Installation: RHEL/RockyLinux/ CentOS

Inhaltsverzeichnis

Installation instructions for RHEL, RockyLinux, CentOS and alike systems with SELinux in enforcing mode.
Based on the official installation instructions:
https://github.com/OpenXE-org/OpenXE/blob/master/SERVER_INSTALL.md
https://github.com/OpenXE-org/OpenXE/blob/master/INSTALL.md

Installation instructions for RHEL, RockyLinux, CentOS and alike systems.

Tested on a RockyLinux 9 VM with SELinux in enforcing mode.

Based on the official installation instructions:

- SERVER_INSTALL.md

- INSTALL.md

1 Setup

Code

```
sudo                                    su                                      -
dnf                             install                             epel-release
dnf                                                                   update
dnf        install        https://rpms.remirepo.net/enterprise/remi-release-9.rpm
#               install               and               start               apache
dnf                                  install                                  httpd
systemctl                                start                                  httpd
systemctl                                enable                                 httpd
dnf                                  install                                    php
#                     install                       php                      modules
dnf install php-mysqlnd php-cli php80-php-imap php-common php-xml php-soap php-pecl-zip php
```

Alles anzeigen

Add the following lines to `/etc/php.ini`

Code

```
pcntl_exec,pcntl_get_last_error,pcntl_setpriority,dl,highlight_file,show_source,proc_open,popen
post_max_size                                   =                                   100M
upload_max_filesize                               =                                 100M


max_execution_time                                =                                 3600
max_input_time                                   =                                  3600
magic_quotes_gpc                                  =                                 Off
file_uploads                                    =                                   Yes
max_file_uploads                                  =                                 20
short_open_tag                                   =                                  On
max_input_vars=3000
memory_limit = 256M
```

Alles anzeigen

Add remis php imap module

Code

```
cat            <<            'EOF'            >            /etc/php.d/50-imap.ini
extension=/opt/remi/php80/root/usr/lib64/php/modules/imap.so
EOF
```

Install further packages and configure mariadb

Code

```
sudo                                        su                                      -
dnf        install        zip        wget        mod_ssl        openssl        git
#                                                                              mariadb
dnf                              install                                 mariadb-server
systemctl                               start                                  mariadb
systemctl                              enable                                  mariadb
mysql_secure_installation
```

> Zitat
>
> For mysql secure installation see: https://github.com/OpenXE-org/…/master/SERVER_INSTALL.md

2 SELinux

2.1 Booleans and user mappings

Code

```
#                                                                   Selinux
restorecon                -F                -r                -vv                /
setsebool                   -P                    httpd_unified                    1
setsebool                 -P                httpd_graceful_shutdown                1
setsebool             -P             selinuxuser_mysql_connect_enabled             1
setsebool                 -P                domain_can_mmap_files                  1
#           list           and           check           booleans           enabled
semanage          boolean          -l          |          grep          httpd_unified
#         semanage          boolean          -l          |          grep          ...
#      OPTIONAL:      if      default      user      mappings      were      changed
#         list         user         to         selinux         user         mappings
semanage                                  login                                  -l
#            map            apache            to            e.g.            user_u
semanage login -a -s user_u apache
```

Alles anzeigen

2.2 Custom SELinux policy

1. Create module file with rules

Code

```
sudo                                    su                                      -
mkdir                                                                   ~/selinux
cd                                                                      ~/selinux
cat               <<                EOF                >                openxe.cil
(allow           user_t           hugetlbfs_t           (file           (write)))
EOF
```

2. Load it into the SELinux server with a priority of e.g. `200`

Code

```
semodule              -X              200              -i              openxe.cil
semodule            --list=full             |             grep             openxe
# If necessary, you can also remove (semodule -r) or temporarily disable (semodule -d) the c
```

3 Git

Clone openxe instead downloading zip (enables UI system upgrade)

Code

```
sudo                                    su                                      -
cd                                                                  /var/www/html
ssh-keygen              -t              ed25519              -a              100
#      add      new      ssh      key      to      your      github      account
git                  clone                  git@github.com:OpenXE-org/OpenXE.git
chown                  -R                  apache:apache                  OpenXE
#      OPTIONAL:      add      custom.css      to      silence      404      error
cd                                                                      OpenXe
touch                                       www/themes/new/css/custom.css
chown                 apache:apache                www/themes/new/css/custom.css
#                   restore                  SELinux                  context
restorecon -F -r -vv /
```

Alles anzeigen

Zitat

https://github.com/OpenXE-org/OpenXE/blob/master/INSTALL.md

Check if crontab was created: `crontab -u apache -l`

Check if SELinux is blocking: `ausearch -i -m avc,user_avc,selinux_err,user_selinux_err -ts today | audit2allow`

4 Apache

Set hostname

Code

```
sudo su -
vi /etc/hostname
```

and add index.php to DirectoryIndex in httpd.conf and allow htaccess overrides in `/etc/httpd/conf/httpd.conf`

Code

```
DocumentRoot "/var/www/html"

<Directory "/var/www/html">
AllowOverride All
</Directory>

<IfModule dir_module>
DirectoryIndex index.html index.php
</IfModule>
```

Alles anzeigen

Reload apache after editing the file

Code

```
systemctl reload httpd
```

5 Custom ssl certificates

Using for example Let's Encrypt wildcard certificates via DNS challenge.

Code

```
sudo                                    su                                      -
mkdir                               -p                              /etc/pki/tls/openxe
/path/to/your-domain.com.fullchain.pem  /etc/pki/tls/openxe/your-domain.com.fullchain.pem
cp      /path/to/your-domain.com.key      /etc/pki/tls/openxe/your-domain.com.key
systemctl                             reload                                httpd
restorecon -F -r -vv /
```

Backup `/etc/httpd/conf.d/ssl.conf` and remove the whole default `<VirtualHost _default_:443>` part

Add the following as the new default

Apache Configuration

```
###               Turn               on               HTTP2               support
Protocols                               h2                                http/1.1


###        Redirect         all         http         urls         to         https
RewriteEngine                                                                  On
RewriteCond                              %{HTTPS}                             off
RewriteRule      (.*)      https://%{HTTP_HOST}%{REQUEST_URI}      [R=302,L,QSA]
<VirtualHost                                                      _default_:443>
DocumentRoot                                                 /var/www/html/OpenXE/
ServerName                                          internal-openxe.your-domain.com


###                                    Log                                    files
ErrorLog                                                       logs/ssl_error_log
TransferLog                                                   logs/ssl_access_log
LogLevel                                                                      warn
SSLEngine                                                                       on


###       No       more       -SSLv2       -SSLv3       -TLSv1       -TLSv1.1
SSLProtocol                                                                          all
SSLHonorCipherOrder
SSLCompression
SSLSessionTickets
SSLCipherSuite


###                        Path                        to                        certs
SSLCertificateFile                                                  /etc/pki/tls/openxe/yo
SSLCertificateKeyFile                                                 /etc/pki/tls/op


#   HSTS   (mod_headers   is   required)   (15768000   seconds   =   6   months)
Header     always     set     Strict-Transport-Security     "max-age=15768000"
<FilesMatch                                          "\.(cgi|shtml|phtml|php)$">
SSLOptions                                                          +StdEnvVars
</FilesMatch>
<Directory                                                    "/var/www/cgi-bin">
SSLOptions                                                          +StdEnvVars
</Directory>
BrowserMatch                   "MSIE                    [2-5]"                    \
nokeepalive                          ssl-unclean-shutdown                        \
downgrade-1.0                                                 force-response-1.0
CustomLog                           logs/ssl_request_log                        \
"%t       %h       %{SSL_PROTOCOL}x       %{SSL_CIPHER}x       \"%r\"       %b"
</VirtualHost>


###                    OCSP                    stapling                    config
SSLUseStapling
SSLStaplingResponderTimeout                                                     5
SSLStaplingReturnResponderErrors                                              off
SSLStaplingCache        shmcb:/var/run/ocsp(128000)
```

Alles anzeigen

6 Firewall

Code

```
sudo su -
firewall-cmd --list-all
firewall-cmd --permanent --zone=public --add-port=80/tcp
firewall-cmd --permanent --zone=public --add-port=443/tcp
firewall-cmd --reload
firewall-cmd                                                                --list-all
```

7 External access

As ssl was setup on the VM's apache, for controlled "external" access and if you have a reverse proxy, it can be configured using a tcp router and passthrough.

e.g. Traefik's dynamic conf file could look like the following:

Code

```
tcp:
  routers:
    openxe-tcp-router:
      entryPoints:


      middlewares:


      tls:


  services:
    openxe-service-secure:
      loadBalancer:
        servers:


  middlewares:
    openxe-ipwhitelist:
      ipWhiteList:
        sourceRange:


          # whitelisting all needed IP's
```

Alles anzeigen

8 Hints

For OnlineShop sync, add "Prozessstarter": `artikeluebertragen`

> Zitat
>
> see xentral docs for other Prozessstarter names.

9 OpenXE upgrade

OpenXE UI: System -> Upgrade