Zadania

Cel ogólny lekcji: Poznanie podstaw konfiguracji sysloga w systemie Linux i zdobycie umiejętności skonfigurowania logowania na różne poziomy i tematy, w tym także na zewnętrzne systemy operacyjne.

Cele szczegółowe lekcji:

1. Zrozumienie roli i działania sysloga oraz umiejętność skonfigurowania logowania z tematu local4 do pliku /var/log/local4.log przy użyciu komendy logger.
2. Umiejętność konfiguracji logowania z tematu local1 na poziomach "err i ważniejsze" do pliku /var/log/local1.err przy użyciu komendy logger.
3. Umiejętność skonfigurowania logowania z tematu local2 tylko na poziomie crit do pliku /var/log/local2-crit.log przy użyciu komendy logger.
4. Umiejętność konfiguracji logowania z tematów local1 i local2 do jednego pliku /var/log/lokalne.log przy użyciu komendy logger.
5. Zdolność do skonfigurowania logowania z wszystkich tematów, poza local0, local1 i local5, do pliku /var/log/prawie-wszystkie.log przy użyciu komendy logger.
6. Umiejętność konfiguracji logowania z tematu local5 na wszystkich poziomach oprócz crit, alert i panic do pliku /var/log/local5.log przy użyciu komendy logger.
7. Zrozumienie potrzeby logowania na zewnętrzne systemy operacyjne oraz umiejętność skonfigurowania sysloga do logowania dodatkowo zdarzeń na inny system przy użyciu odpowiednich komend i narzędzi.

Każde z poniższych zadań przetestuj przy pomocy komendy logger.

1. Skonfiguruj system, aby wszystkie logi pochodzące z tematu local4 syslog zapisywał do pliku /var/log/local4.log. Możesz dodać następującą linię do pliku /etc/rsyslog.conf

local4.* /var/log/local4.log

2. Skonfiguruj system, aby logi pochodzące z tematu local1 na poziomach „err i ważniejsze” syslog zapisywał do pliku /var/log/local1.err. Możesz dodać następującą linię do pliku /etc/rsyslog.conf:

local1.err /var/log/local1.err

3. Skonfiguruj syslog, aby logi pochodzące z tematu local2 na poziomie crit (i tylko tym poziomie) logował do pliku /var/log/local2-crit.log. Możesz dodać następującą linię do pliku /etc/rsyslog.conf:

local2.=crit /var/log/local2-crit.log

4. Skonfiguruj syslog, aby logi pochodzące z tematów local1 i local2 logowal do pliku /var/log/lokalne.log. Możesz dodać następującą linię do pliku /etc/rsyslog.conf:

local1,local2.* /var/log/lokalne.log

5. Skonfiguruj syslog, aby logi pochodzące z wszystkich tematów, poza tematami local0, local1 i local5 logowal do pliku /var/log/prawie-wszystkie.log. Możesz dodać następującą linię do pliku /etc/rsyslog.conf:

.;local0.none;local1.none;local5.none /var/log/prawie-wszystkie.log

6. Skonfiguruj syslog, aby logi z tematu local5, na wszystkich priorytetach oprócz crit, alert i panic, zapisywał do pliku /var/log/local5.log. Możesz dodać następującą linię do pliku /etc/rsyslog.conf:

local5.!crit,!alert,!panic /var/log/local5.log

7. Skonfiguruj system tak, aby syslog logował dodatkowo wszystkie zdarzenia na inny system operacyjny (przygotuj ten system do przyjmowania logów). Możesz dodać następującą linię do pliku /etc/rsyslog.conf12:

. @<ip lub nazwa innego systemu>

Przykładowo, jeśli chcesz wysyłać logi na system o adresie IP 192.168.1.100, możesz użyć:

. @192.168.1.100

Aby przygotować inny system do przyjmowania logów, musisz upewnić się, że usługa rsyslog jest uruchomiona i nasłuchuje na porcie 514 UDP3. Możesz to zrobić, edytując plik /etc/rsyslog.conf na innym systemie i odkomentowując następującą linię3:

$ModLoad imudp

oraz

$UDPServerRun 514

Po dokonaniu zmian w pliku /etc/rsyslog.conf, musisz zrestartować usługę rsyslog, aby zastosować nowe ustawienia. Możesz to zrobić za pomocą następującego polecenia:

sudo systemctl restart rsyslog

Rozwiązanie:

1. Aby skonfigurować system w taki sposób, że wszystkie logi pochodzące z tematu local4 syslog są zapisywane do pliku /var/log/local4.log, wykonaj następujące kroki:

a. Otwórz plik konfiguracyjny syslog za pomocą edytora tekstu, takiego jak nano:

sudo nano /etc/rsyslog.conf

b. Znajdź w pliku linijkę z poniższym tekstem:

local4.* /var/log/local4.log

c. Usuń znak # z początku linii, aby odkomentować ją, a następnie zapisz zmiany i zamknij plik.

2. Aby skonfigurować system w taki sposób, że logi pochodzące z tematu local1 na poziomach „err i ważniejsze” syslog są zapisywane do pliku /var/log/local1.err, wykonaj następujące kroki:

a. Otwórz plik konfiguracyjny syslog za pomocą edytora tekstu:

sudo nano /etc/rsyslog.conf

b. Dodaj na końcu pliku następującą linię:

local1.err /var/log/local1.err

c. Zapisz zmiany i zamknij plik.

3. Aby skonfigurować syslog w taki sposób, że logi pochodzące z tematu local2 na poziomie crit (i tylko tym poziomie) są logowane do pliku /var/log/local2-crit.log, wykonaj następujące kroki:

a. Otwórz plik konfiguracyjny syslog za pomocą edytora tekstu:

sudo nano /etc/rsyslog.conf

b. Dodaj na końcu pliku następującą linię:

local2.crit /var/log/local2-crit.log

c. Zapisz zmiany i zamknij plik.

4. Aby skonfigurować syslog w taki sposób, że logi pochodzące z tematów local1 i local2 są logowane do pliku /var/log/lokalne.log, wykonaj następujące kroki:

a. Otwórz plik konfiguracyjny syslog za pomocą edytora tekstu:

sudo nano /etc/rsyslog.conf

b. Dodaj na końcu pliku następującą linię:

local1,local2.* /var/log/lokalne.log

c. Zapisz zmiany i zamknij plik.

5. Aby skonfigurować syslog w taki sposób, że logi pochodzące z wszystkich tematów, poza tematami local0, local1 i local5, są logowane do pliku /var/log/prawie-wszystkie.log, wykonaj następujące kroki:

a. Otwórz plik konfiguracyjny syslog za pomocą edytora tekstu:

sudo nano /etc/rsyslog.conf

```

b. Dodaj na końcu pliku następującą linię:

```

.;local0.none;local1.none;local5.none /var/log/prawie-wszystkie.log

```

c. Zapisz zmiany i zamknij plik.

6. Aby skonfigurować syslog w taki sposób, że logi z tematu local5, na wszystkich priorytetach oprócz crit, alert i panic, są zapisywane do pliku /var/log/local5.log, wykonaj następujące kroki:

a. Otwórz plik konfiguracyjny syslog za pomocą edytora tekstu:

**sudo nano /etc/rsyslog.conf**

b. Dodaj na końcu pliku następującą linię:

local5.!crit,!alert,!panic /var/log/local5.log c.

Zapisz zmiany i zamknij plik.

7. Aby skonfigurować system tak, aby syslog logował dodatkowo wszystkie zdarzenia na inny system operacyjny, wykonaj następujące kroki:

a. Zainstaluj pakiet rsyslog-gnutls na systemie, na którym chcesz zapisywać logi:

**sudo apt-get install rsyslog-gnutls**

b. Otwórz plik konfiguracyjny syslog za pomocą edytora tekstu:

**sudo nano /etc/rsyslog.conf**

c. Dodaj na końcu pliku następującą linię, zastępując "adres-ip" adresem IP systemu, na którym chcesz zapisywać logi:

*.* @@adres-ip:514;RSYSLOG_SyslogProtocol23Format

d. Zapisz zmiany i zamknij plik.

Po wykonaniu powyższych kroków, syslog będzie działał zgodnie z podanymi wymaganiami. Aby przetestować konfigurację, można użyć komendy logger z odpowiednim tematem i poziomem logowania i sprawdzić, czy logi zostaną zapisane we właściwym pliku. Na przykład:
```

```
logger -p local1.err "To jest test loga local1.err"
```

spowoduje zapisanie loga o treści "To jest test loga local1.err" do pliku /var/log/local1.err, jeśli konfiguracja została poprawnie wykonana.

Podsumowanie:

Po wykonaniu wszystkich czynności z powyższej instrukcji przeczytaj ponownie z zrozumieniem cel ogólny i cele szczegółowe, które znajdują się na pierwszej stronie instrukcji. Jeżeli one zostały niezrealizowane to powtarzaj wykonie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.