

# Vitastor on encrypted volume

## Настройка OSD на зашифрованном томе

### Конфигурация OSD для хранения данных на зашифрованном томе

зашифровать том с помощью luks

настроить osd для хранения с помощью утилиты vitastor-disk

```
vitastor-disk prepare --data_device /dev/mapper/osd02_1 --force --disable_data_fsync off
```

Где:

`--data_device` - устройство, появившееся после расшифровки LUKS

### Конфигурация udev для обнаружения и инициализации OSD

в файле

```
/usr/lib/udev/rules.d/90-vitastor.rules
```

изменить первую строку на:

```
SUBSYSTEM=="block", ENV{DM_NAME}=="osd*", \
```

Где:

`ENV{DM_NAME}=="osd"` будет указывать на то, что данное правило стоит применять тогда, когда в системе появится устройство с именем, начинающимся на `osd`.

При применении этого правила в системе будет появляться файл `/dev/vitastor`, в котором будет появляться симлинк на нужное дисковое устройство, и может быть запущен сервис для `osd`.

После изменения правила udev необходимо применить изменения:

```
udevadm control --reload-rules
```

Так же для проверки можно выполнить: `udevadm trigger`, что заставит эмулировать запуск правила udev

