NoDeny Next

Встановлення NoDeny Next на Debian

Установка NoDeny+ на Debian мені потрібна, т.к. всі свої сервери я тримаю на віртуалках, а як відомо, у FreeBSD проблеми зі швидкістю запису на диск під KVM QEMU!

До того ж, я не використовую файрвол білінгу, який заточений під FreeBSD

NoDeny завантаження

на момент написання статті є 3 репозиторії:

- демоверсія `svn://nodeny-plus.com.ua/nodenyfree`
- стабільна `svn://nodeny-plus.com.ua/release`
- нова гілка `svn://nodeny-plus.com.ua/release/next`

я буду використовувати останній, оскільки у мене є підписка 

і так, завантажуємо білінг

```
cd /usr/local
svn co svn://nodeny-plus.com.ua/release/next nodeny
```

Ставимо пакети для білінгу

```
apt-get install -y libcrypt-rijndael-perl libdbd-mysql-perl libjson-perl libnet-arp-perl libcpanel-json-xs-perl
liblwp-protocol-https-perl libcgi-pm-perl
```

liqpay\pingserver\та інші

```
apt-get install -y libxml-simple-perl libdigest-sha-perl liblwp-useragent-determined-perl libcrypt-ssleay-perl
```

для telegram

```
cpanm -n WWW::Telegram::BotAPI
```

для ponmon

```
apt-get install -y snmp libnet-telnet-cisco-perl libparallel-forkmanager-perl
cpanm -n Net::SNMP::Util
```

Web Server

Встановлення Apache

```
apt-get install -yq apache2
```

Включаємо потрібні нам модулі для опача:

```
sudo a2enmod ssl rewrite suexec include cgid
```

Створимо конфіг замість дефолтного

```
nano /etc/apache2/sites-available/nodeny.conf
```

з таким вмістом

```
<VirtualHost *:80>
    ServerAdmin admin@example.com
    ServerName example.com
    ServerAlias □□www.example.com
    DocumentRoot /var/www/nodeny
<FilesMatch "\.(pl|cgi|shtml|phtml|php)$">
    AddHandler cgi-script .pl
    Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
</FilesMatch>
<IfModule alias_module>
    ScriptAlias □□/cgi-bin/ "/usr/lib/cgi-bin/"
    #ErrorDocument 404 "/cgi-bin/stat.pl"
    DirectoryIndex "/cgi-bin/stat.pl"
</IfModule>
<IfModule !alias_module>
    DirectoryIndex index.html
</IfModule>
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Створимо симлінки для білінгу

```
rm -fR /usr/lib/cgi-bin
ln -s /usr/local/nodeny/htdocs/ /var/www/nodeny
ln -s /usr/local/nodeny/cgi-bin/ /usr/lib/cgi-bin
```

Виставимо права

```
perl /usr/local/nodeny/install.pl -w=www-data
```

Застосовуємо свій конфіг

```
sudo a2ensite nodeny.conf
sudo a2dissite 000-default.conf
```

перевіримо помилки конфігурації

```
sudo apache2ctl configtest
```

Ви повинні побачити наступний результат:

```
Syntax OK
```

Застосовуємо зміни

```
systemctl restart apache2
systemctl status apache2
```

Відкриваємо порти фаєрволу

```
sudo ufw allow http
sudo ufw allow https
sudo ufw reload
```

(1) Для включення https https://www.8host.com/blog/sozdanie-sertifikata-lets-encrypt-dlya-apache-v-debian-10/

База даних

Я не використовуватиму MySQL, оскільки з білінгом чудово працює і MariaDB! Джерело
А на MariaDB можна буде підняти Galera Cluster!

Починаючи з версії MariaDB 10.11 її кодова база суттєво відійшла і втратила сумісність з іншими форками MySql.

Критичні відмінності в роботі з GTID унеможливлюють реплікацію з іншими форками, а одже і міграцію на них без простою БД.

На мою думку, краще використовувати Percona MySQL Server 8

Delete! Цей розділ більше мені не потрібен, тому з часом, його буде видалено

https://blog.programs74.ru/how-to-install-mariadb-10-5-on-debian-10/

```
apt-get install -y mariadb-server libmariadbclient-dev libmariadbclient-dev-compat
systemctl status mariadb
```

```
sudo mysql_secure_installation
```

```
-- It does not ask me for any password
sudo mysql
```

```
-- Then in MariaDB/MySQL console:
UPDATE mysql.user SET plugin = 'mysql_native_password' WHERE USER='root';
FLUSH PRIVILEGES;
exit;
```

https://galeracluster.com/library/documentation/galera-manager-monitoring-clusters.html
https://galeracluster.com/library/documentation/galera-manager.html
https://bogachev.biz/2017/03/28/neskolko-sposobov-vosstanovleniya-mariadb-galera-cluster/
https://galeracluster.com/library/documentation/arbitrator.html

fix [Warning] [MY-013360] [Server] Plugin sha256_password reported

2022/03/05 03:01 · Method

```
mysql -u root -p
```

Створимо базу даних nodeny

```
create database nodeny;
use nodeny;
source /usr/local/nodeny/bill.sql;
```

```
```

Install apache2 php phpMyAdmin

Встановлення Apache

```
apt-get install -yq apache2
```

Включаємо потрібні нам модулі для апача:

```
sudo a2enmod ssl
sudo a2enmod rewrite
sudo a2enmod suexec
sudo a2enmod include
```

Застосовуємо зміни

```
systemctl restart apache2
systemctl status apache2
```

(1) Для включення https https://www.8host.com/blog/sozdanie-sertifikata-lets-encrypt-dlya-apache-v-debian-10/

2022/03/05 02:05 · Method

https://computingforgeeks.com/install-phpmyadmin-with-apache-on-debian-10-buster/

Install phpMyAdmin php

```
sudo apt -y install wget php php-cgi php-pear php-mbstring php8.2-gettext libapache2-mod-php php-common php-phpseclib php-mysql
```

```
cd /tmp
DATA="$(wget https://www.phpmyadmin.net/home_page/latest.txt -q -O-)"
URL="$(echo $DATA | cut -d ' ' -f 3)"
VERSION="$(echo $DATA | cut -d ' ' -f 1)"
wget https://files.phpmyadmin.net/phpMyAdmin/${VERSION}/phpMyAdmin-${VERSION}-all-languages.tar.gz
tar xvf phpMyAdmin-${VERSION}-all-languages.tar.gz
```

Delete compressed file and move the resulting folder to /usr/share/phpmyadmin folder.

```
rm *.tar.gz
sudo mv phpMyAdmin-*/ /var/www/phpmyadmin
```

Create directory for phpMyAdmin temp files.

```
sudo mkdir -p /var/lib/phpmyadmin/tmp
sudo chown -R www-data:www-data /var/lib/phpmyadmin
sudo mkdir /etc/phpmyadmin/
sudo cp /var/www/phpmyadmin/config.sample.inc.php  /var/www/phpmyadmin/config.inc.php
nano /var/www/phpmyadmin/config.inc.php
```

```
#Edit the file and set secret passphrase:
$cfg['blowfish_secret'] = 'H2OxcGXxflSd8JwrwVlh6KW6s2rER63i';
```

```
//Configure Temp directory by add
$cfg['TempDir'] = '/var/lib/phpmyadmin/tmp';
```

```
nano /etc/apache2/conf-available/phpmyadmin.conf
```

```
# phpMyAdmin default Apache configuration

Alias /pma /var/www/phpmyadmin

<Directory /var/www/phpmyadmin>
    Options SymLinksIfOwnerMatch
    DirectoryIndex index.php

    <IfModule mod_php5.c>
        <IfModule mod_mime.c>
            AddType application/x-httpd-php .php
        </IfModule>
        <FilesMatch ".+\.php$">
            SetHandler application/x-httpd-php
        </FilesMatch>

        php_value include_path .
        php_admin_value upload_tmp_dir /var/lib/phpmyadmin/tmp
        php_admin_value open_basedir /var/www/phpmyadmin/:/etc/phpmyadmin/:/var/lib/phpmyadmin/:/var/www/php/php-
gettext/:/var/www/php/php-php-
gettext/:/var/www/javascript/:/var/www/php/tcpdf/:/var/www/doc/phpmyadmin/:/var/www/php/phpseclib/
        php_admin_value mbstring.func_overload 0
    </IfModule>
    <IfModule mod_php.c>
        <IfModule mod_mime.c>
            AddType application/x-httpd-php .php
        </IfModule>
        <FilesMatch ".+\.php$">
            SetHandler application/x-httpd-php
```

```
        </FilesMatch>

        php_value include_path .
        php_admin_value upload_tmp_dir /var/lib/phpmyadmin/tmp
        php_admin_value open_basedir
/var/www/phpmyadmin/:/etc/phpmyadmin/:/var/lib/phpmyadmin/:/usr/share/php/php-gettext/:/usr/share/php/php-php-
gettext/:/usr/share/javascript/:/usr/share/php/tcpdf/:/var/www/doc/phpmyadmin/:/usr/share/php/phpseclib/
        php_admin_value mbstring.func_overload 0
    </IfModule>

</Directory>

# Authorize for setup
<Directory /var/www/phpmyadmin/setup>
    <IfModule mod_authz_core.c>
        <IfModule mod_authn_file.c>
            AuthType Basic
            AuthName "phpMyAdmin Setup"
            AuthUserFile /etc/phpmyadmin/htpasswd.setup
        </IfModule>
        Require valid-user
    </IfModule>
</Directory>

# Disallow web access to directories that don't need it
<Directory /var/www/phpmyadmin/templates>
    Require all denied
</Directory>
<Directory /var/www/phpmyadmin/libraries>
    Require all denied
</Directory>
<Directory /var/www/phpmyadmin/setup/lib>
    Require all denied
</Directory>
```

You can restrict access from specific IP by adding line like below

```
Require ip 127.0.0.1 192.168.18.0/24
```

```
a2enconf phpmyadmin.conf
systemctl reload apache2
systemctl restart apache2
```

Visit phpMyAdmin Web interface Open the URL http://[ServerIP/Hostname]/pma to login into phpMyAdmin dashboard with your Database credentials – username & password.

2022/03/05 03:19 · Method

Webmin

For simply management OS

```
wget https://raw.githubusercontent.com/webmin/webmin/master/setup-repos.sh
sh setup-repos.sh -f
apt-get install --install-recommends webmin
```

Edit webmin config

```
nano /etc/webmin/miniserv.conf
```

Setting port & disable ssl via change next

```
ssl=0
port=8000
```

Apply changes

```
systemctl restart webmin
```

Open firewall

NFTables

```
nft add rule inet filter input ct state new tcp dport 8000 counter accept comment "WEBMIN"
```

Open http://[Host_ip]:8000/ in your browser & log in with your system credentials – username & password.

Сертифікат

Якщо на сервері вже використовується сертифікати для apache або nginx від `Let`s Encrypt`, то наступними кроками можна додати їх до webmin:

встановимо змінну оточення з нашим доменом

```
XDOMAIN="isp.example.com"
```

виконаємо заміну параметрів

```
cat /etc/webmin/miniserv.conf > /etc/webmin/miniserv.conf.bak

# Змінити або додати port
grep -q '^port=' /etc/webmin/miniserv.conf && \
  sed -i "s/^port=.*/port=8000/" /etc/webmin/miniserv.conf || \
  echo "port=8000" >> /etc/webmin/miniserv.conf

# Змінити або додати listen
grep -q '^listen=' /etc/webmin/miniserv.conf && \
  sed -i "s/^listen=.*/listen=8000/" /etc/webmin/miniserv.conf || \
  echo "listen=8000" >> /etc/webmin/miniserv.conf
```

```
# Змінити або додати keyfile
grep -q '^keyfile=' /etc/webmin/miniserv.conf && \
  sed -i "s|^keyfile=.*|keyfile=/etc/letsencrypt/live/${XDOMAIN}/privkey.pem|" /etc/webmin/miniserv.conf || \
  echo "keyfile=/etc/letsencrypt/live/${XDOMAIN}/privkey.pem" >> /etc/webmin/miniserv.conf

# Змінити або додати extracas
grep -q '^extracas=' /etc/webmin/miniserv.conf && \
  sed -i "s|^extracas=.*|extracas=/etc/letsencrypt/live/${XDOMAIN}/fullchain.pem|" /etc/webmin/miniserv.conf || \
  echo "extracas=/etc/letsencrypt/live/${XDOMAIN}/fullchain.pem" >> /etc/webmin/miniserv.conf

# Змінити або додати certfile
grep -q '^certfile=' /etc/webmin/miniserv.conf && \
  sed -i "s|^certfile=.*|certfile=/etc/letsencrypt/live/${XDOMAIN}/cert.pem|" /etc/webmin/miniserv.conf || \
  echo "certfile=/etc/letsencrypt/live/${XDOMAIN}/cert.pem" >> /etc/webmin/miniserv.conf

systemctl restart webmin
```

2022/03/05 03:27 · Method

FreeRadius

https://kifarunix.com/install-freeradius-with-daloradius-on-debian-9/

Даний варіант установки не з офіційної документації і розроблений для нашої мережі, але може бути портований і в інші мережі! Він не має MySQL модуля, але є потужний модуль PERL, який дозволяє робити запити до бази набагато зручніше в плані маніпуляцій. На офіційному сайті FreeRadius сказано, що rlm_perl продуктивніше rlm_sql. Використання цього варіанта ви робите на свій страх і ризик :).

Встановлення пакетів

```
apt-get install freeradius freeradius-mysql freeradius-utils

sudo ufw allow to any port 1812 proto udp
sudo ufw allow to any port 1813 proto udp
sudo ufw reload
```

Видалимо зайве, попередньо зробивши бекап 😬

```
cp -r /etc/freeradius/3.0/ /etc/freeradius/3.0.orig/
rm /etc/freeradius/3.0/sites-enabled/*
rm /etc/freeradius/3.0/mods-enabled/eap
rm /etc/freeradius/3.0/mods-enabled/ntlm_auth
rm /etc/freeradius/3.0/mods-enabled/mschap
```

```
nano /etc/freeradius/3.0/mods-config/attr_filter/access_reject
```

поправимо тут

```
DEFAULT
# EAP-Message = * ANY,
State =* ANY,
Message-Authenticator =* ANY,
Error-Cause =* ANY,
Reply-Message =* ANY,
MS-CHAP-Error = * ANY,
Proxy-State =* ANY
```

Створимо основний конфіг

```
 nano /etc/freeradius/3.0/sites-enabled/nodeny
```

з таким вмістом:

/etc/freeradius/3.0/sites-enabled/nodeny

```
server nodeny {
    listen {
        type = auth
        ipaddr = *
        port = 1812
    }
    listen {
        type = acct
        ipaddr = *
        port = 1813
    }
    authorize {
        detail
        # preprocess
        files
        perl
    }

    authenticate {
        Auth-Type PAP {
            pap
        }
        # Auth-Type CHAP {
            # chap
        # }
        # Auth-Type MSCHAP {
            # mschap
        # }
        Auth-Type Perl {
            perl
```

```
        }
    }

    preacct {
        acct_unique
        preprocess
    }

    accounting {
        attr_filter.accounting_response
        perl
    }

    session {
        radutmp
    }

    post-auth {
        perl
    }

}
```

Також, за бажанням, можна завантажити конфіг сервера статистики

```
ln -s /etc/freeradius/3.0/sites-available/status /etc/freeradius/3.0/sites-enabled/status
```

Опишемо локальний сервер доступу для тестів, сюди ж вписуємо всі свої БРАСи за аналогією

```
echo '' > /etc/freeradius/3.0/clients.conf
nano /etc/freeradius/3.0/clients.conf
```

/etc/freeradius/3.0/clients.conf

```
client 127.0.0.1 {
ipaddr = 127.0.0.1
secret = hardpass5
shortname=NoDenyDB
nastype = cisco
}
```

```
echo '' > /etc/freeradius/3.0/users
nano /etc/freeradius/3.0/users
```

/etc/freeradius/3.0/users

```
DEFAULT Auth-Type = Perl
    Fall-Through = yes
```

```
echo '' > /etc/freeradius/3.0/mods-enabled/perl
nano /etc/freeradius/3.0/mods-enabled/perl
```

/etc/freeradius/3.0/mods-enabled/perl

```
perl {
        filename = /usr/local/nodeny/nod/_radius.pl
}
```

Я не знаю чому, але радіус відмовляється працювати з моїм скриптом на дебіані через недостатні права на файл. я перепробував всі комбінації прав та власників на файл, але результат той самий. Єдине, що допомогло, так це змінити в налаштуваннях самого радіусу користувача і групу або взагалі їх закоментувати. Я так і вчинив:)

```
nano /etc/freeradius/3.0/radiusd.conf
```

у секції “security” коментуємо користувача та групу

```
#user=freerad
# group = freerad
```

Mysql процедури

```
ALTER DATABASE nodeny CHARACTER SET utf8 COLLATE utf8_general_ci;
```

```
DELIMITER $$
CREATE DEFINER=`root`@`localhost` PROCEDURE `p5_radcheck`(IN `login` VARCHAR(64))
BEGIN
  DECLARE real_login VARCHAR(64) DEFAULT NULL;
  SELECT SUBSTRING_INDEX(login, '+', 1) INTO real_login;
  SELECT id, name, 'Password' AS Attribute, AES_DECRYPT(passwd,'hardpass') AS VALUE,'=='
    FROM users WHERE name=real_login;
END$$
DELIMITER ;

DELIMITER $$
CREATE DEFINER=`root`@`localhost` PROCEDURE `p5_radupdate`(IN `login` VARCHAR(64), IN `ip` VARCHAR(16), IN
`properties` VARCHAR(255))
BEGIN
  DECLARE usr_id INT;
  DECLARE usr_ip VARCHAR(15) DEFAULT NULL;
  DECLARE real_login VARCHAR(64) DEFAULT NULL;
  DECLARE ip_index INT ;

  SELECT SUBSTRING_INDEX(login, '+', 1) INTO real_login;
  IF login REGEXP '[+][0-9]+$' THEN
```

```
  SELECT CAST(REPLACE(REPLACE(login, real_login, ''),'+','') AS UNSIGNED) INTO ip_index;
  ELSE SET ip_index=0;END IF;

  SELECT id INTO usr_id FROM users WHERE name=real_login LIMIT 1;
  SELECT get_ip_by_num(usr_id, ip_index) INTO usr_ip;
  CALL set_auth(ip, CONCAT('mod=pppoe;',REPLACE(properties,':','')));
END$$
DELIMITER ;

DELIMITER $$
CREATE DEFINER=`root`@`localhost` PROCEDURE `p5_radreply`(IN `login` VARCHAR(64))
BEGIN
  DECLARE usr_id INT;
  DECLARE ip_index INT ;
  DECLARE usr_ip VARCHAR(15) DEFAULT NULL;
  DECLARE real_login VARCHAR(64) DEFAULT NULL;

  SELECT SUBSTRING_INDEX(login, '+', 1) INTO real_login;

  IF login REGEXP '[+][0-9]+$' THEN
    SELECT CAST(REPLACE(REPLACE(login, real_login, ''),'+','') AS UNSIGNED) INTO ip_index;
  ELSE SET ip_index=0;END IF;

  SELECT id INTO usr_id FROM users WHERE name=real_login LIMIT 1;
  SELECT get_ip_by_num1(usr_id, ip_index) INTO usr_ip;

  SELECT NULL,login,'Framed-IP-Address',usr_ip,'=';
  SELECT NULL,login,'Framed-IP-Netmask','255.255.255.255','=';
  SELECT NULL,login,'Framed-Protocol','PPP','=';
END$$
DELIMITER ;

DELIMITER $$
CREATE DEFINER=`root`@`localhost` PROCEDURE `p5_radparam`(IN `login` VARCHAR(64))
```

```
BEGIN
  DECLARE usr_id INT;
  DECLARE real_login VARCHAR(64) DEFAULT NULL;

  IF login REGEXP '[+][0-9]+$' THEN
    SELECT SUBSTRING_INDEX(login, '+', 1) INTO real_login;
  ELSE SET real_login=login;END IF;

  SELECT id INTO usr_id FROM users WHERE name=real_login LIMIT 1;

  SELECT s.module, s.param FROM `v_services` s
  LEFT JOIN users u ON(s.uid=u.id)
  WHERE u.state='on' AND s.uid=usr_id AND s.tags NOT LIKE '%,wait_pos_balance,%';
END$$
DELIMITER ;

DELIMITER $$
CREATE DEFINER=`root`@`localhost` PROCEDURE `p5_radtraf`(IN `login` VARCHAR(64), IN `ses` VARCHAR(32), IN
`trafin` BIGINT(20), IN `trafout` BIGINT(20))
BEGIN
  DECLARE usr_id INT;
  DECLARE t_in BIGINT;
  DECLARE t_out BIGINT;
  DECLARE real_login VARCHAR(64) DEFAULT NULL;

  IF login REGEXP '[+][0-9]+$' THEN
    SELECT SUBSTRING_INDEX(login, '+', 1) INTO real_login;
  ELSE SET real_login=login;END IF;

  SELECT id INTO usr_id FROM users WHERE name=real_login LIMIT 1;

  SELECT trafin - IFNULL((SELECT traf_in FROM ses_traf WHERE ses_id=ses LIMIT 1),0) INTO t_in;
  SELECT trafout - IFNULL((SELECT traf_out FROM ses_traf WHERE ses_id=ses LIMIT 1),0) INTO t_out;
  UPDATE users_trf SET in1=in1 + t_in, out1=out1 + t_out WHERE uid=usr_id;
```

```
  INSERT INTO ses_traf SET ses_id=ses, traf_in=trafin, traf_out=trafout, TIME=UNIX_TIMESTAMP()
    ON DUPLICATE KEY UPDATE traf_in=trafin, traf_out=trafout, TIME=UNIX_TIMESTAMP();
  SET @s = CONCAT('INSERT INTO X', YEAR(NOW()), '_', MONTH(NOW()), '_', DAY(NOW()), ' VALUES(?,?,?,?,?,?)');
  PREPARE stmt1 FROM @s;
  SET @iface = 0;
  SET @cls = 1;
  SET @ts = CEIL(UNIX_TIMESTAMP() / 60) * 60;
  SET @usr_id = usr_id;
  SET @t_in = t_in;
  SET @t_out = t_out;
  EXECUTE stmt1 USING @usr_id, @iface, @ts, @cls, @t_in, @t_out;
  DEALLOCATE PREPARE stmt1;
END$$
DELIMITER ;
```

Завершение установки

```
systemctl enable freeradius
systemctl restart freeradius
systemctl status freeradius
```

rc.local

https://softnastroy.com/content/vklyuchaem-rclocal-v-debian-9-stretch.html

https://wiki.mikbill.pro/billing/bez_deneg