**Зертханалық сабақ №10:** Оқиғаларды тіркеу жүйесін орнату

В данной главе обсуждаются три отдельных вопроса.

Во-первых, рассматривается механизм журналирования входов в систему: обсуждаются способы получения информации о том, кто, когда и с какого узла осуществил вход в систему. Также рассматриваются способы получения информации о том, кому не удалось осуществить вход в систему, кто не смог воспользоваться утилитой `su` или `ssh`.

Во-вторых, рассматривается процесс настройки демона syslog, а также его тестирования с помощью утилиты `logger`.

Последняя часть главы в основном посвящена `механизму ротации фалов журналов`, а также содержит пояснения относительно использования команд `tail -f и watch` для `отслеживания изменений файлов журналов`.

# 17.1. Журналирование входов в систему

С целью облегчения процесса отслеживания входов пользователей в систему Linux может записывать необходимые данные в файлы журналов `/var/log/wtmp`, `/var/log/btmp`, `/var/run/utmp` и `/var/log/lastlog`.

### 17.1.1. Файл журнала /var/run/utmp (who)

Используйте утилиту `who` для просмотра содержимого файла /var/run/utmp. Эта утилита выводит информацию о пользователях, осуществивших вход в систему и `в данный момент` работающих с ней. Обратите внимание на то, что файл utmp находится в директории /var/run, а не /var/log.

```
[root@rhel4 ~]# who
paul     pts/1        Feb 14 18:21 (192.168.1.45)
sandra   pts/2        Feb 14 18:11 (192.168.1.42)
inge     pts/3        Feb 14 12:01 (192.168.1.33)
els      pts/4        Feb 14 14:33 (192.168.1.19)
```

### 17.1.2. Файл журнала /var/log/wtmp (last)

Содержимое файла журнала /var/log/wtmp обновляется силами `программы login`. Используйте утилиту `last` для просмотра содержимого файла журнала /var/run/wtmp.

```
[root@rhel4a ~]# last | head
paul     pts/1       192.168.1.45     Wed Feb 14 18:39   still logged in
reboot   system boot 2.6.9-42.0.8.ELs Wed Feb 14 18:21          (01:15)
nicolas  pts/5       pc-dss.telematic Wed Feb 14 12:32 - 13:06  (00:33)
stefaan  pts/3       pc-sde.telematic Wed Feb 14 12:28 - 12:40  (00:12)
nicolas  pts/3       pc-nae.telematic Wed Feb 14 11:36 - 12:21  (00:45)
nicolas  pts/3       pc-nae.telematic Wed Feb 14 11:34 - 11:36  (00:01)
dirk     pts/5       pc-dss.telematic Wed Feb 14 10:03 - 12:31  (02:28)
nicolas  pts/3       pc-nae.telematic Wed Feb 14 09:45 - 11:34  (01:48)
dimitri  pts/5       rhel4            Wed Feb 14 07:57 - 08:38  (00:40)
stefaan  pts/4       pc-sde.telematic Wed Feb 14 07:16 - down   (05:50)
[root@rhel4a ~]#
```

Утилита last также может использоваться и для получения информации о последних перезагрузках.

```
[paul@rekkie ~]$ last reboot
```

```
reboot   system boot  2.6.16-rekkie   Mon Jul 30 05:13     (370+08:42)

wtmp begins Tue May 30 23:11:45 2006
[paul@rekkie ~]
```

### 17.1.3. Файл журнала /var/log/lastlog (lastlog)

Используйте утилиту `lastlog` для просмотра содержимого файла /var/log/lastlog.

```
[root@rhel4a ~]# lastlog | tail
tim              pts/5  10.170.1.122     Вт фев 13 09:36:54 +0100 2007
rm               pts/6  rhel4            Вт фев 13 10:06:56 +0100 2007
henk                                     **Никогда не входил в систему**
stefaan          pts/3  pc-sde.telematic Ср фев 14 12:28:38 +0100 2007
dirk             pts/5  pc-dss.telematic Ср фев 14 10:03:11 +0100 2007
arsene                                   **Никогда не входил в систему**
nicolas          pts/5  pc-dss.telematic Ср фев 14 12:32:18 +0100 2007
dimitri          pts/5  rhel4            Ср фев 14 07:57:19 +0100 2007
bashuserrm       pts/7  rhel4            Чт фев 13 10:35:40 +0100 2007
kornuserrm       pts/5  rhel4            Чт фев 13 10:06:17 +0100 2007
[root@rhel4a ~]#
```

### 17.1.4. Файл журнала /var/log/btmp (lastb)

Также существует утилита `lastb`, предназначенная для вывода содержимого файла `/var/log/btmp`. Содержимое этого файла обновляется программой login при вводе некорректного пароля, следовательно, он содержит информацию о неудачных попытках входа в систему. В файловых системах множества компьютеров данный файл может отсутствовать, в результате чего неудачные попытки входа в систему не будут журналироваться.

```
[root@RHEL4b ~]# lastb
lastb: невозможно открыть /var/log/btmp: Нет такого файла или каталога
[root@RHEL4b ~]#
```

Обычно данный файл удаляют по той причине, что пользователи иногда по ошибке вводят свой пароль вместо имени учетной записи, следовательно, читаемый всеми файл является потенциальной угрозой безопасности системы. Вы можете активировать механизм журналирования неудачных попыток входа в систему, просто создав файл с упомянутым именем. В этом случае исполнение команды chmod o-r /var/log/btmp позволит повысить защищенность системы.

```
[root@RHEL4b ~]# touch /var/log/btmp
[root@RHEL4b ~]# ll /var/log/btmp
-rw-r--r-- 1 root root 0 июл 30 06:12 /var/log/btmp
[root@RHEL4b ~]# chmod o-r /var/log/btmp
[root@RHEL4b ~]# lastb

btmp begins Пн июл 30 06:12:19 2007
[root@RHEL4b ~]#
```

Информация о попытках ввода некорректных паролей при использовании утилит ssh, rlogin или su не сохраняется в файле /var/log/btmp. В нем сохраняется исключительно информация о попытках ввода некорректного пароля при работе с терминалами.

```
[root@RHEL4b ~]# lastb
HalvarFl tty3                Mon Jul 30 07:10 - 07:10  (00:00)
Maria    tty1                Mon Jul 30 07:09 - 07:09  (00:00)
Roberto  tty1                Mon Jul 30 07:09 - 07:09  (00:00)

btmp begins Mon Jul 30 07:09:32 2007
[root@RHEL4b ~]#
```

### 17.1.5. Журналирование входов в систему с использованием утилит su и ssh

В зависимости от дистрибутива в файловой системе вашего компьютера вы также можете обнаружить файл `/var/log/secure`, который заполнен сообщениями от вспомогательных модулей auth и/или authpriv демона syslog. Этот файл журнала должен содержать информацию о неудачных попытках входа в систему с использованием утилиты su и/или ssh. В некоторых дистрибутивах данная информация сохраняется в файле `/var/log/auth.log`, поэтому следует проверить конфигурацию демона syslog.

```
[root@RHEL4b ~]# cat /var/log/secure
Jul 30 07:09:03 sshd[4387]: Accepted publickey for paul from ::ffff:19\
2.168.1.52 port 33188 ssh2
Jul 30 05:09:03 sshd[4388]: Accepted publickey for paul from ::ffff:19\
2.168.1.52 port 33188 ssh2
Jul 30 07:22:27 sshd[4655]: Failed password for Hermione from ::ffff:1\
92.168.1.52 port 38752 ssh2
Jul 30 05:22:27 sshd[4656]: Failed password for Hermione from ::ffff:1\
92.168.1.52 port 38752 ssh2
Jul 30 07:22:30 sshd[4655]: Failed password for Hermione from ::ffff:1\
92.168.1.52 port 38752 ssh2
Jul 30 05:22:30 sshd[4656]: Failed password for Hermione from ::ffff:1\
92.168.1.52 port 38752 ssh2
Jul 30 07:22:33 sshd[4655]: Failed password for Hermione from ::ffff:1\
92.168.1.52 port 38752 ssh2
Jul 30 05:22:33 sshd[4656]: Failed password for Hermione from ::ffff:1\
92.168.1.52 port 38752 ssh2
Jul 30 08:27:33 sshd[5018]: Invalid user roberto from ::ffff:192.168.1\
.52
Jul 30 06:27:33 sshd[5019]: input_userauth_request: invalid user rober\
to
Jul 30 06:27:33 sshd[5019]: Failed none for invalid user roberto from \
::ffff:192.168.1.52 port 41064 ssh2
Jul 30 06:27:33 sshd[5019]: Failed publickey for invalid user roberto \
from ::ffff:192.168.1.52 port 41064 ssh2
Jul 30 08:27:36 sshd[5018]: Failed password for invalid user roberto f\
rom ::ffff:192.168.1.52 port 41064 ssh2
Jul 30 06:27:36 sshd[5019]: Failed password for invalid user roberto f\
rom ::ffff:192.168.1.52 port 41064 ssh2
[root@RHEL4b ~]#
```

Вы можете активировать данный механизм журналирования самостоятельно, указав путь к произвольному файлу путем добавления следующей строки в файл конфигурации syslog.conf.

```
auth.*,authpriv.*                  /var/log/customsec.log
```