Serwer Syslog z wykorzystaniem systemu Linux.

W systemie Linux za gromadzenie informacji o zdarzeniach odpowiedzialny jest mechanizm: rsyslog (dawniej – syslog).

Pliki konfiguracyjne odpowiedzialne za działanie tej usługi (i nie tylko tej):

rsyslog - /etc/rsyslog.conf – plik zawierający konfigurację mechanizmu wraz z definicją logowanych zdarzeń,

logrotate - /etc/logrotate – plik zawierający konfigurację mechanizmu odpowiedzialnego za porządkowanie utworzonych logów – planowanie czasu przechowywania logów czy definicja rozmiarów plików zawierających przechwycone zdarzenia.

By móc prowadzić skuteczną rejestrację wystąpienia danych sytuacji w pierwszej kolejności musimy zdecydować jakie kategorie zdarzeń muszą podlegać logowaniu.

Kategorie zdarzeń (selektor), które mogą podlegać logowaniu to:

auth,authpriv - autoryzacja użytkowników,

kern - jądro systemowe,

security - logi bezpieczeństwa,

user - aplikacje wykorzystywane przez użytkowników,

mail - zdarzenia związane z pocztą,

lpr - komunikaty dotyczące obsługi drukarek i procesu wydruku,

ftp - logi serwera ftp,

cron - informacje dotyczące deamona cron.

Po definicji interesującej nas kategorii należy określić ich poziom:

Poziom	Nazwa poziomu	Definicja syslog	Opis
0	Emergency	EMERG	Najwyższy priorytet. Tak jak w przypadku routerów/przełączników awaria na tyle poważna, że uniemożliwia uruchomienie systemu.
1	Alert	ALERT	Potrzebna natychmiastowa interwencja

2	Critical	CRIT	Sytuacja krytyczna
3	Error	ERR	Błędy w działaniu usługi
4	Warning	WARNING	Ostrzeżenie
5	Notice	NOTICE	Powiadomienie, ważniejsze zdarzenia
6	Informational	INFO	Komunikaty informacyjne
7	Debug	DEBUG	Szczegółowe informacje o działaniu danego procesu

Przykładowe wpisy:

security.* /var/log/security - logi bezpieczeństwa o każdym priorytecie będą zapisywane w pliku: /var/log/security,

*.warning;mail.none;ftp.none /var/log/warning - logi wszystkich kategorii o priorytetach od emergency do warning (włącznie) będą zapisywane w pliku: /var/log/warning Rejestracji nie podlegają logi kategorii: mail oraz ftp,

auth.=crit /var/log/authcrit - logi dotyczące kategorii auth będą zapisywane w pliku: /var/log/authcrit Rejestracji podlegają tylko zdarzenia o priorytecie critical (brak rejestracji zdarzeń dotyczących poziomów wyższych).

Sprawdzenie statusu usługi rsyslog następuje po wydaniu polecenia: /etc/init.d/rsyslog status Jak widać poniżej usługa działa a jej numer PID to 3637

Dodatkowo sterowanie usługą możemy kontrolować za pomocą parametrów:

1 - stop - zatrzymanie usługi rsyslog,

2 - start - uruchomienie usługi,

3 - restart - zrestartowanie usługi np. celem wprowadzenia nowych ustawień.

Tak więc aby móc zacząć rejestrować interesujące nas zdarzenia musimy określić kategorię oraz podać poziom zdarzeń, które rejestracji mają podlegać.

Rejestrację zdarzeń określamy poprzez definicję roli. Konfiguracja danej roli odbywa się poprzez edycję pliku: /etc/rsyslog.conf bądź jak w naszym przypadku poprzez edycję pliku: /etc/rsyslog.d/50-default.conf (generalnie definicja roli odbywa się w pliku rsyslog.conf lecz jak to bywa zasada ta nie zawsze jest regułą, w Ubuntu 14.04 oraz 16.04 rolę tą przejął plik: 50-default.conf)