

Предварительная установка ПО (Podman)

Перед инсталляцией Loginom необходимо предварительно установить и настроить ПО.

Протестировано на **РЕД ОС 7.3.2**.

Нужно выполнить пункты:

1. Установить необходимые пакеты.

```
1  sudo dnf update && sudo dnf install -y podman slirp4netns fuse-overlayfs
   dnsmasq python3-pip
2
3  sudo pip3 install podman-compose
```

Для добавления пользователя в группу sudo необходимо добавить в файл `/etc/sudoers` запись, например, для пользователя user: `user ALL=(ALL) ALL`

2. Разрешить Podman-у использовать в непривилегированном режиме порты, начиная с 80.

```
1  grep -q "net.ipv4.ip_unprivileged_port_start=80" "/etc/sysctl.conf" ||
   echo "net.ipv4.ip_unprivileged_port_start=80" | sudo tee -a /etc/sysctl.conf
2
3  sudo sysctl -w net.ipv4.ip_unprivileged_port_start=80
```

3. Разрешить пользовательской сессии оставаться активной после выхода.

```
sudo loginctl enable-linger
```

4. Установить плагин `dnsname`. Установка возможна несколькими путями:

- Самостоятельно откомпилировать плагин из исходных кодов. Страница плагина: <https://github.com/containers/dnsname>, необходимые инструкции можно найти там же (в файле README_PODMAN.md).
- Скопировать уже откомпилированный плагин (файл плагина `dnsname` можно запросить в техподдержке).

Скопировать плагин `dnsname` :

```
sudo cp dnsname /usr/libexec/cni && sudo chmod +x /usr/libexec/cni/dnsname
```

5. Перезагрузить систему. Если не работает после перезагрузки, выполнить:

```
rm -rf $HOME/.local/share/containers/storage/libpod
```

Настройка работы контейнеров Loginom при наличии SELinux

В ОС Linux семейства RHEL, куда относятся, например, RedOS и Fedora, работает модуль безопасности ядра. Для нормальной работы системы контейнеризации возможны варианты:

1. Настроить разрешения SELinux на монтирование томов. Необходимо в файле конфигурации, располагаемом по умолчанию: `${HOME}/loginom/docker-compose.yml`, произвести некоторые изменения. Во все разделы монтирования томов, кроме монтирования файла сокета `run/systemd/journal/socket`, необходимо добавить опцию безопасности `:Z`, например:

```
- "${HTTP_DIR}/server.json:/usr/local/apache2/htdocs/client/server.json:Z"
```

2. Отключить SELinux.

```
1  sudo setenforce 0
2
3  sudo sed -i "s/SELINUX=enforcing/SELINUX=disabled/" /etc/selinux/config
```