

UDV ITM

Руководство администратора
UDV-ITM-VM версии 1.7.0.0

Версия документа: 1.0
Дата выгрузки: 11.1.2024

Содержание

1. Глоссарий.....	4
2. Что нового?.....	7
2.1. Обновления документации.....	7
3. Введение.....	9
3.1. Область применения.....	9
3.2. Назначение и условия применения.....	9
4. Подготовка к работе.....	11
4.1. Состав и содержание дистрибутивного носителя данных.....	11
4.2. Установка UDV-ITM-VM на ОС РЕД ОС.....	11
4.2.1. Настройка синхронизации времени (NTP).....	12
4.2.2. Установка дополнительных пакетов в ОС РЕД ОС 7.3.....	12
4.2.3. Установка дополнительных пакетов в ОС РЕД ОС 7.3 с интернетом.....	13
4.2.4. Установка UDV-ITM-VM с отдельным томом для БД.....	14
4.2.5. Установка СУБД Jatoba версии 1.14 на РЕД ОС 7.3.....	19
4.2.6. Настройка СУБД Jatoba.....	22
4.2.7. Настройка межсетевого экрана iptables.....	26
4.2.8. Установка сервера визуализации и управления UDV-ITM-VM на ОС РЕД ОС.....	28
4.3. Установка UDV-ITM-VM на ОС Centos 8.....	31
4.3.1. Установка ОС Centos 8.....	32
4.3.2. Установка СУБД PostgreSQL v14.....	37
4.3.3. Установка Docker.....	39
4.3.4. Установка дополнительных пактов в ОС Centos 8 с интернетом.....	40
4.3.5. Настройка СУБД PostgreSQL.....	40
4.3.6. Настройка межсетевого экрана iptables.....	44
4.3.7. Установка сервера визуализации и управления UDV-ITM-VM на ОС Centos 8.....	45
4.4. Обновление UDV-ITM-VM с версии 1.6.0.0 до версии 1.7.0.0.....	49
4.5. Выпуск SSL-сертификатов.....	51
4.5.1. Выпуск корневых сертификатов.....	51
4.5.2. Выпуск сертификата и ключа для доступа к веб-интерфейсу UDV-ITM-VM.....	52
4.5.3. Настройка APM Администратора.....	53
4.6. Настройка интеграции с SIEM.....	55

4.7. Подключение к веб-интерфейсу.....	55
5. Резервное копирование и восстановление баз данных.....	57
5.1. Создание резервной копии базы данных Jatoba/PostgreSQL.....	57
5.2. Восстановление резервной копии базы данных Jatoba/PostgreSQL.....	58
6. Нештатные ситуации и способы их устранения.....	61
6.1. Конфликт подсети контейнеров.....	62
6.2. Ошибка интеграции с SIEM.....	66
6.3. Ошибка вида «WARNING overcommit_memory is set to 0! Background save may fail under low memory condition.<...>».....	67
6.4. Не запускаются контейнеры docker.....	67
6.5. Веб-интерфейс UDV-ITM-VM не загружается.....	68
6.6. Не удается зайти в веб-интерфейс UDV-ITM-VM с корректными учетными данными.....	69
6.7. Изменение имени сервера.....	72
6.8. Скрипт для сбора логов.....	73
7. Справочная информация.....	74
7.1. Совместимость компонентов решения для UDV-ITM-VM.....	74
7.2. Роли пользователей и доступные им интерфейсы.....	74
7.3. Структура директорий UDV-ITM-VM.....	75
7.4. Рекомендации по использованию антивируса на сервере UDV-ITM-VM.....	75
7.5. Переменные файла .env.....	76
7.6. Переменные файла .itmm_password_secret_key.....	77
7.7. Механизм интеграции с SIEM.....	77
7.8. Список действий пользователя, о которых отправляются события в SIEM.....	78
7.9. Формат событий для передачи в SIEM.....	78
7.9.1. Типы данных в событиях для передачи в SIEM.....	79
7.10. Содержимое файла iptables.....	82

1. Глоссарий

1.1. Автоматизированная система управления технологическим процессом

Комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления таким оборудованием и процессами.

Аббревиатура: АСУ ТП

1.2. Объект мониторинга

Объект мониторинга (узел сети) – любое устройство, приложение или система, которые подключаются к системе мониторинга для контроля качества их функционирования и предоставляемых услуг.

Аббревиатура: ОМ

1.3. Проблема объекта мониторинга

Состояние контролируемого параметра объекта мониторинга, при котором его значение выходит за пределы диапазона значений при нормальном функционировании объекта мониторинга.

1.4. Система автоматизации процессов обеспечения безопасности

Автоматизированная система, предназначенная для автоматизации процессов управления информационной безопасностью.

Аббревиатура: САОБ

1.5. Система мониторинга безопасности и контроля ресурсов

Комплексная система мониторинга ИТ-ресурсов и компонентов АСУ ТП для реализации требований по защите информации в соответствии с приказом ФСТЭК №239 от 25.12.2017.

Аббревиатура: СМБКР

1.6. Система мониторинга компьютерных инцидентов

Система сбора, анализа и корреляции событий информационной безопасности, созданная на базе решений класса SIEM.

Аббревиатура: СМКИ

1.7. Соглашение об уровне услуг

Соглашение об уровне услуг – установленный уровень качества, который считается приемлемым для данной услуги.

Аббревиатура: SLA

1.8. Технологический комплекс

Технологический комплекс промышленного или производственного предприятия, на котором используется оборудование, управляемое АСУ ТП полевого уровня.

Аббревиатура: ТК

1.9. UDV ITM

UDV ITM – торговое наименование Системы зонтичного мониторинга автоматизированных и информационных систем «Cyberlympha ITM» (свидетельство о регистрации программы для ЭВМ №2022684928, 14.12.2022 г.)

1.10. UDV-ITM-M

UDV-ITM-M – сервер мониторинга.

Применяется для:

- сбора данных о производительности с подключенных объектов мониторинга;
- консолидации данных, в т. ч. полученных с сервера удаленного мониторинга;
- передачи консолидированных данных на сервер визуализации и управления;
- визуализации информации об использовании вычислительных ресурсов и каналов связи объектов мониторинга филиала;
- оповещения ответственных лиц в случае выявления сбоя, либо отклонения показателей функционирования объекта мониторинга от допустимых.

*В ранних версиях использовалось название Сервер консолидации, ITM-K.

1.11. UDV-ITM-RM

UDV-ITM-RM – сервер удаленного мониторинга.

Применяется для:

- сбора данных о производительности с подключенных объектов мониторинга;
- передачи собранных данных на сервер мониторинга.

*В ранних версиях использовалось название Сервер агентов (прокси-сервер), ITM-A.

1.12. UDV-ITM-VM

UDV-ITM-VM – сервер визуализации и управления.

Предназначен для централизованного управления системой мониторинга в целом, консолидации данных мониторинга в масштабах всего предприятия и интеграционного взаимодействия с корпоративными системами обнаружения компьютерных инцидентов и системами автоматизации процессов обеспечения ИБ.

Применяется для:

- сбора данных с серверов консолидации и серверов мониторинга;
- предоставления высокоуровневой информации о состоянии ИТ-ресурсов предприятия пользователям и смежным системам.

2. Что нового?

Основные изменения, касающиеся администрирования ПО сервера UDV-ITM-VM версии 1.7.0.0:

Табл. 2-1 Изменения UDV-ITM-VM версии 1.7.0.0

Категория	Изменения в продукте	Разделы документации
Роли пользователей	1. Для авторизованных пользователей исключена возможность перехода на страницу авторизации без завершения текущей сессии. 2. Для роли «Пользователь» добавлены следующие возможности: <ul style="list-style-type: none">• просмотр списка и карточек пользователей на странице <i>Настройки</i> → <i>Пользователи</i>;• просмотр списка и карточек правил оповещений на странице <i>Настройки</i> → <i>Правила оповещений</i>;• создание, изменение, включение, выключение и удаление собственных правил оповещений на странице <i>Настройки</i> → <i>Правила оповещений</i>	7.2 Роли пользователей и доступные им интерфейсы (74)
Скрипты, переменные	Скрипт генерации переменных больше не генерирует неиспользуемую переменную TZ	—
Переменные, основные настройки	Исключены переменные ITMM_PROBLEM_AGE_IN_DAYS и ITMM_SYNC_HISTORY_LIFETIME_IN_DAYS, которые раньше отвечали за настройку этих параметров	7.5 Переменные файла .env (76)
Оповещения	Добавлен вывод оповещений о внутренних ошибках сервера	—
Синхронизация	Исправлена ошибка синхронизации метаданных	—
SIEM	Изменено событие о неуспешном входе в систему: если указанный при попытке входа пользователь не существует, информация об этом записывается в поле details объекта user_action	7.9.1 Типы данных в событиях для передачи в SIEM (79)

2.1. Обновления документации

Обновления в текущей версии документации:

- Добавлены разделы:
 - 4.7 Подключение к веб-интерфейсу (55)
 - 4.5 Выпуск SSL-сертификатов (51)
 - 4.5.1 Выпуск корневых сертификатов (51)
 - 4.5.2 Выпуск сертификата и ключа для доступа к веб-интерфейсу UDV-ITM-VM (52)
 - 4.5.3 Настройка APM Администратора (53)
- Обновлены разделы:
 - 4.2.6 Настройка СУБД Jatoba (22)
 - 5 Резервное копирование и восстановление баз данных (57)
 - 5.1 Создание резервной копии базы данных Jatoba/PostgreSQL (57)
 - 5.2 Восстановление резервной копии базы данных Jatoba/PostgreSQL (58)
 - 7.1 Совместимость компонентов решения для UDV-ITM-VM (74)
 - 4.2.8 Установка сервера визуализации и управления UDV-ITM-VM на ОС РЕД ОС (28)

- 4.3.7 Установка сервера визуализации и управления UDV-ITM-VM на ОС Centos 8 (45)
- 7.5 Переменные файла .env (76)
- Обновление UDV-ITM-VM с версии 1.4.0.0 до версии 1.7.0.0 ()
- 4.4 Обновление UDV-ITM-VM с версии 1.6.0.0 до версии 1.7.0.0 (49)
- Исключены разделы:
 - «Создание резервной копии всех БД и файлов журналов БД Jatoba»
 - «Восстановление резервной копии всех БД и файлов журналов БД Jatoba»

3. Введение

В этом разделе:

- 3.1 Область применения (9)
- 3.2 Назначение и условия применения (9)

3.1. Область применения

UDV-ITM-VM – сервер визуализации и управления, который используется в корпоративных вертикально-интегрированных решениях по мониторингу и контролю ИТ-ресурсов. UDV-ITM-VM работает на верхнем уровне иерархии, как правило, в администрации предприятия.

3.2. Назначение и условия применения

Сервер визуализации и управления UDV-ITM-VM предназначен для осуществления контроля предоставляемых вычислительных ресурсов и каналов связи в автоматизированных системах управления путем реализации следующих функций:

- Предоставление сводной информации о состоянии функционирования контролируемых ИТ-ресурсов АСУ ТП в филиалах и на технологических объектах предприятия.
- Передача консолидированных данных о свойствах и состоянии функционирования контролируемых ресурсов в смежные корпоративные системы: систему автоматизации процессов обеспечения безопасности (САОБ) и систему мониторинга компьютерных инцидентов (СМКИ).

Сервер визуализации и управления UDV-ITM-VM используется в составе комплексной системы мониторинга и контроля ИТ-ресурсов АСУ ТП UDV ITM.

Архитектура системы UDV ITM приведена на рисунке.

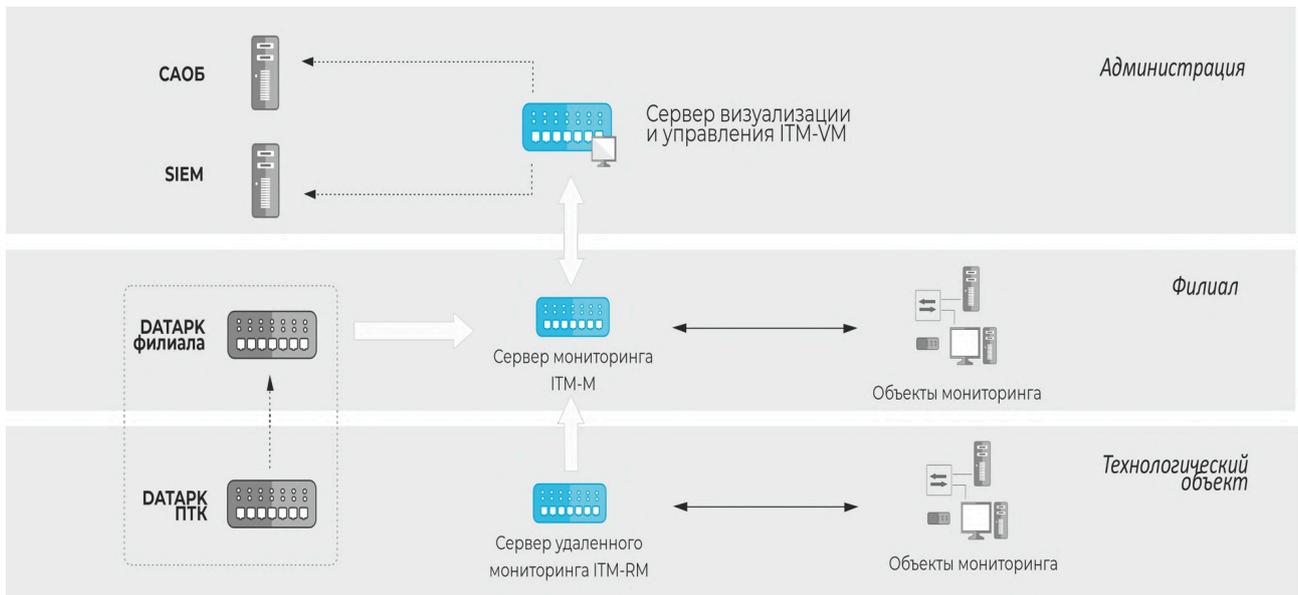


Рис. 3-1 Архитектура системы UDV ITM

4. Подготовка к работе

В этом разделе:

- 4.1 Состав и содержание дистрибутивного носителя данных (11)
- 4.2 Установка UDV-ITM-VM на ОС РЕД ОС (11)
- 4.3 Установка UDV-ITM-VM на ОС Centos 8 (31)
- Обновление UDV-ITM-VM с версии 1.4.0.0 до версии 1.7.0.0 ()
- 4.4 Обновление UDV-ITM-VM с версии 1.6.0.0 до версии 1.7.0.0 (49)
- 4.5 Выпуск SSL-сертификатов (51)
- 4.6 Настройка интеграции с SIEM (55)
- 4.7 Подключение к веб-интерфейсу (55)

4.1. Состав и содержание дистрибутивного носителя данных

В состав дистрибутивного носителя данных входят следующие компоненты:

- `1.4_to_1.5.sh` – скрипт для обновления версии UDV-ITM-VM;
- архив `datapk_itm-vm_[версия_сервера_визуализации_и_управления].tar.gz` с дистрибутивом;
- конфигурационный файл `docker-compose.release.yaml` – содержит список docker-контейнеров с сервисами и их настройками;
- `env_prod_generator.sh` – скрипт для генерации и настройки env-файлов;
- `iptables` – файл с предварительно настроенными правилами межсетевого экрана iptables.

Дистрибутивный носитель также может содержать следующие компоненты:

- `dependencies.zip` – архив с дополнительными пакетами.

4.2. Установка UDV-ITM-VM на ОС РЕД ОС

Установите ОС РЕД ОС 7.3 по инструкции от производителя. В процессе установки ОС:

- В разделе «Раскладка клавиатуры» рекомендуется выбрать английскую раскладку клавиатуры как значение по умолчанию для удобства ввода команд в консоли.
- В разделе «Выбор программ» рекомендуется выбрать базовое окружение «Сервер минимальный» и выбрать следующие дополнения для выбранного окружения:
 - Perl для веб-разработки;
 - Python;
 - Библиотеки совместимости.
- При автоматической разметке дисков с размером более 50 ГБ автоматически создается раздел `/home/`. Рекомендуется удалить данный раздел. Для его удаления необходимо в меню

«Разметка вручную» нажать на кнопку «-», затем выбрать корневой раздел «/» и в поле «Требуемый размер» ввести «100%» для расширения дискового пространства.

В этом разделе:

- 4.2.1 Настройка синхронизации времени (NTP) (12)
- 4.2.2 Установка дополнительных пакетов в ОС РЕД ОС 7.3 (12)
- 4.2.4 Установка UDV-ITM-VM с отдельным томом для БД (14)
- 4.2.5 Установка СУБД Jatoba версии 1.14 на РЕД ОС 7.3 (19)
- 4.2.6 Настройка СУБД Jatoba (22)
- 4.2.7 Настройка межсетевого экрана iptables (26)
- 4.2.8 Установка сервера визуализации и управления UDV-ITM-VM на ОС РЕД ОС (28)

4.2.1. Настройка синхронизации времени (NTP)

Для настройки NTP-клиента:

1. В файле `/etc/ntp.conf`:

- а. добавьте строку `server [IP адрес NTP сервера]`;
- б. прокомментируйте или удалите неиспользуемые записи (например, `server ntp1.vniiftri.ru`).

2. Запустите сервис NTP и добавьте его в автозагрузку:

```
systemctl enable ntpd --now
```

3. Дождитесь полного запуска сервиса (15-20 минут).

4. Убедитесь в корректности произведенных настроек. Для этого выполните команду:

```
ntpq -pn
```

Результат шага:

```
[root@datapkitm-k-demo ~]# ntpq -pn
      remote           refid      st t when poll reach   delay   offset  jitter
-----
*192.168.12.6    192.168.12.7    4 u  13   64    7   0.641  10.256  4.127
[root@datapkitm-k-demo ~]#
```

Рис. 4-1 Пример успешного вывода команды `ntpq -pn`

 **Прим.:**

Символ «*» в начале строки свидетельствует о корректности произведенной настройки, но появиться он может не ранее 15-20 минут после запуска сервиса.

4.2.2. Установка дополнительных пакетов в ОС РЕД ОС 7.3

Для установки дополнительных пакетов:

1. Скопируйте архив `dependencies.zip` на компьютер, где будет установлен UDV-ITM-M.

 **Прим.:**

Архив `dependencies.zip` можно получить вместе с дистрибутивом.

2. Перейдите в режим командной строки установленной ОС.
3. Распакуйте архив с помощью команды:

```
unzip /opt/dependencies.zip -d /opt/
```

4. Перейдите в директорию `dependencies`:

```
cd /opt/dependencies
```

5. Установите пакеты:

```
yum install --disablerepo=base,updates */*.rpm
```

6. Переместите файл `docker-compose`:

```
mv /usr/bin/docker-compose /usr/local/bin/
```

7. Назначьте права на выполнение с помощью команды:

```
chmod +x /usr/local/bin/docker-compose
```

8. Запустите `docker` и добавьте службу в автозагрузку:

```
systemctl enable --now docker
```

9. Проверьте состояние службы с помощью команды:

```
systemctl status docker
```

4.2.3. Установка дополнительных пакетов в ОС РЕД ОС 7.3 с интернетом

1. Установите `docker` и `docker-compose`:

```
yum install docker-ce docker-compose
```

2. Переместите файл `docker-compose`:

```
mv /usr/bin/docker-compose /usr/local/bin/
```

3. Назначьте права на выполнение с помощью команды:

```
chmod +x /usr/local/bin/docker-compose
```

4. Запустите `docker` и добавьте службу в автозагрузку:

```
systemctl enable --now docker
```

5. Установите пакеты для сбора данных по протоколу SNMP и обработки данных по протоколу ICMP:

```
yum install net-snmp net-snmp-utils fping
```

4.2.4. Установка UDV-ITM-VM с отдельным томом для БД

Этот раздел описывает последовательность действий для установки UDV-ITM-VM для случая, когда на сервере используются два тома – первый том для операционной системы, второй том для базы данных.

Если вы планируете использовать только один том, перейдите в раздел 4.2.5 Установка СУБД JatoBa версии 1.14 на РЕД ОС 7.3 (19).

Все нижеописанные действия на сервере производятся после настройки RAID на дисках и установки операционной системы в соответствии с разделами 4.2 Установка UDV-ITM-VM на ОС РЕД ОС (11), 4.2.1 Настройка синхронизации времени (NTP) (12) и 4.2.2 Установка дополнительных пакетов в ОС РЕД ОС 7.3 (12).

В этом разделе:

- 4.2.4.1 Монтирование раздела (14)
- 4.2.4.2 Настройка СУБД (18)

4.2.4.1. Монтирование раздела

Для монтирования раздела:

1. Создайте директорию, в которую будет примонтирован новый том:

```
mkdir /storage
```

2. Просмотрите существующие диски:

```
fdisk -l
```

Результат шага: В выведенном списке должно быть устройство «Диск /dev/sdb».

3. Начните создание раздела с помощью команды:

```
fdisk /dev/sdb
```



Прим.:

Справку о fdisk можно получить с помощью команды `m`.

4. Создайте пустую таблицу разделов GPT с помощью команды `g`.

Результат шага:

```
Команда (m для справки): g  
Created a new GPT disklabel (GUID: B7B9DDF1-7035-43EF-A989-0D587F7B982B).
```

Рис. 4-2 Результат работы команды `g`

5. Создайте раздел с помощью команды `n`.

- a. Укажите номер раздела 1.

b. В качестве значения первого сектора укажите минимальное число из предложенных.

Пример: Для записи вида «Первый сектор (2048-20971486, default 2048)» укажите значение 2048.

с. В качестве значения последнего сектора укажите максимальное число из предложенных, чтобы выделить раздел на весь объем диска.

Пример: Для записи вида «Последний сектор + число секторов или + размер{K,M,G,T,P} (2048-20971486, default 20971486)» укажите значение 20971486.

 **Прим.:**

По умолчанию предлагается значение последнего сектора. Его можно применить, нажав на клавишу Enter.

Результат шага:

```
Команда (h для справки): n
Номер раздела (1-128, default 1): 1
Первый сектор (2048-20971486, default 2048): 2048
Последний сектор + число секторов или + размер{K,M,G,T,P} (2048-20971486, default 20971486)
Создан новый раздел 1 с типом 'Linux filesystem' и размером 10 GiB.
```

Рис. 4-3 Результат работы команды n.

6. Просмотрите информацию о разделе с помощью команды p.

Результат шага:

```
Команда (h для справки): p
Диск /dev/sdb: 10 GiB, 10737418240 байт, 20971520 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
Тип метки диска: gpt
Идентификатор диска: B7B9DDF1-7035-43EF-A989-0D587F7B982B

Устр-во   начало   Конец   Секторы  Размер  Тип
/dev/sdb1  2048    20971486 20969439   10G   файловая система Linux
```

Рис. 4-4 Результат работы команды p.

7. Примените настройки и выйдите из программы с помощью команды w.

Результат шага:

```
Команда (m для справки): w
Таблица разделов была изменена.
Вызывается iocntl() для перечитывания таблицы разделов.
Синхронизируются диски.
```

Рис. 4-5 Результат работы команды w.

8. Создайте файловую систему ext4 с меткой раздела storage с помощью команды:

```
mkfs -t ext4 -L storage /dev/sdb1
```

Результат шага:

```
[root@datapkitm-k2-demo ~]# mkfs -t ext4 -L storage /dev/sdb1
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=storage
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
655360 inodes, 2621179 blocks
131058 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
80 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

Рис. 4-6 Результат работы команды mkfs -t ext4 -L storage /dev/sdb1.

9. Просмотрите файловые системы и UUID в системе одним из следующих способов:

a. с помощью команды `lsblk -f`:

Результат шага:

```
[root@datapkitm-k2-demo ~]# lsblk -f
NAME                                FSTYPE     LABEL     UUID                                 MOUNTPOINT
sda
├─sda1                               ext4        2f799c7b-70f6-4db2-ad80-bf9af804b4f0 /boot
├─sda2                               LVM2_member sUlx7n-83Zf-f23t-cZAC-19Xa-2Uh2-gDZbUg
│   └─ro_datapkitm--k2--demo-root ext4        b6ed2553-6cf0-4155-a8d2-addcell19877a /
sdb
├─sdb1                               ext4        storage  afe0d861-4db9-4ad2-adde-aaa80621ffd8
sr0
```

Рис. 4-7 Результат работы команды lsblk -f

b. с помощью команды `blkid`:

Результат шага:

```
[root@datapkitm-k2-demo ~]# lsblk -f
NAME                                FSTYPE     LABEL     UUID                                         MOUNTPOINT
sda
├─sda1                               ext4        2f799c7b-70f6-4db2-ad80-bf9af804b4f0      /boot
├─sda2                               LVM2_member sU1x7n-832f-f23t-cZAC-19Xa-2Uh2-gDzbUg  /
│   └─ro_datapkitm--k2--demo-root ext4        b6ed2553-6cf0-4155-a8d2-addcell19877a
sdb
├─sdb1                               ext4        storage afe0d861-4db9-4ad2-adde-aaa80621ffd8
sr0
```

Рис. 4-8 Результат работы команды blkid

10. Для автоматического монтирования тома после запуска системы добавим информацию в конфигурационный файл `/etc/fstab`:

а. Перейдите в режим редактирования файла `/etc/fstab`:

```
vi /etc/fstab
```

б. Добавьте в конец файла строку:

```
UUID=afe0d861-4db9-4ad2-adde-aaa80621ffd8 /storage ext4 defaults 0 2
```

```
# /etc/fstab
# Created by anaconda on Tue Dec 21 15:41:54 2021
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/ro_datapkitm--k2--demo-root /          ext4    defaults    1 1
UUID=2f799c7b-70f6-4db2-ad80-bf9af804b4f0 /boot      ext4    defaults    1 2
UUID=afe0d861-4db9-4ad2-adde-aaa80621ffd8 /storage   ext4    defaults    0 2
```

Рис. 4-9 Содержимое файла `/etc/fstab`

с. Сохраните изменения и закройте файл:

```
:wq
```

11. Смонтируйте системы, указанные в `fstab`, без перезагрузки, с помощью команды:

```
mount -a
```

12. Проверьте список смонтированных файловых систем:

```
df -hT
```

Результат шага:

```
[root@datapkitm-k2-demo ~]# df -hT
Файловая система          Тип      Размер  Использовано  Дост  Использовано%  Смонтировано в
devtmpfs                  devtmpfs 3,9G      0             3,9G      0% /dev
tmpfs                     tmpfs     3,9G      0             3,9G      0% /dev/shm
tmpfs                     tmpfs     3,9G      8,8M          3,9G      1% /run
tmpfs                     tmpfs     3,9G      0             3,9G      0% /sys/fs/cgroup
/dev/mapper/ro_datapkitm--k2--demo-root ext4      15G      2,9G          11G      21% /
/dev/sdal                  ext4      976M     100M          809M      11% /boot
overlay                   overlay   15G      2,9G          11G      21% /var/lib/docker
overlay                   overlay   15G      2,9G          11G      21% /var/lib/docker
overlay                   overlay   15G      2,9G          11G      21% /var/lib/docker
shm                       tmpfs     64M      0             64M      0% /var/lib/docker
shm                       tmpfs     64M      0             64M      0% /var/lib/docker
shm                       tmpfs     64M      16K           64M      1% /var/lib/docker
overlay                   overlay   15G      2,9G          11G      21% /var/lib/docker
shm                       tmpfs     64M      0             64M      0% /var/lib/docker
tmpfs                     tmpfs     797M     0             797M     0% /run/user/0
/dev/sdbl                  ext4      9,8G     37M           9,2G     1% /storage
```

Рис. 4-10 Результат работы команды df -hT

4.2.4.2. Настройка СУБД

Для настройки СУБД:

1. Создайте директорию для хранения базы данных на отдельном томе:

```
mkdir /storage/base
```

2. Установите Jatoba до действия установки пакета-активатора в соответствии с разделом 4.2.5 Установка СУБД Jatoba версии 1.14 на РЕД ОС 7.3 (19) (до шага 4.2.5.0 4 (20)).
3. Назначьте СУБД нестандартный каталог для хранения баз данных и конфигурационных файлов.
Для этого:

- a. Перейдите в режим редактирования службы СУБД:

```
systemctl edit jatoba-*.service
```

- b. Введите следующий текст для обозначения нового каталога:

```
[Service]
Environment=PGDATA=/storage/base
```

- c. Сохраните файл и выйдите из режима редактирования:

```
:wq
```

4. Просмотрите содержимое файла с помощью команды:

```
cat /etc/systemd/system/jatoba-*.service.d/override.conf
```

5. Перезагрузите systemd:

```
systemctl daemon-reload
```

6. Назначьте пользователя postgres владельцем каталога с помощью команды:

```
chown -R postgres:postgres /storage/base
```

7. Проинициализируйте установленную версию. Для этого:

- а. Перейдите в директорию расположения исполняемых файлов СУБД:

```
cd /usr/jatoba-*/bin
```

- б. Выполните команду инициализации СУБД:

```
./jatoba-setup initdb jatoba-*
```

 **Внимание:**

После инициализации СУБД основной каталог с конфигурационными файлами располагается в `/storage/base`.

8. При желании просмотрите содержимое директории `/storage/base` с помощью команды:

```
ls -la /storage/base
```

Результат шага:

```
[root@datapkitm-k2-demo bin]# ls -la /storage/base/
итого 124
drwx-----. 20 postgres postgres 4096 янв 28 13:08 .
drwxr-xr-x.  4 root      root      4096 янв 28 12:30 ..
drwx-----.  5 postgres postgres 4096 янв 28 13:08 base
drwx-----.  2 postgres postgres 4096 янв 28 13:08 global
drwx-----.  2 postgres postgres 4096 янв 28 13:08 log
drwx-----.  2 postgres postgres 4096 янв 28 13:08 pg_commit_ts
drwx-----.  2 postgres postgres 4096 янв 28 13:08 pg_dynshmem
-rw-----.  1 postgres postgres 4269 янв 28 13:08 pg_hba.conf
-rw-----.  1 postgres postgres 1636 янв 28 13:08 pg_ident.conf
drwx-----.  4 postgres postgres 4096 янв 28 13:08 pg_logical
drwx-----.  4 postgres postgres 4096 янв 28 13:08 pg_multixact
drwx-----.  2 postgres postgres 4096 янв 28 13:08 pg_notify
drwx-----.  2 postgres postgres 4096 янв 28 13:08 pg_replslot
drwx-----.  2 postgres postgres 4096 янв 28 13:08 pg_serial
drwx-----.  2 postgres postgres 4096 янв 28 13:08 pg_snapshots
drwx-----.  2 postgres postgres 4096 янв 28 13:08 pg_stat
drwx-----.  2 postgres postgres 4096 янв 28 13:08 pg_stat_tmp
drwx-----.  2 postgres postgres 4096 янв 28 13:08 pg_subtrans
drwx-----.  2 postgres postgres 4096 янв 28 13:08 pg_tblspc
drwx-----.  2 postgres postgres 4096 янв 28 13:08 pg_twophase
-rw-----.  1 postgres postgres    3 янв 28 13:08 PG_VERSION
drwx-----.  3 postgres postgres 4096 янв 28 13:08 pg_wal
drwx-----.  2 postgres postgres 4096 янв 28 13:08 pg_xact
-rw-----.  1 postgres postgres   88 янв 28 13:08 postgresql.auto.conf
-rw-----.  1 postgres postgres 24199 янв 28 13:08 postgresql.conf
```

Рис. 4-11 Содержимое директории `/storage/base`

9. Продолжите установку пакета-активатора согласно разделу 4.2.5 Установка СУБД Jatoba версии 1.14 на РЕД ОС 7.3 (19) (с шага 4.2.5.0 4 (20)).

4.2.5. Установка СУБД Jatoba версии 1.14 на РЕД ОС 7.3

Перед установкой СУБД Jatoba необходимо заказать пакет установки и лицензионный ключ у поставщика ПО Jatoba.

 **Подсказка:**

Вместо этой инструкции вы можете использовать документацию разработчика СУБД Jatoba.

Для установки Jatoba версии 1.14 на РЕД ОС 7.3:

1. Создайте каталог для файлов установки СУБД Jatoba командой:

```
mkdir /opt/jatoba
```

2. Для установки Jatoba передайте в ОС UDV-ITM-VM следующие пакеты для установки СУБД Jatoba в директорию `/opt/jatoba`:

```
gis-activator11-1.1.0-0.x86_64.rpm  
jatoba1-client-1.14.1-2318.x86_64.rpm  
jatoba1-contrib-1.14.1-2318.x86_64.rpm  
jatoba1-libs-1.14.1-2318.x86_64.rpm  
jatoba1-securityprofile-1.14.1-2318.x86_64.rpm  
jatoba1-server-1.14.1-2318.x86_64.rpm  
jatoba1-timescaledb-1.14.1-2318.x86_64.rpm
```

 **Прим.:**

Остальные предоставленные пакеты пользователь устанавливает на своё усмотрение, они не являются обязательными для работы UDV-ITM-VM.

3. Перейдите в директорию `/opt/jatoba`:

```
cd /opt/jatoba
```

4. Установите пакет-активатор от производителя с помощью команды:

```
rpm -Uvh gis-activator11-1.1.0-0.x86_64.rpm
```

5. Для установки СУБД введите команду:

```
rpm -Uvh jatoba1-client-1.14.1-2318.x86_64.rpm jatoba1-  
contrib-1.14.1-2318.x86_64.rpm jatoba1-libs-1.14.1-2318.x86_64.rpm jatoba1-  
server-1.14.1-2318.x86_64.rpm jatoba1-securityprofile-1.14.1-2318.x86_64.rpm  
jatoba1-timescaledb-1.14.1-2318.x86_64.rpm
```

6. Проинициализируйте установленную версию СУБД. Для этого:

- a. Перейдите в директорию расположения исполняемых файлов СУБД, выполнив команду:

```
cd /usr/jatoba-1/bin
```

- b. Выполните команду инициализации СУБД:

```
./jatoba-setup initdb jatoba-1
```

```
[root@datapk-itm-red bin]# ./jatoba-setup initdb jatoba-1  
Initializing database ... OK
```

Рис. 4-12 Инициализация СУБД

7. Для установки СУБД необходимо запросить лицензионный ключ у поставщика ПО Jatoba.

Прим.:

Лицензионный ключ также можно запросить через контактные данные технической поддержки СУБД Jatoba – заполнив форму на веб-сайте (<https://www.gaz-is.ru/poddergka/zajavka.html#produkty>), отправив письмо на электронную почту support@gaz-is.ru или по телефону 8 (800) 700-09-87.

8. Запустите активатор СУБД с помощью команды ниже и следуйте его дальнейшим инструкциям:

```
./jactivator
```

9. В меню активатора выберите и выполните оффлайн или онлайн-активацию СУБД Jatoba.

Прим.:

Онлайн активация подразумевает наличие интернета на компьютере с устанавливаемой СУБД. В качестве директории может быть указана текущая директория, которая обозначается символом «точка». Принцип оффлайн-активации описан в документации к СУБД Jatoba.

```
[root@datapk-itm-red bin]# ./jactivator  
Добро пожаловать в центр активации Jatoba  
Введите лицензионный ключ  
[REDACTED]  
Введите email адрес администратора  
[REDACTED]  
Выберите способ активации:  
  Online-активация (введите 1)  
  Offline-активация (введите 2)  
> 1  
Используется сервер лицензирования: https://license.gaz-is.ru  
Выберите режим активации:  
  Обычная активация (введите 1)  
  Реактивация (введите 2)  
> 1  
Время для активации 20 минут  
Введите ключ активации с почты администратора  
[REDACTED]  
Введите путь для сохранения файла лицензии  
.  
-----  
Лицензия выпущена, файл лицензии успешно сохранен  
файл: ./jatoba.cer  
-----
```

Рис. 4-13 Меню активатора СУБД Jatoba

10. Установите полученный в результате активации файл лицензии в директории данных `/usr/jatoba-1/bin`:

```
chown postgres.postgres /usr/jatoba-1/bin/jatoba.cer  
ls -la /usr/jatoba-1/bin/jatoba.cer
```

⚠ Внимание:

при использовании двух томов замените директорию файла на /storage/base.

11. Настройте лицензию Jatoba. Для этого:

a. Откройте файл `postgresql.conf`:

```
vi /var/lib/jatoba/1/data/postgresql.conf
```

⚠ Внимание:

при использовании двух томов замените директорию файла на /storage/base.

b. В конце конфигурационного файла, в разделе «LICENSER OPTION AND PARAMETERS» отредактируйте и раскомментируйте строки, убрав символ «#»:

```
lic_product_name = 'Jatoba'  
lic_file_path = '/usr/jatoba-1/bin/jatoba.cer'  
lic_server_addr = 'https://license.gaz-is.ru'
```

c. Сохраните файл и выйдите из режима редактирования:

```
:wq
```

12. Для запуска СУБД и ее добавления в автозагрузку выполните команду:

```
systemctl enable jatoba-1 --now
```

13. Проверьте состояние службы с помощью команды:

```
systemctl status jatoba-1
```

```
● jatoba-1.service - Jatoba 1 database server  
   Loaded: loaded (/usr/lib/systemd/system/jatoba-1.service; enabled; vendor preset: disabled)  
   Active: active (running) since Пн 2022-04-25 12:19:19 +05; 9 months 6 days ago  
     Docs: https://www.gaz-is.ru/Jatoba/doc  
   Process: 32466 ExecStartPre=/usr/jatoba-1/bin/jatoba-check-db-dir ${PGDATA} (code=exited, status=0/SUCCESS)  
   Main PID: 32476 (postmaster)  
     Tasks: 48  
    Memory: 3.0G  
   CGroup: /system.slice/jatoba-1.service  
           └─ 4247 postgres: datapkitm datapkitm 172.16.239.2(51030) idle  
             └─ 4257 postgres: datapkitm datapkitm 172.16.239.2(51034) idle  
               └─ 4259 postgres: datapkitm datapkitm 172.16.239.2(51036) idle  
                 └─ 4270 postgres: datapkitm datapkitm 172.16.239.2(51040) idle  
                   └─ 4271 postgres: datapkitm datapkitm 172.16.239.2(51042) idle  
                     └─ 4272 postgres: datapkitm datapkitm 172.16.239.2(51044) idle  
                       └─ 4273 postgres: datapkitm datapkitm 172.16.239.2(51046) idle
```

Рис. 4-14 Состояние службы `jatoba-1.service`

4.2.6. Настройка СУБД Jatoba

Настройте СУБД Jatoba для работы с сервером визуализации и управления UDV-ITM-VM. Для этого:

1. Измените пароль пользователя базы данных и добавьте нового пользователя. Для этого:

a. Перейдите в режим командной строки операционной системы, на которой установлен сервер визуализации и управления.

b. Измените текущего пользователя на `postgres`:

```
su postgres
```

c. Войдите в интерактивный терминал для работы с `postgresq`:

```
psql
```

d. Измените пароль пользователя `postgres`, так как по умолчанию пароль не задан:

```
ALTER USER postgres WITH PASSWORD '[пароль]';
```

 **Подсказка:**

При создании пароля к учетной записи рекомендуется следовать требованиям парольной политики:

- длина – не менее 16 символов;
- символы – буквы в нижнем и верхнем регистрах, цифры и специальные символы;
- минимальное количество цифр – 2.

 **Внимание:**

При использовании функционала модуля парольной политики «securityprofile» в составе СУБД Jatoba, его настройку следует осуществлять в соответствии с документацией от разработчика. Имейте в виду, что при использовании модуля парольной политики «securityprofile» после каждой перезагрузки сервера необходимо повторно инициализировать модуль «securityprofile» путем перезапуска службы.

e. Создайте пользователя с именем `itmm_user` и необходимым паролем:

```
create user [имя_пользователя] with createdb password '[пароль]';
```

f. Убедитесь, что пользователь создан:

```
\du
```

g. Покиньте терминал:

```
\q
```

h. Для выхода из пользователя `postgres` введите `exit`.

2. Убедитесь в корректных значениях переменных в файле `postgresql.conf`. Для этого:

a. Перейдите в режим редактирования файла `postgresql.conf`:

```
vi /var/lib/jatoba/[версия jatoba]/data/postgresql.conf
```

В этой команде [версия jatoba] – первая цифра в версии Jatoba.

Пример: Для Jatoba версии 4.5 выполните команду:

```
vi /var/lib/jatoba/4/data/postgresql.conf
```



Внимание:

при использовании двух томов замените директорию файла на `/storage/base`.

b. Исправьте значения переменных, чтобы они соответствовали представленным ниже:

```
listen_addresses = '127.0.0.1,172.17.0.1'  
port = 10265  
shared_buffers = 8GB
```

Где

- 127.0.0.1 – локальный IP-адрес сервера UDV-ITM-M;
- 172.17.0.1 – IP-адрес подсети docker0;
- 8GB – 25% от общего объема оперативной памяти сервера.



Прим.:

IP-адреса должны быть перечислены через запятую без пробелов.



Подсказка:

Если IP-адрес подсети docker0 уже используется в вашей инфраструктуре, его нужно изменить. Подробнее см. в разделе [6.1 Конфликт подсети контейнеров \(62\)](#) [6.1.0 Причина 2 \(63\)](#).

c. Убедитесь, что переменные `log_timezone` и `timezone` соответствуют текущему часовому поясу.

Пример: корректным значением для Екатеринбурга будет `Asia/Yekaterinburg`.

d. Сохраните файл и выйдите из режима редактирования:

```
:wq
```

3. Настройте разрешения по подключению docker-контейнера и пользователей к базам данных.
Для этого:

a. Войдите в режим редактирования файла `pg_hba.conf` с помощью команды:

```
vi /var/lib/jatoba/[jatoba_version]/data/pg_hba.conf
```

В этой команде `jatoba_version` – первая цифра в версии Jatoba.

Пример: Для Jatoba версии 4.5 выполните команду:

```
vi /var/lib/jatoba/4/data/pg_hba.conf
```

 **Внимание:**

При использовании двух томов замените директорию файла на `/storage/base`.

b. Найдите раздел «# IPv4 local connections:».

c. Измените `ident` на `md5` в строке `host all all 127.0.0.1/32 ident`.

d. Измените настройки ограничений на подключение локальных и удаленных пользователей к базам данных. Для этого добавьте следующие строки в раздел «# IPv4 local connections:»

```
host all [имя пользователя БД] [IP-адрес docker-сети/маска в формате CIDR]
[метод аутентификации]
host all [имя пользователя БД] [IP-адрес подсети docker0/маска в формате
CIDR] [метод аутентификации]
```

Где:

- `all` – значение, позволяющее подключиться к нескольким БД;
- [имя пользователя БД] – ранее созданный пользователь БД, которому разрешен доступ к БД;
- [IP-адрес docker-сети/маска в формате CIDR] – IP-адрес для удаленного подключения, зависит от переменной `ITMM_NETWORK` в файле `/opt/itm-vm/.env`;
- [IP-адрес подсети docker0/маска в формате CIDR] – IP-адрес подсети `docker0` для удаленного подключения, по умолчанию имеет значение `172.17.0.1/24`.

 **Прим.:**

Отступ между колонками в одной строке выполняется клавишей «Tab».

Пример: для пользователя БД `itmm_user`, IP-адреса подсети контейнера сервера визуализации и управления по умолчанию `172.15.0.1/24`, IP-адреса подсети `docker0` по умолчанию `172.17.0.1/24` и метода аутентификации `md5` строки будут выглядеть следующим образом:

```
host    all      all      127.0.0.1/32      md5
host    all      itmm_user 172.17.0.0/16     md5
host    all      itmm_user 172.15.0.0/24     md5
```

- e. Закомментируйте строки во всех разделах, кроме «# IPv4 local connections».
- f. Сохраните файл и выйдите из режима редактирования:

```
:wq
```

4. Настройте запуск службы СУБД после службы docker. Для этого:

- a. Перейдите в режим редактирования службы СУБД:

```
systemctl edit jatoba-*.service
```

- b. Добавьте блок [Unit]:

```
[Unit]
After=docker.service
BindsTo=docker.service
ReloadPropagatedFrom=docker.service
```

- c. Если база данных хранится на отдельном томе, добавьте после блока [Unit] блок [Service]:

```
[Service]
Environment=PGDATA=/storage/base
```

Где `/storage/base` – путь к базе данных, который был настроен на шаге 4.2.4.2.0 1 (18) раздела 4.2.4.2 Настройка СУБД (18).

- d. Для применения изменений в настройках службы СУБД выполните команду:

```
systemctl daemon-reload
```

5. Для применения настроек в файлах конфигурации перезапустите СУБД с помощью команды:

```
systemctl restart jatoba-*
```

Прим.:

После перезапуска СУБД и применения настроек из файла `pg_hba.conf`, команда для входа в режим редактирования базы данных изменится. Она будет иметь следующий вид:

```
sudo -u postgres psql -p 10265 -h 127.0.0.1 -U [имя пользователя] [имя базы]
```

Где:

- `-u postgres` – пользователь ОС;
- `-p 10265` – порт, через который будет произведено подключение к базе данных;
- `-h 127.0.0.1` – подключение к хосту 127.0.0.1;
- `-U [имя пользователя]` – подключение от имени указанного пользователя.

4.2.7. Настройка межсетевого экрана iptables

Настройте межсетевой экран iptables для корректной работы UDV-ITM-VM. Для этого:

1. Замените файл `/etc/sysconfig/iptables` на файл `iptables` из комплекта поставки:

```
mv /opt/itm-vm/iptables /etc/sysconfig/
```

2. Отредактируйте файл `iptables`:

- a. Откройте файл для редактирования с помощью команды:

```
vi /etc/sysconfig/iptables
```

- b. Закройте доступ из неиспользуемых подсетей, применяемых в docker-контейнерах других компонентов. Для этого прокомментируйте строки `-A INPUT -s 172.16.239.0/24 -j АССЕРТ` (номер 18) и `-A INPUT -s 172.16.240.0/24 -j АССЕРТ` (номер 21).

 **Прим.:**

Включить отображение номеров строк в файле можно с помощью следующих действий:

- i. Нажмите клавишу «Esc», чтобы перейти в командный режим.
- ii. Введите `:set number` или `:set nu` и нажмите «Enter».
- iii. Нажмите клавишу «i», чтобы перевести редактор в режим ввода текста.
- iv. После закрытия файла нумерация строк отключится автоматически. Чтобы отключить абсолютные номера строк на время редактирования файла, перейдите в командный режим и выполните команду `:set nonumber` или `:set nonu`.

- c. При установке UDV-ITM-M и UDV-ITM-VM на одну машину откройте дополнительные порты web-интерфейса. Для этого раскомментируйте строки `#-A INPUT -p tcp -m tcp --dport 8080 -j АССЕРТ` (номер 38) и `#-A INPUT -p tcp -m tcp --dport 8443 -j АССЕРТ` (номер 39).
- d. Закомментируйте строки `-A INPUT -p tcp -m tcp --dport 10051 -j АССЕРТ` (номер 42) и `-A INPUT -p udp -m udp --dport 162 -j АССЕРТ` (номер 45) (порты для приема zabbix-соединений и SNMP traps).
- e. Если требуется мониторинг сервера с помощью UDV-ITM-M или по протоколу SNMP, раскомментируйте строки `#-A INPUT -p tcp -m tcp --dport 10050 -j АССЕРТ` (номер 51) и `#-A INPUT -p udp -m udp --dport 161 -j АССЕРТ` (номер 48) соответственно.
- f. Сохраните файл и выйдите из режима редактирования:

```
:wq
```

3. Проверьте владельца файла и права доступа командой:

```
ls -l /etc/sysconfig/iptables
```

Владелец и права должны совпадать с указанными на скриншоте:

```
[root@eng-itm-vmk1 ~]# ls -l /etc/sysconfig/iptables
-rw-----. 1 root root 2774 Dec  5 15:33 /etc/sysconfig/iptables
```

Рис. 4-15 Владелец и права файла iptables

В противном случае выполните команду:

```
chown root:root /etc/sysconfig/iptables && chmod 600 /etc/sysconfig/iptables
```

Проверьте, что владелец и права теперь соответствуют указанным на скриншоте.

4. Запустите службу iptables и добавьте ее в автозагрузку:

```
systemctl enable --now iptables.service
```

Результат шага: Правила из файла будут применены на сетевом экране системы, а также будут автоматически применяться после перезагрузки.

4.2.8. Установка сервера визуализации и управления UDV-ITM-VM на ОС РЕД ОС

Прим.:

При установке UDV-ITM-VM и UDV-ITM-M на один сервер совпадающие настройки UDV-ITM-VM и UDV-ITM-M (кроме подготовки сертификатов) достаточно выполнить один раз.

Для установки UDV-ITM-VM:

1. Перейдите в режим командной строки операционной системы, на которой будет установлен сервер визуализации и управления.
2. Создайте директорию для установки UDV-ITM-VM:

```
mkdir /opt/itm-vm
```

Прим.:

Для использования UDV-ITM-VM и UDV-ITM-M на одном сервере директории для их установки должны различаться.

3. Скопируйте следующие файлы из комплекта поставки в директорию `/opt/itm-vm`:
 - `env_generator.sh`;
 - `docker-compose.release.yaml`;
 - `udv_itm-vm_1.7.0.0.tar.gz`.

4. Перейдите в директорию `/opt/itm-vm`:

```
cd /opt/itm-vm
```

5. Загрузите образы в операционную систему, на которой установлен сервер визуализации и управления:

```
docker load -i udv_itm-vm_1.7.0.0.tar.gz
```

6. Создайте env-файлы и настройте значения переменных. Для этого:

a. Назначьте скрипту `env_generator.sh` полные права доступа:

```
chmod +x env_generator.sh
```

b. Запустите скрипт:

```
./env_generator.sh
```

Результат шага: Откроется всплывающее окно для настройки переменных.

c. Выполните настройку переменных:

- Чтобы изменить переменную, введите новое значение и нажмите клавишу «Enter».
- Чтобы оставить значение переменной по умолчанию, которое указано в квадратных скобках, нажмите клавишу «Enter».
- Чтобы ответить на вопрос «да», нажмите клавишу «у».
- Чтобы ответить на вопрос «нет», нажмите клавишу «п».

 **Прим.:**

- Если IP-адрес подсети контейнеров уже используется в вашей инфраструктуре, его нужно изменить. Подробнее см. в разделе 6.1 Конфликт подсети контейнеров (62) 6.1.0 Причина 2 (63).
- При установке UDV-ITM-VM и UDV-ITM-M на один сервер для UDV-ITM-VM рекомендуется указать порт для подключения к веб-интерфейсу 8080 и SSL порт для подключения к веб-интерфейсу 8443.

Результат шага: В директории `/opt/itm-vm` появятся файлы `.env` и `.itm_password_secret_key` с настроенными переменными.

d. Для более подробной настройки переменных `.env`-файла или для правки ранее введенных переменных:

i. Откройте для редактирования файл `.env`:

```
vi .env
```

ii. Настройте переменные.

 **Прим.:**

Рекомендуемые и возможные значения переменных приведены в разделе 7.5 Переменные файла `.env` (76).

iii. Сохраните изменения и закройте файл:

```
:wq
```

7. Подготовьте сертификаты для входа в веб-интерфейс. Подробнее см. в разделе 4.5 Выпуск SSL-сертификатов (51).

 **Прим.:**

При установке UDV-ITM-VM и UDV-ITM-M на один сервер необходимо подготовить сертификаты в рабочей директории для каждого из уровней.

8. Измените настройку выделения памяти `vm.overcommit_memory`. Для этого:

- a. Откройте для редактирования файл `/etc/sysctl.conf`:

```
vi /etc/sysctl.conf
```

 **Подсказка:**

В случае отсутствия файла `/etc/sysctl.conf` используйте эту же команду для создания файла и перехода в режим редактирования.

- b. Добавьте в содержимое файла следующее значение:

```
vm.overcommit_memory=1
```

- c. Сохраните файл и выйдите из режима редактирования:

```
:wq
```

- d. перезагрузите сервер для применения изменений.

 **Подсказка:**

Вы можете перезагрузить сервер сразу либо после выполнения пункта 4.2.8.0 11 (31).

Результат шага:

- a. в логах контейнера `itm_m_redis` нет ошибки «WARNING overcommit_memory is set to 0!»;
- b. в файле `/etc/sysctl.conf` установлено значение `vm.overcommit_memory=1`;
- c. в файле `/proc/sys/vm/overcommit_memory` установлено значение 1.

9. Убедитесь, что имя сервера и переменная `$HOSTNAME` соответствуют нужным вам значениям. Актуальное имя сервера отображается в приглашении командной строки. Посмотреть переменную окружения `$HOSTNAME` можно с помощью команды `echo $HOSTNAME`. При необходимости изменения имени сервера см. раздел 6.7 Изменение имени сервера (72).

10. Перейдите в каталог, содержащий `compose`-файлы:

```
cd /opt/itm-vm
```

11. Запустите контейнеры:

```
docker-compose up -d
```

12. Для входа в веб-интерфейс в адресной строке введите IP-адрес UDV-ITM-VM.

 **Прим.:**

При установке UDV-ITM-VM и UDV-ITM-M на один сервер UDV-ITM-VM будет доступен по адресу `https://[ip-адрес]:8443`.

Для первичной настройки в окне авторизации введите логин и пароль учетной записи по умолчанию:

- логин: **itm**;
- пароль: **P@ssw0rd1234**.

Авторизация

Логин *

Пароль *

Войти

Рис. 4-16 Окно авторизации ITM-VM

 **Внимание:**

При первой настройке комплекса необходимо изменить пароль встроенной учетной записи.

4.3. Установка UDV-ITM-VM на ОС Centos 8

В этом разделе:

- 4.3.1 Установка ОС Centos 8 (32)
- 4.3.2 Установка СУБД PostgreSQL v14 (37)
- 4.3.3 Установка Docker (39)
- 4.3.4 Установка дополнительных пакетов в ОС Centos 8 с интернетом (40)
- 4.3.5 Настройка СУБД PostgreSQL (40)
- 4.3.6 Настройка межсетевого экрана iptables (44)
- 4.3.7 Установка сервера визуализации и управления UDV-ITM-VM на ОС Centos 8 (45)

4.3.1. Установка ОС Centos 8

1. Включите сетевой интерфейс.

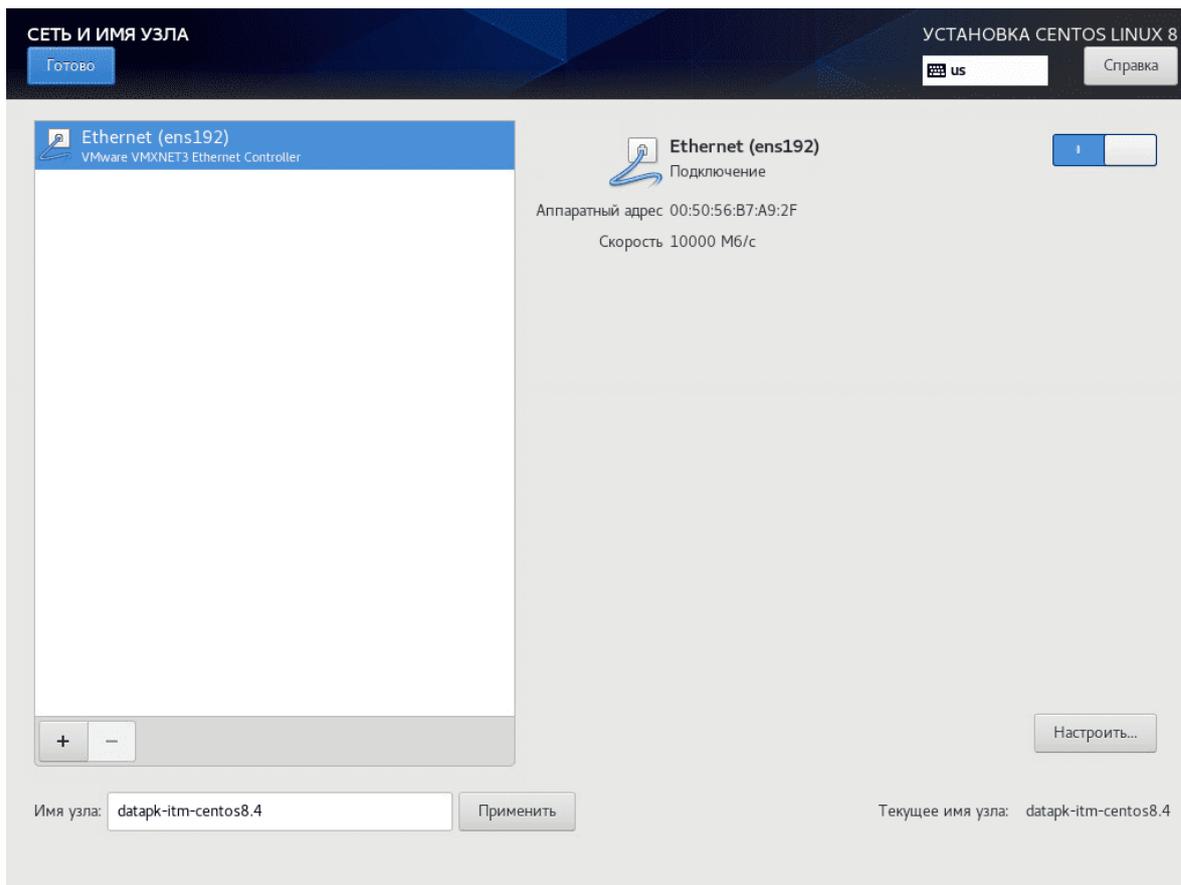


Рис. 4-17 Включение сетевого интерфейса

2. В «Выбор программ» выберите базовое окружение «Минимальная установка» и дополнительное ПО:

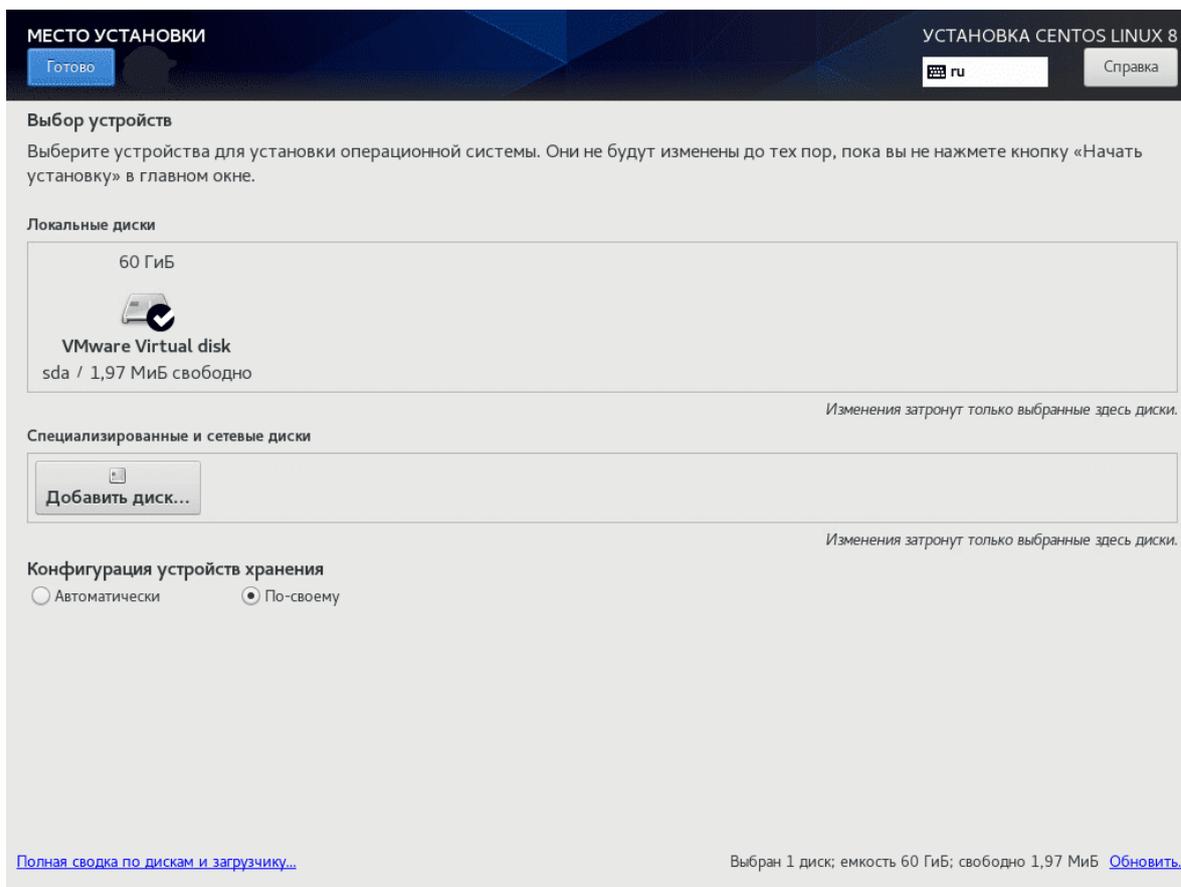


Рис. 4-19 Выбор конфигурации устройств хранения

4. Если в открывшемся окне «Разметка вручную» нет раздела `/home/`, пропустите этот шаг. Если в этом окне есть раздел `/home/`, удалите его. Для этого:
 - a. Выделите раздел `/home/`.
 - b. Нажмите на кнопку «-» в нижней части области выбора раздела.
 - c. Подтвердите удаление раздела `/home/` в появившемся окне.

Прим.:

Раздел `/home/` появляется при автоматической разметке дисков с размером более 50 ГБ.

5. Увеличьте размер корневого раздела. Для этого:
 - a. В окне «Разметка вручную» выберите корневой раздел `/`.

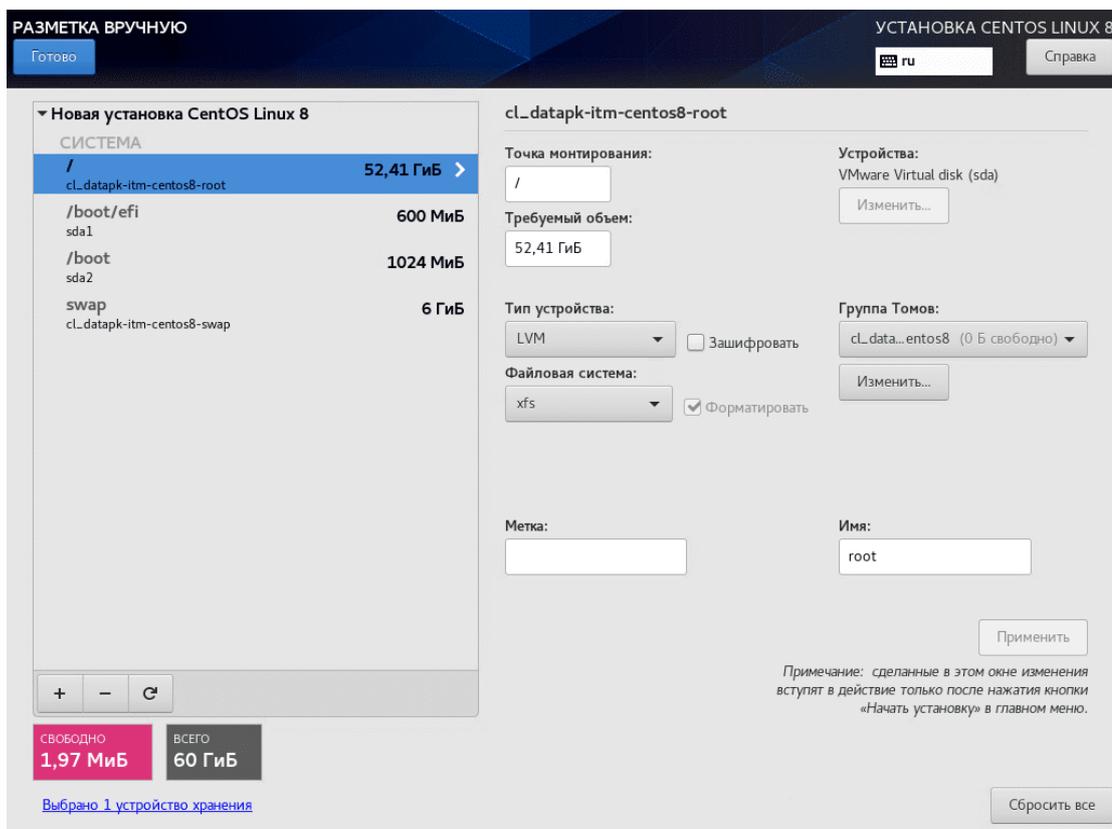


Рис. 4-20 Разметка разделов вручную

b. В поле «Требуемый размер» введите значение «100%» для расширения дискового пространства.

c. Установите курсор на любой другой раздел.

Результат шага: значения полей обновятся, и инсталляция займет все свободное место.

d. Нажмите на кнопку «Готово».

Результат шага: появится окно «Обзор изменений».

e. Убедитесь в корректности произведенных изменений.

f. Нажмите на кнопку «Принять изменения».

6. Установите пароль для учетной записи root:

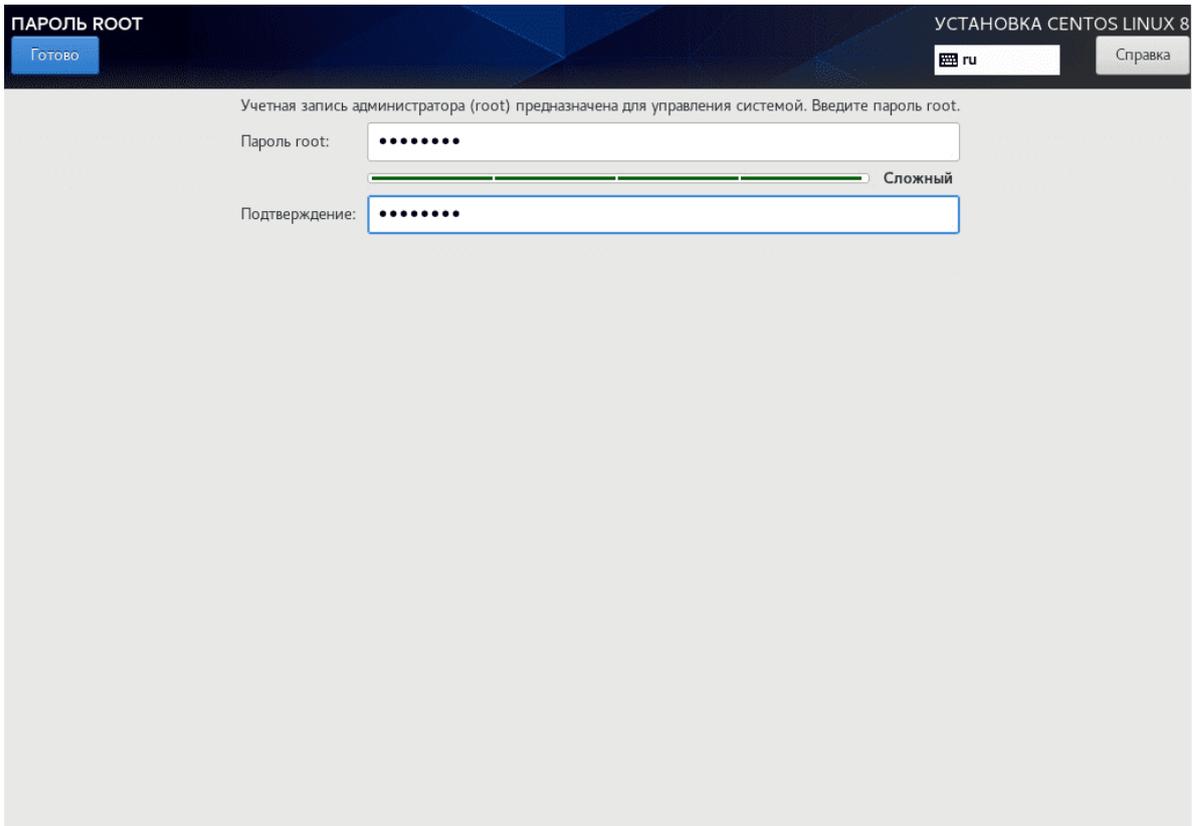


Рис. 4-21 Установка пароля для учетной записи root

7. Создайте пользователя и пароль для него:

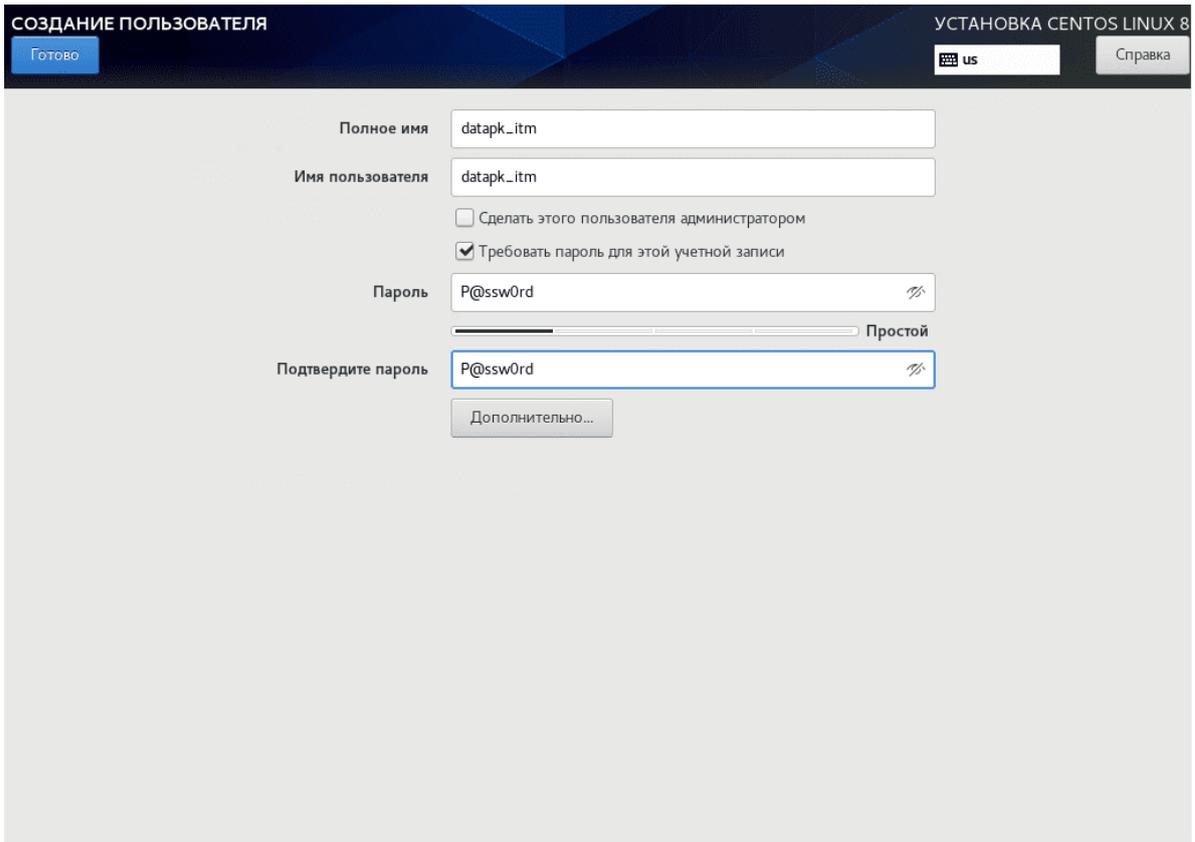


Рис. 4-22 Создание пользователя

8. Нажмите «Начать установку».

4.3.2. Установка СУБД PostgreSQL v14

1. Установите необходимые пакеты из репозитория:

```
sudo dnf install -y https://download.postgresql.org/pub/repos/yum/reporepms/EL-8-x86_64/pgdg-redhat-repo-latest.noarch.rpm
```

```
[root@datapk-itm-centos8 ~]# sudo dnf install -y https://download.postgresql.org/pub/repos/yum/reporepms/EL-8-x86_64/pgdg-redhat-repo-latest.noarch.rpm
Последняя проверка окончания срока действия метаданных: 0:17:58 назад, Пн 19 сен 2022 09:06:40.
pgdg-redhat-repo-latest.noarch.rpm 7.1 kB/s | 13 kB 00:01
Зависимости разрешены.
```

Пакет	Архитектура	Версия	Репозиторий	Размер
Установка: pgdg-redhat-repo	noarch	42.0-26	@commandline	13 k

```

=====
Результат транзакции
=====
Установка 1 Пакет
Общий размер: 13 k
Объем изменений: 13 k
Загрузка пакетов:
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакции проведен успешно
Выполнение транзакции
Подготовка      :                               | 1/1
Установка       : pgdg-redhat-repo-42.0-26.noarch | 1/1
Проверка        : pgdg-redhat-repo-42.0-26.noarch | 1/1
Установлен:
pgdg-redhat-repo-42.0-26.noarch
Выполнено!
```

Рис. 4-23 Установка пакетов

2. Отключите модули PostgreSQL:

```
sudo dnf -qy module disable postgresql
```

```
[root@datapk-itm-centos8 ~]# sudo dnf -qy module disable postgresql
Импорт GPG-ключа 0x442DF0F8:
Идентификатор пользователя: "PostgreSQL RPM Building Project <pgsql-pkg-yum@postgresql.org>"
Отпечаток: 68C9 E2B9 1A37 D136 FE74 D176 1F16 D2E1 442D F0F8
Источник: /etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
Импорт GPG-ключа 0x442DF0F8:
Идентификатор пользователя: "PostgreSQL RPM Building Project <pgsql-pkg-yum@postgresql.org>"
Отпечаток: 68C9 E2B9 1A37 D136 FE74 D176 1F16 D2E1 442D F0F8
Источник: /etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
Импорт GPG-ключа 0x442DF0F8:
Идентификатор пользователя: "PostgreSQL RPM Building Project <pgsql-pkg-yum@postgresql.org>"
Отпечаток: 68C9 E2B9 1A37 D136 FE74 D176 1F16 D2E1 442D F0F8
Источник: /etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
Импорт GPG-ключа 0x442DF0F8:
Идентификатор пользователя: "PostgreSQL RPM Building Project <pgsql-pkg-yum@postgresql.org>"
Отпечаток: 68C9 E2B9 1A37 D136 FE74 D176 1F16 D2E1 442D F0F8
Источник: /etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
Импорт GPG-ключа 0x442DF0F8:
Идентификатор пользователя: "PostgreSQL RPM Building Project <pgsql-pkg-yum@postgresql.org>"
Отпечаток: 68C9 E2B9 1A37 D136 FE74 D176 1F16 D2E1 442D F0F8
Источник: /etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
```

Рис. 4-24 Отключение модулей PostgreSQL

3. Установите СУБД PostgreSQL v14:

```
sudo dnf install -y postgresql14-server
```

```
[root@datapk-itm-centos8 ~]# sudo dnf install -y postgresql14-server
Последняя проверка окончания срока действия метаданных: 0:00:44 назад, Пн 19 сен 2022 09:26:34.
Зависимости разрешены.
```

Пакет	Архитектура	Версия	Репозиторий	Размер
Установка:				
postgresql14-server	x86_64	14.5-1PGDG.rhel8	pgdg14	5.7 М
Установка зависимостей:				
lz4	x86_64	1.8.3-3.el8_4	baseos	103 k
postgresql14	x86_64	14.5-1PGDG.rhel8	pgdg14	1.5 М
postgresql14-libs	x86_64	14.5-1PGDG.rhel8	pgdg14	278 k

```

Результат транзакции
=====
Установка 4 Пакета

Объем загрузки: 7.6 М
Объем изменений: 32 М
Загрузка пакетов:
(1/4): lz4-1.8.3-3.el8_4.x86_64.rpm                72 kB/s | 103 kB    00:01
(2/4): postgresql14-libs-14.5-1PGDG.rhel8.x86_64.rpm 168 kB/s | 278 kB    00:01
(3/4): postgresql14-14.5-1PGDG.rhel8.x86_64.rpm    148 kB/s | 1.5 MB   00:10
(4/4): postgresql14-server-14.5-1PGDG.rhel8.x86_64.rpm 309 kB/s | 5.7 MB   00:18
-----
Общий размер                                383 kB/s | 7.6 MB   00:20
PostgreSQL 14 for RHEL / Rocky 8 - x86_64    1.6 MB/s | 1.7 kB    00:00
Импорт GPG-ключа 0x442DF0F8:
Идентификатор пользователя: "PostgreSQL RPM Building Project <pgsql-pkg-yum@postgresql.org>"
Отпечаток: 68C9 E2B9 1A37 D136 FE74 D176 1F16 D2E1 442D F0F8
Источник: /etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
Импорт ключа успешно завершен
Проверка транзакции

```

Рис. 4-25 Установка СУБД

4. Инициализируйте БД:

```
sudo /usr/pgsql-14/bin/postgresql-14-setup initdb
```

```
[root@datapk-itm-centos8 ~]# sudo /usr/pgsql-14/bin/postgresql-14-setup initdb
Initializing database ... OK
```

Рис. 4-26 Инициализация БД

5. Добавьте сервис в автозагрузку и запустите его:

```
systemctl enable postgresql-14 --now
systemctl start postgresql-14
```

```
[root@datapk-itm-centos8 ~]# sudo systemctl enable postgresql-14
Created symlink /etc/systemd/system/multi-user.target.wants/postgresql-14.service → /usr/lib/systemd/system/postgresql-14.service.
[root@datapk-itm-centos8 ~]# sudo systemctl start postgresql-14
```

Рис. 4-27 Добавление сервиса в автозагрузку и его запуск

6. Проверьте статус сервиса postgresql:

```
systemctl status postgresql-14
```

```
[root@datapk-itm-centos8 ~]# systemctl status postgresql-14
● postgresql-14.service - PostgreSQL 14 database server
   Loaded: loaded (/usr/lib/systemd/system/postgresql-14.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-09-19 09:29:10 EDT; 38s ago
     Docs: https://www.postgresql.org/docs/14/static/
   Process: 110556 ExecStartPre=/usr/pgsql-14/bin/postgresql-14-check-db-dir ${PGDATA} (code=exited, status=0/SUCCESS)
   Main PID: 110563 (postmaster)
     Tasks: 8 (limit: 101070)
    Memory: 16.8M
    CGroup: /system.slice/postgresql-14.service
            └─110563 /usr/pgsql-14/bin/postmaster -D /var/lib/pgsql/14/data/
              └─110565 postgres: logger
                └─110567 postgres: checkpointer
                  └─110568 postgres: background writer
                    └─110569 postgres: walwriter
                      └─110570 postgres: autovacuum launcher
                        └─110571 postgres: stats collector
                          └─110572 postgres: logical replication launcher

сен 19 09:29:10 datapk-itm-centos8 systemd[1]: Starting PostgreSQL 14 database server ...
сен 19 09:29:10 datapk-itm-centos8 postmaster[110563]: 2022-09-19 09:29:10.146 EDT [110563] СООБЩЕНИЕ: передача вы
сен 19 09:29:10 datapk-itm-centos8 postmaster[110563]: 2022-09-19 09:29:10.146 EDT [110563] ПОДСКАЗКА: В дальнейше
сен 19 09:29:10 datapk-itm-centos8 systemd[1]: Started PostgreSQL 14 database server.
```

Рис. 4-28 Проверка статуса сервиса postgresql:

4.3.3. Установка Docker

1. Добавьте репозиторий docker:

```
dnf config-manager
--add-repo=https://download.docker.com/linux/centos/docker-ce.repo
```

2. Установите docker:

```
dnf install docker-ce --allowrhsm
```

3. Запустите службу docker:

```
systemctl start docker
```

4. Добавьте службу docker в автозагрузку:

```
systemctl enable --now docker
```

5. Проверьте состояние службы docker:

```
systemctl status docker
```

6. Установите docker-compose:

```
wget https://github.com/docker/compose/releases/download/1.29.2/docker-compose-
$(uname -s)-$(uname -m)
cd /root
mv docker-compose-Linux-x86_64 /usr/local/bin/docker-compose
chmod +x /usr/local/bin/docker-compose
```

7. Проверьте версию docker-compose:

```
docker-compose --version
```

```
[root@datapk-itm-centos8 ~]# docker-compose --version
docker-compose version 1.29.2, build 5becea4c
```

Рис. 4-29 Проверка версии docker-compose

4.3.4. Установка дополнительных пакетов в ОС Centos 8 с интернетом

1. Перенаправьте репозитории `/etc/yum.repos.d/` на `http://vault.centos.org` вместо `http://mirror.centos.org`.

2. Установите `docker` и `docker-compose`:

```
dnf config-manager --add-repo=https://download.docker.com/linux/centos/docker-ce.repo
dnf install docker-ce
curl -L "https://github.com/docker/compose/releases/download/1.29.2/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose
chmod +x /usr/local/bin/docker-compose
ln -s /usr/local/bin/docker-compose /usr/bin/docker-compose
```

3. Добавьте службу `docker` в автозагрузку:

```
systemctl enable --now docker
```

4. Установите пакеты для сбора данных по протоколу SNMP и обработки данных по протоколу ICMP:

```
dnf install net-snmp net-snmp-utils fping
```

4.3.5. Настройка СУБД PostgreSQL

Настройте СУБД PostgreSQL для работы с сервером визуализации и управления UDV-ITM-VM. Для этого:

1. Создайте базу данных, пользователя и пароль для него. Для этого:

a. Войдите в интерактивный терминал СУБД [используемая СУБД]:

```
sudo -u postgres psql
```

b. Измените пароль пользователя `postgres` в базе данных:

```
ALTER USER postgres WITH PASSWORD '[пароль]';
```

***i* Подсказка:**

При создании пароля к учетной записи рекомендуется следовать требованиям парольной политики:

- длина – не менее 16 символов;
- символы – буквы в нижнем и верхнем регистрах, цифры и специальные символы;
- минимальное количество цифр – 2.

с. Создайте пользователя с именем `itmm_user` и необходимым паролем:

```
CREATE USER itmm_user WITH PASSWORD '[пароль служебного пользователя]';
```

d. Убедитесь, что пользователь создан:

```
\du
```

e. Создайте базу данных `datapkitm`, в качестве распорядителя которой указан пользователь `itmm_user`:

```
CREATE DATABASE datapkitm OWNER itmm_user;
```

f. Убедитесь, что база данных `datapkitm` создана:

```
\l
```

Список баз данных					
Имя	Владелец	Кодировка	LC_COLLATE	LC_CTYPE	Права доступа
datapkitm	itmm_user	UTF8	ru_RU.UTF-8	ru_RU.UTF-8	
postgres	postgres	UTF8	ru_RU.UTF-8	ru_RU.UTF-8	
template0	postgres	UTF8	ru_RU.UTF-8	ru_RU.UTF-8	=c/postgres + postgres=CTc/postgres
template1	postgres	UTF8	ru_RU.UTF-8	ru_RU.UTF-8	=c/postgres + postgres=CTc/postgres
(4 строки)					

Рис. 4-30 Список созданных БД

g. Покиньте терминал:

```
\q
```

h. Для выхода из пользователя `postgres` введите `exit`.

2. Убедитесь в корректных значениях переменных в файле `postgresql.conf`. Для этого:

a. Перейдите в режим редактирования файла `postgresql.conf`:

```
vi /var/lib/pgsql/14/data/postgresql.conf
```

b. Исправьте значения переменных, чтобы они соответствовали представленным ниже:

```
listen_addresses = '127.0.0.1,172.17.0.1'
port = 10265
```

```
shared_buffers = 8GB
```

Где

- 127.0.0.1 — локальный IP-адрес сервера UDV-ITM-M;
- 172.17.0.1 — IP-адрес подсети docker0;
- 8GB — 25% от общего объема оперативной памяти сервера.

 **Прим.:**

IP-адреса должны быть перечислены через запятую без пробелов.

 **Подсказка:**

Если IP-адрес подсети docker0 уже используется в вашей инфраструктуре, его нужно изменить. Подробнее см. в разделе [6.1 Конфликт подсети контейнеров \(62\)](#) [6.1.0 Причина 2 \(63\)](#).

- c. Убедитесь, что переменные `log_timezone` и `timezone` соответствуют текущему часовому поясу.

Пример: корректным значением для Екатеринбурга будет `Asia/Yekaterinburg`.

- d. Сохраните файл и выйдите из режима редактирования:

```
:wq
```

3. Настройте разрешения по подключению docker-контейнера и пользователей к базам данных.

Для этого:

- a. Войдите в режим редактирования файла `pg_hba.conf` с помощью команды:

```
vi /var/lib/pgsql/14/data/pg_hba.conf
```

- b. Найдите раздел «# IPv4 local connections:».

- c. Измените `ident` на `md5` в строке `host all all 127.0.0.1/32 ident;`

- d. Измените настройки ограничений на подключение локальных и удаленных пользователей к базам данных. Для этого добавьте следующие строки в раздел «# IPv4 local connections:»

```
host all [имя пользователя БД] [IP-адрес docker-сети/маска в формате CIDR]
[метод аутентификации]
host all [имя пользователя БД] [IP-адрес подсети docker0/маска в формате
CIDR] [метод аутентификации]
```

Где:

- `all` — значение, позволяющее подключиться к нескольким БД;

- [имя пользователя БД] – ранее созданный пользователь БД, которому разрешен доступ к БД;
- [IP-адрес docker-сети/маска в формате CIDR] – IP-адрес для удаленного подключения, зависит от переменной ITMM_NETWORK в файле /opt/itm-vm/.env;
- [IP-адрес подсети docker0/маска в формате CIDR] – IP-адрес подсети docker0 для удаленного подключения, по умолчанию имеет значение 172.17.0.1/24.

 **Прим.:**

Отступ между колонками в одной строке выполняется клавишей «Tab».

Пример: для пользователя БД `itmm_user`, IP-адреса подсети контейнера сервера визуализации и управления по умолчанию `172.15.0.1/24`, IP-адреса подсети `docker0` по умолчанию `172.17.0.1/24` и метода аутентификации `md5` строки будут выглядеть следующим образом:

```
host    all      all      127.0.0.1/32      md5
host    all      itmm_user 172.17.0.0/16     md5
host    all      itmm_user 172.15.0.0/24     md5
```

е. Закомментируйте строки во всех разделах, кроме «# IPv4 local connections».

ф. Сохраните файл и выйдите из режима редактирования:

```
:wq
```

4. Для применения настроек в файлах конфигурации перезапустите СУБД:

```
systemctl restart postgresql-14
```

 **Прим.:**

После перезапуска СУБД и применения настроек из файла `pg_hba.conf`, команда для входа в режим редактирования базы данных изменится. Она будет иметь следующий вид:

```
sudo -u postgres psql -p 10265 -h 127.0.0.1 -U [имя пользователя] [имя базы]
```

Где:

- `-u postgres` – пользователь ОС;
- `-p 10265` – порт, через который будет произведено подключение к базе данных;
- `-h 127.0.0.1` – подключение к хосту 127.0.0.1;
- `-U [имя пользователя]` – подключение от имени указанного пользователя.

5. Проверьте статус СУБД:

```
systemctl status postgresql-14
```

```
[root@datapk-itm-centos8 itm-k]# systemctl status postgresql-14
● postgresql-14.service - PostgreSQL 14 database server
   Loaded: loaded (/usr/lib/systemd/system/postgresql-14.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2022-09-20 02:33:25 EDT; 7min ago
     Docs: https://www.postgresql.org/docs/14/static/
   Process: 128489 ExecStartPre=/usr/pgsql-14/bin/postgresql-14-check-db-dir ${PGDATA} (code=exited, status=0/SUCCESS)
  Main PID: 128496 (postmaster)
    Tasks: 8 (limit: 101070)
   Memory: 17.6M
   CGroup: /system.slice/postgresql-14.service
           └─128496 /usr/pgsql-14/bin/postmaster -D /var/lib/pgsql/14/data/
             └─128498 postgres: logger
               └─128500 postgres: checkpointer
                 └─128501 postgres: background writer
                   └─128502 postgres: walwriter
                     └─128503 postgres: autovacuum launcher
                       └─128504 postgres: stats collector
                         └─128505 postgres: logical replication launcher

сен 20 02:33:25 datapk-itm-centos8 systemd[1]: Starting PostgreSQL 14 database server ...
сен 20 02:33:25 datapk-itm-centos8 postmaster[128496]: 2022-09-20 11:33:25.357 +05 [128496] СООБЩЕНИЕ: передача вы
сен 20 02:33:25 datapk-itm-centos8 postmaster[128496]: 2022-09-20 11:33:25.357 +05 [128496] ПОДСКАЗКА: В дальнейше
сен 20 02:33:25 datapk-itm-centos8 systemd[1]: Started PostgreSQL 14 database server.
```

Рис. 4-31 Проверка статуса СУБД

4.3.6. Настройка межсетевого экрана iptables

Настройте межсетевой экран iptables для корректной работы UDV-ITM-VM. Для этого:

1. Установите пакет iptables-services:

```
yum install iptables-services
```

2. Замените файл /etc/sysconfig/iptables на файл iptables из комплекта поставки:

```
mv /opt/itm-vm/iptables /etc/sysconfig/
```

3. Отредактируйте файл iptables:

- a. Откройте файл для редактирования с помощью команды:

```
vi /etc/sysconfig/iptables
```

- b. Закройте доступ из неиспользуемых подсетей, применяемых в docker-контейнерах других компонентов. Для этого закомментируйте строки `-A INPUT -s 172.16.239.0/24 -j АССЕРТ` (номер 18) и `-A INPUT -s 172.16.240.0/24 -j АССЕРТ` (номер 21).

 **Прим.:**

Включить отображение номеров строк в файле можно с помощью следующих действий:

- i. Нажмите клавишу «Esc», чтобы перейти в командный режим.
- ii. Введите `:set number` или `:set nu` и нажмите «Enter».
- iii. Нажмите клавишу «i», чтобы перевести редактор в режим ввода текста.
- iv. После закрытия файла нумерация строк отключится автоматически. Чтобы отключить абсолютные номера строк на время редактирования файла, перейдите в командный режим и выполните команду `:set nonumber` или `:set nonu`.

- c. При установке UDV-ITM-M и UDV-ITM-VM на одну машину откройте дополнительные порты web-интерфейса. Для этого раскомментируйте строки `#-A INPUT -p tcp -m tcp --dport 8080 -j ACCEPT` (номер 38) и `#-A INPUT -p tcp -m tcp --dport 8443 -j ACCEPT` (номер 39).
- d. Закомментируйте строки `-A INPUT -p tcp -m tcp --dport 10051 -j ACCEPT` (номер 42) и `-A INPUT -p udp -m udp --dport 162 -j ACCEPT` (номер 45) (порты для приема zabbix-соединений и SNMP traps).
- e. Если требуется мониторинг сервера с помощью UDV-ITM-M или по протоколу SNMP, раскомментируйте строки `#-A INPUT -p tcp -m tcp --dport 10050 -j ACCEPT` (номер 51) и `#-A INPUT -p udp -m udp --dport 161 -j ACCEPT` (номер 48) соответственно.
- f. Сохраните файл и выйдите из режима редактирования:

```
:wq
```

4. Проверьте владельца файла и права доступа командой:

```
ls -l /etc/sysconfig/iptables
```

Владелец и права должны совпадать с указанными на скриншоте:

```
[root@eng-itm-vmk1 ~]# ls -l /etc/sysconfig/iptables
-rw-----. 1 root root 2774 Dec  5 15:33 /etc/sysconfig/iptables
```

Рис. 4-32 Владелец и права файла iptables

В противном случае выполните команду:

```
chown root:root /etc/sysconfig/iptables && chmod 600 /etc/sysconfig/iptables
```

Проверьте, что владелец и права теперь соответствуют указанным на скриншоте.

5. Запустите службу iptables и добавьте ее в автозагрузку:

```
systemctl enable --now iptables.service
```

Результат шага: Правила из файла будут применены на сетевом экране системы, а также будут автоматически применяться после перезагрузки.

4.3.7. Установка сервера визуализации и управления UDV-ITM-VM на ОС Centos 8

Прим.:

При установке UDV-ITM-VM и UDV-ITM-M на один сервер совпадающие настройки UDV-ITM-VM и UDV-ITM-M (кроме подготовки сертификатов) достаточно выполнить один раз.

Для установки UDV-ITM-VM:

1. Перейдите в режим командной строки операционной системы, на которой будет установлен сервер визуализации и управления.
2. Создайте директорию для установки UDV-ITM-VM:

```
mkdir /opt/itm-vm
```

 **Прим.:**

Для использования UDV-ITM-VM и UDV-ITM-M на одном сервере директории для их установки должны различаться.

3. Скопируйте следующие файлы в директорию `/opt/itm-vm`:

- `env_generator.sh`;
- `docker-compose.release.yaml`;
- `udv_itm-vm_1.7.0.0.tar.gz`.

4. Перейдите в директорию `/opt/itm-vm`:

```
cd /opt/itm-vm
```

5. Загрузите образы в операционную систему, на которой установлен сервер визуализации и управления:

```
docker load -i udv_itm-vm_1.7.0.0.tar.gz
```

6. Создайте env-файлы и настройте значения переменных. Для этого:

- a. Назначьте скрипту `env_generator.sh` полные права доступа:

```
chmod +x env_generator.sh
```

- b. Запустите скрипт:

```
./env_generator.sh
```

Результат шага: Откроется всплывающее окно для настройки переменных.

- c. Выполните настройку переменных:

- Чтобы изменить переменную, введите новое значение и нажмите клавишу «Enter».
- Чтобы оставить значение переменной по умолчанию, которое указано в квадратных скобках, нажмите клавишу «Enter».
- Чтобы ответить на вопрос «да», нажмите клавишу «y».
- Чтобы ответить на вопрос «нет», нажмите клавишу «n».

 **Прим.:**

- Если IP-адрес подсети контейнеров уже используется в вашей инфраструктуре, его нужно изменить. Подробнее см. в разделе 6.1 Конфликт подсети контейнеров (62) 6.1.0 Причина 2 (63).
- При установке UDV-ITM-VM и UDV-ITM-M на один сервер для UDV-ITM-VM рекомендуется указать порт для подключения к веб-интерфейсу 8080 и SSL порт для подключения к веб-интерфейсу 8443.

Результат шага: В директории `/opt/itm-vm` появятся файлы `.env` и `.itmm_password_secret_key` с настроенными переменными.

d. Для более подробной настройки переменных `.env`-файла или для правки ранее введенных переменных:

i. Откройте для редактирования файл `.env`:

```
vi .env
```

ii. Настройте переменные.

 **Прим.:**

Рекомендуемые и возможные значения переменных приведены в разделе 7.5 Переменные файла `.env` (76).

iii. Сохраните изменения и закройте файл:

```
:wq
```

7. Подготовьте сертификаты для входа в веб-интерфейс. Подробнее см. в разделе 4.5 Выпуск SSL-сертификатов (51).

 **Прим.:**

При установке UDV-ITM-VM и UDV-ITM-M на один сервер необходимо подготовить сертификаты в рабочей директории для каждого из уровней.

8. Измените настройку выделения памяти `vm.overcommit_memory`. Для этого:

a. Откройте для редактирования файл `/etc/sysctl.conf`:

```
vi /etc/sysctl.conf
```

 **Подсказка:**

В случае отсутствия файла `/etc/sysctl.conf` используйте эту же команду для создания файла и перехода в режим редактирования.

b. Добавьте в содержимое файла следующее значение:

```
vm.overcommit_memory=1
```

c. Сохраните файл и выйдите из режима редактирования:

```
:wq
```

d. перезагрузите сервер для применения изменений.

 **Подсказка:**

Вы можете перезагрузить сервер сразу либо после выполнения пункта 4.3.7.0 11 (48).

Результат шага:

a. в логах контейнера itm_m_redis нет ошибки «WARNING overcommit_memory is set to 0!»;

b. в файле `/etc/sysctl.conf` установлено значение `vm.overcommit_memory=1`;

```
# sysctl settings are defined through files in
# /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
#
# Vendors settings live in /usr/lib/sysctl.d/.
# To override a whole file, create a new file with the same in
# /etc/sysctl.d/ and put new settings there. To override
# only specific settings, add a file with a lexically later
# name in /etc/sysctl.d/ and put new settings there.
#
# For more information, see sysctl.conf(5) and sysctl.d(5).
vm.overcommit_memory=1
```

Рис. 4-33 Содержимое файла `sysctl.conf`

c. в файле `/proc/sys/vm/overcommit_memory` установлено значение 1.

9. Убедитесь, что имя сервера и переменная `$HOSTNAME` соответствуют нужным вам значениям.

Актуальное имя сервера отображается в приглашении командной строки. Посмотреть переменную окружения `$HOSTNAME` можно с помощью команды `echo $HOSTNAME`. При необходимости изменения имени сервера см. раздел 6.7 Изменение имени сервера (72).

10. Перейдите в каталог, содержащий `compose`-файлы:

```
cd /opt/itm-vm
```

11. Запустите контейнеры:

```
docker-compose up -d
```

12. Для входа в веб-интерфейс в адресной строке введите IP-адрес UDV-ITM-VM.

 **Прим.:**

При установке UDV-ITM-VM и UDV-ITM-M на один сервер UDV-ITM-VM будет доступен по адресу `https://[ip-адрес]:8443`.

Для первичной настройки в окне авторизации введите логин и пароль учетной записи по умолчанию:

- логин: **itm**;
- пароль: **P@ssw0rd1234**.

Авторизация

Логин *

Пароль *

Войти

Рис. 4-34 Окно авторизации ITM-VM

 **Внимание:**

При первой настройке комплекса необходимо изменить пароль встроенной учетной записи.

4.4. Обновление UDV-ITM-VM с версии 1.6.0.0 до версии 1.7.0.0

Для обновления сервера UDV-ITM-VM с версии 1.6.0.0 до версии 1.7.0.0:

1. Перейдите в рабочую директорию UDV-ITM-VM:

```
cd /opt/itm-vm
```

2. Остановите работу сервера:

```
docker-compose down
```

3. Переименуйте старую рабочую директорию UDV-ITM-VM:

```
mv /opt/itm-vm /opt/itm-vm-bkp
```

4. Создайте директорию для новой версии UDV-ITM-VM:

```
mkdir /opt/itm-vm
```

5. Загрузите в директорию `/opt/itm-vm` на сервере UDV-ITM-VM следующие файлы из каталога с обновленным дистрибутивом:

- a. `udv_itm-vm_1.7.0.0.tar.gz`;
- b. `docker-compose.release.yaml`.

6. Перейдите в директорию, куда были перемещены файлы с обновленным дистрибутивом UDV-ITM-VM:

```
cd /opt/itm-vm
```

7. Установите обновленные образы командой:

```
docker load -i udv_itm-vm_1.7.0.0.tar.gz
```

8. Скопируйте данные из старой рабочей директории `/opt/itm-vm-bkp` в новую директорию `/opt/itm-vm`:

```
cp -r /opt/itm-vm-bkp/.env /opt/itm-vm-bkp/env /opt/itm-vm-bkp/.itmm_password_secret_key /opt/itm-vm
```

9. Удалите из файла `.env` переменные, которые теперь будут настраиваться в веб-интерфейсе.

 Подсказка:

Если вы изменяли значения переменных на отличные от значений по умолчанию, зафиксируйте их перед изменением файла `.env`.

a. Откройте файл `.env` для редактирования:

```
vi .env
```

b. Удалите переменную «Срок хранения проблем»:

```
ITMM_PROBLEM_AGE_IN_DAYS=180
```

c. Удалите переменную для обозначения часового пояса `TZ=`.

d. Удалите переменную «Срок хранения истории задач синхронизации»:

```
ITMM_SYNC_HISTORY_LIFETIME_IN_DAYS=4
```

e. Удалите переменные для настройки интеграции с SIEM:

```
#-----Настройка интеграции с SIEM-----
SIEM_INTEGRATION=true
SIEM_SYSLOG_HOST=127.0.0.1
SIEM_SYSLOG_PORT=514
SIEM_SYSLOG_PROTOCOL=TCP
ITMM_IP_ADDRESS=
```

f. Сохраните и закройте файл:

```
:wq
```

10. Запустите контейнеры:

```
docker-compose up -d
```

11. Проверьте результат обновления. Для этого перейдите в веб-интерфейс UDV-ITM-VM по ранее использовавшемуся адресу.

12. Если обновление прошло успешно, удалите директорию с предыдущей версией UDV-ITM-VM 1.6.0.0:

```
rm -rf /opt/itm-vm-bkp/
```

13. Настройте в веб-интерфейсе следующие параметры, если в UDV-ITM-VM версии 1.6.0.0 меняли их значения в файле `.env`:

- Настройка интеграции с SIEM. Подробнее см. в Руководстве по эксплуатации UDV-ITM-VM в разделе «Настройка интеграции с SIEM».
- Период хранения истории проблем. Подробнее см. в Руководстве по эксплуатации UDV-ITM-VM в разделе «Изменение основных свойств сервера».
- Период хранения истории синхронизаций. Подробнее см. в Руководстве по эксплуатации UDV-ITM-VM в разделе «Изменение основных свойств сервера».

4.5. Выпуск SSL-сертификатов

В этом разделе рассмотрен выпуск доверенных сертификатов для доступа к веб-интерфейсу UDV-ITM-VM по сетевому имени.

Перед выпуском сертификатов остановите UDV-ITM-VM командой:

```
cd /opt/itm-vm && docker-compose down
```

Выпуск сертификатов для UDV-ITM-VM состоит из следующих этапов:

- 4.5.1 Выпуск корневых сертификатов (51)
- 4.5.2 Выпуск сертификата и ключа для доступа к веб-интерфейсу UDV-ITM-VM (52)
- 4.5.3 Настройка APM Администратора (53)

4.5.1. Выпуск корневых сертификатов

Корневой сертификат, выпущенный на сервере UDV-ITM-VM, можно также использовать для настройки доступа по сетевому имени к серверам UDV-ITM-M. Для этого нужно поместить выпущенные на сервере UDV-ITM-VM ключ `local_ca.key` и сертификат `local_ca.crt` в директорию `/opt/itm-k/env/nginx/certs/` настраиваемого сервера UDV-ITM-M, пропустить в документации UDV-ITM-M раздел «Выпуск корневых сертификатов» и перейти к разделу «Выпуск сертификата и ключа для доступа к веб-интерфейсу UDV-ITM-M» .

Если на предприятии имеется корневой сертификат, то можно использовать его вместо `local_ca.key` и `local_ca.crt`, но необходимо знать пароль ключа.

1. Перейдите в режим командной строки операционной системы, на которой установлен сервер UDV-ITM-VM.
2. Выпустите ключ для корневого сертификата командой:

```
openssl genrsa -aes256 -out /opt/itm-vm/env/nginx/certs/local_ca.key 2048
```

Дважды введите пароль для генерируемого ключа.

3. Сгенерируйте корневой сертификат командой:

```
openssl req -key /opt/itm-vm/env/nginx/certs/local_ca.key -new -x509 -days 3650 \
-subj "/C=RU/L=UDV/O=[CompanyName]/OU=CLITM/CN=clitm-ca" -sha256 \
-out /opt/itm-vm/env/nginx/certs/local_ca.crt
```

В этой команде параметр [CompanyName] – название эксплуатирующей организации.

Пример: Для эксплуатирующей организации CyberLympha команда будет выглядеть следующим образом:

```
openssl req -key /opt/itm-vm/env/nginx/certs/local_ca.key -new -x509 -days 3650 \
-subj "/C=RU/L=UDV/O=CyberLympha/OU=CLITM/CN=clitm-ca" -sha256 \
-out /opt/itm-vm/env/nginx/certs/local_ca.crt
```

Введите пароль ключа `local_ca.key`.

4.5.2. Выпуск сертификата и ключа для доступа к веб-интерфейсу UDV-ITM-VM

1. Задайте локальную переменную `hn`, равную сетевому имени UDV-ITM-VM:

```
hn=$(cat /etc/hostname)
```

2. Создайте файл формата `.pem`, который будет содержать в себе `local_ca.key`:

```
openssl req -x509 -new -nodes -key /opt/itm-vm/env/nginx/certs/local_ca.key \
-sha256 \
-days 3650 -subj "/C=RU/L=UDV/O=[CompanyName]/OU=CLITM/CN=$hn" \
-out /opt/itm-vm/env/nginx/certs/local_ca.pem
```

В этой команде параметр [CompanyName] – название эксплуатирующей организации.

Пример: Для эксплуатирующей организации CyberLympha команда будет выглядеть следующим образом:

```
openssl req -key /opt/itm-vm/env/nginx/certs/local_ca.key -new -x509 -days 3650 \
-subj "/C=RU/L=UDV/O=CyberLympha/OU=CLITM/CN=clitm-ca" -sha256 \
-out /opt/itm-vm/env/nginx/certs/local_ca.crt
```

Введите пароль ключа `local_ca.key`.

3. Сгенерируйте ключ для сертификата доступа к веб-интерфейсу UDV-ITM-VM:

```
openssl genrsa -out /opt/itm-vm/env/nginx/certs/nginx.key 2048
```

4. Создайте файл запроса на генерацию сертификата командой:

```
openssl req -new -key /opt/itm-vm/env/nginx/certs/nginx.key \
-subj "/C=RU/L=UDV/O=[CompanyName]/OU=CLITM/CN=$hn" -out /opt/itm-vm/env/nginx/
certs/local.csr
```

В этой команде параметр `[CompanyName]` – название эксплуатирующей организации.

Пример: Для эксплуатирующей организации CyberLympha команда будет выглядеть следующим образом:

```
openssl req -new -key /opt/itm-vm/env/nginx/certs/nginx.key \
-subj "/C=RU/L=UDV/O=CyberLympha/OU=CLITM/CN=$hn" -out /opt/itm-vm/env/nginx/
certs/local.csr
```

5. Создайте файл с параметрами, которые будут использоваться при генерации сертификата:

```
echo -e "basicConstraints=CA:FALSE\nsubjectAltName = @alt_names\n
\n[alt_names]\nDNS.1 = $hn" > /opt/itm-vm/env/nginx/certs/local.ext
```

6. Сгенерируйте сертификат для доступа к веб-интерфейсу UDV-ITM-VM:

```
openssl x509 -req -in /opt/itm-vm/env/nginx/certs/local.csr -CA /opt/itm-vm/env/
nginx/certs/local_ca.crt \
-CAkey /opt/itm-vm/env/nginx/certs/local_ca.key -CAcreateserial -out /opt/itm-vm/
env/nginx/certs/nginx.crt \
-days 3650 -sha256 -extfile /opt/itm-vm/env/nginx/certs/local.ext
```

Введите пароль ключа `local_ca.key`.

7. Удалите лишние файлы:

```
cd /opt/itm-vm/env/nginx/certs && rm -f local.csr local.ext local_ca.pem
local_ca.srl
```

8.  **Внимание:**

Если вы устанавливаете сервер UDV-ITM-VM с нуля, пропустите этот шаг.

Запустите UDV-ITM-VM:

```
cd /opt/itm-vm && docker-compose up -d
```

4.5.3. Настройка АРМ Администратора

1. Добавьте в файл `C:\Windows\System32\drivers\etc\hosts` следующую запись:

```
<ip_addr> <hostname>
```

В этой записи `<ip_addr>` – IP-адрес сетевого интерфейса управления UDV-ITM-VM, `<hostname>` – сетевое имя UDV-ITM-VM.

 **Прим.:**

Если на АРМ Администратора установлена Unix-like ОС, то запись в таком же формате добавьте в файл `/etc/hosts`.

2. Импортируйте выпущенный корневой сертификат `local_ca.crt` в веб-браузер, в котором будете подключаться к UDV-ITM-VM. Для этого:

a. Загрузите с сервера UDV-ITM-VM файл `local_ca.crt` на АРМ Администратора.

b. Если используется веб-браузер Google Chrome:

- i. Перейдите на страницу настроек «Настройка и управление Google Chrome» → «Настройки» → «Конфиденциальность и безопасность» → «Безопасность» → «Управление сертификатами устройства».
- ii. В новом окне откройте вкладку «Доверенные корневые центры сертификации». Нажмите «Импорт».
- iii. В открывшемся окне нажмите «Далее». В поле «Имя файла:» нажмите «Обзор». Выберите файл `local_ca.crt`, загруженный с сервера UDV-ITM-VM. Нажмите «Далее».
- iv. Убедитесь, что выбран вариант «Поместить все сертификаты в следующее хранилище» и в поле «Хранилище сертификатов:» выбрано «Доверенные корневые центры сертификации». Нажмите «Далее» и «Готово».
- v. В окне предупреждения безопасности импорта сертификата нажмите «Да» для подтверждения импорта. Закройте окно управления сертификатами.

c. Если используется веб-браузер Mozilla Firefox:

- i. Перейдите на страницу настроек «Открыть меню приложения» → «Настройки» → «Приватность и защита» → «Просмотр сертификатов...».
- ii. Откройте вкладку «Центры сертификации», нажмите «Импортировать». Выберите файл `local_ca.crt`, загруженный с сервера UDV-ITM-VM.
- iii. В окне «Загрузка сертификата» установите чекбокс в поле «Доверять при идентификации веб-сайтов», нажмите «ОК» два раза.

3. Откройте веб-интерфейс сервера UDV-ITM-VM, введя в адресной строке браузера адрес `https://<hostname>`, где `<hostname>` – сетевое имя сервера UDV-ITM-VM.

 **Внимание:**

Проверка будет возможна после запуска сервера UDV-ITM-VM.

4.6. Настройка интеграции с SIEM

Для интеграции с SIEM нужно задать несколько переменных окружения. Для этого:

1. Перейдите в режим командной строки.
2. Перейдите в режим редактирования файла `.env`:

```
vi /opt/itm-vm/.env
```

3. Проверьте и при необходимости измените значение переменной `SIEM_INTEGRATION`:

- `SIEM_INTEGRATION=true` — включает интеграцию с SIEM;
- `SIEM_INTEGRATION=false` — отключает интеграцию с SIEM.

4. Задайте следующие переменные окружения:

- a. `SIEM_SYSLOG_HOST` — IP-адрес syslog-сервера.

Пример: `SIEM_SYSLOG_HOST=127.0.0.1`

- b. `ITMM_IP_ADDRESS` — IP-адрес хоста с UDV-ITM-VM.

Пример: `ITMM_IP_ADDRESS=10.51.30.99`

5. При необходимости задайте переменные окружения:

- a. `SIEM_SYSLOG_PORT` — Порт syslog-сервера.

Пример: `SIEM_SYSLOG_PORT=514`

- b. `SIEM_SYSLOG_PROTOCOL` — Протокол, по которому будут отправляться события: TCP или UDP.

Пример: `SIEM_SYSLOG_PROTOCOL=TCP`

6. Сохраните файл и выйдите из режима редактирования:

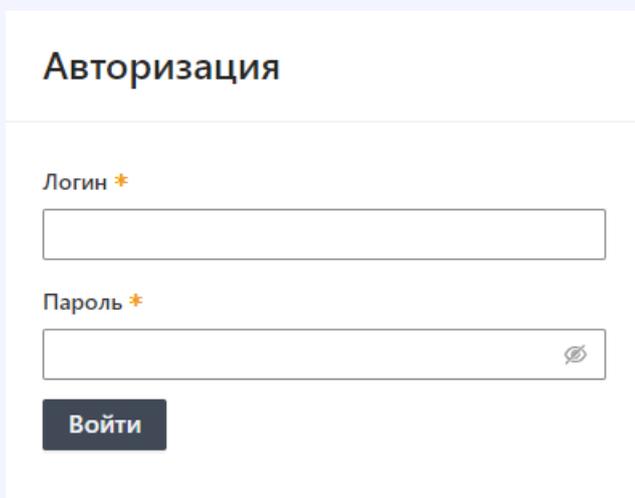
```
:wq
```

4.7. Подключение к веб-интерфейсу

Для подключения к веб-интерфейсу UDV-ITM-VM:

1. В браузере в адресной строке введите IP-адрес UDV-ITM-VM.

Результат шага: отобразится окно входа в веб-интерфейс UDV-ITM-VM.



Авторизация

Логин *

Пароль *

Войти

Рис. 4-35 Окно авторизации

2. В окне входа введите логин и пароль учетной записи.

Для встроенной учетной записи по умолчанию заданы логин **itm** и пароль **P@ssw0rd1234**. При первой настройке комплекса необходимо изменить логин и пароль встроенной учетной записи.

 **Внимание:**

При вводе неправильного логина или пароля 5 раз IP-адрес, с которого пользователь пытается авторизоваться, блокируется на 5 минут.

3. Нажмите на кнопку «Войти».

Результат шага: выполнен вход на главную страницу веб-интерфейса UDV-ITM-VM.

 **Подсказка:**

Чтобы завершить сеанс работы в веб-интерфейсе UDV-ITM-VM, нажмите на кнопку  («Выйти») в нижней части главного меню.

5. Резервное копирование и восстановление баз данных

В этом разделе рассматриваются два способа резервного копирования и восстановления баз данных:

1. Резервное копирование одной конкретной базы данных. Использование этого метода позволяет восстанавливать БД в том состоянии, в котором она была на момент резервного копирования.

Прим.:

Рекомендуется использовать этот способ для резервного копирования установленных на отдельном сервере UDV-ITM-M или UDV-ITM-RM, так как они используют одну БД.

См. подразделы:

- 5.1 Создание резервной копии базы данных Jatoba/PostgreSQL (57)
 - 5.2 Восстановление резервной копии базы данных Jatoba/PostgreSQL (58)
2. Резервное копирование всех баз данных и файлов журнала БД в двоичном виде. Использование этого метода позволяет восстанавливать БД в состоянии на определенное время.

Прим.:

Рекомендуется использовать этот способ для резервного копирования UDV-ITM-VM, а также UDV-ITM-M , если он находится на том же сервере, так как в этом случае используется несколько БД. Для настройки резервного копирования БД с помощью утилиты `pg_basebackup` с помощью `wal`-файлов воспользуйтесь документацией поставщика СУБД.

5.1. Создание резервной копии базы данных Jatoba/PostgreSQL

1. Создайте архив с резервной копией БД:

```
pg_dump -Fc <db_name> -U <db_user> -h <host> -p <port> -f <dir>/<db_archive>.dump
```

Где:

- `db_name` — наименование базы данных;
- `db_user` — имя пользователя;
- `host` — имя или IP-адрес компьютера, на котором работает сервер;
- `port` — порт подключения;
- `dir` — директория для сохранения архива базы данных;
- `db_archive` — наименование архива базы данных;
- `-Fc` — гибкий формат резервных файлов типа «custom».

Пример: Команда для выгрузки БД `itmk_db` с пользователем `itmk_user`, IP-адресом сервера `127.0.0.1` и портом `10265` в архив с именем `itmbackup3010` в директории `/opt` будет выглядеть следующим образом:

```
pg_dump -Fc itmk_db -U itmk_user -h 127.0.0.1 -p 10265 -f /opt/itmbackup3010.dump
```

 **Прим.:**

Подробную информацию о параметрах `pg_dump` можно узнать с помощью команды:

```
pg_dump --help
```

2. Введите пароль пользователя для доступа к базе данных.

Результат шага: После успешного ввода пароля начнется создание файла с базой данных.

5.2. Восстановление резервной копии базы данных Jatoba/PostgreSQL

Способ 1: развертывание резервной копии с форматом «custom»

Способ подходит для резервных копий, которые были созданы с помощью команды `pg_dump -Fc` и имеют пользовательский формат.

1. Убедитесь, что на сервере для восстановления находится файл архива, полученный в результате работы `pg_dump`.
2. Восстановите базу данных Jatoba из файла архива, созданного командой `pg_dump`:

```
psql -U [db_user] -h [host] -p [port] [db_name] < [db_dump_path]
```

В этой команде:

- `db_user` — имя пользователя;
- `host` — имя или IP-адрес компьютера, на котором работает сервер;
- `port` — порт подключения;
- `db_name` — наименование базы данных;
- `db_dump_path` - путь до резервной копии.

Пример: Команда для восстановления БД с пользователем `itmm_user`, IP-адресом сервера `127.0.0.1`, портом `10265`, наименованием `itmm_db` и путем для резервной копии `/opt/itmm_db_260723.dump` будет выглядеть следующим образом:

```
psql -U itmm_user -h 127.0.0.1 -p 10265 itmm_db < /opt/itmm_db_260723.dump
```

3. Введите пароль пользователя для доступа к базе данных.

После успешного ввода пароля начнется восстановление из файла с выгруженной базой данных.

Способ 2: развертывание резервной копии с текстовым форматом

Способ подходит для резервных копий, которые были созданы с помощью команды `pg_dump` без использования дополнительных ключей.

1. Создайте базу, в которую будут скопированы данные из резервной копии:

a. Войдите в интерактивный терминал для работы с postgresql под пользователем `postgres`:

```
sudo -u postgres psql
```

b. Создайте базу данных для восстановления данных из резервной копии, в качестве распорядителя которой указан пользователь `db_user`:

```
CREATE DATABASE [db_name] WITH OWNER '[db_user]';
```

В этой команде:

- `db_name` — наименование базы данных;
- `db_user` — имя пользователя.

c. Убедитесь, что база данных `[db_name]` создана:

```
\l
```

d. Покиньте терминал:

```
\q
```

e. Для выхода из пользователя `postgres` введите `exit`.

2. Восстановите базу данных Jatoba из файла архива с текстовым форматом, созданного командой `pg_dump`:

```
psql -h [host] -p [port] -U [db_user] [db_name] < [dir]/[db_archive].dump
```

В этой команде:

- `host` — имя или IP-адрес компьютера, на котором работает сервер;
- `port` — порт подключения;
- `db_user` — имя пользователя;
- `db_name` — наименование базы данных;
- `dir` — директория для сохранения архива базы данных;
- `db_archive` — наименование архива базы данных.

Прим.:

В качестве пользователя для развертывания рекомендуется указать пользователя с правами супер-администратора. Права на базу будут соответствовать пользователю, от чьего имени база была создана, либо пользователю, который был указан в значении ключа `WITH OWNER`.

Пример: Команда для выгрузки БД `datarkit` с пользователем `postgres`, IP-адресом сервера `127.0.0.1` и портом `10265` в архив с именем `datarkit` в директории `/opt` будет выглядеть следующим образом:

```
psql -h 127.0.0.1 -p 10265 -U postgres datapkitm < /opt/datapkitm.dump
```

3. Введите пароль пользователя для доступа к базе данных.

Результат шага: После успешного ввода пароля начнется создание файла с базой данных.

6. Нештатные ситуации и способы их устранения

При выявлении нештатного функционирования ПО сервера UDV ITM рекомендуется изучить документацию и воспользоваться рекомендациями по устранению неисправностей из настоящего раздела.

Для получения технической поддержки необходимо оформить заявку в сервисный центр в соответствии с регламентом. Подробности см. по ссылке <https://www.ussc.ru/product/servisnaya-podderzhka/>.

При обращении в сервисный центр рекомендуется предоставить техническую информацию о параметрах сервера и его конфигурации.

Перечень технической информации, необходимой для диагностики функционирования сервера UDV ITM:

- версия UDV ITM;
- общее количество ОМ, проблем функционирования ОМ и ИТ-услуг на момент обращения;
- количество подключенных серверов нижних уровней иерархии;
- краткое словесное описание ошибки;
- подробное пошаговое описание действий, которые привели к ошибке;
- скриншот ошибки в web-интерфейсе;
- результаты ошибочных запросов (см. панель разработчика в браузере, вкладка response у проблемного запроса);
- логи сопутствующих контейнеров;
- данные по аппаратной платформе (сервер, процессор, объем оперативной памяти, объем дискового пространства, тип дисков);
- версия ОС;
- используемая СУБД, версия.

Дополнительно может потребоваться следующая информация:

- полная техническая информация о системе и логи (используйте скрипт сбора детальной информации о системе, подробнее см. в разделе 6.8 Скрипт для сбора логов (73));
- свободное место на корневом разделе диска;



Подсказка:

используйте команду `df -h /`.

- свободная оперативная память, текущий список процессов;



Подсказка:

используйте команду `htop`.

- значение Load Average;

- загрузка диска.



Подсказка:

используйте команду `iotop`.

В этом разделе:

- 6.1 Конфликт подсети контейнеров (62)
- 6.2 Ошибка интеграции с SIEM (66)
- 6.3 Ошибка вида «WARNING overcommit_memory is set to 0! Background save may fail under low memory condition.<...>» (67)
- 6.4 Не запускаются контейнеры docker (67)
- 6.5 Веб-интерфейс UDV-ITM-VM не загружается (68)
- 6.6 Не удается зайти в веб-интерфейс UDV-ITM-VM с корректными учетными данными (69)
- 6.7 Изменение имени сервера (72)
- 6.8 Скрипт для сбора логов (73)

6.1. Конфликт подсети контейнеров

В качестве причин конфликта подсети контейнеров рассмотрены следующие:

- Адрес подсети контейнеров уже используется в вашей инфраструктуре.
- Адрес подсети `docker0` используется в вашей инфраструктуре.

Причина 1

Адрес подсети контейнеров уже используется в вашей инфраструктуре.

Способ устранения

Для устранения проблемы измените подсеть контейнеров Docker:

1. Остановите работу контейнеров:

```
docker-compose down
```

2. Дождитесь остановки работы всех контейнеров (3-5 минут).
3. Проверьте и при необходимости отредактируйте файл `.env`:

- a. Перейдите в режим редактирования файла:

```
vi .env
```

- b. Если в файле `.env` не заданы переменные `ITMM_NETWORK` и `ITMM_NETWORK_GATEWAY`, добавьте в файл строки:

```
ITMM_NETWORK=XXX.XXX.XXX.XXX/XX
```

```
ITMM_NETWORK_GATEWAY=XXX.XXX.XXX.XXX
```

Где XXX.XXX.XXX.XXX/XX — новая подсеть, XXX.XXX.XXX.XXX — новый сетевой шлюз.

c. Если в файле `.env` уже указаны значения переменных `ITMM_NETWORK` и `ITMM_NETWORK_GATEWAY`, задайте им новые значения.

d. Сохраните файл и выйдите из режима редактирования:

```
:wq
```

4. Отредактируйте файл `pg_hba.conf`. Для этого:

a. Перейдите в режим редактирования файла `pg_hba.conf` с помощью команды:

```
vi /var/lib/jatoba/1/data/pg_hba.conf
```

b. Измените IP-адрес и маску подсети контейнеров Docker в разделе «# IPv4 local connections:» в строке вида:

```
host [имя БД] [имя пользователя БД] [IP-адрес docker-сети/маска в формате CIDR] [метод аутентификации]
```

c. Сохраните файл и выйдите из режима редактирования:

```
:wq
```

d. Перезапустите СУБД для применения настроек:

```
systemctl restart jatoba-1*
```

5. Запустите работу контейнеров:

```
docker-compose up -d
```

Причина 2

Адрес подсети `docker0` используется в вашей инфраструктуре.

Способ устранения 1

1. Остановите и удалите все контейнеры, которые не указаны в `docker-compose` файлах:

```
docker-compose down --remove-orphans
```

2. Просмотрите список маршрутов одной из команд:

- `route -n`

```
[root@exp-itm-k2 itm-k_1.3]# route -n
Kernel IP routing table
Destination        Gateway            Genmask           Flags Metric Ref    Use Iface
0.0.0.0            10.51.16.1       0.0.0.0          UG    100    0      0 ens32
10.51.16.0         0.0.0.0          255.255.255.0   U      100    0      0 ens32
172.15.0.0         0.0.0.0          255.255.255.0   U      0      0      0 br-5161bd905f12
172.16.238.0       0.0.0.0          255.255.255.0   U      0      0      0 br-5dacd4385727
172.16.239.0       0.0.0.0          255.255.255.0   U      0      0      0 br-9e06ddc5bf9a
172.17.0.0         0.0.0.0          255.255.0.0     U      0      0      0 docker0
172.18.0.0         0.0.0.0          255.255.0.0     U      0      0      0 br-df1f16558abc
172.19.0.0         0.0.0.0          255.255.0.0     U      0      0      0 br-b829e0f8fb21
```

Рис. 6-1 Результат работы команды route -n

- ip r

```
[root@exp-itm-k2 itm-k_1.3]# ip r
default via 10.51.16.1 dev ens32 proto static metric 100
10.51.16.0/24 dev ens32 proto kernel scope link src 10.51.16.126 metric 100
172.15.0.0/24 dev br-5161bd905f12 proto kernel scope link src 172.15.0.1
172.16.238.0/24 dev br-5dacd4385727 proto kernel scope link src 172.16.238.1
172.16.239.0/24 dev br-9e06ddc5bf9a proto kernel scope link src 172.16.239.1
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
172.18.0.0/16 dev br-df1f16558abc proto kernel scope link src 172.18.0.1 linkdown
172.19.0.0/16 dev br-b829e0f8fb21 proto kernel scope link src 172.19.0.1 linkdown
```

Рис. 6-2 Результат работы команды ip r

3. Убедитесь, что в списке маршрутов отсутствуют контейнерные подсети, кроме docker0. Для этого просмотрите список контейнерных подсетей командой:

```
docker network ls
```

4. При наличии в списке других подсетей найдите их идентификаторы сети в столбце NETWORK ID.

Пример:

```
[root@datapk-itm-red ~]# docker network ls
NETWORK ID          NAME                                DRIVER                SCOPE
bf34584f056d        bridge                             bridge                local
133b26ee44e1        datapkitm_zbx_net_backend         bridge                local
df078bf57e14        datapkitm_zbx_net_frontend        bridge                local
```

Рис. 6-3 Список контейнерных подсетей

В приведенном выше списке идентификатор сети с именем bridge — bf34584f056d.

5. При необходимости удалите контейнерные подсети, кроме docker0:

```
docker network rm [идентификатор подсети]
```

 **Внимание:**

рекомендуется удалять контейнерную подсеть только в случае проблем с инициализацией.

6. Создайте файл /etc/docker/daemon.json.
7. Добавьте в файл адрес узла сети и маску сети.

Пример:

```
{
  "bip": "172.17.77.1/24"
}
```

Результат шага: Подсеть docker0 примет значение, равное добавленному в файл.

8. Перезапустите службу docker:

```
systemctl restart docker
```

9. Отредактируйте файл `pg_hba.conf`. Для этого:

a. Перейдите в режим редактирования файла `pg_hba.conf` с помощью команды:

```
vi /var/lib/jatoba/1/data/pg_hba.conf
```

b. Измените IP-адрес и маску подсети контейнеров Docker в разделе «# IPv4 local connections:» в строке вида:

```
host [имя БД] [имя пользователя БД] [IP-адрес docker-сети/маска в формате CIDR] [метод аутентификации]
```

c. Сохраните файл и выйдите из режима редактирования:

```
:wq
```

10. Отредактируйте файл `postgresql.conf`. Для этого:

a. Перейдите в режим редактирования файла `postgresql.conf`:

```
vi /var/lib/jatoba/1/data/postgresql.conf
```

b. Измените значение переменной `listen_addresses` в разделе «CONNECTIONS AND AUTHENTICATION», чтобы оно соответствовало представленному ниже:

```
listen_addresses = '127.0.0.1,172.17.77.1'
```

Где:

- 127.0.0.1 – локальный IP-адрес сервера UDV-ITM-VM;
- 172.17.77.1 – IP-адрес подсети docker0, заданный на шаге 6.1.0 7 (64).

c. Сохраните файл и выйдите из режима редактирования:

```
:wq
```

d. Перезапустите СУБД для применения настроек:

```
systemctl restart jatoba-1*
```

11. Запустите работу контейнеров:

```
docker-compose up -d
```

Способ устранения 2



Внимание:

рекомендуется использовать этот способ, только если другие способы не сработали.

1. Удалите все остановленные Docker-контейнеры:

```
docker container prune -f
```

2. Удалите все Docker-контейнеры, включая запущенные контейнеры:

```
docker rm -f $(docker ps -a -q)
```

 **Внимание:**

При использовании UDV-ITM-VM версии старше 1.3.1.0 эта команда приведет к удалению базы данных.

3. Просмотрите наименования и идентификаторы подсетей:

```
docker network ls
```

4. Удалите все frontend и backend подсети:

```
docker network rm [идентификатор или наименование подсети]
```

5. Загрузите docker командой:

```
docker load -i [имя_архива].tar.gz
```

6.2. Ошибка интеграции с SIEM

Происходит перезапуск контейнера itm_m_siem_connector. В логах текст «Для интеграции с SIEM не переданы обязательные переменные окружения SIEM_SYSLOG_HOST и ITMM_IP_ADDRESS».

Причина

Отсутствие переменных SIEM_SYSLOG_HOST и ITMM_IP_ADDRESS в файле `.env` при включенной интеграции с SIEM.

Способ устранения

1. Перейдите в режим командной строки.
2. Перейдите в режим редактирования файла `.env`:

```
vi /opt/itm-vm/.env
```

3. Проверьте наличие в файле переменных SIEM_SYSLOG_HOST и ITMM_IP_ADDRESS.
4. В случае отсутствия переменных SIEM_SYSLOG_HOST и ITMM_IP_ADDRESS добавьте их в файл.

Пример:

```
SIEM_SYSLOG_HOST=127.0.0.1  
ITMM_IP_ADDRESS=10.51.30.99
```

5. Сохраните файл и выйдите из режима редактирования:

```
:wq
```

6.3. Ошибка вида «WARNING overcommit_memory is set to 0! Background save may fail under low memory condition.<...>»

В логах контейнера itm_m_redis содержится сообщение об ошибке «WARNING overcommit_memory is set to 0! Background save may fail under low memory condition. To fix this issue add 'vm.overcommit_memory = 1' to /etc/sysctl.conf and then reboot or run the command 'sysctl vm.overcommit_memory=1' for this to take effect.».

Причина

Значение `vm.overcommit_memory=0`, из-за чего при недостатке памяти может не работать автосохранение в фоновом режиме.

Способ устранения

Измените настройку выделения памяти `vm.overcommit_memory`. Для этого:

- a. Откройте для редактирования файл `/etc/sysctl.conf`:

```
vi /etc/sysctl.conf
```

Подсказка:

В случае отсутствия файла `/etc/sysctl.conf` используйте эту же команду для создания файла и перехода в режим редактирования.

- b. Добавьте в содержимое файла следующее значение:

```
vm.overcommit_memory=1
```

- c. Сохраните файл и выйдите из режима редактирования:

```
:wq
```

- d. Перезагрузите сервер для применения изменений.

6.4. Не запускаются контейнеры docker

В командной строке при попытке запуска контейнеров docker появляются сообщения об ошибке вида: «for <имя сервиса> cannot create container for service <имя сервиса>: invalid IP address <...>».

Причина

Устаревшая версия docker.

Способ устранения

Обновите docker до версии 20. Для этого выполните действия, описанные в разделе 4.2.2 Установка дополнительных пакетов в ОС РЕД ОС 7.3 (12).

6.5. Веб-интерфейс UDV-ITM-VM не загружается

В качестве причин недоступности веб-интерфейса UDV-ITM-М рассмотрены следующие:

- запуск службы docker после службы СУБД;
- изменение переменных при включенных контейнерах.

Причина 1

Запуск службы docker после службы СУБД.

Описание проблемы

Веб-интерфейс UDV-ITM-VM недоступен, в логах содержится ошибка «**** PostgreSQL server is not available. Waiting 5 seconds...».

Способ устранения

1. Убедитесь, что причина проблемы в запуске службы docker после службы СУБД. На это указывают следующие признаки:
 - a. При проверке статуса службы СУБД командой `systemctl status jatoba-1` выясняется, что служба не запущена.
 - b. Появляется сообщение «СООБЩЕНИЕ: не удалось привязаться к адресу IPv4 "172.16.239.1": Cannot assign requested address ПРЕДУПРЕЖДЕНИЕ: не удалось создать принимающий сокет для "172.16.239.1"».
 - c. При запуске команды `lsof -i -P -n` в выводе нет сокета для 172.16.239.1.
2. Настройте запуск службы СУБД после службы docker. Для этого:
 - a. Перейдите в режим редактирования службы СУБД:

```
systemctl edit jatoba-1.service
```
 - b. Добавьте блок [Unit]:

```
[Unit]
After=docker.service
BindsTo=docker.service
ReloadPropagatedFrom=docker.service
```
 - c. Если база данных хранится на отдельном томе, добавьте после блока [Unit] блок [Service]:

```
[Service]
Environment=PGDATA=/storage/base
```

Где `/storage/base` — путь к базе данных, который был настроен на шаге 4.2.4.2.0 1 (18) раздела 4.2.4.2 Настройка СУБД (18).
 - d. Для применения изменений в настройках службы СУБД выполните команду:

```
systemctl daemon-reload
```

3. Проверьте состояние службы `jatoba-1`

```
systemctl status jatoba-1
```

4. Если служба `Jatoba` выключена, запустите ее с помощью команды:

```
systemctl start jatoba-*
```

Причина 2

Изменение переменных при включенных контейнерах.

Описание проблемы

Веб-интерфейс не загружается либо при загрузке при вызове окна «инструменты разработчика» через F12 в браузере отображаются ошибки 502. При этом не все контейнеры запущены.

Способ устранения

1. Перейдите в режим командной строки операционной системы, на которой установлен UDV-ITM-VM.
2. Перейдите в рабочую директорию UDV-ITM-VM:

```
cd /opt/itm-vm
```

3. Перезапустите контейнеры:

```
docker-compose down && docker-compose up -d
```

6.6. Не удается зайти в веб-интерфейс UDV-ITM-VM с корректными учетными данными

В качестве причин недоступности веб-интерфейса UDV-ITM-M рассмотрены следующие:

- не задано значение переменной `ITMM_PASSWORD_SECRET_KEY` в файле `.itmm_password_secret_key` либо переменная `ITMM_PASSWORD_SECRET_KEY` закомментирована;
- в файле `pg_hba.conf` указано значение только для одной базы данных, а не для нескольких.
- модуль управления паролльными политиками «`securityprofile`» не был повторно инициализирован после перезагрузки сервера СУБД или перезапуска службы `jatoba-1`.

Причина 1

Не задано значение переменной `ITMM_PASSWORD_SECRET_KEY` в файле `.itmm_password_secret_key` либо переменная `ITMM_PASSWORD_SECRET_KEY` закомментирована.

Описание проблемы

Не удается зайти в веб-интерфейс UDV-ITM-VM с корректными учетными данными. При запуске контейнеров UDV-ITM-VM командой `docker-compose up -d` происходит одно из следующих действий:

- в консоли выводится сообщение: «The ITMM_PASSWORD_SECRET_KEY variable is not set. Defaulting to a blank string.».
- перезапускаются контейнеры itm_m_zabbix_connector, itm_m_notifier_service, itm_m_user_service. В логах itm_m_zabbix_connector содержится запись вида: «Значение поля "key" (Ключ для шифрования паролей) из переменной окружения ITMM_PASSWORD_SECRET_KEY не прошло валидацию: Значение должно равняться 32 байтам. Текущая длина — <...> байт».

Способ устранения

1. Остановите работу контейнеров:

```
docker-compose down
```

2. Сгенерируйте новый ключ для шифрования и дешифрования паролей:

```
LC_ALL=C tr -dc 'A-Za-z0-9!$%^*' </dev/urandom | head -c 32 ; echo ''
```

3. Откройте для редактирования файл `.itmm_password_secret_key`.
4. Удалите старый ключ.



Внимание:

При повторном изменении или утере значения переменной ITMM_PASSWORD_SECRET_KEY локальные пользователи не смогут войти в веб-интерфейс UDV-ITM-VM, перестанет работать синхронизация с UDV-ITM-M, LDAP и SMTP.

5. Вставьте новый ключ.
6. Сохраните изменения и закройте файл `.itmm_password_secret_key`.
7. Обратитесь в техподдержку по адресу `itm@ussc.ru` и запросите скрипт для удаления баз данных.

Причина 2

В файле `pg_hba.conf` указано следующее значение для подключения:

```
host itmm itmm_user 172.15.0.1/24 md5
```

Это значение подходит только для одной базы данных, нужно разрешить подключение для нескольких баз данных.

Описание проблемы

При попытке зайти в веб-интерфейс UDV-ITM-VM выводится сообщение «Внутренняя ошибка сервера». При вызове окна «инструменты разработчика» через F12 выводятся сообщения о некорректном шлюзе.

При этом контейнеры не перезапускаются, в контейнере itm_m_user_service ошибка вида:

```
"Не удалось подключиться к БД postgresql+asyncpg//postgres:*****@host.docker.internal:10265/user_service - в pg_hba.conf нет записи для компьютера "172.15.0.6", пользователя "itmm_user", базы "user_service", SSL выкл."
```

Способ устранения

1. Остановите работу контейнеров:

```
docker-compose down
```

2. Отредактируйте файл `pg_hba.conf`:

- a. перейдите в режим редактирования файла:

```
vi /var/lib/jatoba/1/data/pg_hba.conf
```

- b. найдите строку, вызывающую ошибку:

```
host itmm [имя пользователя БД] 172.15.0.1/24 md5
```

Пример: для пользователя `itmm_user` строка будет иметь вид:

```
host itmm itmm_user 172.15.0.1/24 md5
```

- c. отредактируйте строку, чтобы установить подключение к нескольким БД:

```
host all [имя пользователя БД] 172.15.0.1/24 md5
```

- d. Сохраните файл и выйдите из режима редактирования:

```
:wq
```

3. Перезапустите СУБД для применения настроек:

```
systemctl restart jatoba-*
```

4. Запустите работу контейнеров:

```
docker-compose up -d
```

Причина 3

Модуль управления паролными политиками «securityprofile» не был повторно инициализирован после перезагрузки сервера СУБД или перезапуска службы `jatoba-1`.

Описание проблемы

После перезагрузки сервера СУБД или перезапуска службы `jatoba-1` не удается зайти в веб-интерфейс UDV-ITM-VM с корректными учетными данными. При попытке авторизации в веб-интерфейсе появляется сообщение «Внутренняя ошибка сервера», а в логах СУБД, расположенных в директории `/var/lib/jatoba/1/data/log`, содержится ошибка «FATAL: Extension securityprofile need to be initialized by superuser.».

Способ устранения

Повторно инициализируйте модуль управления паролными политиками пользователей СУБД «securityprofile». Для этого:

1. Войдите в интерактивный терминал для работы с postgresql под пользователем postgres:

```
sudo -u postgres psql -p 10265 -h 127.0.0.1 -U [имя пользователя] [имя базы]
```

Где:

- `-u postgres` — пользователь ОС;
- `-p 10265` — порт, через который будет произведено подключение к базе данных;
- `-h 127.0.0.1` — подключение к хосту 127.0.0.1;
- `-U [имя пользователя]` — подключение от имени указанного пользователя.

2. Инициализируйте модуль «securityprofile» с помощью команды:

```
SELECT SECURITYPROFILE.SYNCHRONIZE();
```

3. Покиньте терминал:

```
\q
```

4. Выйдите из учетной записи пользователя postgres:

```
exit
```

6.7. Изменение имени сервера

Переменная окружения `$HOSTNAME`, даже если она задана, не передается автоматически как переменная окружения в контейнер. Если переменная не передана, то в качестве имени сервера (`hostname`) UDV-ITM-VM будет отображаться имя контейнера в виде случайного набора символов.

Имя сервера присваивается при установке ОС и хранится в файле `/etc/hostname`.

Чтобы имя сервера было присвоено контейнерам, нужно, чтобы выполнялся экспорт переменной окружения `$HOSTNAME`, значение которой берется из файла `/etc/hostname`.

По умолчанию, экспорт переменной `$HOSTNAME` уже настроен, убедиться в этом можно, выполнив команду **export**. В выводе результата команды должна быть переменная `$HOSTNAME` и ее актуальное значение.

Изменение имени сервера (hostname)

1. Перейдите в режим командной строки.
2. Перейдите в директорию с контейнерами:

```
cd /opt/itm-vm
```

3. Остановите контейнеры:

```
docker-compose down
```

4. Измените имя сервера:

```
hostnamectl set-hostname <новое имя сервера>
```

5. Перезагрузите ОС.
6. Запустите контейнеры:

```
docker-compose up -d
```

Экспорт переменной окружения HOSTNAME

Выполняется в случае отсутствия переменной \$HOSTNAME в выводе команды export. Для экспорта переменной:

1. Откройте файл /etc/profile:

```
vi /etc/profile
```

2. В конце открывшегося файла добавьте строку:

```
export $HOSTNAME
```

3. Сохраните файл и выйдите из режима редактирования:

```
:wq
```

6.8. Скрипт для сбора логов

Скрипт `logs_collector.sh` собирает и упаковывает в архив следующие данные:

- логи всех контейнеров, представленных в файле `docker-compose.release.yaml`;
- логи СУБД Jatoba;
- конфигурационные файлы;
- данные о сетях, например, списки сетевых интерфейсов и сетей Docker, таблицу маршрутизации.

Рекомендуется выполнить скрипт перед обращением в техподдержку, чтобы приложить к заявке полученный архив.

Для выполнения скрипта:

1. Перейдите в режим командной строки с правами root.
2. Назначьте скрипту полные права доступа:

```
chmod +x logs_collector.sh
```

3. Запустите скрипт одним из способов:

- a. Способ 1:

Запустите скрипт, указав абсолютный путь к директории с конфигурационными файлами в качестве первого аргумента скрипта:

```
bash logs_collector.sh [ваш путь]
```

- b. Способ 2:

- i. Переместите скрипт в директорию с конфигурационными файлами.
- ii. Запустите скрипт командой:

```
bash logs_collector.sh
```

7. Справочная информация

7.1. Совместимость компонентов решения для UDV-ITM-VM

В таблице указаны поддерживаемые версии компонентов решения для UDV-ITM-VM v. 1.7.0.

Табл. 7-1 Совместимость компонентов решения для UDV-ITM-VM

Компонент решения	Версия ПО	Примечание
Подключаемые серверы мониторинга	<ul style="list-style-type: none"> UDV-ITM-M v. 1.6*; 1.5; 1.4; 1.3 Zabbix v. 5.2; 5.0; 4.0 	При подключении Zabbix v. 4.0 отсутствует сбор данных журналов аудита.
Операционная система	<ul style="list-style-type: none"> РЕД ОС v. 7.3*; 7.2 CentOS v. 8.4 Astra Linux Special Edition (Смоленск) v. 1.6 	
СУБД	<ul style="list-style-type: none"> Jatoba v. 4.5*; 1.14 PostgreSQL v. 14 	
Виртуализация	Docker v. 20	

Где * – рекомендованная версия, обеспечивающая весь доступный функционал и стабильность работы.

7.2. Роли пользователей и доступные им интерфейсы

Табл. 7-2

Роль	Список доступных для роли интерфейсов	Список доступных страниц
Пользователь	Интерфейс авторизации	
	Интерфейс управления	<ul style="list-style-type: none"> Панель информации – доступны просмотр и работа с графиками. Серверы мониторинга – только просмотр списка и карточки сервера. Объекты мониторинга – просмотр списков и карточек. ИТ-услуги – просмотр списка и карточек ИТ-услуг. Проблемы – просмотр списка и карточки со списком событий. Настройки → Правила оповещений – просмотр списка и карточек правил; создание, изменение, включение, выключение и удаление собственных правил оповещений. Окно «Свойства пользователя» при нажатии на кнопку  в нижнем левом углу – просмотр параметров своей учетной записи, изменение пароля. Окно «О системе» при нажатии на кнопку  в нижнем левом углу – просмотр информации
Администратор	Интерфейс авторизации	
	Интерфейс управления	Все разделы со всем функционалом в полном объеме
Техническая	Техническая учетная запись предназначена для доступа смежных систем к данным по API. Не рекомендуется использовать техническую учетную запись для доступа в веб-интерфейс, так как корректная работа при этом не гарантируется.	
Оператор мониторинга	Интерфейс авторизации	
	Интерфейс управления	<ul style="list-style-type: none"> Панель информации – доступны просмотр и работа с графиками. Окно «Свойства пользователя» при нажатии на кнопку  в нижнем левом углу – просмотр параметров своей учетной записи.

Табл. 7-2

Роль	Список доступных для роли интерфейсов	Список доступных страниц
		<ul style="list-style-type: none"> Окно «О системе» при нажатии на кнопку  в нижнем левом углу — просмотр информации. <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Прим.: Для этой роли время пользовательской сессии не ограничено</p> </div>

7.3. Структура директорий UDV-ITM-VM

Список директорий UDV-ITM-VM и их описание представлены в таблице ниже.

Табл. 7-3 Директории UDV-ITM-M

Директория (Файл)	Назначение
opt/itm-vm	Основная рабочая директория UDV-ITM-VM
/opt/itm-vm/env	Директория для хранения файлов конфигурации
/var/lib/jatoba/1/data/	Директория данных СУБД Jatoba по умолчанию
/storage/base	Директория для хранения базы данных на отдельном томе
env/nginx/certs/	Директория для хранения сертификатов

7.4. Рекомендации по использованию антивируса на сервере UDV-ITM-VM

В соответствии политикой антивирусной защиты предприятия (Политика АВЗ) может потребоваться установка программного обеспечения антивирусной защиты (ПО АВЗ).

ПО АВЗ, устанавливаемое на серверы UDV-ITM-VM, UDV-ITM-M, UDV-ITM-RM следует настраивать с учетом следующих рекомендаций:

- Ограничьте использование оперативной памяти во время выполнения задач антивирусной проверки (на минимальном уровне в соответствии с рекомендациями разработчика ПО АВЗ).
- Включите режим низкого приоритета процессов АВЗ по отношению другим программам.
- Отключите участие ПО АВЗ в сервисах типа Security Network.
- Отключите задачи поведенческого анализа системы в постоянном режиме работы.
- Включите другие режимы оптимизации производительности, предусмотренные разработчиком ПО АВЗ (например, исключение повторных проверок проверенных и неизмененных файлов и т.п.).
- Установите расписание для обновления баз и модулей ПО АВЗ в часы наименьшей нагрузки.
- Проводите полное антивирусное сканирование системы под контролем администратора системы с периодичностью в соответствии с Политикой АВЗ предприятия в часы наименьшей нагрузки. Первое полное сканирование следует выполнить сразу после завершения установки системы. При выполнении первого полного сканирования измерьте влияние ПО АВЗ на систему по показателям производительности защищаемой системы. В случае существенного влияния ПО АВЗ на защищаемую систему (более 10% по показателю загрузки процессора и заметном

снижении производительности в интерфейсе), выполняйте полное антивирусное сканирование системы в периоды технического обслуживания.

7.5. Переменные файла .env

Файл `.env` содержит переменные окружения.

Табл. 7-4 Переменные для корректной работы ITM-VM

Название переменной	Описание	Обязательность	Значение по умолчанию (жирным) или пример
COMPOSE_FILE	Имя файла с описанием настроек для контейнеров.	Да	docker-compose.release.yaml
ITMM_LOG_LEVEL	<p>Выбор уровня детализированности логов, может принимать одно из перечисленных значений:</p> <ul style="list-style-type: none"> • ERROR — логирование ошибок. • WARN — логирование ошибок и предупреждений. • INFO — логирование ошибок, предупреждений и сообщений. • DEBUG — логирование всех событий при отладке. • TRACE — логирование всех событий. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p> ОСТОРОЖНО: Не рекомендуется использовать значение TRACE, так как это существенно уменьшает производительность приложения.</p> </div>	Да	INFO

Табл. 7-5 Переменные для настройки Jatoba

Название переменной	Описание	Обязательность	Значение по умолчанию (жирным) или пример
ITMM_DB_HOST	Хост базы данных.	Да	host.docker.internal
ITMM_DB_PORT	Порт для взаимодействия с базой данных.	Да	10265
ITMM_DB_USER	Пользователь базы данных.	Да	itmm_user
ITMM_DB_PASSWORD	<p>Пароль пользователя базы данных.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p> Подсказка: При создании пароля к учетной записи рекомендуется следовать требованиям парольной политики предприятия.</p> </div>	Да	password

Табл. 7-6 Переменные для настройки UDV-ITM-VM

Название переменной	Описание	Обязательность	Значение по умолчанию (жирным) или пример
ITMM_FRONT_SSL_PORT	HTTPS-порт, по которому будет доступен web-интерфейс UDV-ITM-VM.	Нет	443
ITMM_FRONT_PORT	HTTP-порт, по которому будет доступен web-интерфейс UDV-ITM-VM.	Нет	80

Табл. 7-7 Переменные для настройки сетей

Название переменной	Описание	Обязательность	Значение по умолчанию (жирным) или пример
ITMM_NETWORK	Подсеть для работы контейнеров.	Да	172.15.0.0/24
ITMM_NETWORK_GATEWAY	Шлюз подсети для работы контейнеров.	Да	172.15.0.1

7.6. Переменные файла .itmm_password_secret_key

Табл. 7-8 Переменные для настройки UDV-ITM-VM

Название переменной	Описание	Обязательность	Значение по умолчанию (жирным) или пример
ITMM_PASSWORD_SECRET_KEY	<p>Ключ для шифрования и дешифрования паролей, хранящихся в базе данных.</p> <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;"> <p>⚠ Внимание: При повторном изменении или утере значения переменной ITMM_PASSWORD_SECRET_KEY локальные пользователи не смогут войти в веб-интерфейс UDV-ITM-VM, перестанет работать синхронизация с UDV-ITM-M, LDAP и SMTP.</p> </div>	Да	2Fe2e6y9jliJ1wT4ISfVs8imdlAtrll-T

7.7. Механизм интеграции с SIEM

Интеграция с SIEM происходит на уровне администрации UDV-ITM-VM. Для интеграции должно выполняться одно из условий:

- На сервере UDV-ITM-VM происходит действие пользователя, которое ведет к каким-либо изменениям в системе.

или

- UDV-ITM-VM получает проблемы и действия пользователей с сервера UDV-ITM-M в процессе синхронизации.

При интеграции с SIEM UDV-ITM-VM создает для проблемы или действия событие соответствующего типа:

- **AuditLog** — для всех действий пользователя в UDV-ITM-VM и UDV-ITM-M, которые ведут к каким-либо изменениям в системе;
- **Problems** — для всех проблем с UDV-ITM-M.

Подсказка:

Подробнее см. в разделе 7.9 Формат событий для передачи в SIEM (78).

7.8. Список действий пользователя, о которых отправляются события в SIEM

Табл. 7-9 Список действий пользователя в ITM-VM, о которых отправляются события в SIEM

Действие	Значение поля resource	Значение поля action	Примечание
Создание сервера мониторинга	itm_servers	0	
Обновление сервера мониторинга	itm_servers	1	
Удаление сервера мониторинга	itm_servers	2	
Изменение параметров подключения к серверу мониторинга	itm_servers	2	
Успешная авторизация пользователя	login	3	
Не успешная авторизация пользователя	login	7	В поле user – придет ip-адрес клиента. В случае, если клиент неправильно ввел логин/пароль 5 раз подряд, то он его IP-адрес будет заблокирован на 5 минут, в таком случае в поле severity придет большее значение, чем для простой не успешной авторизации.
Создание пользователя	users	0	
Обновление пользователя	users	1	
Блокировка пользователя	users	1	
Разблокировка пользователя	users	1	
Удаление пользователя	users	2	
Создание правила уведомления	notification_rule	0	
Обновление правила уведомления	notification_rule	1	
Удаление правила уведомления	notification_rule	2	
Обновление базовых настроек	base_settings	1	
Обновление настроек периода сбора данных	sync_settings	1	
Обновление длительности сессии	session_settings	1	

7.9. Формат событий для передачи в SIEM

Передача событий в SIEM разрабатывалась для ПО Ankey SIEM. UDV-ITM-VM отправляет событие в SIEM в виде сообщения.

Типы событий:

- Действия пользователей, ведущие к изменению (AuditLog). Подробнее см. в разделе 7.8 Список действий пользователя, о которых отправляются события в SIEM (78).
- Проблемы сервера мониторинга (Problems).

Заголовок сообщения

В заголовке сообщения все поля имеют значение по умолчанию, кроме следующих:

- PRI – это поле для всех событий одинаково, так как не несет важной информации.

- fqdn(hostname) – hostname и IP-адрес UDV-ITM-VM в формате {hostname}-{ip}. Например, 10.51.30.99-develop99.

Время, указанное в заголовке – это время появления события.

Сообщение

Сообщение – список полей и значений в формате JSON. Поля сообщения описаны в таблице ниже.

Табл. 7-10 Поля сообщения

Поле	Описание	Обязательность	Тип данных	Пример
created_at	Timestamp в utc, когда сообщение было создано в UDV-ITM-VM.	ДА	int	"created_at": 1635310595
itm_level	Уровень ИТМ, с которого пришло событие.	ДА	string Enum ITMLevel • "ITM-M" • "ITM-K"	"itm_level": "ITM-K"
user_action	Объект, который содержит информацию о действии пользователя.	НЕТ, но в событии должен обязательно быть передан объект user_action или problem, причем только один из них.	Объект user_action	"user_action": {"user": "itm", "severity": "INFORMATION", "action": "LOGIN", "resource": "LOGIN", "item_id": "1", "item_name": "itm"}}
problem	Объект, который содержит информацию о проблеме.	НЕТ, но в событии должен обязательно быть передан объект user_action или problem, причем только один из них.	Объект problem	"problem": {"itm_k_hostname": "datapkitm-vm-test", "itm_k_ip": "192.168.243.162", "eventid": 27925, "objectid": 18312, "acknowledged": false, "clock": 1627524433, "ns": 639844032, "name": "2-Average-High CPU utilization", "severity": "WARNING", "opdata": "", "hosts": [], "r_eventid": null, "r_clock": null, "r_ns": null, "correlationid": null}}

Прим.:

подробное про типы данных см. в разделе [7.9.1 Типы данных в событиях для передачи в SIEM \(79\)](#).

7.9.1. Типы данных в событиях для передачи в SIEM

В этом разделе рассмотрены типы данных, которые используются в сообщениях событий для отправки в SIEM:

- Объекты:
 - user_action;
 - problem;
 - Host.
- Строки следующих типов:
 - Enum Action;
 - Enum ItmmResource;
 - Enum ZabbixResource;
 - Enum Severity;
 - Enum ITMLevel.

Табл. 7-11 Объект user_action

Поле	Описание	Обязательность	Тип данных	Пример
action	Действие пользователя	ДА	string Enum Action	"action": "LOGIN"
client_ip_address	IP-адрес клиента	ДА	string	"client_ip_address": "192.168.243.162"
item_id	Идентификатор объекта, который изменил пользователь в UDV-ITM-VM или Zabbix	НЕТ	string	"item_id": "1"
item_name	Название объекта, который изменил пользователь в UDV-ITM-VM или Zabbix	НЕТ	string	"item_name": "itm"
itm_k_hostname	Имя хоста UDV-ITM-M, если событие о действии пользователя пришло с UDV-ITM-M (zabbix)	НЕТ для событий с UDV-ITM-VM, ДА для событий с UDV-ITM-M	string	"itm_k_hostname": "datapkitm-vm-test"
itm_k_ip	IP-адрес UDV-ITM-M, если событие о действии пользователя пришло с UDV-ITM-M (zabbix)	НЕТ для событий с UDV-ITM-VM, ДА для событий с UDV-ITM-M	string	"itm_k_ip": "192.168.243.162"
resource	Ресурс, который изменял пользователь	ДА	string Enum ZabbixResource или Enum ItmmResource	"resource": "USERS"
severity	Критичность	ДА	string Enum Severity	"severity": "WARNING"
				 Прим.: Если клиент неправильно ввел логин/пароль 5 раз подряд и его IP-адрес был заблокирован на 5 минут, в поле severity придет значение 4
user	Имя пользователя в UDV-ITM-VM или UDV-ITM-M	ДА	string	"user": "itm"
				 Прим.: Если клиент пытается ввести логин несуществующего пользователя, то в событии в поле user будет указано то значение, которое вводит клиент
details	Текстовое описание событий	ДА	string	"details": "Пользователь не существует"
note	Текстовое описание событий	ДА	string	"note": "Ошибка входа"

Табл. 7-12 Объект problem

Поле	Описание	Обязательность	Тип данных	Примечание	Пример
eventid	Идентификатор события в zabbix.	ДА	int		"eventid": 27925
objectid	Идентификатор триггера.	ДА	int		"objectid": 18312
severity	Критичность.	ДА	string Enum Severity		"severity": "WARNING"
acknowledged	Проблема была помечена пользователем, как подтвержденная.	ДА	bool		"acknowledged": false
clock	Время создания проблемы в timestamp в секундах, наносекунды придут в поле ns.	ДА	int		"clock": 1627524433
ns	Наносекунды времени создания проблемы, основная часть придет в поле clock.	ДА	int		"ns": 639844032

Табл. 7-12 Объект problem

Поле	Описание	Обязательность	Тип данных	Примечание	Пример
name	Название тригера, который сработал.	ДА	string		"name": "2-Average-High CPU utilization"
opdata	Рабочие данные с расширенными макросами.	ДА	string	Содержит пустую строку, если тригер не передает расширенные макросы.	"opdata": "Текущая утилизация: 0.7178 %"
hosts	Список узлов, привязанных к проблеме.	ДА	List[Host]	Проблема может быть привязана сразу к нескольким событиям. Если тригер был удален, то придет пустой список. Обычно приходит список из одного элемента.	"hosts": [{"hostid": "10770", "host": "ADM-PC"}]
r_eventid	Идентификатор события восстановления.	ДА	int	Равен 0, если не было события восстановления.	"r_eventid": 1201
r_clock	Время создания события восстановления в формате timestamp.	ДА	int	Равен 0, если не было события восстановления.	"r_clock": 1627524433
r_ns	Наносекунды времени создания события восстановления.	ДА	int	Равен 0, если не было события восстановления.	"r_ns": 639844032
itm_k_hostname	Имя хоста UDV-ITM-M, если событие о действии пользователя пришло с UDV-ITM-M (zabbix).	НЕТ для событий с UDV-ITM-VM, ДА для событий с UDV-ITM-M	string		"itm_k_hostname": "datapkitm-vm-test"
itm_k_ip	IP-адрес UDV-ITM-M, если событие о действии пользователя пришло с UDV-ITM-M (zabbix).	НЕТ для событий с UDV-ITM-VM, ДА для событий с UDV-ITM-M	string		"itm_k_ip": "192.168.243.162"
action	Действие, совершенное с проблемой. Возможные значения: <ul style="list-style-type: none">"created" — создание проблемы;"updated" — обновление проблемы;"solved" — решение проблемы.	ДА	string		"action": "created"

Табл. 7-13 Объект Host

Поле	Описание	Обязательность	Тип данных	Пример
hostid	Идентификатор узла сети в zabbix.	ДА	string	"hostid": "10770"
host	Имя хоста.	ДА	string	"host": "ADM-PC"

Табл. 7-14 Типы строк

Тип данных	Допустимые значения
Enum Action	<ul style="list-style-type: none"> "ADD" "UPDATE" "DELETE" "LOGIN" "LOGOUT" "ENABLE" "DISABLE"
Enum ItmmResource	<ul style="list-style-type: none"> "login" "itm_servers" "users" "base_settings" "sync_settings"
Enum ZabbixResource	<ul style="list-style-type: none"> USER CONFIGURATION_OF_ZABBIX MEDIA HOST ACTION GRAPH GRAPH_ELEMENT

Табл. 7-14 Типы строк

Тип данных	Допустимые значения
	<ul style="list-style-type: none"> • USER_GROUP • APPLICATION • TRIGGER • HOST_GROUP • ITEM • IMAGE • VALUE_MAP • SERVICE • MAP • SCREEN • WEB_SCENARIO • DISCOVERY_RULE • SLIDE_SHOW • SCRIPT • PROXY • MAINTENANCE • REGULAR_EXPRESSION • MACRO • TEMPLATE • TRIGGER_PROTOTYPE • ICON_MAPPING • DASHBOARD • EVENT_CORRELATION • GRAPH_PROTOTYPE • ITEM_PROTOTYPE • HOST_PROTOTYPE • AUTOREGISTRATION • MODULE
Enum Severity	<ul style="list-style-type: none"> • "NOT_CLASSIFIED" • "INFORMATION" • "WARNING" • "AVERAGE" • "HIGH" • "DISASTER"
Enum ITMLevel	<ul style="list-style-type: none"> • "ITM-M" • "ITM-K"

7.10. Содержимое файла iptables

*filter

#Политики по умолчанию. Сбрасываем все входящие и пересылаемые пакеты. Исходящие разрешаем

:INPUT DROP [0:0]

:FORWARD DROP [0:0]

:OUTPUT ACCEPT [0:0]

#Разрешаем установленные соединения

-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

#Разрешаем все icmp-соединения

-A INPUT -p icmp -j ACCEPT

#Разрешаем все соединения от используемых подсетей docker. Неиспользуемые закомментировать.

#itm-vm

-A INPUT -s 172.15.0.0/24 -j ACCEPT

#itm-k

-A INPUT -s 172.16.239.0/24 -j ACCEPT

```
#itm-a
-A INPUT -s 172.16.240.0/24 -j ACCEPT
#Дефолтная подсеть docker
-A INPUT -s 172.17.0.0/24 -j ACCEPT
#Разрешаем все соединения на loopback-интерфейс (для подключения консолю к jatob'e)
-A INPUT -i lo -j ACCEPT
#Разрешаем соединения на определённые порты с внешнего интерфейса ens32
#ssh
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
#web (для itm-k или itm-vm)
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
#Доп. порты web для инсталляции itm-k + itm-vm
#-A INPUT -p tcp -m tcp --dport 8080 -j ACCEPT
#-A INPUT -p tcp -m tcp --dport 8443 -j ACCEPT
#zabbix сервер (для itm-k или itm-a)
-A INPUT -p tcp -m tcp --dport 10051 -j ACCEPT
#snmp traps (для itm-k или itm-a)
-A INPUT -p udp -m udp --dport 162 -j ACCEPT
#snmp (при необходимости внешнего мониторинга)
#-A INPUT -p udp -m udp --dport 161 -j ACCEPT
#zabbix агент (при необходимости внешнего мониторинга)
#-A INPUT -p tcp -m tcp --dport 10050 -j ACCEPT
#Всё остальное запрещаем (TCP сбрасываем. UDP - порт недоступен)
-A INPUT -p tcp -j REJECT --reject-with tcp-reset
-A INPUT -p udp -j REJECT --reject-with icmp-port-unreachable
-A INPUT -f -j DROP
#По умолчанию закрываем пересылку пакетов. Docker сам добавит нужные правила
-A FORWARD -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -j REJECT --reject-with icmp-host-unreachable
COMMIT
```