



Керування користувачами і групами

Керування користувачами і групами

- Механізм тіньових паролів
- /etc/passwd
- /etc/group
- /etc/shadow
- /etc/gshadow



/etc/passwd

права доступа: rw- r- r—
root:x:0:0:root:/root:/bin/bash

**Shadow
Password
Suite**

/etc/gshadow

права доступа: r-- --- ---
root:::root

/etc/group

права доступа: rw- r-- r--
root:x:0:root

/etc/shadow

права доступа: r-- --- ---
root:\$1\$1LwDVWVi\$JfnIW4Fx97o3qAAolfs.1:14707:0:99999:7:::

Файл /etc/passwd

Поле	Значення
1	ім'я користувача
2	інформація про пароль
3	UID (ідентифікатор користувача)
4	GID (ідентифікатор основної групи користувача)
5	інформація про користувача
6	домашній каталог
7	shell за замовчуванням

Файл `/etc/group`

Поле	Значення
1	ім'я групи
2	інформація пароль
3	GID (ідентифікатор групи)
4	члени групи



Файл /etc/shadow

Поле	Значення
1	ім'я користувача
2	пароль в зашифрованому вигляді
3	час, що минув з останньої зміни пароля (кількість днів з 01.01.1970)
4	мінімальний термін служби пароля; якщо більше нуля, то пароль може бути змінений протягом цієї кількості днів
5	максимальний термін служби пароля; зазвичай встановлюється рівним 99999 днів, що відповідає 275 років

Файл /etc/shadow

Поле	Значення
6	попередження про термін дії; користувачі попереджаються за вказану кількість днів до закінчення максимального терміну дії пароля
7	час переходу в неактивний стан; обліковий запис вважається неактивним через задану кількість днів після закінчення терміну дії пароля
8	час через який обліковий запис повинен бути відключений, вказується в кількості днів, що минули з 01.01.1970

Файл `/etc/gshadow`

Поле	Значення
1	ім'я групи
2	пароль
3	GID (ідентифікатор групи)
4	члени групи

Керування користувачами і групами

- ОС Linux використовує 4 файли для збереження даних про користувачів і групи: `/etc/passwd`, `/etc/group`, `/etc/shadow`, `/etc/gshadow`.
- Файли `/etc/shadow` і `/etc/gshadow` можуть бути прочитані тільки користувачем `root`, на відміну від файлів `/etc/passwd` і `/etc/group`, які доступні для читання всім.
- Каталог `/etc/skel` містить файли, які додаються в домашній каталог при створенні нового користувача.



Керування користувачами і групами

- useradd
- userdel
- usermod
- passwd
- groupadd
- groupdel
- groupmod
- gpasswd
- chage



користувачі

групи

useradd

`useradd -d /home/user`

userdel

`userdel -r user`

usermod

`usermod -L user`
`usermod -U user`

passwd

`passwd user`

chage

`chage -i user`

**Shadow
Password
Suite**

`/etc/passwd`
`/etc/group`
`/etc/shadow`
`/etc/gshadow`

groupadd

`groupadd -g 10000 group`

groupdel

`groupdel group`

groupmod

`groupmod -g 10000 group`

Ключі команди useradd

-c	додати коментарі в файл /etc/passwd до поля даного користувача
-d	вказати домашній каталог, замість наданого за замовчуванням
-e	дата закінчення терміну дії облікового запису
-f	задати кількість днів, що пройшли після закінчення терміну дії пароля, коли обліковий запис повинен бути відключений
-g	вказати ідентифікатор групи (GID) для користувача, замість використовуваного за замовчуванням



Ключі команди useradd

-G	вказати додаткові групи по імені
-m	створити домашній каталог для користувача, якщо він ще не існує
-s	вказати оболонку для користувача
-u	вказати UID, замість використовуваного за замовчуванням



Ключі команди usermod

-aG	ім'я групи; додати користувача в зазначену групу або список груп
-l	задати користувачеві нове ім'я
-L	заблокувати обліковий запис
-U	розблокувати обліковий запис

Ключі команди chage

-d	вказати кількість днів, починаючи з 01.01.1970, що минули з дати останньої зміни пароля
-E	задати термін закінчення дії облікового запису
-I	задати кількість днів між закінченням терміну дії пароля і датою деактивації облікового запису
-l	перевірити поточні налаштування пароля для даного облікового запису
-m	задати мінімальний термін використання користувачем поточного пароля
-W	задати кількість днів, за які користувач буде попереджений, перед закінченням терміну дії пароля



Журналювання операцій в Linux

Журналювання операцій в Linux

- syslogd
- klogd
- /etc/syslog.conf
- logger
- journald



/etc/syslog.conf

authpriv.*
cron.*
daemon.*
ftp.*
kernel.*
local
uucp.news.crit

logger

`logger -p auth.info -t localhost Hello World`

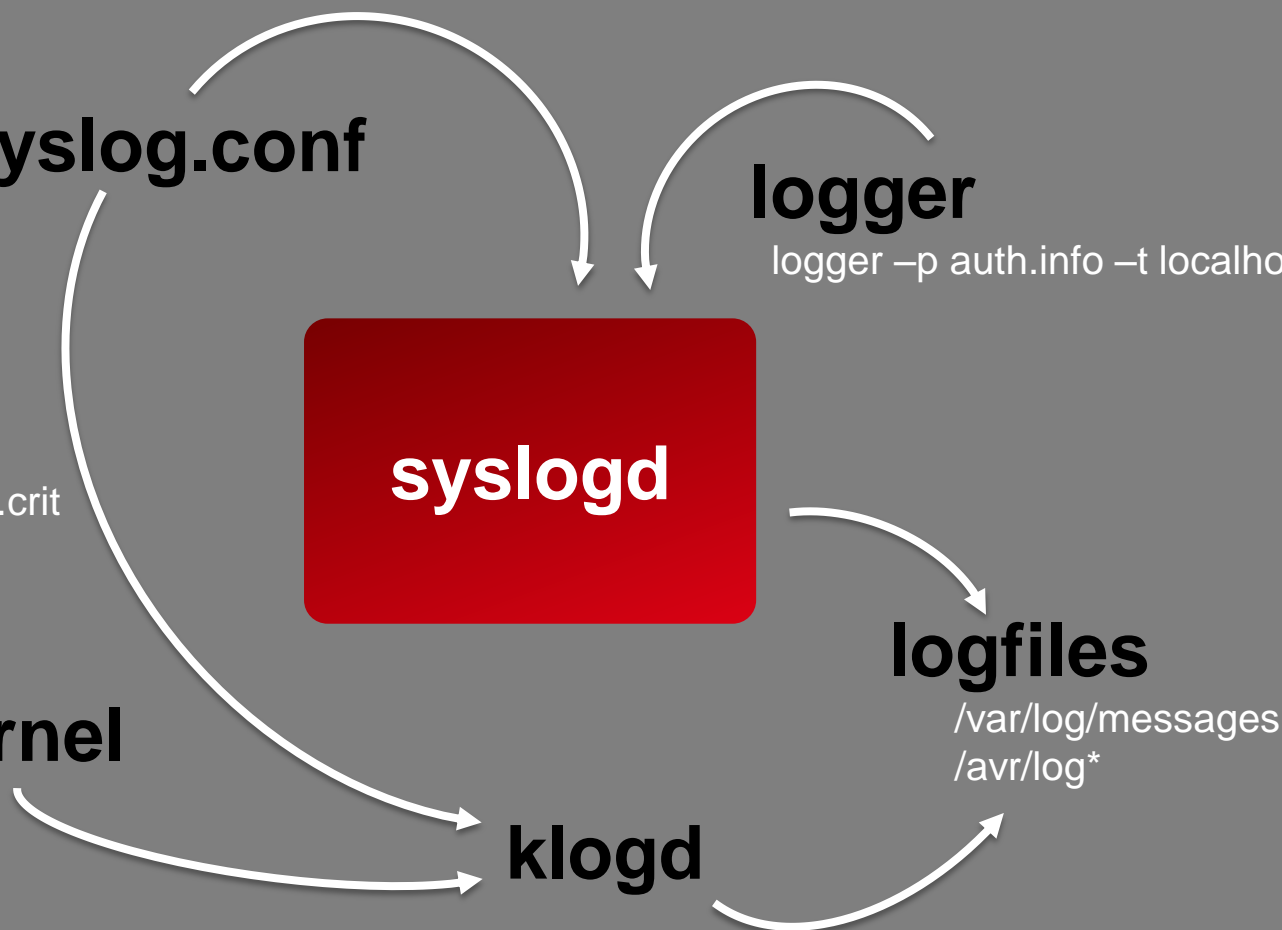
syslogd

logfiles

`/var/log/messages`
`/avr/log*`

kernel

klogd



Джерела подій syslog

auth, authpriv, security	повідомлення служби безпеки / аутентифікації, такі як вхід в систему
cron	системні повідомлення від демонів cron і at
daemon	системні повідомлення від загальних демонів, без використання додаткових засобів журналювання
ftp	базові повідомлення від FTP серверів, зазвичай замінюються на спеціальні файли журналів
kern	повідомлення від ядра



Джерела подій syslog

local0- local7	журнали користувача
lpd	повідомлення від застарілого сервісу Line Print Demon
mail	повідомлення від поштових серверів
news	повідомлення від INN (сервер Usenet)
syslog	журнал демона syslogd
user	повідомлення сервісів рівня користувача
uucp	програмні повідомлення від UUCP (user to user copy)

Пріоритети `syslog.conf`

emerg, panic (0)	повідомлення зупинки системи
alert (1)	важливі проблеми, що вимагають термінового вирішення
crit (2)	критичні проблеми, що вимагає термінового вирішення
error (3)	помилки
warn, warning (4)	попередження про небезпеку, які не зупиняють процес
notice (5)	повідомлення про звичайні, але важливі події
info (6)	інформаційні повідомлення
debug (7)	налагоджувальні повідомлення



Планувальник завдань в Linux



Планувальник завдань в Linux

- /etc/crontab
- /etc/cron.hourly
- /etc/cron.daily
- /etc/cron.weekly
- /etc/cron.monthly
- /var/spool/cron
- crontab



Заплановані задачі

/etc/crontab

42 4 1 * * root run-parts /etc/cron.monthly

/etc/cron.hourly
/etc/cron.daily
/etc/cron.weekly
/etc/cron.monthly

Сценарії

certwatch
logrotate
0anacron
...

**Демон
cron**

Задачі користувача

crontab -e

налаштування
задач користувача

crontab -l
crontab -r

0 * * * * /home/user/test

/var/spool/cron/

<user>

ls <user>

0 * * * * /home/user/test

Файл /etc/crontab

хв. : год. : дата : місяць : день тижня : користувач : задача

Поле	Значення
1	хвилини 0..59
2	години 0..23
3	дні місяця 1..31
4	місяць 1..12
5	день тижня 0..7, 0 - неділя
6	користувач, від імені якого виконується команда
7	команда і її параметри

Значення часу в /etc/crontab

Час	Значення
05 15 * * *	Кожного дня в 15:05
05 15 17 2 *	Кожного 17 лютого в 15:05
05 15 * * 6	Кожної субботи в 15:05
05 15 1 1 1	Кожне 1-е січня, якщо випадає на понеділок о 15:05
05,40 * * * *	У 5 і 40 хв. Кожної години
*/15 * * * *	Кожні 15 хвилин
05 15 * * 1-5	По буднях о 15:05



Планувальник завдань в Linux

- Демон cron виконує заплановані команди і завдання
- Завдання для cron зберігаються в конфігураційному файлі `/etc/crontab`
- Користувачі можуть самі створювати їх завдання за допомогою команди `crontab -e`
- Можна перевірити створені завдання за допомогою команди `crontab -l`



Планувальник завдань в Linux

- Для видалення всіх записів в crontab використовується команда `crontab -r`
- Демон `cron` зчитує необхідну для виконання завдань інформацію з каталогу `/var/spool/cron`.
Для кожного користувача, який має свої завдання для демона `cron`, в цьому каталозі створюється відповідний файл
- Доступ до демона `cron` контролюється адміністратором в файлах `/etc/cron.allow` і `/etc/cron.deny`

Планувальник завдань в Linux

- anacron
- at
- atq
- atrm
- /etc/at.deny
- /etc/at.allow

cron

anacron

/etc/anacrontab

Завдання присутні в
планувальнику?

ТАК

виконати
задачу

НІ

нічого не
робити

at

**доступ
до at**
/etc/at.deny
/etc/at.allow

at

at now + 3 hours
at> /home/user/script
CTRL-D

atq

список задач

atrm

видалити усі задачі
atrm номер-задачі

Планування завдань за допомогою команди at

Поле	Значення
at now + 5 minutes	почати виконання завдання через 5 хвилин
at now + 10	почати виконання завдання через 10 годин
at now + 2 days	почати виконання завдання через 48 годин
at now + 1 week	почати виконання завдання через 7 днів
at teatime	почати виконання завдання о 4 годині дня



Планування завдань за допомогою команди at

- anacron шукає усі cron завдання, виконання яких не було розпочато вчасно і запускає їх на виконання
- anacron зчитує список завдань з конфігураційного файлу, зазвичай це `/etc/anacrontab`
- Команда `at` запускає одноразове виконання завдання
- Що б вийти з режиму команди `at` в звичайний режим командного рядка необхідно натиснути `Ctrl + D`



Планування завдань за допомогою команди `at`

- Команда `atq` перераховує які завдання були запущені через `at`
- Команда `atrm` супроводжується числом, що вказує кількість завдань, запущених через `at`, які будуть видалені
- Якщо ім'я користувача немає в файлі `at.deny`, то він може запускати завдання через `at`
- Якщо файл `/etc/at.deny` буде видалений, то всі користувачі, крім користувача `root`, втратять доступ до демона `at`, якщо не існує `/etc/at.allow`
- Якщо ім'я користувача вказано і в `/etc/at.deny` і в `/etc/at.allow`, то він може створювати `at` завдання