

Школьный сервер через ssh

Автор: Владимир Волков

Практически все необходимые для администрирования школьного сервера функции выполняются через веб-интерфейс. Но в некоторых случаях (например, как в случае с установкой какой-то своей CMS или LMS) необходимо выполнить ряд действий непосредственно из shell. Если сервер это компьютер, который стоит под рукой, и к нему подключены клавиатура и монитор, то проблем нет, всегда можно войти в обычный shell. Но если сервер установлен "как надо", то есть вдали от всех людей, и монитор от него отключен, а клавиатура старательно скрыта от глаз, то встает вопрос о доступе к серверу через ssh.

Сделать это очень просто, как говорится, в три приема.

Создание ключа

На том компьютере (назовем его клиентским), с которого вы хотите получить доступ на сервер, и под той учетной записью на клиентском компьютере, из-под которой вы хотите осуществлять администрирование, нужно создать пару ключей RSA. Для этого нужно на клиентском компьютере запустить Konsole, и выполнить команду **ssh-keygen**:

```
[shkoliar@localhost ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/shkoliar/.ssh/id_rsa):
/home/shkoliar/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/shkoliar/.ssh/id_rsa.
Your public key has been saved in /home/shkoliar/.ssh/id_rsa.pub.
The key fingerprint is:
8e:d8:db:b0:bb:05:46:50:34:0d:e4:71:01:32:d3:2e shkoliar@localhost.localdomain
[shkoliar@localhost ~]$ █
```

В ходе выполнения программы **ssh-keygen** вам будут заданы вопросы:

Enter file in which to save the key (/home/shkoliar/.ssh/id_rsa) - Введите полное имя файла, в котором будет сохранен ключ. Как видите, по умолчанию программа предлагает сохранить ключ в домашнем каталоге, в скрытой папке `/.ssh` - пусть там и сохраняет.

Второй вопрос: **Enter passphrase (empty for no passphrase) - Введите пароль, если пароль не нужен, нажмите Enter.** Это место нуждается в пояснении. Пароль, по большому счету, тут не нужен вообще. Но если вы оставляете свое рабочее место, и опасаетесь, что за то время, пока вы отсутствуете, кто-то может из вашей учетной записи запустить ssh и поадминить Школьный Сервер - в этом случае вы можете защитить ssh-авторизацию дополнительным паролем, который нужно будет вводить при установлении ssh-соединения.

После того, как вы введете дважды, или вообще не введете пароль, программа **ssh-keygen** создаст пару ключей. Один из этих ключей является приватным, и должен оставаться там, где был создан, а вот второй ключ, публичный, вам надо извлечь из скрытой папки. Лучше всего скопировать файл `id_rsa.pub` на рабочий стол. На этом создание ключа можно считать завершенным.

Настройка сервера

Для того, чтобы настроить сервер для работы по ssh, нужно запустить веб-интерфейс к системе управления сервером. Предположим, что **NAME** это имя или ip-адрес компьютера, на котором находится сервер. С клиентской машины нужно в строке браузера набрать **https://NAME:8080**. На экран будет выведено

окно инструмента настройки сервера.

В этом окне слева щелкните на пункте **Сеть - Брандмауэр**. У меня по непонятной причине на экран было выведено окно с независимыми пунктами выбора, в которых не был установлен ни один флажок. **ВНИМАНИЕ:** минимум флажков, которые вы должны установить, показан на рисунке ниже.

Разрешить входящие соединения на внешних интерфейсах:

- | | |
|--------|---|
| Службы | <input checked="" type="checkbox"/> Центр управления системой (www) |
| | <input type="checkbox"/> Система печати CUPS |
| | <input type="checkbox"/> DHCP-сервер |
| | <input type="checkbox"/> DNS-сервер |
| | <input type="checkbox"/> Передача файлов (FTP) |
| | <input type="checkbox"/> Служебные пакеты (ICMP) |
| | <input type="checkbox"/> Почтовый сервер (IMAP) |
| | <input type="checkbox"/> LDAP |
| | <input type="checkbox"/> Почтовый сервер (POP3) |
| | <input type="checkbox"/> Прокси-сервер |
| | <input type="checkbox"/> Файловый сервер (Samba) |
| | <input type="checkbox"/> Почтовый сервер (SMTP) |
| | <input type="checkbox"/> Управление сетью (SNMP) |
| | <input checked="" type="checkbox"/> Удалённый доступ (SSH) |
| | <input type="checkbox"/> Удалённый доступ (telnet) |
| | <input checked="" type="checkbox"/> Web-сервер (HTTP/HTTPS) |

Если вы установите только флажок ssh, то после щелчка на кнопке **Применить** у вас и будет работать только ssh, а все остальное работать перестанет, и веб-интерфейс "отвалится". Ну и, естественно, все службы сервера, к которым вы планируете обращаться извне, тоже нужно пометить флажками, и щелкнуть на кнопке **Применить**.

Теперь нужно "скормить" серверу ваш публичный ключ. Для этого слева щелкните на пункте **Пользователи - Администратор системы**. Найдите справа поле **Положить публичный ключ для входа через ssh**, и щелкните на кнопке **Обзор**. Найдите на своем рабочем столе файл id_rsa.pub, выберите его, и затем щелкните на кнопке **Положить**. Под этой кнопкой появятся сведения о положенном вами ключе. Настройка сервера завершена.

Вход на сервер через ssh

Это происходит просто: запускаете Konsole, набираете в командной строке:

```
ssh root@NAME -C
```

и оказываетесь в shell сервера с административной учетной записью. Думаю, вы не забыли, что **NAME** это имя или ip-адрес сервера. Ключ командной строки **-C** обеспечивает сжатие данных на лету, если все происходит в высокоскоростной локальной сети, этот ключ вам может не понадобиться. Вы можете добавить простых пользователей на сервер, и входить с их учетной записью. Только вот оно вам нужно?