Logowanie zdarzeń i demon logów

Zasada działania

Dzięki logom można śledzić aktualne poczynania aplikacji, można badać wykorzystanie systemu, jego komponentów. Logi są ważne szczególnie wtedy, gdy jesteśmy zmuszeni diagnozować jakiś problem konfiguracyjny lub w działaniu samej aplikacji.

W systemie Linux przyjęto założenie, że logi są zapisywane w plikach tekstowych w często możliwym do dopracowania i zdefiniowania formacie. Podstawowa zasada, której starają trzymać się twórcy programów to zapis jednego zdarzenia do jednej linii tekstowej. Jedno zdarzenie nie powinno być „złamane" na kilka linii, aby łatwiej można było filtrować i analizować później logi.

Wyobraźmy sobie najprostszą metodę, która może wprowadzić twórca aplikacji:

Program → plik-na-dysku

Program w swoim kodzie źródłowym sam zapisuje logi do określonego pliku.

Przykładowo w skrypcie mogłoby to wyglądać następująco:

```
echo "`date`: Nie moge wyslac poczty" >> /var/log/program.log
```

Inną i przyjętą za domyślną w systemie jest zapis przy pomocy demona logów. Demon logów to nic innego jak pośrednik do którego aplikacja wysyła komunikat zdarzenia wraz z wymaganymi parametrami, natomiast później demon logów, na podstawie konfiguracji przygotowanej przez administratora zdarzenie zapisuje w jednym lub wielu miejscach. Celem może być nie tylko plik lub kilka plików, ale również baza danych, konsola systemu czy zdalny serwer.

Program → demon-logów(analizuje-wiadomości) → plik(i)/baza-danych/konsola/zdalny-serwer

Przykładowo fragment skryptu wykorzystującego program logger, który wysyła treść zdarzenia do lokalnego demona logów.

```
logger -p mail.err -t "SerwerPocztowy" "Nie mogę wysłać poczty"
```

Dalszą pracą komunikatu „Nie mogę wysłać poczty" zajmuje się demon logów.

Demony logowania

/usr/sbin/rsyslogd - system logger daemon

System logging wymaga znajomości narzędzi syslogd klogd i pliku konfiguracyjnego syslog.conf. Narzędzia te w wielu popularnych dystrybucjach (w tym RedHat i Debian) zostały porzucone na rzecz demona rsyslog (plik konfiguracyjny rsyslog.conf). Plik konfiguracyjne demonów rsyslog i syslog mają identyczną składnię w zakresie podstawowej konfiguracji - używany wcześniej plik syslog.conf powinien być poprawnie interpretowany przez demon rsyslog.

Uruchamiane przy starcie systemu za pomoca skryptu: /etc/init.d/rsyslog

Plik konfiguracyjny: /etc/rsyslog.conf

Kilka metod na sprawdzenie, czy demon działa:

service rsyslog status

pgrep -l rsyslogd

Zmiany konfiguracyjny mogą być odczytane przez demon po jego restarcie.

Restart demona i zmuszenie go do pobrania zmodyfikowanej konfiguracji /etc/rsyslog.conf:

service rsyslog restart

W starszych wersjach dystrybucji linuksowych można spotkać osobne dwa demony do logowania zdarzeń systemowych i z jądra systemu:

- /etc/sbin/syslogd - system logger daemon
- /usr/sbin/klogd - kernel logger daemon
- /etc/syslog.conf - plik konfiguracyjny dla powyższych

Logi systemowe

Katalog w którym przechowywane są logi systemu i demonów: /var/log/

Przeglądanie logów on-line:

tail -f /var/log/maillog

tail -f -n 0 /var/log/messages

Wyszukiwanie fraz w logach:

grep fraza /var/log/messages | less

Komenda wysyłająca zdarzenie na serwer logów:

logger -p TEMAT.PRIORYTET -t "Nagłówek" "Wiadomość"

Przykłady:

$ logger -p mail.err -t "SerwerPocztowy" "Blad w dostarczaniu poczty"

$ logger -p user.info -t "DemonIntegralnosci" "System nie zostal zmodyfikowany od ostatniego testu"

Spis tematów wg man syslog.conf: „auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, security (same as auth), syslog, user, uucp and local0 through local7”

Tematy logowania określają, z jakim typem wiadomości związana jest przekazywana informacja. Np. wszystkie programy związane z działaniem poczty (serwery, klienci, przekaźniki poczty itp.) powinny wysyłać do sysloga wiadomości z tematem „mail”. Programy związane z obsługa drukarek i drukowania, powinny wysyłać informacje do demona logow z tematem „lpr” (local printers).

Priorytet (poziom logowania) - określa ważność zdarzenia zapisywanego w logach.

Ważniejsze dla systemu (i administratora) są informacje o tym, że poczta nie dotarła do zdalnego serwera (usterka→błąd→problem) niż te, które opisują pomyślne wysłanie maila.

Na podstawie „man syslog” i „man syslog.conf”:

w zapisie słownym	w zapisie numerycznym
panic	0
emerg	0
alert	1
crit	2
error	3
err	3
warning	4

warn	4
notice	5
info	6
debug	7

Im niższy numer poziomu tym wyższy priorytet (ważniejsze dla systemu zdarzenie).

Konfiguracja - /etc/rsyslog.conf

Przykładowe wpisy w /etc/rsyslog.conf:

```
mail.warn                       -/var/log/mailwarnings.log
; logowanie do pliku /var/log/mailwarnigs.log zdarzen
; zwiazanych z dzialaniem poczty (z serwerow pocztowych
; i programow obslugujacych poczte) o prorytetach warn
; i wazniejszych (err,crit,alert,emerg)
mail.*                          /var/log/maillog
; loguj wszystkie zdarzenia z tematu mail
*.err                           /var/log/errors
; loguj zdarzenia na poziomie err lub wazniejszym
; z wszystkich tematow
*.warn;cron.none;mail.none;news.none     -/var/log/syslog
; logowanie do pliku /var/log/syslog zdarzen o priorytetach
; warn i wazniejszych, z wszystkich tematow poza cron,
; mail i news.
*.=info;*.=notice               -/var/log/info.log
; logowanie do pliku /var/log/info.log zdarzen pochodzacych
```

; z wszystkich tematow, ktorych priorytety to info i notice

local5.*;local5.!=info -/var/log/local5.log

; logowanie do pliku /var/log/local5.log zdarzen pochodzacych

; z tematu loal5 na wszystkich poziomach, poza poziomem info

Zdalne zapisywanie logów

Konfiguracja demona, aby działał jako usługa sieciowa - przyjmował logi od innych hostów

Aby demon ryslogd przyjmował logi ze zdalnych klientów, musi nasłuchiwać na porcie sieciowym. Domyślna konfiguracja wielu dystrybucji ma wyłączone nasłuchiwanie na porcie dedykowanym dla serwera logów - 514 UDP.

Aby to zrealizować należy odkomentować poniższe linie w pliku konfiguracyjnym /etc/rsyslog.conf

$ModLoad imudp

$UDPServerRun 514

Po zmianie konfiguracji należy zrestartować demona.

service rsyslog restart

Od tej porty serwer powinien nasłuchiwać na porcie 514 UDP:

netstat -lunp | grep :514

listen ports, **u**dp, **n**o dns lookup, **p**rocesses

Firewall w CentOS i RedHat

W dystrybucjach CentOS i Redhat może być konieczna dodatkowa konfiguracja firewalla iptables, aby port 514 UDP był dostępny dla innych hostów (w poniższym przykładzie tylko host o adresie 192.168.122.132 będzie mógł korzystać z rsyslogd na naszym systemie.

```
iptables -I INPUT -s 192.168.122.132 -p udp --dport 514 -j ACCEPT
service iptables save
```

Konfiguracja klienta

Po stronie klienta (systemu, który będzie wysyłał logi na zdalny serwer), należy zamieścić w pliku konfiguracyjnym następującą, przykładową linię:

```
*.*                     @10.1.254.2
```

Powyższe spowoduje logowanie wszystkich zdarzeń dodatkowo na zdalny serwer logów o adresie IP 10.1.254.2

Filtrowanie po nazwie hosta, który wysyła logi

Po stronie serwera, który odbiera logi z wielu innych serwerów może zajść potrzeba filtrowania po hoście - zapisywania logów do określonego pliku zdarzeń pochodzących od konkretnego serwera. Można to zrealizować przykładowo takim zapisem konfiguracyjnym:

```
if $fromhost == 'debiansrv03' then /var/log/debiansrv03/all.log
```