Содержание

4 System requirements to install the operating system for SORM-3 information system

Устанавливается ОС CentOS 7 x86_64 (http://mirror.yandex.ru/centos/7/isos/x86_64/CentOS-7-x86_64-Minimal-1804.iso). SELinux выключать не нужно. После установки пользователем root выполнить команду `yum update -y`. После завершения установки обновлений выполнить перезагрузку (`shutdown -r now`).

После перезагрузки выполнить установку вспомогательного ПО командой `yum install -y vim-enhanced sudo mc git gcc openssl-devel wget screen sysstat setroubleshoot ntp lvm2 epel-release vsftpd`.

1. Характеристики подсистемы ввода-вывода:

a. Диски, видимые в операционной системе, должны иметь резервирование (> RAID0), подразумевающее работу системы при выходе из строя одного физического диска;

b. Тома, на которых создаётся файловая система для PostgreSQL, должны обеспечивать latency не выше 10-12 ms при 3000 iops на запись (sequential write) и 7000 iops на чтение (sequential read).

2. Распределение дискового пространства OS:

a. Установка должна использовать LVM для всех файловых систем;

b. При совмещении корневой файловой системы и файловой системы /var необходим размер не менее 100GB для совмещённой файловой системы;

c. Если корневая файловая система не совмещена с файловой системой /var, то размер этих файловых систем должен быть не менее 50GB;

d. Файловая система /opt должна располагаться на отдельном logical volume в отдельной volume group; размер не менее 100GB;

e. Файловая система /var/lib/pgsql должна располагаться на отдельном logical volume в отдельной volume group; размер рассчитывается оператором исходя из пропускной способности канала Типовые варианты оборудования СОРМ-3. В случае использования нескольких дисков для данной VG, LV должен создаваться с использованием stripe (ключи -i и -I); количество stripes == количеству дисков.

3. Требования к настройке ОС

a. Пользователям группы wheel устанавливается разрешение использовать все команды в контексте всех пользователей: добавить в /etc/sudoers строку `%wheel ALL=(ALL) NOPASSWD: ALL`

b. создать пользователей:

```
useradd -m -g wheel -u 3000 AAlekseenko
useradd -m -g wheel -u 3001 Ilya.Volzhev
useradd -m -g wheel -u 3002 denis.alexandrov
useradd -m -g wheel -u 3003 stanislav.polevik
useradd -m -g wheel -u 3004 andrey.voloshin
useradd -m -g wheel -u 3005 alexander.suleymanov
useradd -m -g wheel -u 3006 kirill.ivanov
useradd -m -g wheel -u 3007 konstantin.mikhaylov

openssl rand -base64 32 | passwd --stdin AAlekseenko
openssl rand -base64 32 | passwd --stdin Ilya.Volzhev
openssl rand -base64 32 | passwd --stdin denis.alexandrov
openssl rand -base64 32 | passwd --stdin stanislav.polevik
openssl rand -base64 32 | passwd --stdin andrey.voloshin
openssl rand -base64 32 | passwd --stdin alexander.suleymanov
openssl rand -base64 32 | passwd --stdin kirill.ivanov
openssl rand -base64 32 | passwd --stdin konstantin.mikhaylov
```

с соответствующими SSH-ключами, доступными для аутентификации:

```
mkdir ~AAlekseenko/.ssh && echo 'ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIPWzgE2at7UudgJZLAzwKlF/5Rmctqmju2qEbR8yboEi
AAlekseenko@ssh.vasexperts.ru' > ~AAlekseenko/.ssh/authorized_keys && chown
-R AAlekseenko:wheel ~AAlekseenko/.ssh
mkdir ~Ilya.Volzhev/.ssh && echo 'ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIGbzw32CWCgHfEFn68uGojHXEAzuEA8kSvPLrZQOz7/B
Ilya.Volzhev@ssh.vasexperts.ru' > ~Ilya.Volzhev/.ssh/authorized_keys &&
chown -R Ilya.Volzhev:wheel ~Ilya.Volzhev/.ssh
mkdir ~denis.alexandrov/.ssh && echo 'ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIMUlzwCAxyXDACbJ57ZtrbKstD0QJhWsfm+F6yPb5KJd
denis.alexandrov@ssh.vasexperts.ru' > ~denis.alexandrov/.ssh/authorized_keys
&& chown -R denis.alexandrov:wheel ~denis.alexandrov/.ssh
mkdir ~stanislav.polevik/.ssh && echo 'ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIBNlqVYWkvUn4pJuX7OPkUucgp4cihiZ6fFIzTUnKtEk
stanislav.polevik@ssh.vasexperts.ru' >
~stanislav.polevik/.ssh/authorized_keys && chown -R stanislav.polevik:wheel
~stanislav.polevik/.ssh
mkdir ~andrey.voloshin/.ssh && echo 'ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIPsdFrdFNudtBBWr3iIn/xyJeCL5/yLSQZT9A5LKG2GS
andrey.voloshin@ssh.vasexperts.ru' > ~andrey.voloshin/.ssh/authorized_keys
&& chown -R andrey.voloshin:wheel ~andrey.voloshin/.ssh
mkdir ~alexander.suleymanov/.ssh && echo 'ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIDJyZH9r+Pbfsklh1hjtmQwyqCVn57x8cj7y20HqfP2t
alexander.suleymanov@ssh.vasexperts.ru' >
~alexander.suleymanov/.ssh/authorized_keys && chown -R
alexander.suleymanov:wheel ~alexander.suleymanov/.ssh
mkdir ~kirill.ivanov/.ssh && echo 'ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIKSbxFhBHiPxRYvReknp0Rez5YK76p2LFkcOn7mj03co
kirill.ivanov@ssh.vasexperts.ru' > ~kirill.ivanov/.ssh/authorized_keys &&
chown -R kirill.ivanov:wheel ~kirill.ivanov/.ssh
```

```
mkdir ~konstantin.mikhaylov/.ssh && echo 'ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAII/0LHqdxq6Fo4v+w55rbYoe3ElJWk4Vf+/dY3GCWYY/
konstantin.mikhaylov@ssh.vasexperts.ru' >
~konstantin.mikhaylov/.ssh/authorized_keys && chown -R
konstantin.mikhaylov:wheel ~konstantin.mikhaylov/.ssh
```

c. Пользователю root в качестве доступных для аутентификации ключей добавить следующие ключи:

```
mkdir /root/.ssh
echo 'ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAILBz8xQUuLBZzVqSph0RGVLIuqyYMOTLYp/y1e3jmV7F
evgueni.gavrilov@it-grad.ru' >> /root/.ssh/authorized_keys
echo 'ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAILLzeWIDUXmUqFIriBvLUkv/PFdcm8rgThYyG8ZnwdLq
dmitry.kozlov@it-grad.ru' >> /root/.ssh/authorized_keys
```

Кроме того, необходимо убедиться, что аутентификация пользователя root в sshd возможна с помощью SSH-ключей: в файле `/etc/ssh/sshd_config` параметр `PermitRootLogin` не должен быть выставлен в значение `no`; допустимыми значениями является `without-password` (аутентификация только по ключам) или `yes` (аутентификация доступна и по паролю, и по ключу).

d. В качестве firewall используется firewalld

e. Переключить sshd на порт 22022/tcp.

в SELinux добавить нестандартный порт к списку разрешённых к использованию командой

```
semanage port -a -t ssh_port_t -p tcp 22022
```

Внести изменение в файл конфигурации `/etc/ssh/sshd_config` по-умолчанию можно следующей командой:

```
sed -i.BAK -e 's,^#Port 22,Port 22022,' /etc/ssh/sshd_config
```

либо вручную изменить параметр `Port` на значение 22022.

Добавить доступ с ssh.vasexperts.ru (5.101.76.50):

```
firewall-cmd --permanent --add-rich-rule='rule family="ipv4" source
address="5.101.76.50/32" port port=22022 protocol="tcp" accept'
firewall-cmd --reload
```

непосредственно переключение на использование нестандартного порта произвести командой

```
systemctl reload sshd
```

g. аналогичным образом при необходимости добавить "свои" IP-адреса

h. создать пользователя cdr (от этого пользователя будет производиться выгрузка данных оператора связи из биллинга или NAT трансляций):

```
useradd -m -s /sbin/nologin cdr
openssl rand -base64 32 | passwd --stdin cdr
```

i. конфигурацию vsftpd (файл `/etc/vsftpd/vsftpd.conf`) привести к следующему виду:

```
listen=YES
background=YES
pam_service_name=vsftpd
tcp_wrappers=YES
anonymous_enable=NO
local_enable=YES
write_enable=YES
connect_from_port_20=NO
xferlog_enable=NO
xferlog_file=/var/log/vsftpd.log
async_abor_enable=YES
chroot_local_user=YES
chroot_list_enable=NO
chroot_list_file=/etc/vsftpd/chroot_list
allow_writeable_chroot=YES
userlist_enable=NO
userlist_deny=NO
user_config_dir=/etc/vsftpd/users
force_dot_files=YES
local_umask=022
dirmessage_enable=YES
pasv_enable=YES
pasv_max_port=10100
pasv_min_port=10090
hide_file=NO
tcp_wrappers=YES
ascii_upload_enable=YES
ascii_download_enable=YES
local_umask=022
```