

Porady: Syslog

Rejestrowanie zdarzeń systemowych

Systemy uniksowe zbierają komunikaty w centralnym repozytorium, ułatwiając ich zarządzanie i radzenie sobie z powstałymi problemami. Syslog jest usługą, od której wcześniej czy później uzależniają się wszyscy administratorzy systemów.

MARC ANDRE SELIG

Większość programów generuje dwa rodzaje danych. Jednym z nich są standardowe dane, których się spodziewamy, np. gra będzie generować obrazy na ekranie, a klient FTP będzie pobierał dane z serwera. W trakcie działania programu może on generować także raporty postępu. Gra może informować użytkownika o zakończeniu inicjalizacji karty graficznej. W tym samym czasie może zgłaszać brak joysticka. Z kolei klient FTP może informować użytkownika o ustanowieniu połączenia lub o brakującym pliku. Tak więc pomiędzy danymi głównymi generowanymi przez program, a komunikatami diagnostycznymi tego programu, jest znacząca różnica.

Uruchomione programy wyświetlają interaktywnie komunikaty diagnostyczne bezpośrednio na ekranie. Powodują wyskakiwanie okien dialogowych spotykanych typowo w pakietach biurowych. Demony zajmujące się usługami uruchamianymi w tle, nie powinny jednak ujawniać się na ekranie monitora. Generowane przez nie komunikaty zwracałyby niepotrzebnie głowę użytkownikowi pracującemu na konsoli, szczególnie w chwilach, kiedy miałyby niewiele lub nic wspólnego z obecnie wykonywanym przez niego zdaniem. Jednak najgorsza sytuacja występuje wtedy, gdy komunikaty są po pro-

stu gubione w natłoku innych zadań i pozostają w tym stanie do czasu, gdy ktoś będzie ponownie pracował na konsoli.

Rozwiązaniem tego problemu są pliki protokołu. Jeżeli program działający w tle musi wygenerować komunikat diagnostyczny, konieczne jest użycie jakiegoś pliku. Jest to odwieczny problem serwerów, a nawet takie systemy operacyjne jak Windows posiadają podstawowe pliki dziennika. Tworzenie osobnych plików dziennika dla poszczególnych aplikacji nie jest wydajnym rozwiązaniem. Zasoby systemowe zostałyby pochłonięte w znacznej mierze przez dużą liczbę otwartych plików – skąd zatem dany program ma wiedzieć, gdzie przechowywać swoje dane? Z kolei umożliwienie programistom decydowania o miejscu przechowywania plików dziennika doprowadziłoby do kompletnego chaosu.

Syslog

Większość systemów uniksowych korzysta z wydajnego i praktycznego rozwiązania, jakim jest syslog. Komunikaty, zamiast być przechowywane w plikach, przekazywane są do demona centralnego przy pomocy funkcji z biblioteki. Demon dokonuje sortowania wpisów i decyduje o ich dalszych losach, stosując dwa kryteria przy podjęciu decyzji: priorytet i źródło komunikatu.

Niektóre komunikaty są na tyle istotne (np. komunikaty krytyczne), że syslog niezwłocznie informuje wszystkich użytkowników zalogowanych do systemu. Przykładowo, jeżeli stan akumulatorów w naszym laptopie jest bardzo niski, powinniśmy o tym zostać poinformowani jak najszybciej, nawet (a może szczególnie wtedy) gdy korzystamy właśnie z edytora tekstów. Przeciwnieństwem będzie tutaj np. status obciążenia lokalnej pamięci podręcznej DNS, który jest dla nas w zasadzie nieistotny.

Sortowanie komunikatów według ich źródła pochodzenia jest także pomocne. Wielu administratorów zbiera komunikaty poczty przy-



chodzącej i wychodzącej w określonym pliku. Umożliwia to generowanie na tej podstawie statystyk ruchu w sieci lub kontrolę stanu brakujących wiadomości. Poza tym, niektóre z tych wiadomości mogą być poufne. Usuwanie problemów dotyczących modułu uwierzytelniania lub demona PPP może ujawnić nam hasła w formie tekstowej. Pliki dziennika tego rodzaju wymagają zatem lepszej ochrony niż statystyki dostępu do serwera sieci Web. Takie przypadki usprawiedliwiają, a wręcz zmuszają nas do przechowywania tych informacji w oddzielnych plikach.

Oczywiście od każdej reguły jest wyjątek i ta prosta zasada znajduje swoje potwierdzenie także przy rejestrowaniu zcentralizowanym w systemie Unix. Rysunek 1 pokazuje ogólny schemat najważniejszych mechanizmów i wyjątków. Większość programów wysyła komunikaty do demona syslog o nazwie syslogd, w celu sortowania i przekazania ich we właściwe miejsce. Komunikaty dotyczące jądra systemu wysyłane są jednak do demona rejestrującego jądro – klogd. Demon zwykle przesyła je do syslog. Z kolei programy wykonujące wiele operacji rejestrowania korzystają zwykle ze swoich plików we własnym zakresie – dobrym przykładem jest tutaj Apache.

Syslog od środka

Większość obecnych dystrybucji przechowuje pliki syslog w katalogu `/var/log` – oczywiście możemy skonfigurować ścieżkę dostępu do tych plików wedle własnego uznania. Na Listingu 1 pokazano kilka typowych przykładów wpisów syslog.

Format komunikatu tworzony jest zawsze według tego samego wzorca podstawowego. Na początku znajduje się data i czas, po których podawana jest nazwa komputera (w naszym przykładzie komputer nazywał się `undine`) oraz właściwy komunikat, rozpoczynający się nazwą programu, z którego pochodzi i numerem procesu w nawiasie kwadratowym.

Pierwszy komunikat, znajdujący się na Listingu 1, został wygenerowany przez jądro (kernel). Komputer z kartą sieciową WLAN znajdował się zbyt daleko od swojego punktu dostępu. Jak już pokazaliśmy to na rysunku 1, demon rejestrujący jądro przekazał komunikat do demona syslog. Problem, który wywołał pojawienie się tego komunikatu, trwał kilkanaście sekund. W tym czasie jądro wygenerowało cały zestaw identycznych ostrzeżeń. Syslog potrafi rozpoznawać takie powtórzenia i stosuje proste rozwiązanie, które zaoszczędza miejsce na dysku i czas administratorów – zamiast powtarzać wiadomość za każdym razem, syslog wypisuje po prostu ilość wystąpień komunikatu.

Trzecia i czwarta linijka zawierają wiadomości wygenerowane przez programy zewnętrzne. W tym przypadku demon CRON wydał polecenie, a użytkownik `mas` użył programu `su`, aby uzyskać uprawnienia użytkownika głównego (`root-a`). Za format komunikatu odpowiedzialne są tutaj same programy. CRON używa dużych liter i podaje identyfikator, `su` jest pod tym względem znacznie skromniejszy. W dolnej linijce znajduje się komunikat samego syslogd. Usługa korzysta ze swego rodzaju wskaźników, które pojawiają się okresowo, oznaczając brak jakiegokolwiek aktywności wartej zapisania w dzienniku. Jest to bardzo użyteczna funkcja, szczególnie podczas wykonywania ekspertyzy sądowej, umożliwia ona bowiem potwierdzenie działania systemu

przed wystąpieniem awarii. Na szczęście system Linux nie choruje zbyt często na awarie i zawieszenia systemu, zdarza się więc, że administratorzy wyłączają tę funkcję.

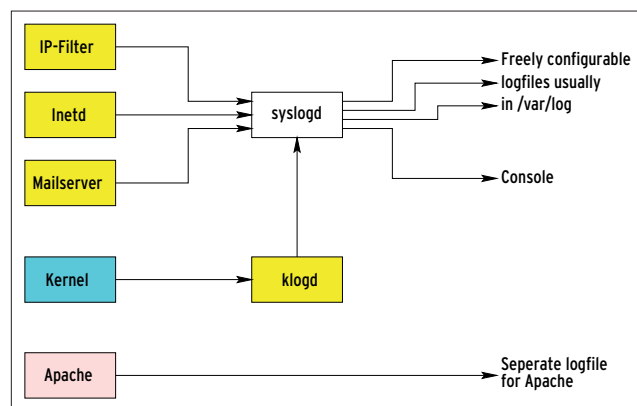
Konfiguracja

Jedną z najpraktyczniejszych cech syslog jest możliwość jego szczegółowej konfiguracji. Administrator może zdecydować, gdzie przechowywać pliki dziennika – do tego celu uży-

wany jest główny plik konfiguracyjny `/etc/syslog.conf` (Listing 2). Plik konfiguracyjny przypisuje źródłom komunikatu (po lewej) miejsce przeznaczenia pliku dziennika (po prawej). Źródło składa się z tzw. funkcji, będącej obszarem funkcjonalnym systemu, z którego pochodzi komunikat oraz priorytetu (oddzielonego kropką). Dotyczy to poczty, wiadomości, FTP, auth, kern i innych. Priorytety w kolejności od najmniej ważnego do najważniejszego: wyszukiwanie błędów, informacja, uwaga, ostrzeżenie, błąd, wyjątek krytyczny, alert i awaria.

Plik `syslog.conf` z Listingu 2 powoduje wysłanie występujących komunikatów do konsoli wirtualnej `/dev/tty8`. Aby przejrzeć komunikaty, wystarczy nacisnąć kombinację klawiszy `CTRL+F8`. Działania podsystemu pocztowego (poza komunikatami wyszukiwania błędów) przechowywane są w osobnym pliku o nazwie `/var/log/mail`. Pozostałe komunikaty są przekazywane do `/var/log/messages`.

W ostatniej linijce znajduje się specjalna aplikacja, do której syslog przekazuje komunikaty krytyczne na komputerze o nazwie `loghost.zpid.com`, dzięki temu wiadomości nie giną, nawet jeżeli komputer, który wygenerował komunikat krytyczny, zostanie w chwilę potem unieruchomiony. Administratorzy mogą przesłać wiadomości syslog do systemu centralnego i użyć pliku konfiguracyjnego syslog



Rysunek 1: Większość programów linuxowych rejestruje komunikaty przy pomocy głównego demona syslog. Jądro systemu korzysta z demona klogd. Ponadto Syslog przechowuje pliki dziennika lub przekazuje je w inne miejsca.

systemu docelowego. Umożliwia to łatwą diagnostykę przy pomocy klastrów.

Znak minus (-) po lewej stronie nazwy pliku w trzeciej linijce jest sprytną sztuczką – syslogd zwykle zmusza system do zapisywania każdego pliku bezpośrednio na dysku. Jeżeli podczas pracy generowanych jest wiele komunikatów, dysk twardy będzie musiał pracować przez cały czas. Pliki ze znakiem minus (-) nie są zapisywane od razu na dysku, lecz w standardowej pamięci podręcznej systemu Linux. Tak więc komunikaty będą przechowywane w pamięci maksymalnie do 30 sekund, zmniejszając tym samym obciążenie systemu.

Oczywiście administratorzy systemu powinni zadbać o aktualizowanie pliku `syslog.conf`, jeżeli w ich systemach zachodzą jakieś zmiany. Można tego dokonać przy pomocy polecenia `/etc/init.d/syslog reload`, a jeżeli używana dystrybucja nie obsługuje tego polecenia, można wykorzystać do tego celu sygnał HUP (rozłączenie).

```
# ps ax | grep syslog
442 ? S 0:00 /sbin/syslogd
# kill -HUP 442
```

Sygnały są jednym z wielu sposobów komunikacji programów Linuksa między sobą. Poruszymy ten temat w kolejnym wydaniu. ■

Listing 1. Komunikaty Syslog

```
Dec 8 21:50:21 undine kernel: Tx error occurred (error 0x10)!! (maybe distance too high?)
Dec 8 21:50:28 undine last message repeated 36 times
Dec 8 21:59:00 undine /USR/SBIN/CRON[1730]: (root) CMD ( rm -f /var/spool/cron/lastrun/cron.hourly)
Dec 8 22:10:06 undine su: (to root) mas on /dev/pts/0
Dec 8 22:29:18 undine -- MARK --
```

Listing 2. Konfiguracja Syslog

```
*.* /dev/tty8
mail.info /var/log/mail
*.*;mail.none -/var/log/messages
*.crit @loghost.zpid.com
```