Temat: Diagnozowanie i monitorowanie systemu za pomocą oprogramowania narzędziowego w Linux.

Bezpieczeństwo systemu komputerowego zależy nie tylko od tego, jak jest zabezpieczony przed intruzami. Bardzo ważne dla bezpieczeństwa jest to, czy administrator ma dostępne informacje o funkcjonowaniu systemu. Dobre narzędzie do monitorowania pracy systemu jest niezbędne do jego użytkowania i zabezpieczania.

W systemie GNU/Linux, podobnie jak w systemach Unix, stosuje się pakiet Syslog, który umożliwia monitorowanie systemu. Jest to program o bardzo dużych możliwościach, lecz wymagający,

podobnie jak inne narzędzia systemowe, odpowiedniej konfiguracji.

Program Syslog jest jednym z najważniejszych narzędzi systemowych. Umożliwia rejestrowanie zdarzeń zachodzących w systemie przy pomocy zcentralizowanego mechanizmu. Pozwala na rejestrowanie informacji pochodzących z trzech źródeł: zgłoszeń przekazywanych przez bibliotekę systemową, oraz informacji pochodzących od jadra systemu. Przyjmowaniem informacji zgłaszanych przez bibliotekę systemową zajmuje się demon syslogd.

Aplikacje, najczęściej różne demony, przekazują informacje poprzez standardową funkcje syslog.

Są one następnie przekazywane do demona syslogd, który w zależności od ich typu i priorytetu, zapisuje je w odpowiednich plikach, tak zwanych *plikach rejestrowych* (ang. *log files*). Każdy

wpis do pliku rejestrowego dokonywany przez syslogd zawiera informacje dotyczące czasu jego powstania, maszyny i procesu.

Raporty od jadra systemu Linux zbiera demon klogd. Ponieważ mają one inna postać niż te, które przekazuje biblioteka systemowa, zostają poddane obróbce przed przesłaniem ich do syslogd. Ta obróbka polega na opatrzeniu ich informacjami o typie i priorytecie wiadomości zgodnymi z syslogd. Syslog ma jeszcze jeden interfejs umożliwiający wymianę zbieranych informacji. Obsługuje mianowicie gniazda UDP umożliwiające przesyłanie wiadomości pomiędzy różnymi maszynami w sieci.

Podstawowy mechanizm generowania raportów zapewnia

aplikacjom biblioteka systemowa. Udostępnia one trzy funkcje: openlog(), syslog() i closelog(), które umożliwiają odpowiednio: otwarcie komunikacji (stworzenie deskryptora), przesłanie wiadomości i zamkniecie komunikacji. Z tych funkcji korzystają demony i aplikacje pracujące w systemie. Możliwe jest przesyłanie wiadomości do Syslog również z poziomu skryptów, na przykład skryptów w sh. Wygodnie jest do tego wykorzystać program logger, który wysyła informacje poprzez syslogd. Natomiast w skryptach napisanych w języku Perl można użyć pakietu Sys::Syslog, który jest interfejsem do opisanych powyżej wywołań funkcji systemowych.

Syslog by spełniać dobrze swoje funkcje powinien być uruchamiany jako jeden z pierwszych demonów. Uruchamia się go przeważnie przez wywołanie ze skryptów startowych podczas uruchamiania

systemu. W dystrybucjach Debian/GNU i RedHat skrypt nazywa się po prostu syslogdi znajduje się w katalogu /etc/init.d lub /etc/rc.d/init.d. Skrypt, oprócz standardowych opcji start i stop przyjmuje również restart i reload, które powodują odpowiednio zatrzymanie i ponowne uruchomienie Syslog, oraz powtórne przeczytanie pliku konfiguracyjnego. Skrypt zatrzymuje i uruchamia demon syslogd oraz klogd.