Vyšší odborná škola obalové techniky
a střední škola, Štětí

Digitální učební materiály

Operační systémy - Linux

Ivan Pomykacz

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Licence

Disclaimer

Tento PDF dokument byl strojově vygenerován z HTML stránek

http://dumy.odbornaskola.cz/pomykacz/.

Je tedy možné, že sazba textu může obsahovat chyby. Jde převážně o vizuální a typografické chyby, které mohou narušit plynulou čitelnost textu. V některých případech může být ohrožena i funkčnost některých komponent (jako vnitřní odkazy).

Vzhledem k tomu, že vypracované materiály nebyly nikdy určeny pro výstupní formát PDF, autor se zříkává jakékoli odpovědnosti za nalezené chyby. Nesnažte se proto v této souvislosti autora kontaktovat.

Operační systémy

Linux

Obsah

Logování

Název školy	Vyšší odborná škola obalové techniky a Střední škola, Štětí, příspěvková organizace		
Adresa školky	Kostelní 134, 411 08 Štětí		
IČ	46773509		
Název operačního programu	OP Vzdělávání pro konkurenceschopnost		
Registrační číslo	CZ.1.07/1.5.00/34.1006		
Označení vzdělávacího materiálu	VY_32_INOVACE_21_PSS_415		
Název tématické oblasti (sady)	Operační systémy		
Název materiálu	Logování		
Anotace	Text seznamuje se způsobem záznamu událostí v systému do tzv. logů. Popisuje přístup k logům, jejich prohlížení a interpretace. Představuje některé možnosti pro analýzu log souborů. Objasňuje automatickou archivaci a rotaci logů.		
Autor	Ivan Pomykacz	**Jazyk**	český
Očekávaný výstup	Lokalizuje systémový log nebo log pro odpovídající službu v systému. Prohlíží a analyzuje log soubor. Používá nástroje pro automatickou analýzu log souborů.		
Klíčová slova	log soubor, rotace logů, analýza logů		
Druh výukového zdroje	Výklad	**Věková skupina žáků**	17+
Typ interakce	aktivita	**Ročník**	3.
Speciální vzdělávací potřeby	žádné		
Zhotoveno, (datum/období)	6.5.2014	**Celková velikost**	

Obsah

Každý systémový administrátor ví, že operační systém by měl logovat nejlépe všechno, a zároveň je potřeba tyto logy kontrolovat pro chyby, varování a podezřelé aktivity.

V Debianu je předinstalovaný logovací daemon *rsyslogd*. Je to služba, která ukládá informace, které ji posílají jiné služby, ať lokální nebo vzdálené. To mj. znamená, že v síti může být centrální počítač pro pouze logovací účely.

V našem případě se budeme zabývat pouze lokálním logováním.

Syslog

V adresáři `/var/log` se ukládají všechny logy.

```
root@wheezy:~# ls -l /var/log/
celkem 1840
-rw-r--r-- 1 root        root  17566 dub 21 18:55 alternatives.log
drwxr-xr-x 2 root        root   4096 dub 21 18:48 apt
-rw-r--r-- 1 root        root   4111 dub 21 18:51 aptitude
-rw-r----- 1 root        adm   24279 kvě 25 09:17 auth.log
-rw-rw---- 1 root        utmp      0 dub 21 18:47 btmp
-rw-r----- 1 root        adm   11234 kvě 25 08:12 daemon.log
-rw-r----- 1 root        adm  106472 kvě 25 08:12 debug
-rw-r----- 1 root        adm   25442 kvě 25 08:12 dmesg
-rw-r----- 1 root        adm   25461 kvě 24 14:03 dmesg.0
-rw-r----- 1 root        adm    8187 kvě 24 07:37 dmesg.1.gz
-rw-r----- 1 root        adm    8124 kvě 23 09:09 dmesg.2.gz
-rw-r----- 1 root        adm    8035 kvě 23 08:20 dmesg.3.gz
-rw-r----- 1 root        adm    8180 kvě 23 08:14 dmesg.4.gz
-rw-r--r-- 1 root        root 245497 kvě 24 18:20 dpkg.log
drwxr-s--- 2 Debian-exim adm    4096 dub 21 18:59 exim4
-rw-r--r-- 1 root        root  24072 kvě 24 18:20 faillog
drwxr-xr-x 2 root        root   4096 dub 21 18:48 fsck
drwxr-xr-x 3 root        root   4096 dub 21 18:59 installer
-rw-r----- 1 root        adm  412939 kvě 25 08:12 kern.log
-rw-rw-r-- 1 root        utmp 292876 kvě 25 08:48 lastlog
-rw-r----- 1 root        adm       0 dub 21 18:59 lpr.log
-rw-r----- 1 root        adm       0 dub 21 18:59 mail.err
-rw-r----- 1 root        adm       0 dub 21 18:59 mail.info
-rw-r----- 1 root        adm       0 dub 21 18:59 mail.log
-rw-r----- 1 root        adm       0 dub 21 18:59 mail.warn
-rw-r----- 1 root        adm  306646 kvě 25 08:12 messages
drwxr-xr-x 2 root        root   4096 dub 21 18:59 news
-rw-r----- 1 root        adm  434886 kvě 25 09:17 syslog
-rw-r----- 1 root        adm    1714 kvě 25 08:12 user.log
-rw-rw-r-- 1 root        utmp 140544 kvě 25 08:48 wtmp
```

Názvy souborů jsou definovány v konfiguračním souboru `/etc/rsyslogd.conf`. V systému momentálně nejsou nainstalovány služby jako apache, postfix nebo mysql. "Jediné" co nyní můžeme sledovat jsou výpisy jádra (`dmesg`), lokální pošta (`mail`), autentizace uživatelů (`auth.log`, včetně ssh) a obecný systémový log (`syslog`).

Podívejme se do takového logu, např. syslog.

```
root@wheezy:~# tail /var/log/syslog
May 25 08:12:00 wheezy acpid: 1 rule loaded
May 25 08:12:00 wheezy acpid: waiting for events: event logging is off
May 25 08:12:00 wheezy /usr/sbin/cron[2108]: (CRON) INFO (pidfile fd = 3)
May 25 08:12:00 wheezy /usr/sbin/cron[2109]: (CRON) STARTUP (fork ok)
```

```
May 25 08:12:00 wheezy /usr/sbin/cron[2109]: (CRON) INFO (Running @reboot
jobs)
May 25 08:12:01 wheezy /usr/sbin/gpm[2409]: *** info [daemon/startup.c(131)]:
May 25 08:12:01 wheezy /usr/sbin/gpm[2409]: Started gpm successfully. Entered
daemon mode.
May 25 08:12:10 wheezy kernel: [   15.664189] eth0: no IPv6 routers present
May 25 08:17:01 wheezy /USR/SBIN/CRON[2527]: (root) CMD (   cd / && run-parts
--report /etc/cron.hourly)
May 25 09:17:01 wheezy /USR/SBIN/CRON[2588]: (root) CMD (   cd / && run-parts
--report /etc/cron.hourly)
```

Příkazem `tail` se vypíše posledních 10 řádků ze souboru. Logy jsou ve většině případů obyčejné textové soubory, kde na každém řádku je (většinou) nová zpráva. Na konci souboru jsou ty nejnovější záznamy (proto `tail`).

Pokud byste chtěli sledovat soubor po nějakou delší dobu, můžete s výhodou využít parametr `-f` u příkazu `tail`. Po spuštění příkazu `tail -f /var/log/syslog` program neskončí, ale čeká na změny v souboru, a potom je okamžitě vypíše. Klávesami `Ctrl+C` ukončíte činnost programu.

Informace z logu

U každého záznamu je časový údaj, za nímž následuje název počítače (zde wheezy). Následuje název démona, kterého se událost týká. Ve výpisu výše to jsou `acpid` a `cron`. `kernel` není přímo démon, ale v syslogu se objeví i výpisy z jádra.

Analýza logů

Není možné ručně procházet všechny logy, na všech systémech. Pro tyto potřeby byly vytvořeny různé analyzátory, které parsují logy a sestavují reporty, které pak zobrazí správci, např. v e-mailu. Můžete najít analyzátory logů pro konkrétní služby nebo obecné, které pomocí pluginů rozšiřují své možnosti.

Jedním z obecných analyzátorů je např. `logwatch`. Provádí analýzu vybraných logů a následně zasílá reporty na e-mail správce.

```
root@wheezy:~# apt-get install logwatch
root@wheezy:~# mkdir /var/cache/logwatch
root@wheezy:~# cp /usr/share/logwatch/default.conf/logwatch.conf
/etc/logwatch/conf/
root@wheezy:~# nano /etc/logwatch/conf/logwatch.conf
```

V příkazech výše jsem trochu předběhl a vytvořil adresář `/var/cache/logwatch`, který se uvádí v konfiguračním souboru `/etc/logwatch/conf/logwatch.conf`. Konfigurační soubor byl zkopírován z výchozí konfigurace. Kde jsem zjistil, že to tak musím udělat? Z manuálových stránek `man logwatch`. V konfiguračním souboru nás může zajímat:

```
Output = mail
Format = text
MailTo = root
```

```
MailFrom = Logwatch
Range = yesterday
Detail = Low
```

Až na *Output* jsem vše ponechal beze změny.

Po instalaci přibyl v adresáři `/etc/cron.daily` soubor `00logwatch`.

```
root@wheezy:~# ls /etc/cron.daily/
apt  aptitude  bsdmainutils  dpkg  exim4-base  logrotate  man-db  mlocate
passwd  quota  00logwatch
```

Nebudeme čekat do zítra a spustíme `logwatch` už teď, abychom se mohli podívat na výstup.

```
root@wheezy:~# /etc/cron.daily/00logwatch
```

Nyní byl odeslán e-mail uživateli *root*, resp. *tux*. Ve výchozím stavu se e-maily pro uživatele root přesměrovávají uživateli vytvořenému při instalalaci systému. Více v souboru `/etc/aliases`. Přihlásíme-li se jako *tux*, uvidíme v shellu zprávu.

```
You have mail.
Last login: Mon Apr 21 19:52:27 2014
tux@wheezy:~$
```

Programem `mutt` si můžeme došlou zprávu přečíst.

```
tux@wheezy:~$ mutt
```

```
q:Konec  d:Smazat  u:Obnovit  s:Uložit  m:Psát  r:Odepsat  g:Skupině
?:Nápověda
   1 N   May 25 logwatch@wheezy ( 101) Logwatch for wheezy (Linux)
```

```
---Mutt: /var/mail/tux [Msgs:1 New:1 3,5K]---(threads/da-
e)-------------------------------------(all)---
```

Pro zobrazení zprávy stiskneme Enter.

```
Date: Sun, 25 May 2014 10:20:05 +0200
From: logwatch@wheezy.odbornaskola.cz
To: root@wheezy.odbornaskola.cz
Subject: Logwatch for wheezy (Linux)
```

```
 ################### Logwatch 7.4.0 (05/02/12) ####################
        Processing Initiated: Sun May 25 10:20:04 2014
        Date Range Processed: yesterday
```

```
                              ( 2014-May-24 )
                              Period is day.
       Detail Level of Output: 0
       Type of Output/Format: mail / text
       Logfiles for Host: wheezy
 ##################################################################

 -------------------- dpkg status changes Begin ----------------------

 Installed:
    dbus:i386 1.6.8-1+deb7u1
    gdisk:i386 0.8.5-1
    libdbus-1-3:i386 1.6.8-1+deb7u1
    libicu48:i386 4.8.1.1-12+deb7u1
    libnl-3-200:i386 3.2.7-4
    libnl-genl-3-200:i386 3.2.7-4
    libsystemd-login0:i386 44-11+deb7u4
    quota:i386 4.00-4+deb7u1

 ---------------------- dpkg status changes End ------------------------


 --------------------- Kernel Begin ------------------------


 WARNING:  Kernel Errors Present
    EXT3-fs (sdb1): error: couldn't mount  ...:  1 Time(s)
    EXT4-fs (sda1): re-mounted. Opts: errors=remount-ro ...:  2 Time(s)
    Error: Driver 'pcspkr' ...:  2 Time(s)

 ---------------------- Kernel End -------------------------
```

Rotace logů

Syslog (rsylogd) se automaticky stará o tzv. rotaci logů. Soubory časem nakynou a zabírají místo. Objemné soubory se pomaleji parsují, a navíc obsahují i stará data. Syslog provádí pravidelnou tzv. rotaci log souborů, kdy vezme aktuální log soubor a zkomprimuje jej pomocí gzip. Výsledek je hezky vidět na logu `dmesg`.

```
root@wheezy:~# ls -l /var/log/dmesg*
-rw-r----- 1 root adm 25442 kvě 25 08:12 /var/log/dmesg
-rw-r----- 1 root adm 25461 kvě 24 14:03 /var/log/dmesg.0
-rw-r----- 1 root adm  8187 kvě 24 07:37 /var/log/dmesg.1.gz
-rw-r----- 1 root adm  8124 kvě 23 09:09 /var/log/dmesg.2.gz
-rw-r----- 1 root adm  8035 kvě 23 08:20 /var/log/dmesg.3.gz
-rw-r----- 1 root adm  8180 kvě 23 08:14 /var/log/dmesg.4.gz
```

Nejaktuálnější log je v souboru `dmesg` a ten nejstarší v souboru `dmesg.4.gz`. Pro prohlížení souboru `.gz` lze využít program `zcat`, který transparentně provádí dekompresi.

```
root@wheezy:~# zcat /var/log/dmesg.4.gz | head
[    0.000000] Initializing cgroup subsys cpuset
[    0.000000] Initializing cgroup subsys cpu
[    0.000000] Linux version 3.2.0-4-486 (debian-kernel@lists.debian.org)
(gcc version 4.6.3 (Debian 4.6.3-14) ) #1 Debian 3.2.54-2
[    0.000000] BIOS-provided physical RAM map:
[    0.000000]  BIOS-e820: 0000000000000000 - 000000000009fc00 (usable)
[    0.000000]  BIOS-e820: 000000000009fc00 - 00000000000a0000 (reserved)
[    0.000000]  BIOS-e820: 00000000000f0000 - 0000000000100000 (reserved)
[    0.000000]  BIOS-e820: 0000000000100000 - 000000001fff0000 (usable)
[    0.000000]  BIOS-e820: 000000001fff0000 - 0000000020000000 (ACPI data)
[    0.000000]  BIOS-e820: 00000000fffc0000 - 0000000100000000 (reserved)
```