



Базовое Администрирование Linux

Занятие 4



Дмитрий
Молчанов

Настройки



1. Пользователи и группы
2. О правах и их получении
3. AAA/RAM
4. Системные настройки

Пользователи и Группы



Пользователь – учетные записи которым предоставляется доступ в системы

Группа – учетные записи (пользователи) могут объединяться в группы (списки пользователей) для разграничения прав.

Группы бывают первичные и дополнительные.

- Суперпользователь (root/система)
- Непривелигированный пользователь

- Стандартный
- Простой
- Негибкий
- Требуется знание целевого пароля
- Применение:
 - Получение root-доступа
 - Смена текущего пользователя на другого (для рута)

SU



```
d.molchanov@balinux-net01:~$ whoami
d.molchanov
d.molchanov@balinux-net01:~$ su -
Password:
root@balinux-net01:~# whoami
root
root@balinux-net01:~# █
```

sudo



- Гибкий
- Настраиваемый
 - Определенным пользователям/группам
 - Определенных команды, вплоть до параметров
 - возможно безпарольное выполнение
 - от имени разных пользователей
- не требует пароля root

sudo



```
d.molchanov@balinux-net01:~$ whoami
d.molchanov
d.molchanov@balinux-net01:~$ sudo -l
Matching Defaults entries for d.molchanov on this host:
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User d.molchanov may run the following commands on this host:
    (ALL : ALL) ALL
    (ALL : ALL) NOPASSWD: ALL
d.molchanov@balinux-net01:~$ sudo -i
root@balinux-net01:~# whoami
root
root@balinux-net01:~# exit
logout
d.molchanov@balinux-net01:~$ sudo bash
Thu Oct 15 18:16:58 MSK 2015 Hello
root@balinux-net01:~# whoami
root
root@balinux-net01:~# exit
exit
d.molchanov@balinux-net01:~$ sudo whoami
root
d.molchanov@balinux-net01:~$ █
```

AAA/PAM



PAM – Pluggable authentication modules.

Для разных действий (authentication, authorization, session, password-check) разные стеки модулей.

- service
- type
 - Auth – authentication
 - Account – authorization
 - password – password manipulation
 - session – accounting/hooks
- control
 - required
 - requisite
 - sufficient
 - optional



PAM/su



Пример использования pam-модулей для управления доступа к su

1. # Uncomment this if you want wheel members to be able to
2. # su without a password.
3. # auth sufficient pam_wheel.so trust

4. # Uncomment this if you want members of a specific group to not
5. # be allowed to use su at all.
6. # auth required pam_wheel.so deny group=nosu

Системные настройки



- Имя системы
- Время
- Пользователи
- Ограничения пользователей
- Умолчания для пользователей
- настройки доступа
- Пользователи и группы
- Периодические задачи

Имя системы



- hostname
 - без параметров – вывод
 - с параметром-именем – установка нового имени
- /etc/hostname – для сохранения между загрузками
- /etc/hosts – локальный файл соответствия ip-name

- `/etc/localtime` – текущая таймзона (копия файла из `/usr/share/zoneinfo`)
- `date` – вывод/установка времени
- `ntpdate` – разовая синхронизация времени
- `ntp` – локальный ntp-сервер

Управление пользователями и группами



- useradd/adduser
- usermod
- groupadd
- groupdel
- vipw
- файлы/каталоги:
 - /etc/passwd, /etc/shadow
 - /etc/group
 - /etc/login.defs
 - /etc/skel

Периодические задачи



- crontab
 - user
 - system
- at

Ограничения пользователей



- ulimit
- /etc/security/limits.conf

Настройки доступа



- `/etc/ssh/sshd_config` – настройки sshd
- `/etc/pam.d` – настройки PAM
- `/etc/sudoers` – настройки sudo

crontabs



- user
 - m h dom m dow command
 - 5 1 12 6 * echo test > /dev/null
- system
 - m h dom m dow user command

