

Автор:

16.03.12 10:02 - Последнее обновление 16.03.12 10:07

Вот написал скрипты по обновлению антивирусных баз NOD32 V2* и V3*. В описаниях, все что касается V3* - стоит в скобках.

Содержание

[[убрать](#)]

- [1 Версии скрипта](#)
- [1.1 NOD32 V2*](#)
- [1.2 NOD32 V3*](#)

- [2 Что умеет скрипт.](#)
- [3 Из чего состоит](#)
- [4 Установка RAR](#)
- [5 Инсталяция](#)
- [5.1 Настройка сервера Apache для доступа к базам по паролю](#)
- [5.1.1 Создание файла с паролями](#)
- [5.1.2 Настройка сервера Apache](#)
- [5.1.3 Создание файлов .htaccess](#)

Версии скрипта

Буду тут выкладывать описание версий с датами для более удобного отслеживания за изменениями

NOD32 V2*

1. **Версия 2.8** от 20.08.2008

1. Исправлена ошибка вывода имени файла, при выкачивании, если файла не существует.

Автор:

16.03.12 10:02 - Последнее обновление 16.03.12 10:07

2. **Версия 2.7** от 17.04.2008

1. Исправлены файлы name_section1, name_section2 для выкачивания новой секции [HELPER0], [HELPER1] и [HELPER2].

2. **Версия 2.6** от 20.09.2007

1. Добавлена возможность установки пароля на базы в Apache.
2. Исправлен файл NOD32UPDATE.sh. Если базы закрыты паролем, а файл update.ver - не заархивирован, возникала ошибка.

3. **Версия 2.5** от 7.09.2007

1. Исправлен файл name_section1, для выкачивания секции [CHARON2]

2. **Версия 2.4** от 1.06.2007

1. Исправлена ошибка, при разархивации update.ver

2. **Версия 2.3** от 31.05.2007

1. Исправлена ошибка, если при обновлении билд нового файла меньше старого.

NOD32 V3*

1. Версия 2.3 - Добавлена секция [MAILSERVER].

2. Версия 2.2 - Теперь можно обновлять базы для NOD32 V4. Добавлены секции, которых не было в версии V3 [SYSTEMSTATUS0], [SYSTEMSTATUS1], [SYSTEMSTATUS2], [SYSTEMSTATUS640], [SYSTEMSTATUS641], [SYSTEMSTATUS642], [SELFDEFENSE0], [SELFDEFENSE1], [SELFDEFENSE2], [SELFDEFENSE640], [SELFDEFENSE641], [SELFDEFENSE642]. Обновляются только файлы секций arc/name_section1, arc/name_section2.

3. Версия 2.1 - Добавлены возможность скачивать базы с триального сервера <http://update.eset.com>

4. Версия 2.0 - Добавлены секции [ANTISTEALTH640], [ANTISTEALTH641], [ANTISTEALTH642], [ANTISTEALTH0], [ANTISTEALTH1], [ANTISTEALTH2]

5. Версия 1.2 beta - Исправлена ошибка в скрипте убраны лишние строки с section2 и исправлены файлы section1 и section3 (добавлена секции [SMON0],[SMON1],[SMON2].

Автор:

16.03.12 10:02 - Последнее обновление 16.03.12 10:07

6. Версия 1.1 beta - Исправлена ошибка в скрипте (не записывался номер версии файлов в update.ver)
7. Версия 1.0 beta - Пока в стадии тестирования.

Что умеет скрипт.

1. Обновляет антивирусные базы с официальных и свободных серверов.
2. Сам создает файл **update.ver**. Те при обновлении с зеркал обновляются только компоненты с более новыми версиями.
3. При ошибке обновления восстанавливает базу в том виде, которая была до обновления.
4. Создает папку на веб сервере с файлами обновления.

Из чего состоит

1. **NOD32UPDATE.sh (NOD32_3UPDATE.sh)** - Сам скрипт
2. **update.sh (update3.sh)** - Скрипт обновления веб и восстановления базы
3. **conv.sh** - Скрипт по переводу всех файлов из кодировки utf8 (по умолчанию) в koi8-r
4. **install.htm** - Описание и установка в html формате
5. **install.txt** - Описание и установка в utf8 (преобразуется скриптом conv.sh)
6. И три файла со списком разделов обновлений.
 1. **name_section1** - основные секции
 2. **name_section2** - дополнительные секции (В версии V3* этого файла нет)
 3. **name_section3** - секции, которые могут отсутствовать в update.ver

Содержание файлов для различных версий - отличается

Установка RAR

Автор:

16.03.12 10:02 - Последнее обновление 16.03.12 10:07

Файл update.ver на офе заархивирован с помощью архиватора rar. И для работы скрипта его необходимо установить, тк он не входит в дистрибутив linux

1. Идем на <http://www.rarlab.com/download.htm> и качаем дистрибутив распаковываем его в /usr/local/src и устанавливаем rar for Linux.

```
# cd /usr/local/src/rar # make
```

Инсталляция

Выкачиваем архив [nod32update.V2.8.tar.bz2](#) , ([nod32updateV3-2.3.tar.bz2](#)) распаковываем:

1. Если Ваша система работает в **koi8-r**, то запускаем **conv.sh**. Он преобразует все необходимые файлы в koi8-г.

2. Файлы **NOD32UPDATE.sh (NOD32_3UPDATE.sh)** и **update.sh (update3.sh)** кладем в папку **/etc/upd_prog** , но можно и в другую (см ниже), а файлы **name_section*** необходимо положить в директорию **/var/lib/nod32/mirror/arc (/var/lib/nod32/mirror3/arc)**

3. В файле **NOD32UPDATE.sh (NOD32_3UPDATE.sh)** нужно указать путь, где будут храниться базы данных (**/var/lib/nod32/mirror (/var/lib/nod32/mirror3)**), имя и пароль, если обновление будет качаться с официального сайта (если со свободного, то эти строки надо закомментировать), а также имя сайта обновлений.

4. В файле **update.sh (update3.sh)** нужно указать: путь, где лежат скрипты (**/etc/upd_prog**), путь где будут лежать базы для апача (**/var/www/nod32 (/var/www/nod323)**) и путь где храняться базы (см выше)(**/var/lib/nod32/mirror (/var/lib/nod32/mirror)**).

5. Теперь в **crontab** прописываем запуск скрипта

Автор:

16.03.12 10:02 - Последнее обновление 16.03.12 10:07

```
# Обновление баз NOD32 V2* 00 09,15 * * * root /etc/upd_prog/update.sh # Обновление
баз NOD32 V3* 05 09,15 * * * root /etc/upd_prog/update3.sh
```

и наслаждаемся автоматическим обновлением 2 раза в сутки

Настройка сервера Apache для доступа к базам по паролю

Инструкция взята [тут](#)

Итак, если нам хочется настроить Ваше зеркало так, что бы только нужные пользователи могли обновляться с нашего сервера, то тогда нужно сделать следующее.

Создание файла с паролями

Файл с учетными данными обычно называется **.htpasswd** и располагается в каталоге, доступ к которому необходимо ограничить. По умолчанию в Apache запрещен доступ ко всем файлам, которые начинаются на **.ht**, так что файл с паролями, как и файл **.htaccess**, не сможет быть прочитан ни одним посетителем вашего сайта. Но для ускорения работы сервера лучше использовать конфигурационный файл **apache** и файл паролей.

В каждой строке файла паролей хранятся данные об одном пользователе. Логин и зашифрованный пароль разделены двоеточием. Пример:

```
admin:YFC5nYLiUI2ig vasya:bnqw1eZHP2Ujs
```

Допустим, что мы хотим создать доступ по паролю пользователя **admin**.

Для шифрации паролей применяется утилита **htpasswd**, которая поставляется в комплекте с Apache. Чтобы создать новый файл с данными о пользователе **admin**, войдите в каталог, где нужно ограничить доступ и будет лежать файл паролей (я использовал каталог с настройками **apache** -

```
/var/www/html/nod32 (/var/www/html/nod323)
```

и введите команду:

```
$ htpasswd -c .htpasswd admin
```

Внимание- При использовании ключа **-c** будет затерт старый файл с паролями, без всякого предупреждения.

Для добавления в уже существующий файл используется команда:

Автор:

16.03.12 10:02 - Последнее обновление 16.03.12 10:07

```
$ htpasswd .htpasswd vasya
```

После запуска, утилита попросит дважды ввести пароль и, если они совпадут, данные о пользователе будут добавлены.

Настройка сервера Apache

Теперь, чтобы включить запрос на авторизацию при попытке доступа, необходимо внести изменения в файл конфигурации.

Эти строки нужно вставить в файл конфигурации вашего сервера:

```
<Directory "/var/www/html/nod32">    AllowOverride All </Directory> <Directory  
"/var/www/html/nod323">    AllowOverride All </Directory>
```

AllowOverride AuthConfig или **AllowOverride All** - необходимо, что бы сервер при работе учитывал параметры файла

ccess

Если данные параметры установлены на весь сервер, то тут их вписывать необязательно.

После внесения изменений в файл конфигурации, не забудьте перезагрузить Apache.

.hta

Создание файлов .htaccess

Интересное описание структуры .htaccess с примерами я нашел [тут](#) .

В директориях с файлами баз (/var/www/html/nod32 и /var/www/html/nod323, в моем случае) создаем файлы .htaccess, следующего содержания

```
<FilesMatch ".(nup)$">    AuthName "Private zone"    AuthType Basic    require valid-user  
    AuthUserFile /var/www/nod323/.htpasswd    Order deny,allow    Deny from all    Allow  
from 172.16.130.0/24    Satisfy Any </FilesMatch>
```

FilesMatch ".(nup)\$" - означает, что на все файлы в данной директории с расширением .nup, сервер будет запрашивать пароль.

Вам необходимо изменить путь к файлу с паролями (AuthUserFile)- путь должен быть полным и строку-приглашение (AuthName), которая выдается на экран пользователю при запросе пароля.

Автор:

16.03.12 10:02 - Последнее обновление 16.03.12 10:07

Если Вы хотите, что бы в вашей локальной сети (172.16.130.0/24 - в моем случае) все обновлялись без пароля, добавьте еще три строки

Order deny,allow Deny from all Allow from 172.16.130.0/24 Satisfy Any

Я их показал снова, что бы было понятно, что за что отвечает.

Значение других директив вы можете узнать из документации Apache.

оригинал: [http://www.volmed.org.ru/wiki/index.php/%D0%A1%D0%BA%D1%80%D0%B8%D0%BF%D1%82_%D0%BF%D0%BE_%D0%BE%D0%B1%D0%BD%D0%BE%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8E_%D0%B0%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%BD%D1%8B%D1%85_%D0%B1%D0%B0%D0%B7_NOD32_%D0%BF%D0%BE%D0%B4_Linux_\(BASH\)#.D0.A1.D0.BE.D0.B7.D0.B4.D0.B0.D0.BD.D0.B8.D0.B5_.D1.84.D0.B0.D0.B9.D0.BB.D0.B0_.D1.81_.D0.BF.D0.B0.D1.80.D0.BE.D0.BB.D1.8F.D0.BC.D0.B8](http://www.volmed.org.ru/wiki/index.php/%D0%A1%D0%BA%D1%80%D0%B8%D0%BF%D1%82_%D0%BF%D0%BE_%D0%BE%D0%B1%D0%BD%D0%BE%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8E_%D0%B0%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%BD%D1%8B%D1%85_%D0%B1%D0%B0%D0%B7_NOD32_%D0%BF%D0%BE%D0%B4_Linux_(BASH)#.D0.A1.D0.BE.D0.B7.D0.B4.D0.B0.D0.BD.D0.B8.D0.B5_.D1.84.D0.B0.D0.B9.D0.BB.D0.B0_.D1.81_.D0.BF.D0.B0.D1.80.D0.BE.D0.BB.D1.8F.D0.BC.D0.B8)

ссылка на материал: http://thin.kiev.ua/index.php?option=com_content&view=article&id=546:nod32update&catid=39:linux&Itemid=63

{comments on}