm centralnego rejestrowania zdarzeń z określonym poziomem pilności i kategorią podsystemu, serwer rejestruje na pliku(ach) komunikaty wybrane według specyfikacji zadanej przez administratora:

/etc/syslog.conf:

```
*.err;kern.notice;auth.notice;user.none      /dev/console
*.err;kern.debug;daemon.notice;auth.none; \
 daemon.none;lpr.none;mail.none;user.none    /var/adm/messages

*.alert;kern.err;daemon.err;user.none        operator
*.alert;user.none                            root

*.emerg;user.none                            *
auth.notice                                  ifdef(‘LOGHOST’, /var/log/authlog, @loghost)

auth.debug                                   /var/log/authlog
daemon.debug                                 /var/log/daemonlog
mail.debug                                   /var/log/maillog
local0.debug                                 /var/log/iplog
local1.info                                  /var/log/tcplog
local2.debug                                 /var/log/sshlog
lpr.debug                                    /var/log/lprlog
mark.debug                                   /var/log/syslog
```


- syslog i tworzone przezeń rejestry są jednym z podstawowych narzędzi pracy administratora systemu

- ALE, intensywne rejestrowanie zdarzeń nie ma sensu, jeśli nie analizuje się ich na bieżąco i nie wyciąga wniosków

- konieczne jest okresowe skracanie rejestrów

System activity report — sar

`sar -c`	-	system calls
`sar -d`	-	disk activity
`sar -g`	-	paging
`sar -k`	-	kernel memory
`sar -m`	-	message queues, semaphores
`sar -p`	-	paging
`sar -q`	-	run queue/swap queue length
`sar -r`	-	memory
`sar -u`	-	cpu
`sar -w`	-	system swapping, process switches

System accounting

`acctcom` - wszystkie procesy uruchamiane w systemie

System plików `/proc`

Wirtualny system plików `/proc` miał w założeniu wypełnić lukę brakujących narzędzi badania różnych atrybutów procesów. Jednocześnie miał powstać standardowy, jednolity interface do takiego badania.

Pierwszy cel został osiągnięty. System plików `/proc` doczekał się bogatej implementacji na większości współczesnych Unixach. Niestety, zarówno zakres dostępnych informacji o procesach, jak i metody dostępu do tych informacji kompletnie różnią się między systemami.

Np. Linux: pliki w katalogach /proc/* są tekstowe i można je czytać.

Np. Solaris: pliki w /proc/* są binarne i czytelne za pomocą narzędzi:
`man proc`: `ptree`, `pstack`, pfiles=, ...

Narzędzia systemu Solaris

`iostat -xtc 5`	-	statystyki wejścia/wyjścia
`prstat -m`	-	statystyki aktywnych procesów
`mpstat 5`	-	statystyki procesora/ów
`vmstat -s`	-	statystyki pamięci wirtualnej