

Лабораторная работа 1

Целью этой лабораторной работы является демонстрация некоторых возможностей файлов в каталоге **/etc/sysconfig**. Это возможность для вас поэкспериментировать, посмотреть, как такие файлы можно использовать для изменения способа запуска службы.

В этой лабораторной работе вы будете работать с файлом **/etc/sysconfig**, связанным с **веб-сервером Apache, httpd**. Как и в случае любого другого файла конфигурации, вы должны сделать его резервную копию перед внесением каких-либо изменений. Если вы еще не установили **веб-сервер Apache**, следуйте соответствующим инструкциям в теле главы 1.

1. Сделайте резервную копию текущей версии **/etc/sysconfig/httpd**.
2. Убедитесь, что **веб-сервер Apache** работает; Вы можете перезапустить его с помощью команды **systemctl restart httpd**. Просмотрите текущие **процессы Apache** с помощью команды **ps aux | grep httpd**. Сколько процессов **Apache** в настоящее время работает?
3. Откройте файл **/etc/sysconfig/httpd** и добавьте следующую директиву:
OPTIONS="-l"
4. Просмотрите страницу руководства **httpd**. Как вы думаете, этот вариант будет делать?
5. Перезапустите **веб-сервер Apache**. Что происходит?
6. Есть ли в данный момент какие-то **процессы Apache**?
7. Восстановите исходную версию файла **/etc/sysconfig/httpd**.
8. Будь смелым. Предполагая, что вы сохранили резервную копию файла конфигурации **/etc/sysconfig/httpd**, попробуйте использовать другую опцию, основанную на шагах с 4 по 8.

Лабораторная работа 2

В этой лабораторной работе вы настроите аутентификацию на основе **открытого/закрытого ключа** между двумя системами **RHEL 7**. Любые две системы будут работать для этой цели. Просто будьте готовы использовать те же две системы в лабораториях 3, 4 и 5. При подготовке к этой лаборатории убедитесь, что у каждой системы есть обычный пользователь с именем **hawaii**. Используйте следующую кодовую фразу:

I love Linux!

Лабораторная работа 3

Повторите лабораторную работу 2, но с двумя отличиями: настройте пару ключей **ECDSA** и настройте пользователя по имени **tonga** на клиенте, настроенного для подключения к учетной записи пользователя **hawaii** на сервере.

Лабораторная работа 4

В этой лабораторной работе вы настроите безопасность на уровне пользователя на сервере **SSH**. Используйте те же системы, которые были настроены для **лабораторий 2 и 3**. Ограничьте доступ для пользователя **hawaii**, настроенного в **лаборатории 2**, а затем попытайтесь получить доступ к другой

учетной записи на **сервере SSH**. Попробуйте снова получить доступ к учетной записи администратора **root на сервере SSH**.

Лабораторная работа 5

В этой лабораторной работе вы настроите **SSH-сервер**, настроенный в предыдущих лабораторных работах, на **TCP-порт 8122**. После этого перезагрузите службу. Попробуйте подключиться локально. Настройте системы так, чтобы вы также могли подключаться из удаленной системы. В качестве дополнительной задачи повторите то же упражнение, используя **порт 8022**. Что происходит?

Лабораторная работа 6

В этой лабораторной работе вы настроите каталог **/virtual/web** с тем же контекстом файла **SELinux**, что и каталог **/var/www**. Кроме того, настройте каталог **/virtual/web/cgi-bin** с тем же контекстом файла **SELinux**, что и каталог **/var/www/cgi-bin**.