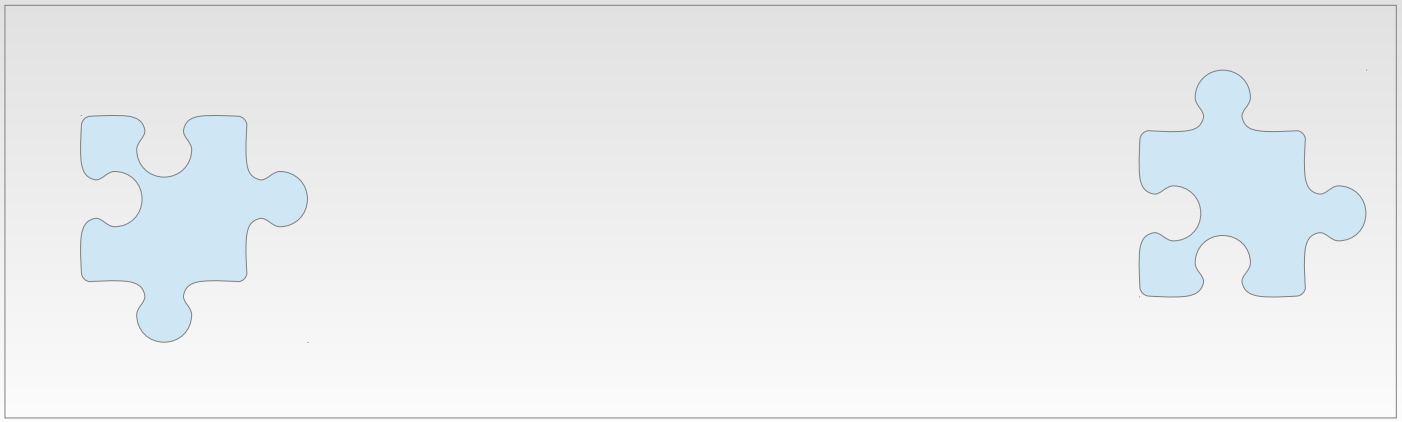
Курс "Администрирование суперкомпьютеров"

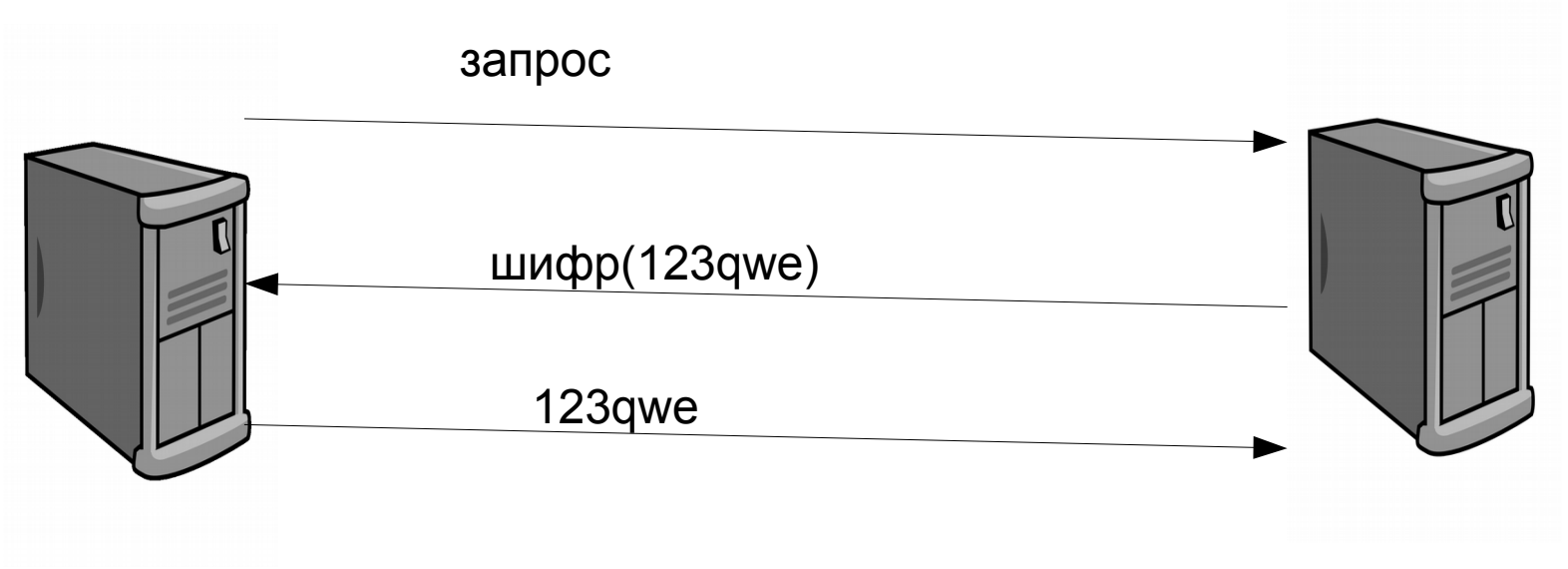
Жуматий С.А.

SSH

закрытый

открытый





OpenSSH

/etc/ssh/sshd_config

- AllowUsers / AllowGroups (DenyUsers/...)
- X11forward
- UseLogin
- Banner
- PermitRootLogin without-password
- PubkeyAuthentication yes
- PasswordAuthentication no

OpenSSH 2

Match:

User, Group, Host, Address

AuthorizedKeysFile, Banner, ChrootDirectory,

ForceCommand,MaxAuthTries, **MaxSessions**,

PasswordAuthentication,

PermitEmptyPasswords, **PermitRootLogin**,

PubkeyAuthentication, X11Forwarding

OpenSSH 3

- AcceptEnv / SendEnv
- Match Address 10.0.0.0/8
  - PasswordAuthentication yes
  - KbdInteractiveAuthentication yes
  - PermitRootLogin yes

OpenSSH 4

.ssh/authorized_keys:

command="....." ssh-rsa r123hbedf123h12g...

.ssh/config:

```
Host work
    Address 1.2.3.4
    User pupkin
    IdentityFile ~/.ssh/work
```

OpenSSH 5

- Доступ без паролей:

  ssh-keygen -N '' -q [-o ~/.ssh/id_rsa]

  id_rsa = закрытый ключ,

  id_rsa.pub = открытый ключ

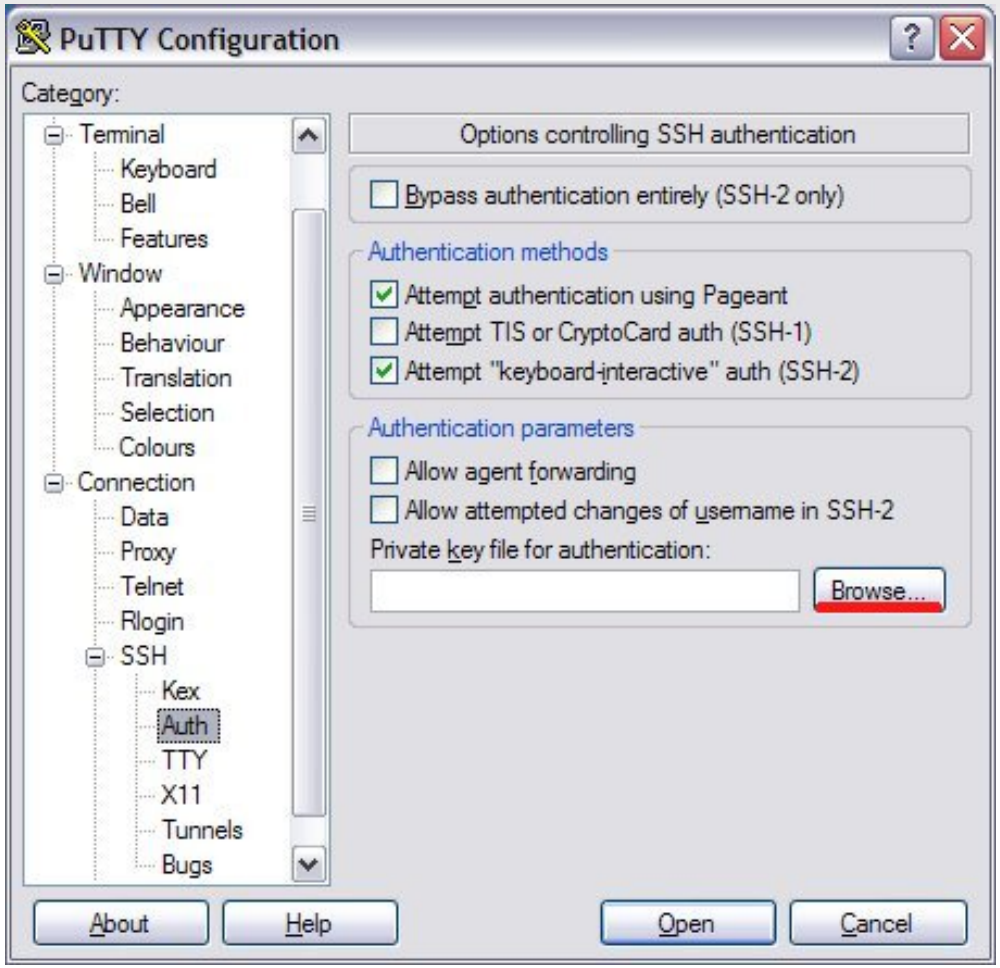
  .ssh/authorized_keys — открытые ключи

OpenSSH 6

~?	список команд
~~	~
~^Z	в фон
~.	завершение

Putty

- Putty / puttygen



Удалённый доступ: sftp/scp

Linux: scp / mc / Dolphin / Nautilus / Filezilla / …

+sshfs

Windows: FAR / WinSCP / Filezilla / …

ssh-agent / pagent

Учётные записи

LDAP

NIS+

Passwd + rsync

OpenLDAP установка 1

```
# yum install openldap-servers openldap-clients
nss_ldap
```

```
# cd /etc/openldap/
```

```
# cp DB_CONFIG.example /var/lib/ldap/DB_CONFIG
```

OpenLDAP установка 2

```
# slappasswd

>>>  {SSHA}ABCDEF1234567890

# vi /etc/openldap/slapd.conf
```

OpenLDAP установка 3

```
database bdb
suffix "dc=ldap,dc=server,dc=ru"
rootdn "cn=Manager,dc=ldap,dc=server,dc=ru"
rootpw {SSHA}ABCDEF1234567890
```

OpenLDAP установка 3.5

```
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/redhat/autofs.schema
include         /etc/openldap/schema/openldap.schema
include         /etc/openldap/schema/misc.schema
```

OpenLDAP установка 4

```
# service ldap start

# cat /etc/openldap/ldap-init.ldif

dn: dc=ldap,dc=server,dc=ru
objectclass: dcObject
objectclass: organization
o: Servidor LDAP ldap
dc: ldap
dn: cn=Manager,dc=ldap,dc=server,dc=ru
objectclass: organizationalRole
cn: Manager
```

OpenLDAP установка 5

```
# /usr/bin/ldapadd -a -x -D 'cn=Manager,dc=ldap,dc=server,dc=ru' -W
-f ldap-init.ldif

> Enter LDAP Password:

adding new entry "dc=ldap,dc=server,dc=ru"

adding new entry "cn=Manager,dc=ldap,dc=server,dc=ru"
```

OpenLDAP установка 6

```
# ldapsearch -h 127.0.0.1 -x -b "dc=ldap,dc=server,dc=ru"
# ldap.server.ru
dn: dc=ldap,dc=server,dc=ru
objectClass: dcObject
objectClass: organization
o: Servidor LDAP ldap
dc: ldap
# Manager, ldap.server.ru
dn: cn=Manager,dc=ldap,dc=server,dc=ru
objectClass: organizationalRole
cn: Manager
# search result
search: 2
result: 0 Success
# numResponses: 3
# numEntries: 2
```

OpenLDAP установка 7

 # openssl passwd -1 -salt 12312345
 # vi user.ldif

```
dn: uid=user1,dc=ldap,dc=server,dc=ru
uid: user1
cn: user1
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {crypt}$1$12312345$xxxyyyaaazzzwwweee
shadowLastChange: 14335
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/user1
gecos: user1
```

OpenLDAP установка 8

```
# ldapadd -a -x -D 'cn=Manager,dc=ldap,dc=server,dc=ru' -W -f user.ldif
```

OpenLDAP установка 9

 # cat /etc/ldap.conf

```
host 127.0.0.1
base dc=ldap,dc=server,dc=ru
rootbinddn cn=Manager,dc=ldap,dc=server,dc=ru
port 389
scope sub
pam_filter objectclass=posixAccount
pam_login_attribute uid
nss_base_passwd ldap,dc=server,dc=ru?sub?objectClass=posixAccount
nss_base_shadow ldap,dc=server,dc=ru?sub?objectClass=posixAccount
nss_base_group  ldap,dc=server,dc=ru?sub?objectClass=posixGroup
ssl no
pam_password md5
```

OpenLDAP установка 10

```
# echo PASSWORD > /etc/ldap.secret
# chmod 600 /etc/ldap.secret
# chmod root:root /etc/ldap.secret
```

```
# cat /etc/nsswitch.conf
passwd:     files ldap
shadow:     files ldap
group:      files ldap
```

OpenLDAP установка 11

```
# grep ldap /etc/pam.d/system-auth

auth        sufficient    /lib/security/pam_ldap.so use_first_pass
account     sufficient    /lib/security/pam_ldap.so
password    sufficient    /lib/security/pam_ldap.so use_authtok
session     optional      /lib/security/pam_ldap.so
```

autoconfig

OpenLDAP справка

DN=Distinguished Name
CN=Common Name
O=organizationName
OU=organizationalUnitName
DC=domainComponent
UID=userId

-x	Простая аутентификация
-D «cn=...,dc=...»	bind
-w … -W	password
-y /...	Password file
-h host	адрес

Учётные записи: LDAP

phpLDAPadmin

LDAP Account Manager

OpenLDAP / Fedora Directory Server / Apache Directory Project / Mandriva Directory Server

Учётные записи: NIS+

Не делайте так :)

Учётные записи: passwd

passwd, shadow, hosts, tcb, group, …

Rsync — только с узлов!

$ rsync -a server:/etc/passwd /etc/passwd

Управление

- ssh
- ssh + bash
- pdsh
- IPMI / ILO
- iKVM

PDSH

```
$ pdsh -w 'node-[01-10]' 'w| grep loadaverage'
```

-a	выполнить команду на всех машинах, перечисленных в hostfile (см. ниже)
-w	выполнить команду на перечисленных узлах. Список задаётся через запятую (без пробелов), можно использовать диапазоны чисел, например node-[10-20]. Если в качестве списка указан '-', то список читается со стандартного ввода.
-x	исключить перечисленные узлы
-g	запустить команду на узлах перечисленных групп, список групп задаётся через запятую

PDSH

-f	задать число параллельных потоков исполнения
-u	задать таймаут в секундах выполнения команды на узле (по умолчанию таймаута нет)
-l	Выполнять команду от имени указанного пользователя (аналогично ssh)
-b	Прекращать выполнение по нажатию Ctrl-C (по умолчанию по нажатию Ctrl-C выдаётся текущий статус выполнения, а по второму выполнение прекращается)

PDSH

/etc/pdsh/machines

/etc/**dsh**/group/{g1,g2,g3...}
~/**.dsh**/group/{g1,g2,g3...}

WCOLL = имя файла со списком узлов

Screen

Ctrl+a

c = create
k = kill
d = detach
n = next
p = prev.
h/H = hardcopy/start log
C-x = lock

IPMI

ipmitool

```
modprobe    ipmi_devintf
            ipmi_si
            ipmi_msghandler
```

```
Ipmitool -I lan/lanplus -H host -U user
         -P password  COMMAND
```

IPMI

Команды:

lan	настройка сети
power	on/off/reset/cycle
mc	управление контроллером
sensor	печать датчиков
sol	activate
user	управление пользователями
channel	настройка каналов
session	информация о сессии
shell	ввод команд интерактивно

IPMI

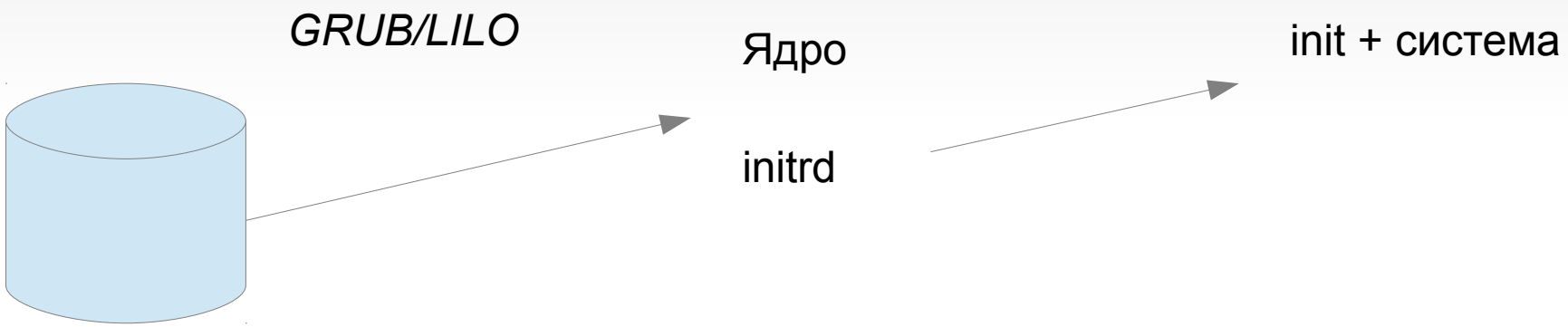
 # ipmitool lan print

```
Set in Progress         : Set Complete
Auth Type Support       : NONE MD2 MD5 PASSWORD
Auth Type Enable        : Callback : NONE MD2 MD5 PASSWORD
                        …
                        : OEM      : NONE MD2 MD5 PASSWORD
IP Address Source       : Static Address
IP Address              : 172.21.30.111
Subnet Mask             : 255.255.255.0
MAC Address             : 00:e0:81:46:0b:7d
Default Gateway IP      : 0.0.0.0
Default Gateway MAC     : 00:00:00:00:00:00
Backup Gateway IP       : 0.0.0.0
Backup Gateway MAC      : 00:00:00:00:00:00
802.1q VLAN ID          : Disabled
802.1q VLAN Priority    : 0
```

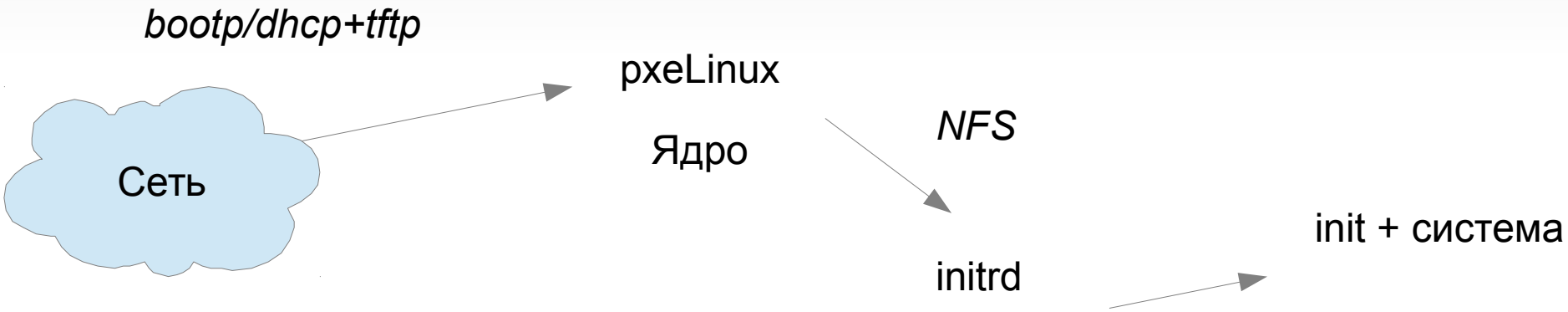
IPMI

```
# ipmitool lan set

usage: lan set <channel> <command> [option]

LAN set commands:
  ipaddr <x.x.x.x>                  Set channel IP address
  netmask <x.x.x.x>                 Set channel IP netmask
  macaddr <x:x:x:x:x:x>             Set channel MAC address
  defgw ipaddr <x.x.x.x>            Set default gateway IP address
  defgw macaddr <x:x:x:x:x:x>       Set default gateway MAC address
  bakgw ipaddr <x.x.x.x>            Set backup gateway IP address
  bakgw macaddr <x:x:x:x:x:x>       Set backup gateway MAC address
  password <password>               Set session password for this
channel
```

Сетевая загрузка



Сетевая загрузка



Сетевая загрузка

- Одновременная загрузка
- Каталоги /var, /tmp, /etc
- Раздел подкачки
- Имя узла
- Syslog

DHCP

DHCP (Dynamic Host Configuration Protocol)
BOOTP

Порт: 67 (68)

DHCPDISCOVER DHCPOFFER
DHCPREQUEST DHCPACK

DHCP

```
max-lease-time 1200;
default-lease-time 600;
ddns-update-style none; ddns-updates off;

subnet 10.0.0.0 netmask 255.0.0.0 {
        range 10.0.5.0 10.0.5.100;
        allow unknown-clients;

        allow bootp;
        filename "pxelinux.0";
        next-server 10.0.0.2;
        option routers 10.0.0.2;
        option ntp-servers 10.2.0.1;
        option domain-name-servers 10.0.0.1,10.0.0.2;
        host monitor-1 {
                fixed-address 10.0.0.11;
                hardware ethernet 00:30:48:7E:00:42;
                option host-name monitor-1;
        }
}
```

PXE+TFTP

Syslinux → /var/lib/tftpboot

pxelinux.cfg/default

```
default myimage
prompt 1
timeout 5

label myimage
  kernel img1/vmlinuz
  append initrd=img1/initrd ip=dhcp root=/dev/nfs
nfsroot=10.0.0.2:/noderoot.new,rsize=8192,wsize=8192,retrans
=10,soft,intr console=tty0 console=ttyS1,115200n8
```

Хранение данных

Файловый сервер

Сервер архивирования

- ✔ Дисковый массив - NAS / распределённая ФС
- ✗ iSCSI / ATA over Ethernet / ...

Сетевые файловые системы

NFS

PanFS

Lustre

GPFS

GlusterFS

GFS

Hadoop/GoogleFS/...

NFS

RPC, portmap

portmap, nfsd, mountd

Число nfsd-процессов ~ число активных клиентов

Файловые системы

NFS

/etc/exports: список экспортируемых файловых систем

/path/to/fs кому_можно(опции) [кому_можно(опции) ...]

кому_можно: *, 1.2.3.4/24

опции:
- (no_)root_squash
- sync/async
- no_subtree_check
- ro/rw

exportfs -v / -r

NFS

/etc/exports

/export/dir host1,host2,host3(rw,root_squash)

all_squash	все пользователи клиента будет иметь права nobody (см. ниже) на сервере
anonuid	пользователь, права которого будут даны клиентам при операциях root_squash или all_squash (по умолчанию — nobody)
anonguid	аналогично anonuid, но для группы
(no_)subtree_check	не производить проверки прав пользователей в каталогах выше точки монтирования
async	позволить серверу подтверждать операции до их реального выполнения
sync	подтверждать операции только после их выполнения.

NFS

/etc/fstab

1.2.3.4/export/dir /dir nfs rw,sync 0 0

soft/hard	hard (по умолчанию) заставляет клиента повторять запрос до тех пор, пока не будет получен ответ. soft прекращает посылки после retrans посылок
retrans=n	число перепосылок запроса серверу
rsize/wsize=n	максимальный размер пакета для операций чтения/записи в байтах
ac/noac	клиент может/нет кешировать атрибуты файлов.
proto=udp/tcp	какой протокол использовать для соединения
intr/nointr	можно/нельзя прерывать файловые операции
acl/noacl	использовать/нет вспомогательный протокол NFSACL
nfsvers=N	использовать версию NFS N
sync/async	отсылать данные серверу до выхода из системного вызова
lock/nolock	разрешить/нет использование дополнительного протокола, позволяющего делать вызов flock для файлов на NFS

NFS

$ exportfs -r

$ exportfs -a

$ showmount -a

$ showmount -e

Управление: блокировки

chage -E 1 (-E -1)

passwd -L

Не работают для ssh. Можно включить и настроить pam, тогда заработают.

chmod 0 .ssh/authorized_keys

pam_listfile

pam_access

Управление: блокировки

pam_access:

/etc/security/access.conf

+/- : кто : откуда

+ : root @sudo : crond :0 tty1 tty2 tty3

- : root : ALL

+ : @sudo : 192.168.

- : @sudo : ALL

Управление: квоты

Дисковые: quota/quotacheck/setquota

setquota -u | -g NAME -a | /dev/sda

repquota …

quotaon/quotaoff

quotacheck

Управление: квоты

Процессор, память, и т. п.: ulimit

/etc/secure/limits.conf

ulimit -l = locked memory

ulimit -s = stack size

ulimit -u = user processes

ulimit -t = cpu time

Управление: квоты

/etc/security/limits:

```
*              soft    cpu             100
@users         hard    nproc           50
```

/etc/securetty