Утвержден

РДЦП.10001-02-УД

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

ПРОГРАММНЫЙ КОМПЛЕКС «СРЕДСТВА ВИРТУАЛИЗАЦИИ «БРЕСТ»

Руководство администратора. Часть 1

РДЦП.10001-02 95 01-1

Листов 105

2023

Литера $О_1$

АННОТАЦИЯ

Настоящий документ является руководством администратора программного изделия «Программный комплекс «Средства виртуализации «Брест» (ПК СВ «Брест») РДЦП.10001-02 (далее — ПК СВ) и предназначен для администраторов операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 очередное обновление 1.7, осуществляющих установку и развертывание ПК СВ.

В документе приведено описание порядка развертывания и настройки ПК СВ с учетом особенностей ОС СН, под управлением которой функционирует ПК СВ.

Документ предназначен для использования совместно с эксплуатационными документами согласно ведомости РДЦП.10001-02 20 01 «Программный комплекс «Средства виртуализации «Брест». Ведомость эксплуатационных документов».

Руководство администратора состоит из двух частей:

- РДЦП.10001-02 95 01-1 «Программный комплекс «Средства виртуализации «Брест». Руководство администратора. Часть 1»;
- РДЦП.10001-02 95 01-2 «Программный комплекс «Средства виртуализации «Брест». Руководство администратора. Часть 2».

В первой части руководства описан порядок развертывания и первичной настройки ПК СВ.

Во второй части руководства представлен порядок администрирования ПК СВ с учетом ролевого управления доступа, использования среды виртуализации, обеспечения отказоустойчивости и масштабирования развернутого ПК СВ.

Порядок применения средств защиты информации ПК СВ приведен в документе РДЦП.10001-02 97 01 «Программный комплекс «Средства виртуализации «Брест». Руководство по КСЗ». Порядок применения ПК СВ пользователями приведен в документе РДЦП.10001-02 34 01 «Программный комплекс «Средства виртуализации «Брест». Руководство пользователя».

Дополнительная информация о порядке эксплуатации, а также варианты реализации отдельных решений приведены на официальном сайте `wiki.astralinux.ru/brest`.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Назначение

ПК СВ предназначен для управления средой виртуализации, создание и защита которой обеспечивается средствами операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 очередное обновление 1.7 (далее по тексту — ОС СН).

1.2. Обзор архитектуры

Создание и защита среды виртуализации обеспечиваются встроенными средствами ОС СН, интегрированными с подсистемой безопасности PARSEC, предназначенной для реализации функций ОС СН по защите информации от несанкционированного доступа:

- модулем ядра KVM, который использует аппаратные возможности архитектуры x86-64 по виртуализации процессоров;
- средствами эмуляции аппаратного обеспечения на основе QEMU;
- сервером виртуализации на основе libvirt.

ПК СВ может функционировать в двух режимах:

1) в сервисном режиме все ВМ запускаются от имени непривилегированного пользователя. Идентификация и аутентификация пользователей основываются на использовании механизма PAM, реализованного в ОС СН. При этом аутентификация осуществляется с помощью локальной БД пользователей (файл /etc/passwd) и локальной БД пользовательских паролей (файл /etc/shadow);

2) в дискреционном режиме обеспечивается функционирование защищенной среды виртуализации, в том числе дискреционное и мандатное управление доступом к ВМ. В таком режиме ВМ запускаются от имени доменного пользователя, авторизовавшегося в ПК СВ. Для работы в дискреционном режиме необходимо, чтобы все компьютеры, на которых развернуты программные компоненты ПК СВ, входили в один домен FreeIPA.

Режим функционирования устанавливается на этапе развертывания ПК СВ. После установки и инициализации программных компонент переключение режимов функционирования ПК СВ не предусмотрено.

В ПК СВ входят следующие программные компоненты серверной части:

- сервер виртуализации — для возможности создания виртуальных машин посредством эмуляции аппаратного обеспечения;
- сервер управления — для возможности управления через веб-интерфейс, из командной строки (консольный интерфейс) и с помощью XML-RPC API.

В качестве клиентской части ПК СВ может выступать средство вычислительной

техники, с которого выполняется подключение к серверу управления или виртуальной машине.

В качестве дополнительных программных компонентов (не входят в состав ПК СВ) могут выступать:

- хранилище — система, предназначенная для хранения образов дисков виртуальных машин. Может быть построена на базе следующих технологий хранения:
  - файловой технологии хранения (с использованием локальной файловой системы или кластерной файловой системы, например, ocfs2 или nfs),
  - блочной технологии хранения с использованием LVM,
  - технологии хранения Ceph;
- контроллер домена — служба, обеспечивающая аутентификацию пользователей в рамках единого пространства пользователей (не используется в сервисном режиме работы ПК СВ).

Примечание. В ПК СВ в качестве службы управления единым пространством пользователей используется FreeIPA из состава ОС СН. Если на объекте эксплуатации уже имеется настроенный домен FreeIPA, то разворачивать дополнительный контроллер домена нет необходимости. Все серверы вводятся в существующий домен.

ПК СВ может быть развернут как на группе компьютеров, так и на виртуальных машинах в пределах одного компьютера для тестирования. Для объединения компьютеров, обеспечения выполнения операций управления и поддержки виртуальных сетей используется локальная сеть.

Примечание. Допускается разворачивать несколько программных компонент ПК СВ на одном компьютере.

ВНИМАНИЕ! В связи с особенностью функционирования домена FreeIPA, конфигурация, при которой разворачиваются контроллер домена и служба сервера управления на одном компьютере, недопустима.

1.3. Последовательность развертывания ПК СВ

Развертывание ПК СВ выполняется пользователем, создаваемым при установке ОС СН, который включается по умолчанию в группу `astra-admin`. Пользователям, входящим в названную группу, через механизм `sudo` предоставляются права для выполнения действий по настройке ОС СН, требующих привилегий суперпользователя `root`. Далее по тексту такой пользователь именуется администратором ОС СН.

Для развертывания ПК СВ необходимо выполнить следующие действия:

1) на компьютерах установить ОС СН. Процесс установки ОС СН описан в доку-

менте РУСБ.10015-01 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по установке» (файл `OS-inst-help.pdf`, размещенный на установочном носителе в директории `install-doc`). При этом следует учитывать следующие особенности установки:

- на странице «Выбор программного обеспечения» выбрать для установки пункты «Консольные утилиты» и «Средства удаленного подключения SSH». Пункт «Графический интерфейс Fly» допускается не выбирать для установки;
- на странице «Дополнительные настройки ОС»:
  - если планируется функционирование ПК СВ в дискреционном режиме, выбрать максимальный уровень защищенности «Смоленск» или усиленный уровень защищенности «Воронеж».

    ВНИМАНИЕ! Мандатное управление доступом к экземплярам функционирующих ВМ и файлам-образам ВМ доступно только в ОС СН, функционирующей на максимальном уровне защищенности («Смоленск»);
  - если планируется функционирование ПК СВ в сервисном режиме, выбрать базовый уровень защищенности «Орел»;
- при настройке параметров безопасности на странице «Дополнительные настройки ОС» снять флаг «Запрос пароля для команды `sudo`».

Примечание. Флаг «Запрет автонастройки сети» также должен быть снят.

2) на всех компьютерах установить оперативные обновления БЮЛЛЕТЕНЬ № 2023-0426SE17 (оперативное обновление 1.7.4) и БЮЛЛЕТЕНЬ № 2023-0630SE17MD (оперативное обновление 1.7.4.UU.1) в соответствии с указаниями, представленными в бюллетенях.

Примечание. Допускается сразу устанавливать оперативное обновление 1.7.4.UU.1 (БЮЛЛЕТЕНЬ № 2023-0630SE17MD) без предварительной установки оперативного обновления 1.7.4 (БЮЛЛЕТЕНЬ № 2023-0426SE17);

3) после установки оперативного обновления на всех компьютерах необходимо установить ядро `linux-5.15-generic`;

4) настроить локальную сеть, объединяющую компьютеры. Порядок настройки сети представлен в документе РУСБ.10015-01 95 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1» из комплекта поставки;

5) настроить контроллер домена (не выполняется, если планируется функционирование ПК СВ в сервисном режиме). Порядок настройки контроллера домена представлен в документе РУСБ.10015-01 95 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1»

из комплекта поставки;

Примечание. При установке ОС СН на компьютер, выполняющий функцию контроллера домена, также необходимо выбрать максимальный уровень защищенности «Смоленск» или усиленный уровень защищенности «Воронеж».

6) все компьютеры ввести в домен (не выполняется, если планируется функционирование ПК СВ в сервисном режиме). Порядок ввода компьютера в домен представлен в документе РУСБ.10015-01 95 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1» из комплекта поставки;

7) установить и инициализировать службу сервера управления на необходимое количество компьютеров (см. 2.3);

8) если требуется обеспечить отказоустойчивость системы управления, настроить взаимодействие серверов управления по алгоритму Raft (см. 2.4).

ВНИМАНИЕ! Поддержка технологии Raft реализована только в дискреционном режиме функционирования ПК СВ.

9) настроить подключение к веб-интерфейсу ПК СВ (см. 2.5);

10) установить и инициализировать службу сервера виртуализации на необходимое количество компьютеров (см. 2.6);

11) настроить хранилище (см. раздел 3);

12) настроить виртуальную сеть (см. раздел 4);

13) выполнить дополнительное конфигурирование службы сервера управления (см. раздел 5);

14) при необходимости выполнить дополнительную настройку систем мониторинга и регистрации событий (см. раздел 6);

Примечание. Несколько экземпляров ПК СВ могут быть объединены в единый центр обработки и хранения данных (ЦОХД), называемый «федерация». Подробная информация представлена в разделе 7.

2. УСТАНОВКА ПРОГРАММНЫХ КОМПОНЕНТОВ ПК СВ

ВНИМАНИЕ! Действия по установке и настройке программных компонентов ПК СВ выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности.

2.1. Подготовка к установке программных компонентов ПК СВ

Перед установкой служб сервера управления и/или сервера виртуализации на компьютере необходимо выполнить следующие действия:

1) настроить доступ к репозиториям:
   - основному репозиторию (репозиторию установочного диска, main);
   - оперативному обновлению основного репозитория 1.7.4 (БЮЛЛЕТЕНЬ № 2023-0426SE17);
   - оперативному обновлению основного репозитория 1.7.4.UU.1 (БЮЛЛЕТЕНЬ № 2023-0630SE17MD).

Примечание. Допускается настраивать доступ только к репозиторию установочного диска (main) и репозиторию оперативного обновления 1.7.4.UU.1 основного репозитория (БЮЛЛЕТЕНЬ № 2023-0630SE17MD).

При этом может быть указан сетевой репозиторий или копия репозитория в локальной файловой системе (ФС). Для того чтобы подключить репозиторий ОС СН, следует в файле `/etc/apt/sources.list` добавить строку вида:

```
deb <путь_к_репозиторию> 1.7_x86-64 main contrib non-free
```

Примеры:

1. копия репозитория в локальной файловой системе

```
deb file:/srv/repo/main/ 1.7_x86-64 main contrib non-free
deb file:/srv/repo/0630SE17MD/ 1.7_x86-64 main contrib non-free
```

где `/srv/repo/main/` — каталог, в котором размещены файлы установочного диска ОС СН (основной репозиторий);

`/srv/repo/0630SE17MD/` — каталог, в котором размещены файлы оперативного обновления основного репозитория (БЮЛЛЕТЕНЬ № 2023-0630SE17MD).

2. интернет-репозитории ОС СН:

```
# Репозиторий файлов установочного диска ОС~СН (основной репозиторий)
deb https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-main \
      1.7_x86-64 main contrib non-free
# Репозиторий оперативного обновления основного репозитория
# (БЮЛЛЕТЕНЬ 2023-0630SE17MD)
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.4/uu/1/\
```

```
repository-update/ 1.7_x86-64 main contrib non-free
```

2) настроить доступ к репозиторию ПК СВ, при этом может быть указан сетевой репозиторий или копия репозитория в локальной ФС. Для того чтобы подключить репозиторий ПК СВ, следует в файле `/etc/apt/sources.list` добавить строку вида:

```
deb <путь_к_репозиторию> brest main non-free
```

Пример

```
deb file:/srv/repo/brest/ brest main non-free
```

где `/srv/repo/brest/` — каталог, в котором размещены файлы установочного диска ПК СВ.

3) выполнить повторную синхронизацию файлов описаний пакетов с их источником командой:

```
sudo apt update
```

4) выполнить обновление пакетов командой:

```
sudo astra-update -A -r
```

5) ввести компьютер в домен FreeIPA (не выполняется если планируется функционирование ПК СВ в сервисном режиме). Порядок ввода компьютера в домен представлен в документе РУСБ.10015-01 95 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1» из комплекта поставки.

2.2. Дополнительная настройка контроллера домена

На контроллере домена необходимо настроить используемую политику паролей для обеспечения следующих требований:

- пароль пользователя должен содержать не менее 8 символов при алфавите пароля не менее 70 символов;
- максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки — 4.

Пример

Настройка параметров используемой политики паролей с помощью инструмента командной строки `ipa`:

1) вывести значения параметров используемой политики паролей командой:

```
ipa pwpolicy-show
```

Пример вывода после выполнения команды:

```
Группа: global_policy
Максимальный срок действия (в днях): 90
```

```
Минимальный срок действия (в часах): 1
Размер журнала : 0
Классы символов: 0
Минимальная длина: 8
Максимальное количество ошибок: 6
Интервал сброса ошибок: 60
```

2) задать количество используемых классов символов равное 4 (обеспечивает размер алфавита пароля не менее 70 символов) и максимальное количество ошибок (ввода неправильного пароля) равное 4. Для этого выполнить команду:

```
ipa pwpolicy-mod global_policy --minclasses=4 --maxfail=4
```

Пример вывода после выполнения команды:

```
Группа: global_policy
Максимальный срок действия (в днях): 90
Минимальный срок действия (в часах): 1
Размер журнала : 0
Классы символов: 4
Минимальная длина: 8
Максимальное количество ошибок: 4
Интервал сброса ошибок: 60
```

2.3. Установка и инициализация службы сервера управления

В данном подразделе представлен порядок установки и инициализации службы сервера управления для дискреционного режима работы ПК СВ. Особенности установки и инициализации программных компонентов для сервисного режима работы ПК СВ представлены в 2.8.

Примечание. Процесс инициализации службы сервера управления с помощью плейбука Ansible (из состава ОС СН) описан в 2.7.

Для установки и инициализации службы сервера управления необходимо выполнить следующие действия:

1) на компьютере установить пакет `brestcloud-ipa` командой:

```
sudo apt install brestcloud-ipa
```

В открывшемся окне «ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ» нажать кнопку **[Принять]**.

ВНИМАНИЕ! В процессе установки пакета `brestcloud-ipa` локальному администратору будет присвоен максимальный уровень целостности равный 127;

2) после установки пакета `brestcloud-ipa` перезагрузить компьютер;

3) выполнить инициализацию службы сервера управления командой:

```
sudo brestcloud-configure
```

В процессе инициализации службы сервера управления необходимо:

а) ввести «имя администратора ipa-сервера» (имя администратора доме-

на FreeIPA, заданное во время выполнения действий по установке и настройке контроллера домена) и нажать клавишу **<Enter>**;

б) ввести «`пароль администратора сервера`» (пароль администратора домена FreeIPA, заданный во время выполнения действий по установке и настройке контроллера домена) и нажать клавишу **<Enter>**;

в) задать «`логин для администратора Бреста`» (имя учетной записи администратора ПК СВ — администратора средства виртуализации, который будет включен в группу `brestadmins`);

ВНИМАНИЕ! В ПК СВ зарезервированы и не могут быть использованы следующие имена пользователей:

- `admin`;
- `brestadmin`;
- `oneadmin`;
- `serveradmin`.

Кроме того, в имени пользователя не допускается использование:

- служебных символов;
- букв в верхнем регистре;
- цифрового знака в начале имени пользователя.

г) задать «`пароль для администратора Бреста`» (пароль учетной записи администратора ПК СВ).

ВНИМАНИЕ! Пароль администратора ПК СВ должен удовлетворять следующим требованиям сложности:

- пароль пользователя должен содержать не менее 8 символов при алфавите пароля не менее 70 символов;
- максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки — 4.

Об успешной инициализации службы сервера управления будет свидетельствовать следующая надпись:

```
Настройка прошла успешно!
```

2.4. Алгоритм Raft

2.4.1. Общие сведения

Для обеспечения отказоустойчивости сервера управления в ПК СВ применяется технология Raft. Под термином «сервер управления» подразумевается компьютер, на котором установлена и инициализирована служба сервера управления (см. 2.3).

ВНИМАНИЕ! Поддержка технологии Raft реализована только в дискреционном режиме функционирования ПК СВ.

Алгоритм Raft позволяет объединять несколько экземпляров сервера управления в зону, конфигурацию которой можно менять (добавлять и удалять экземпляры сервера управления), не прерывая работу ПК СВ. Для этой зоны выделяется плавающий (способный при необходимости переходить от одного экземпляра к другому) IP-адрес. Из доступных экземпляров выбирается лидер, которому присваивается ранее выделенный IP-адрес. Лидер обслуживает все входящие запросы. Все изменения на лидере синхронизируются с остальными экземплярами сервера управления в зоне. Если работа лидера прерывается на 100 миллисекунд, то выбирается новый лидер из числа исправных экземпляров. Выделенный для зоны IP-адрес присваивается новому лидеру. Таким образом обеспечивается высокая доступность сервера управления.

Для работы Raft должны быть соблюдены следующие требования:

1) настроен по крайней мере один контроллер домена;

2) настроено нечетное количество (рекомендуется 3 или 5) экземпляров сервера управления (см. 2.3), при этом на всех экземплярах нужно указать одинаковое имя учетной записи администратора ПК СВ;

3) ни на одном из экземпляров не развернута служба `apache2` в режиме «AstraMode off»;

4) выделен IP для настройки плавающего IP-адреса кластера;

5) настроен беспарольный доступ для пользователя `root` между всеми экземплярами сервера управления;

6) настроено общее хранилище для образов дисков и файлов.

2.4.2. Настройка беспарольного доступа для пользователя root

Чтобы настроить беспарольный доступ для пользователя `root` необходимо выполнить следующие действия:

1) на каждом экземпляре сервера управления создать ssh-ключ от имени пользователя `root` командой `sudo ssh-keygen`. Для всех параметров оставлять значения по умолчанию (сразу нажимать клавишу **<Enter>**;

2) на каждом экземпляре сервера управления выполнить обмен ключами командами:

```
KEY=$(sudo cat /root/.ssh/id_rsa.pub)
ssh <local-admin>@<front-1-hostname> \
      "sudo bash -c \"echo $KEY >> /root/.ssh/authorized_keys\""
ssh <local-admin>@<front-2-hostname> \
      "sudo bash -c \"echo $KEY >> /root/.ssh/authorized_keys\""
...
ssh <local-admin>@<front-N-hostname> \
      "sudo bash -c \"echo $KEY >> /root/.ssh/authorized_keys\""
```

где <front-N-hostname> — сетевое имя (hostname) N-го экземпляра сервера управления. Допускается вместо имен указывать IP-адреса;

<local-admin> — имя локального администратора компьютера, заданное при установке ОС СН;

а) при появлении приглашения для ввода вида:

```
Are you sure you want to continue connecting (yes/no)?
```

ввести «yes» и нажать клавишу **<Enter>**;

б) ввести пароль локального администратора компьютера, заданный при установке ОС СН.

ВНИМАНИЕ! В том числе необходимо выполнить обмен ключами «сам на себя»;

3) проверить обмен ключами, для этого:

а) в терминале первого экземпляра сервера управления выполнить вход по ssh на другой экземпляр командой:

```
sudo ssh <front-N-hostname>
```

б) выполнить вход по ssh на первый экземпляр сервера управления командой:

```
sudo ssh <front-1-hostname>
```

где <front-N-hostname> — сетевое имя (hostname) N-го экземпляра сервера управления. Допускается вместо имен указывать IP-адреса.

Настройка считается успешно завершенной, если после выполнения команды был осуществлен вход без пароля;

в) последовательно закрыть сессии ssh командами:

```
exit
exit
```

4) аналогичным образом проверить беспарольный доступ на остальных экземплярах сервера управления.

2.4.3. Настройка зоны объединения экземпляров сервера управления

Для автоматической настройки зоны, объединяющей несколько экземпляров сервера управления, можно воспользоваться скриптом brestcloud-raft-configure, который запускается на одном из серверов управления от имени администратора ОС СН командой:

```
sudo brestcloud-raft-configure
```

В процессе работы мастера настройки объединения экземпляров сервера управления необходимо:

1) указать количество экземпляров сервера управления;

2) указать сетевой интерфейс, на который будет назначен плавающий IP-адрес (обычно указывается интерфейс, на котором настроен статический IP-адрес);

3) указать плавающий IP-адрес;

4) последовательно указать сетевые имена экземпляров сервера управления;

5) указать короткое плавающее имя (эта A-запись будет зафиксирована в DNS FreeIPA).

После завершения работы мастера настройки объединения экземпляров сервера управления необходимо выполнить настройку браузера Mozilla Firefox для подключения к веб-интерфейсу ПК СВ в соответствии с 2.5.

2.4.4. Вывод из зоны объединения экземпляра сервера управления

Для вывода из зоны объединения экземпляра сервера управления необходимо на лидере выполнить команду:

```
sudo onezone server-del <идентификатор_зоны> \
      <идентификатор_удаляемого_экземпляра>
```

2.4.5. Ввод экземпляра сервера управления в зону объединения

Для ввода экземпляра сервера управления в зону объединения необходимо выполнить следующие действия:

1) на компьютере установить и инициализировать службу сервера управления (см. 2.3), при этом нужно указать существующее имя учетной записи администратора ПК СВ;

2) проверить, что сервер управления находится в одиночном режиме командой:

```
sudo onezone show 0
```

Пример вывода после выполнения команды:

```
*ZONE 0 INFORMATION *
ID : 0
NAME : OpenNebula
ZONE TEMPLATE
ENDPOINT="http://localhost:2633/RPC2"
```

3) на новом сервере управления настроить беспарольный доступ для пользователя `root` на все и со всех экземпляров сервера управления;

4) на лидере сделать бекап базы данных командой:

```
sudo onedb backup /tmp/db.backup -f -t postgresql -S localhost \
      -u oneadmin -p "<пароль_БД_лидера>" -d brest
```

где `<пароль_БД_лидера>` соответствует значению параметра `PASSWD`, указанному в файле `/etc/one/one.d/db.conf`;

5) скопировать бекап базы данных на новый сервер управления, для этого на лидере выполнить команду:

```
sudo scp /tmp/db.backup <new-front-hostname>:/tmp
```

где `<new-front-hostname>` — сетевое имя нового сервера управления. Допускается вместо сетевых имен указывать IP-адреса;

6) на новом сервере управления остановить службу сервера управления командой:

```
sudo systemctl stop opennebula
```

7) на новом сервере управления восстановить БД командой:

```
sudo onedb restore -f /tmp/db.backup -t postgresql -S localhost \
     -u oneadmin -p "<пароль_БД_нового_сервера>" -d brest
```

где <пароль_БД_нового_сервера> соответствует значению параметра PASSWD, указанному в файле /etc/one/one.d/db.conf;

8) скопировать директорию «.one», размещенную на лидере, на новый сервер управления. Для этого на лидере выполнить команду:

```
sudo scp -r /var/lib/one/.one/ <new-front-hostname>:/var/lib/one/
```

где <new-front-hostname> — сетевое имя нового сервера управления. Допускается вместо сетевых имен указывать IP-адреса;

9) на лидере добавить новый сервер управления командой:

```
sudo onezone server-add <идентификатор_зоны> \
     --name <полное_доменное_имя_нового_сервера> --rpc \
     http://<полное_доменное_имя_нового_сервера>:2633/RPC2
```

10) с лидера скопировать файл конфигурации raft на новый сервер управления командой:

```
sudo scp /etc/one/one.d/raft.conf <new-front-hostname>:/etc/one/one.d/
```

где <new-front-hostname> — сетевое имя нового сервера управления. Допускается вместо имен указывать IP-адреса;

11) на новом сервере управления в файле /etc/one/one.d/raft.conf скорректировать значение параметра SERVER_ID (идентификатор нового сервера). Идентификатор нового сервера можно получить, выполнив команду:

```
sudo onezone show 0
```

12) на новом сервере управления запустить службу сервера управления и перезапустить службу веб-интерфейса, выполнив последовательно команды:

```
sudo systemctl start opennebula
sudo systemctl restart opennebula-sunstone
```

13) с лидера скопировать сертификаты короткого плавающего имени командой:

```
sudo scp /etc/one/ssl/<короткое_плавающее_имя>.* \
     <new-front-hostname>:/etc/one/ssl/
```

где <new-front-hostname> — сетевое имя нового сервера управления. Допускается вместо сетевого имени указать IP-адрес;

14) с лидера скопировать файлы конфигурации apache на новый сервер управления командами:

```
sudo scp /etc/apache2/sites-available/ipa-one-apache2-float.conf \
     <new-front-hostname>:/etc/apache2/sites-available/
```

```
sudo scp /etc/apache2/apache2.<короткое_плавающее_имя>.keytab \
      <new-front-hostname>:/etc/apache2/
```

где <new-front-hostname> — сетевое имя нового сервера управления. Допускается вместо сетевого имени указать IP-адрес;

15) на новом сервере управления применить файлы конфигурации apache командами:

```
sudo ktutil << EOF
rkt /etc/apache2/apache2.<короткое плавающее имя>.keytab
wkt /etc/apache2/apache2.keytab
q
EOF
sudo a2ensite ipa-one-apache2-float.conf
sudo systemctl restart apache2
```

16) проверить корректность новой конфигурации командой:

```
sudo onezone show 0
```

2.5. Настройка браузера Mozilla Firefox и подключение к веб-интерфейсу ПК СВ

В данном подразделе представлен порядок настройки браузера Mozilla Firefox для подключения к веб-интерфейсу ПК СВ, функционирующему в дискреционном режиме. Особенности настройки браузера Mozilla Firefox для сервисного режима работы ПК СВ представлены в 2.8.

Управление ПК СВ осуществляется с помощью веб-интерфейса по адресу https://<полное_доменное_имя>/,

где <полное_доменное_имя> — полное доменное имя компьютера, на котором развернута служба сервера управления.

Примечание. Подключение к веб-интерфейсу ПК СВ можно осуществить с любого компьютера, имеющего сетевой доступ к серверу управления.

Чтобы настроить браузер Mozilla Firefox для подключения к веб-интерфейсу ПК СВ, необходимо выполнить следующие действия:

1) установить браузер Mozilla Firefox (если при установке ОС СН не был выбран пункт «Средства работы в сети») командой:

```
sudo apt install firefox
```

2) запустить браузер, например, с использованием графического интерфейса: «Пуск — Сеть — Веб-браузер Firefox»;

3) в адресную строку ввести about:config и нажать клавишу **<Enter>**;

4) на открывшейся странице «Расширенные настройки» в поле поиска ввести сле-

дующее слово: `negotiate`;

5) для параметров `network.negotiate-auth.trusted-uris` и `network.negotiate-auth.delegation-uris` установить значение: «`http://, https://`»;

6) добавить в исключение самоподписанный SSL-сертификат, для этого:

а) перейти по адресу: `https://<полное_доменное_имя>:2616`, где `<полное_доменное_имя>` — полное доменное имя компьютера, на котором развернута служба сервера управления,

б) на открывшейся странице с предупреждением нажать кнопку **[Дополнительно]**, а затем — кнопку **[Принять риск и продолжить]**,

в) на открывшейся странице «Open Nebula» вводить ничего не нужно;

7) аналогичным образом добавить в исключение самоподписанный SSL-сертификат для порта 29876 (используется для подключения к удаленному рабочему столу ВМ). Открывшуюся страницу с сообщением об ошибке можно закрыть;

8) перейти к веб-интерфейсу ПК СВ по адресу `https://<полное_доменное_имя>`;

9) на открывшейся странице с предупреждением нажать кнопку **[Дополнительно]**, а затем — кнопку **[Принять риск и продолжить]**.

Примечание. Если подключение к веб-интерфейсу осуществляется не от имени доменного пользователя, то откроется окно авторизации;

10) в открывшемся окне авторизации ввести имя и пароль доменной учетной записи (например, аутентификационные параметры администратора ПК СВ, заданные во время выполнения действий по инициализации службы сервера управления — см. 2.3) и нажать кнопку **[Войти]**;

11) на открывшейся странице «Брест» нажать кнопку **[Войти]**.

2.6. Установка и инициализация службы сервера виртуализации

В данном подразделе представлен порядок установки и инициализации службы сервера виртуализации для дискреционного режима работы ПК СВ.

Особенности установки и инициализации сервисного режима работы ПК СВ представлены в 2.8.

Примечание. Процесс инициализации службы сервера виртуализации с помощью плейбуков Ansible (из состава ОС СН) описан в 2.7.

Для установки и инициализации службы сервера виртуализации необходимо выполнить следующие действия:

1) установить пакет `ipa-libvirt-qemu` командой:

```
sudo apt install ipa-libvirt-qemu
```

В открывшемся окне «ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ» нажать кнопку **[Принять]**.

ВНИМАНИЕ! В процессе установки пакета `ipa-libvirt-qemu` локальному администратору будет присвоен максимальный уровень целостности равный 127;

2) перезагрузить компьютер;

3) выполнить инициализацию службы сервера виртуализации командой:

```
sudo ipa-libvirt-qemu-configure
```

В процессе инициализации сервера виртуализации необходимо:

а) ввести «`имя администратора ipa-сервера`» (имя администратора домена FreeIPA, заданное во время выполнения действий по установке и настройке контроллера домена) и нажать клавишу **<Enter>**;

б) ввести «`пароль администратора ipa-сервера`» (пароль администратора домена FreeIPA, заданный во время выполнения действий по установке и настройке контроллера домена) и нажать клавишу **<Enter>**;

в) ввести «`полное доменное имя фронтальной машины Брест`» (полное доменное имя компьютера, на котором развернута служба сервера управления) и нажать клавишу **<Enter>**.

ВНИМАНИЕ! Если для обеспечения отказоустойчивости службы сервера управления применяется технология Raft, то необходимо указывать полное доменное имя экземпляра сервера управления, выступающего в качестве лидера;

г) ввести «`имя локального администратора фронтальной машины Брест`» (имя локального администратора компьютера, на котором развернут сервер управления) и нажать клавишу **<Enter>**;

д) ввести «`пароль локального администратора фронтальной машины Брест`» (пароль локального администратора компьютера, на котором развернут сервер управления) и нажать клавишу **<Enter>**;

Об успешной инициализации сервера виртуализации будет свидетельствовать следующая надпись:

```
Настройка прошла успешно!
```

4) на всех компьютерах (как выполняющего функцию сервера управления, так и выполняющего функцию сервера виртуализации) в файле `/etc/hosts` добавить строку вида:

```
<IP-адрес_сервера_виртуализации> <имя_сервера_виртуализации>
```

где <IP-адрес_сервера_виртуализации> — IP-адрес нового компьютера, выполняющего функцию сервера виртуализации;

<имя_сервера_виртуализации> — сетевое имя нового компьютера, выполняющего функцию сервера виртуализации;

5) на новом компьютере, выполняющем функцию сервера виртуализации, в файл /etc/hosts добавить IP-адреса и сетевые имена имеющихся серверов виртуализации.

ВНИМАНИЕ! Если для обеспечения отказоустойчивости службы сервера управления применяется технология Raft, то на каждом экземпляре сервера управления необходимо настроить беспарольный доступ для пользователя oneadmin к новому компьютеру, выполняющему функцию сервера виртуализации.

Примечание. На экземпляре сервера управления, выступающего в качестве лидера, беспарольный доступ для пользователя oneadmin настраивается автоматически в ходе инициализации службы сервера виртуализации.

Чтобы настроить беспарольный доступ для пользователя oneadmin, на новом компьютере, выполняющем функцию сервера виртуализации, необходимо выполнить следующие действия:

1) получить ssh-ключ пользователя oneadmin от экземпляра сервера управления, имеющего статус follower. Для этого можно воспользоваться командой:

```
KEY=$(ssh <local-admin>@<front-N-hostname> "sudo -u oneadmin /bin/bash \
      -c \"/bin/cat ~/.ssh/id_rsa.pub\"")
```

где <front-N-hostname> — сетевое имя (hostname) N-го экземпляра сервера управления. Допускается вместо имен указывать IP-адреса;

<local-admin> — имя локального администратора компьютера, выполняющего функцию сервера управления;

2) при появлении приглашения для ввода вида:

```
Are you sure you want to continue connecting (yes/no)?
```

ввести «yes» и нажать клавишу **<Enter>**;

3) ввести пароль локального администратора компьютера, выполняющего функцию сервера управления;

4) сохранить полученный ssh-ключ пользователя oneadmin командой:

```
sudo -u oneadmin bash -c "/bin/echo ${KEY} >> \
      /var/lib/one/.ssh/authorized_keys"
```

5) повторить предыдущие шаги для остальных экземпляров сервера управления, имеющих статус follower.

2.7. Инициализация программных компонентов ПК СВ с помощью плейбуков Ansible

В домене FreeIPA с помощью программного средства Ansible (из состава ОС СН) возможно удаленно инициировать сервер управления и сервер виртуализации.

Примечание. На компьютерах предварительно должны быть установлены пакеты `brestcloud-ipa` (для сервера управления) или `ipa-libvirt-qemu` (для сервера виртуализации).

Для того чтобы инициировать службы сервера управления и сервера виртуализации, необходимо на компьютере, с которого будет производиться настройка, от имени администратора ОС СН с максимальным уровнем целостности выполнить следующие шаги:

1) установить пакет `brest-ansible` командой:

```
sudo apt install brest-ansible -t brest
```

2) скопировать каталог с плейбуками Ansible в домашний каталог, выполнив команду:

```
cp -r /var/lib/brest-ansible $HOME
```

3) скорректировать файл `~/brest-ansible/inventory.ini`;

Пример

```
[all:vars]
### FreeIPA
freeipa_server_fqdn="astral.m.dom"
freeipa_admin="admin"
freeipa_admin_pass="Asdf1234"
### Брест
freeipa_brestadmin="brestchief"
freeipa_brestadmin_pass="Asdf1234"

[brest-front]
brest_front ansible_host='10.10.10.108' ansible_user='toor'
ansible_password='qwertyl23' ansible_become_pass='{{ ansible_password }}'

[brest-nodes]
brest_node_l ansible_host='10.10.10.103' ansible_user='toor'
ansible_password='qwertyl23' ansible_become_pass='{{ ansible_password }}'
```

где `freeipa_server_fqdn` — полное доменное имя контроллера домена;

`freeipa_admin` — имя администратора домена;

`freeipa_admin_pass` — пароль администратора домена;

`freeipa_brestadmin` — имя доменной учетной записи администратора ПК СВ;

ВНИМАНИЕ! В ПК СВ зарезервированы и не могут быть использованы следующие имена пользователей:

- `admin`;
- `brestadmin`;
- `oneadmin`;
- `serveradmin`.

Кроме того, в имени пользователя не допускается использование:

- служебных символов;
- букв в верхнем регистре;
- цифрового знака в начале имени пользователя.

`freeipa_brestadmin_pass` — пароль администратора ПК СВ.

ВНИМАНИЕ! Пароль администратора ПК СВ должен удовлетворять следующим требованиям сложности:

- пароль пользователя должен содержать не менее 8 символов при алфавите пароля не менее 70 символов;
- максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки — 4;

`[brest-front]` — группа для описания серверов управления;

`[brest-nodes]` — группа для описания серверов виртуализации;

`ansible_host` — IP-адрес или полное доменное имя компьютера (выполняющего функции сервера управления или сервера виртуализации);

`ansible_user` — имя локального администратора компьютера (выполняющего функции сервера управления или сервера виртуализации);

`ansible_password` — пароль локального администратора компьютера (выполняющего функции сервера управления или сервера виртуализации);

`ansible_become_pass` — пароль для команды sudo. Если совпадает с паролем администратора или пароль для sudo не требуется, оставить без изменений значение «`{{ ansible_password }}`»;

4) перейти в каталог с плейбуками:

```
cd ~/brest-ansible
```

5) запустить плейбук конфигурирования:

- команда для инициализации сервера управления:

```
ansible-playbook brestcloud_ipa_configure.yml
```

- команда для инициализации сервера виртуализации:

```
ansible-playbook brestcloud_ipa_kvm_nodes.yml
```

Об успешной инициализации программных компонентов будет свидетельствовать следующая надпись:

```
Настройка прошла успешно!
```

2.8. Особенности установки и инициализации сервисного режима работы ПК СВ

Для установки и инициализации сервисного режима работы ПК СВ необходимо выполнить следующие действия:

1) установить и инициировать службу сервера управления на необходимое количество компьютеров, для этого:

а) установить пакет `brestcloud-base` командой:

```
sudo apt install brestcloud-base
```

В открывшемся окне «ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ» нажать кнопку **[Принять]**;

Примечание. Во время установки пакета `brestcloud-base` автоматически будет выполнена инициализация служб сервера управления и сервера виртуализации.

б) назначить пароль локальному пользователю `brestadmin` командой:

```
sudo passwd brestadmin
```

Примечание. Учетная запись пользователя `brestadmin` создается автоматически во время установки пакета `brestcloud-base`.

в) перезагрузить компьютер;

2) установить и инициировать службу сервера виртуализации на необходимое количество компьютеров, для этого:

а) установить пакет `opennebula-node-kvm` командой:

```
sudo apt install opennebula-node-kvm
```

В открывшемся окне «ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ» нажать кнопку **[Принять]**.

б) перезагрузить компьютер, выполняющий функцию сервера виртуализации;

Примечание. На компьютере, выполняющем функцию сервера управления, служба сервера виртуализации устанавливается и инициируется автоматически при установке пакета

`brestcloud-base`.

3) настроить подключение к веб-интерфейсу ПК СВ в браузере Mozilla Firefox на компьютере, выполняющем функцию сервера управления, (или на любой другой машине, имеющей сетевой доступ к этому компьютеру), для этого:

а) установить браузер Mozilla Firefox (если при установке ОС СН не был выбран пункт «Средства работы в сети») командой:

```
sudo apt install firefox
```

б) запустить браузер, например, с использованием графического интерфейса: «Пуск — Сеть — Веб-браузер Firefox»;

в) добавить в исключение самоподписанный ssl сертификат, для этого:

- перейти по адресу: `https://<полное_доменное_имя>:2616`,

  где `<полное_доменное_имя>` — полное доменное имя компьютера, на котором развернута служба сервера управления,

- на открывшейся странице с предупреждением нажать кнопку **[Дополнительно]**, а затем — кнопку **[Принять риск и продолжить]**,

- на открывшейся странице «Open Nebula» вводить ничего не нужно;

г) аналогичным образом добавить в исключение самоподписанный SSL-сертификат для порта 29876 (используется для подключения к удаленному рабочему столу ВМ). Открывшуюся страницу с сообщением об ошибке можно закрыть;

д) перейти к веб-интерфейсу ПК СВ по адресу:

`https://<полное_доменное_имя>`;

е) на открывшейся странице с предупреждением нажать кнопку **[Дополнительно]**, а затем — кнопку **[Принять риск и продолжить]** (дважды);

ж) на открывшейся странице «Брест»:

- в поле «Логин» ввести «`brestadmin`»,

- в поле «Пароль» ввести пароль локального пользователя `brestadmin`, который был задан во время выполнения действий по установке и инициализации службы сервера управления,

- нажать кнопку **[Войти]**;

4) зарегистрировать сервер виртуализации в веб-интерфейсе ПК СВ, для этого:

а) на компьютере, выполняющем функцию сервера управления, в файле `/etc/hosts` добавить строку вида:

```
<IP-адрес_сервера_виртуализации> <имя_сервера_виртуализации>
```

где `<IP-адрес_сервера_виртуализации>` — IP-адрес компьютера, выполняющего функцию сервера виртуализации;

`<имя_сервера_виртуализации>` — сетевое имя компьютера, выполняющего функцию сервера виртуализации;

б) перейти к веб-интерфейсу ПК СВ по адресу:

`https://<полное_доменное_имя>`;

в) в веб-интерфейсе ПК СВ в меню слева выбрать пункт меню «Инфраструктура — Узлы» и на открывшейся странице «Узлы» нажать кнопку **[+]**;

г) на открывшейся странице «Создать узел»:

- в поле «Имя хоста» указать сетевое имя компьютера, выполняющего функцию сервера виртуализации;
- в поле «Логин администратора» ввести имя локального администратора компьютера, выполняющего функцию сервера виртуализации;
- в поле «Пароль администратора» ввести пароль локального администратора компьютера, выполняющего функцию сервера виртуализации;
- нажать кнопку **[Создать]**;

д) на открывшейся странице «Узлы» появится запись о зарегистрированном сервере виртуализации. Необходимо дождаться пока в столбце «Статус» для этого сервера виртуализации значение `Инициализация` не изменится на `ВКЛ`. Для обновления значения статуса можно воспользоваться кнопкой **[Обновить]**.

3. НАСТРОЙКА ХРАНИЛИЩА

Действия по настройке ПК СВ для использования хранилищ выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности. Действия по регистрации хранилищ в ПК СВ выполняются под учетной записью администратора ПК СВ.

3.1. Общие сведения

В ПК СВ используется два основных типа хранилища данных:

- хранилище образов (Images Datastore) — предназначено для хранения всех зарегистрированных образов, которые могут использоваться для создания ВМ. В качестве таких образов могут выступать:
  - образ операционной системы (образ загрузочного диска),
  - CD-ROM — файл в формате ISO, содержащий образ оптического диска. Такие образы предназначены только для чтения,
  - общий блок данных — образ диска, на котором могут быть размещены любые данные, необходимые пользователю;
- системное хранилище (System Datastore) — используется для размещения образов дисков созданных ВМ. Эти образы могут быть полными копиями исходного образа, дельтами или символическими ссылками на исходный образ, в зависимости от используемой технологии хранения. При использовании файловой технологии хранения в системном хранилище размещаются служебные файлы ВМ, создаваемые при формировании снимка состояния этой ВМ.

Кроме того, отдельно выделяют хранилище файлов (Files Datastore), которое используется для хранения обычных файлов. Такими файлами могут быть резервные копии виртуальных машин или контекстные файлы. Например, в хранилище файлов можно поместить определенный init-скрипт и указать его в контекстуализации для ВМ. Этот файл будет размещен на контекстном CD-ROM, доступном в ОС этой ВМ. Таким образом можно настроить выполнение указанного init-скрипта при загрузке ОС виртуальной машины. Процесс настройки хранилища файлов описан в 3.7.

При размещении в хранилище образов каждому образу диска необходимо присвоить атрибут «постоянный» или «непостоянный»:

- «постоянный» (persistent) — диск постоянного хранения данных. Изменения, внесенные в такой образ диска, будут сохранены после удаления ВМ или отсоединения его от ВМ. В любой момент времени может быть только одна ВМ, использующая постоянный образ;
- «непостоянный» (non-persistent) — диск непостоянного хранения данных. Изменения не сохранятся после удаления ВМ или отсоединения этого образа диска от

ВМ. Непостоянные образы могут использоваться несколькими ВМ одновременно, поскольку каждая из них будет работать со своей собственной копией.

Особенности использования «постоянных» и «непостоянных» образов диска, в том числе порядок формирования снимков состояния диска, зависит от используемой технологии хранения. И представлены в разделах, описывающих особенности методов передачи данных между хранилищем образов и системным хранилищем для каждой технологии хранения.

Для построения хранилища данных используются следующие базовые технологии хранения:

- файловая технология хранения (см. 3.3);
- блочная технология хранения с использованием LVM (logical volume manager — менеджер логических томов) — см. 3.4;
- программно-определяемая технология хранения Ceph (см. 3.5);
- Raw Device Mapping — прямое подключение к ВМ существующих блочных устройств, используется только для организации хранилища образов (см. 3.6).

Базовые технологии хранения (параметр `DS_MAD`) и соответствующие им методы передачи данных между хранилищем образов и системным хранилищем (параметр `TM_MAD`) представлены в таблице 1.

Таблица 1

Базовая технология хранения	Значение параметра `DS_MAD`	Значение параметра `TM_MAD`	Описание метода передачи данных (драйвера)
Файловая технология хранения	fs	ssh	Образы копируются с помощью ssh-протокола
		shared	Образы экспортируются в соответствующий каталог системного хранилища на сервере виртуализации
		qcow2	Аналогично shared, но для образов формата `qcow2`. Образы создаются и передаются с помощью команды `qemu-img` с использованием оригинального образа в качестве опорного файла
Блочная технология хранения с использованием LVM	fs	fs_lvm	Образы хранятся как обычные файлы, при создании ВМ они выгружаются в логические тома (LV)
	lvm	lvm_lvm	При загрузке образа диска ВМ в хранилище образов автоматически создается LVM-том, в который записывается загружаемый образ в формате `raw`. При развертывании ВМ в системном хранилище автоматически создается копия LVM-тома из хранилища образов
	lvm_thin	lvm_thin	При загрузке образа диска ВМ в хранилище образов автоматически создается LVM-том, в который пишется загружаемый образ в формате `raw`. При развертывании ВМ в системном хранилище из образа диска автоматически создается тонкий LVM-том в формате `qcow2`

Окончание таблицы 1

Базовая технология хранения	Значение параметра DS_MAD	Значение параметра TM_MAD	Описание метода передачи данных (драйвера)
Ceph	ceph	ceph	Все образы экспортируются в Ceph-пулы
Raw Device Mapping	dev	dev	Прямое подключение к ВМ существующих блочных устройств, используется только для организации хранилища образов

Тип хранилища определяется параметром TYPE, который может принимать следующие значения:

- IMAGE_DS — для хранилища образов;
- SYSTEM_DS — для системного хранилища;
- FILE_DS — для хранилища файлов.

Кроме того, для хранилищ можно дополнительно определить значения параметров, представленных в таблице 2.

Таблица 2

Параметр	Описание
RESTRICTED_DIRS	Перечень каталогов, разделенных символом пробела, в которых запрещается размещать образы. По умолчанию имеет значение «/» — корневой каталог
SAFE_DIRS	Перечень каталогов, разделенных символом пробела, в которых разрешается размещать образы. Используется, если необходимо разместить образ в дочернем каталоге «запрещенного» каталога. По умолчанию имеет значение «/var/tmp»
NO_DECOMPRESS	Если имеет значение «yes», то перед размещением в хранилище файл не будет распакован, если он был предварительно архивирован или сжат.
LIMIT_TRANSFER_BW	Максимальная скорость (байтов в секунду) загрузки файла из URL-источника. Возможно использование суффиксов K, M или G
DATASTORE_CAPACITY_CHECK	Если имеет значение «yes», то перед созданием нового образа будет проведена проверка наличия свободного дискового ресурса
LIMIT_MB	Разрешенный максимальный размер хранилища (Мбайт)
DRIVER	Формат файла образа диска (RAW или Qcow2)
COMPATIBLE_SYS_DS	Используется только для хранилищ образов. Перечень идентификаторов системных хранилищ, разделенных запятой, с которыми совместимо и может быть использовано хранилище образов (например, «0,100»)

По умолчанию после инициализации программных компонентов ПК СВ (см. раз-

дел 2) хранилища настроены на использование локальной файловой системы (каталоги /var/lib/one/datastores/<идентификатор_хранилища>). При этом в качестве метода передачи данных между хранилищем образов и системным хранилищем установлен ssh.

Идентификаторы и наименования хранилищ, созданных по умолчанию во время инициализации программных компонентов ПК СВ, приведены в таблице 3.

Таблица 3

Идентификатор	Наименование	Описание
0	system	системное хранилище
1	default	хранилище образов
2	files	хранилище файлов и ядер

Примечание. Стандартный путь для хранилищ /var/lib/one/datastores можно изменить в конфигурационном файле /etc/one/oned.conf через параметр настройки DATASTORE_LOCATION (см. 5.3).

3.2. Создание хранилищ

Для создания хранилища необходимо выполнить следующую последовательность действий:

1) подготовить систему хранения данных в соответствии с выбранной технологией хранения;

2) выполнить дополнительную настройку ПК СВ для использования выбранной системы хранения;

3) в ПК С создать логическую сущность хранилища (зарегистрировать), указав его имя, тип, базовую технологию хранения и метод передачи данных. После регистрации хранилища будет создан каталог с идентификатором хранилища (по умолчанию /var/lib/one/datastores/<идентификатор_хранилища>). Значение идентификатора хранилищ, создаваемых пользователем, формируется автоматически путем последовательного увеличения значения, начиная с числа 100;

4) на сервере управления и серверах виртуализации смонтировать подготовленную систему хранения данных в каталог хранилища.

Подробнее процесс создания хранилищ, построенных на базе различных технологий хранения, описан в 3.3–3.6

3.3. Хранилища на базе файловой технологии хранения

3.3.1. Особенности файловой технологии хранения

Файловая технология хранения позволяет хранить образы дисков в виде файла. В качестве системы хранения данных (СХД) может выступать локальное хранилище сервера (например, специально выделенное блочное устройство) или внешнее хранилище. В ПК СВ поддерживаются внешние хранилища, построенные на таких технологиях, как NAS и SAN:

- NAS (Network Attached Storage — сетевое хранилище данных) обеспечивает доступ к данным на уровне файлов;
- SAN (Storage Area Network — сеть хранения данных) обеспечивает доступ к данным на уровне блочных устройств.

SAN обеспечивает предоставление блочных устройств посредством сетевых протоколов, таких как Fibre Channel или iSCSI. Для доступа к определенному сетевому блочному устройству используется специализированный адрес этого устройства — LUN (Logical Unit Number — номер логического устройства). Для организации хранения в ПК СВ требуется выделение как минимум двух LUN (один — для хранилища образов, второй — для системного хранилища). Эти LUN должны быть презентованы каждому компьютеру, на котором развернуты службы сервера управления и/или сервера виртуализации.

Файловая технология хранения подразумевает, что подключенные системы хранения данных размечены с использованием одной из файловых систем.

ВНИМАНИЕ! Сетевая файловая система NFS не поддерживает использование меток безопасности. Если планируется использование этой файловой системы при построении хранилища, функционирующего в мандатном контексте, то для ВМ следует установить уровень целостности, назначаемый по умолчанию, равным 0 (см. 3.3.2).

Рекомендуется иметь несколько хранилищ, построенных на базе файловой технологии хранения и с применением различных методов передачи данных, для:

- распределения операций ввода-вывода между серверами хранения данных;
- обеспечения непрерывности обслуживания.

3.3.2. Ограничения, связанные с функционированием файловой системы NFS

В дискреционном режиме функционирования ПК СВ при использовании NFS на каждом сервере виртуализации следует установить уровень целостности, назначаемый по умолчанию для ВМ, равным 0. Для этого необходимо выполнить следующие действия:

1) остановить службу `libvirtd` командой:

```
sudo systemctl stop libvirtd.service
```

2) в конфигурационном файле `/etc/libvirt/libvirtd.conf`, установить значение параметра `ilev_vm` равное 0:

```
ilev_vm = 0
```

3) запустить службу `libvirtd` командой:

```
sudo systemctl start libvirtd.service
```

3.3.3. Особенности использования методов передачи данных

3.3.3.1. Методы передачи Shared и Qcow2

При использовании драйвера `shared` (метода совместной передачи — shared transfer driver) образы дисков ВМ экспортируются в соответствующий каталог системного хранилища на сервере виртуализации. При этом на всех узлах виртуализации должна быть установлена и настроена общая распределенная (или кластерная) файловая система.

Драйвер `qcow2` является разновидностью метода совместной передачи и ориентирован на работу с образами дисков формата Qcow2. Образы создаются и передаются с помощью инструмента командной строки `qemu-img` с использованием исходного образа в качестве опорного файла. Стандартные параметры инструмента командной строки `qemu-img` можно скорректировать, указав необходимые значения в конфигурационном файле `/etc/one/tmrc` (переменная `QCOW2_OPTIONS`).

Схема функционирования представлена на рис. 1.

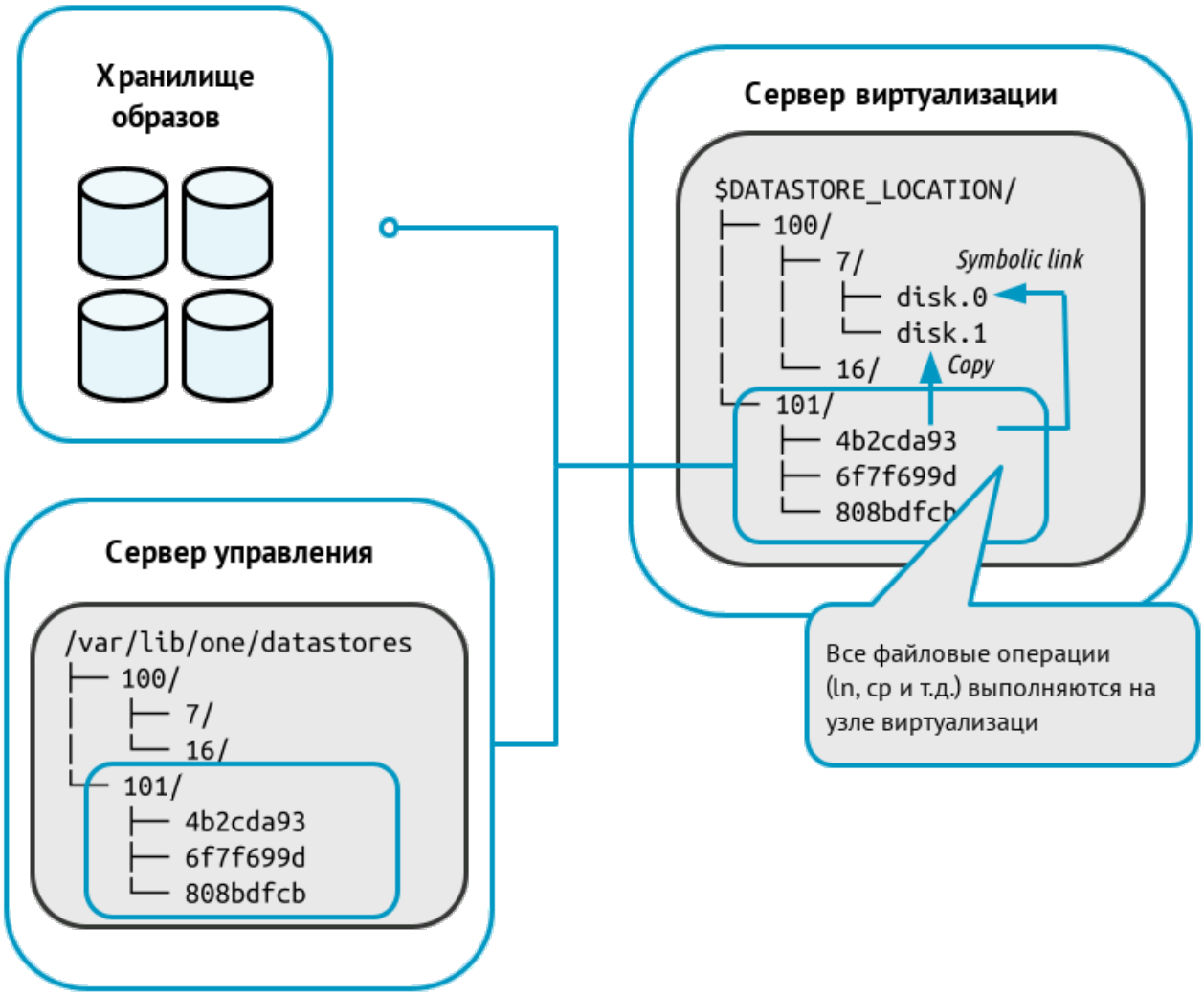

Рис. 1

При развертывании ВМ на сервере виртуализации в каталоге системного хранилища (100) создается рабочий каталог ВМ с наименованием, соответствующем идентификатору этой ВМ (7). Из каталога хранилища образов (101) в рабочий каталог ВМ копируется файл непостоянного образа, указанный в шаблоне ВМ (disk.1) и/или формируется символическая ссылка на файл постоянного образа (disk.0). Цифра после префикса «disk.» соответствует номеру диска, указанному в шаблоне.

При создании снимка состояния работающей ВМ в рабочем каталоге записывается файл состояния этой ВМ с наименованием вида «snap-<номер>.xml»,
где <номер> — порядковый номер снимка, начиная с цифры «0».

При использовании драйвера qcow2 во время создания снимка состояния работающей ВМ также формируется снимок состояния диска этой ВМ. В файл снимка состояния диска записываются изменения в данных, содержащихся на диске (дельта). В качестве наименования файлов снимков состояния диска выступает порядковый номер снимка, начиная с цифры «0». При этом файлы снимков состояния диска размещаются в следующих каталогах:

- для непостоянных образов:

```
/var/lib/one/datastores/<идентификатор_системного_хранилища>/ \
      <идентификатор_ВМ>/disk.<идентификатор_диска>.snap/
```

Пример

Для примера, представленного на рис. 1

```
/var/lib/one/datastores/100/7/disk.1.snap/
```

При этом файл disk.1 будет являться символической ссылкой на файл актуального снимка состояния диска.

- для постоянных образов:

```
/var/lib/one/datastores/<идентификатор_хранилища_образов>/ \
      <идентификатор_образа>.snap/
```

Пример

Для примера, представленного на рис. 1

```
/var/lib/one/datastores/101/6f7f699d.snap/
```

При этом файл disk.0 будет являться символической ссылкой на файл актуального снимка состояния диска.

Кроме того, в рабочем каталоге ВМ будет создана символическая ссылка с наименованием disk.0.snap, которая указывает на каталог со снимками состояний диска (/var/lib/one/datastores/100/6f7f699d.snap/).

При использовании драйвера qcow2 можно отдельно создать снимок состояния диска как работающей, так и выключенной ВМ. Файлы снимков состояния диска будут

размещены в каталогах, описанных выше.

При использовании драйвера `shared` создание снимка состояния диска работающей ВМ не поддерживается. В качестве снимка состояния диска выключенной ВМ создается полная копия файла диска ВМ. Файлы снимков состояния диска размещаются в каталогах, описанных выше.

3.3.3.2. Метод передачи SSH

Метод передачи `ssh` использует локальную файловую систему узлов виртуализации для размещения образов виртуальных машин. Таким образом все файловые операции выполняются локально, но образы дисков всегда необходимо копировать на серверы виртуализации. Данный драйвер не допускает использование динамических перемещений между серверами виртуализации.

Схема функционирования представлена на рис. 2.

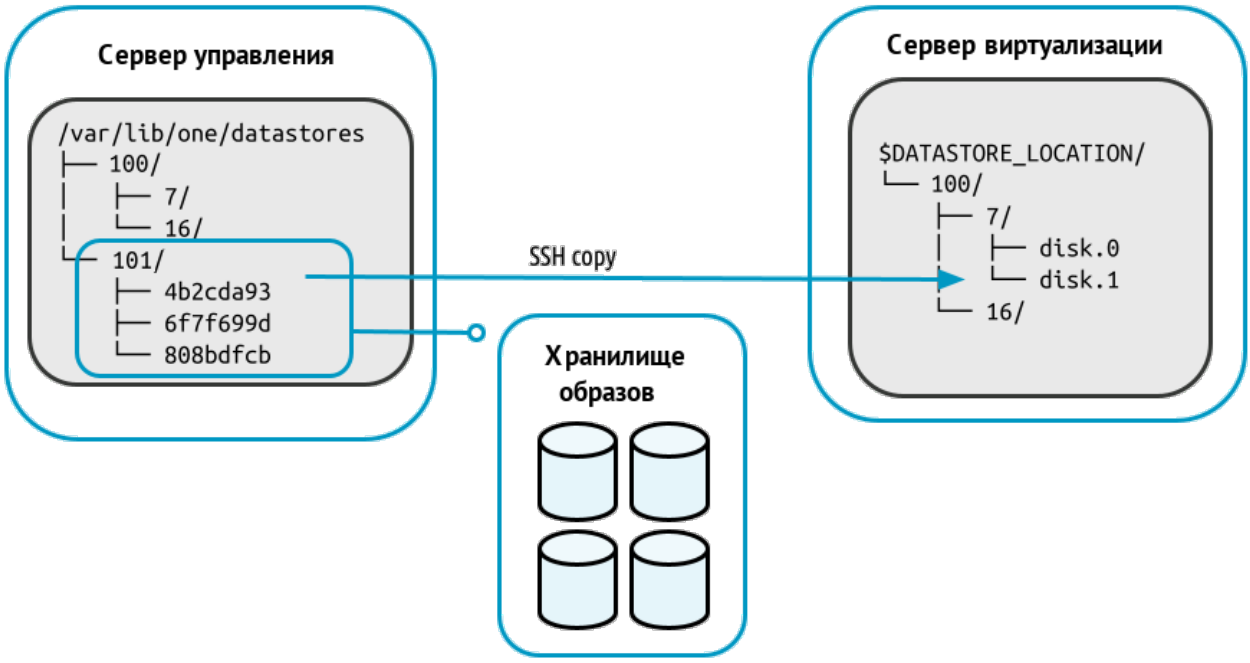

Рис. 2

При развертывании ВМ на сервере виртуализации в каталоге системного хранилища (100) создается рабочий каталог ВМ с наименованием, соответствующем идентификатору этой ВМ (7). Из каталога хранилища образов (101) в рабочий каталог ВМ копируется файл исходного образа, указанного в шаблоне ВМ. Копии исходных образов имеют наименование вида `disk.<номер>`, где `<номер>` — цифра, соответствующая номеру диска в шаблоне.

ВНИМАНИЕ! Необходимо убедиться в том, что все компьютеры, включая сервер управления, могут осуществлять ssh-передачу на любой другой компьютер, включая самих себя. В противном случае перемещения не будут выполняться.

При создании снимка состояния работающей ВМ в рабочем каталоге этой ВМ создается файл состояния ВМ с наименованием вида «snap-<номер>.xml»,

где <номер> — порядковый номер снимка, начиная с цифры «0».

Для выключенной ВМ можно зафиксировать состояние диска этой ВМ (сделать снимок). При этом файлы снимков состояния диска являются полной копией файла диска ВМ и размещаются в каталоге:

```
/var/lib/one/datastores/<идентификатор_системного_хранилища>/ \
      <идентификатор_ВМ>/disk.<номер>.snap/
```

где <номер> — цифра, соответствующая номеру диска в шаблоне.

Пример

Для файла образа диска «disk.1» (см. рис. 2)

```
/var/lib/one/datastores/100/7/disk.1.snap/
```

В качестве наименования файлов снимков состояния диска, размещенных в этом каталоге, выступает порядковый номер снимка, начиная с цифры «0».

Если в качестве исходного выступал постоянный образ, то при уничтожении ВМ все файлы снимков состояний диска будут перемещены в хранилище образов в каталог:

```
/var/lib/one/datastores/<идентификатор_хранилища_образов>/ \
      <идентификатор_образа>.snap/
```

Пример

Для файла образа диска «disk.1» (см. рис. 2) все файлы из каталога

```
/var/lib/one/datastores/100/7/disk.1.snap/
```

будут перемещены в каталог

```
/var/lib/one/datastores/101/4b2cda93.snap/
```

3.3.4. Регистрация хранилищ

ВНИМАНИЕ! Действия по регистрации хранилищ в ПК СВ выполняются под учетной записью администратора ПК СВ.

3.3.4.1. Регистрация системного хранилища

При регистрации нового системного хранилища необходимо указать значения параметров в соответствии с таблицей 4.

Таблица 4

Параметр	Значение
NAME	<Наименование_хранилища>
TYPE	SYSTEM_DS

Окончание таблицы 4

Параметр	Значение
TM_MAD	Одно из следующих значений: shared, qcow2 или ssh. В зависимости от используемого метода передачи данных между хранилищем образов и системным хранилищем

ВНИМАНИЕ! Необходимо использовать одинаковый метод передачи данных (параметр TM_MAD) для системного хранилища и для хранилища образов.

Пример

Регистрация системного хранилища, в котором используется драйвер qcow2:

1) создать файл systemds.txt следующего содержания:

```
NAME = fs_system
TYPE  = SYSTEM_DS
TM_MAD = qcow2
```

2) выполнить команду:

```
onedatastore create systemds.txt
```

Пример вывода после выполнения команды:

```
ID: 100
```

3.3.4.2. Регистрация хранилища образов

При регистрации нового хранилища образов необходимо указать значения параметров в соответствии с таблицей 5.

Таблица 5

Параметр	Значение
NAME	<Наименование_хранилища>
TYPE	IMAGE_DS
DS_MAD	fs
TM_MAD	Одно из следующих значений: shared, qcow2 или ssh. В зависимости от используемого метода передачи данных между хранилищем образов и системным хранилищем
SAFE_DIRS	Перечень каталогов, разделенных символом пробела, в которых разрешается размещать образы. По умолчанию имеет значение «/var/tmp»

ВНИМАНИЕ! Необходимо использовать одинаковый метод передачи данных (параметр TM_MAD) для системного хранилища и для хранилища образов.

Пример

Регистрация хранилища образов, в котором используется драйвер qcow2:

1) создать файл imageds.txt следующего содержания:

```
NAME = fs_images
```

```
TYPE = IMAGE_DS
DS_MAD = fs
TM_MAD = qcow2
```

2) выполнить команду:

```
onedatastore create imageds.txt
```

Пример вывода после выполнения команды:

```
ID: 101
```

3.3.5. Монтирование блочных устройств в каталоги хранилищ

ВНИМАНИЕ! Действия по монтированию блочных устройств выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности.

3.3.5.1. Особенности монтирования блочных устройств в ПК СВ

На сервере виртуализации необходимо создать каталоги для созданных ранее хранилищ на базе файловой технология хранения (по умолчанию /var/lib/one/datastores/<идентификатор_хранилища>). Для этого последовательно выполнить команды:

```
sudo mkdir /var/lib/one/datastores/<идентификатор_системного_хранилища>
sudo mkdir /var/lib/one/datastores/<идентификатор_хранилища_образов>
```

Пример

Создание каталогов хранилищ, с идентификаторами «100» и «101»:

```
sudo mkdir /var/lib/one/datastores/100
sudo mkdir /var/lib/one/datastores/101
```

На сервере виртуализации необходимо смонтировать подготовленную систему хранения данных в каталог хранилища. Если все хранилища одного типа, можно смонтировать весь каталог /var/lib/one/datastores.

На сервере управления необходимо смонтировать только хранилище образов.

Кроме того, необходимо убедиться в том, что на смонтированном дисковом ресурсе достаточно места для хранения образов и дисков виртуальных машин, которые находятся в состоянии «остановлена» и «не размещена».

3.3.5.2. Монтирование сетевых блочных устройств с OCFS2

В общем случае для монтирования блочных устройств, размеченных с использованием кластерной файловой системы OCFS2, необходимо выполнить следующую последовательность действий:

1) определить идентификаторы (UUID) сетевых блочных устройств командой:

```
sudo blkid
```

Пример вывода после выполнения команды:

```
/dev/vda1: UUID="b5fd411a-4c96-491b-bfc0-b4e9e2670e9c" TYPE="ext4" \
```

```
      PARTUUID="50741579-01"
/dev/vda5: UUID="31daa40d-8e07-44cc-b851-d985f2121bb7" TYPE="swap" \
      PARTUUID="50741579-05"
/dev/sdb: UUID="3bd71b84-6463-42ec-8aff-106cafdae2e2" TYPE="ocfs2"
/dev/sda: UUID="41ff6399-368e-4b81-bae4-bdfa4aedd45a" TYPE="ocfs2"
```

где в качестве блочных устройств sda и sdb выступают сетевые блочные устройства;

2) в файл /etc/fstab добавить строки с описанием настроек монтирования сетевых блочных устройств следующего вида:

```
UUID=<идентификатор_блочного_устройства> <точка_монтирования> \
      ocfs2 _netdev,x-systemd.requires=o2cb.service 0 0
```

Пример

При монтировании сетевых блочных устройств, представленных в примере выше, в каталоги каталогов хранилищ с идентификаторами «100» и «101» строки будут иметь следующий вид:

```
UUID=41ff6399-368e-4b81-bae4-bdfa4aedd45a /var/lib/one/datastores/100 \
      ocfs2 _netdev,x-systemd.requires=o2cb.service 0 0
UUID=3bd71b84-6463-42ec-8aff-106cafdae2e2 /var/lib/one/datastores/101 \
      ocfs2 _netdev,x-systemd.requires=o2cb.service 0 0
```

3) выполнить монтирование командой:

```
sudo mount -a
```

Результатом выполнения команды должен быть пустой вывод без ошибок;

4) перезагрузить компьютер.

ВНИМАНИЕ! После добавления записи об автоматическом монтировании в файле /etc/fstab и перезагрузки компьютера, необходимо назначить на каталог этого хранилища владельца oneadmin. В противном случае при перезагрузке компьютера владелец меняется на root и использование хранилища будет не доступно.

Для того чтобы назначить на каталог хранилища владельца oneadmin необходимо выполнить команду:

```
sudo chown oneadmin:oneadmin /var/lib/one/datastores/<идентификатор_хранилища>
```

3.3.5.3. Монтирование сетевых ресурсов с NFS

ВНИМАНИЕ! Для каждого сетевого каталога, предоставляемого сетевым хранилищем, предварительно необходимо назначить владельцем пользователя с UID равным 9869 (соответствует пользователю oneadmin). А в качестве группы-владельца — группу с GID равным 9869 (соответствует группе oneadmin).

Для монтирования сетевых ресурсов, предоставляемого NFS-сервером, на каждом компьютере (выполняющем функцию сервера управления или сервера виртуализации) необходимо выполнить следующую последовательность действий:

1) установить службу клиента NFS командой:

```
sudo apt install nfs-common
```

2) просмотреть перечень доступных сетевых ресурсов командой:

```
sudo showmount -e <IP-адрес_сервера_NAS>
```

Пример

Вывод списка сетевых ресурсов, предоставляемых NFS-сервером с IP-адресом 192.168.1.10

```
sudo showmount -e 192.168.1.10
```

Пример вывода после успешного выполнения команды:

```
Export list for 192.168.1.10:
/mnt/nfs-images node?,front
/mnt/nfs-system node?,front
```

где «/mnt/nfs-system» и «<mntnfs-images» — сетевые ресурсы, предоставляемые NFS-сервером,

запись «node?,front» означеает, что доступ предоставлен компьютерам, сетевое имя которых начинается с последовательности символов «node» (далее следует один любой символ), а также компьютеру с сетевым именем «front»;

3) настроить автоматическое монтирование сетевых ресурсов в точки монтирования. Для этого в файл /etc/fstab добавить строки с описанием настроек монтирования сетевых ресурсов:

```
<IP-адрес_сервера_NFS>:<сетевой_ресурс> <точка_монтирования> \
      nfs _netdev,timeo=14,intr 0 0
```

В качестве точек монтирования необходимо указать каталоги созданных хранилищ.

Пример

Для сетевых ресурсов, представленных выше, строки будут иметь следующий вид:

```
192.168.1.10:/mnt/nfs-images /var/lib/one/datastores/101 \
      nfs _netdev,timeo=14,intr 0 0
192.168.1.10:/mnt/nfs-system /var/lib/one/datastores/100 \
      nfs _netdev,timeo=14,intr 0 0
```

4) выполнить монтирование командой:

```
sudo mount -a
```

Результатом выполнения команды должен быть пустой вывод без ошибок;

3.4. Хранилища LVM

Блочная технология хранения с использованием LVM обеспечивает возможность использования LVM-томов вместо обычных файлов образов в системном хранилище. При

этом нет необходимости в организации файловой системы.

Примечание. В ПК СВ для хранилища LVM не требуется настройка кластерного управления логическими томами (CLVM) в кластере. Драйверы обновляют метаданные LVM каждый раз, когда образ требуется на другом сервере виртуализации.

В ПК СВ поддерживаются внешние хранилища, построенные базе технологии SAN (Storage Area Network — сеть хранения данных), которая обеспечивает доступ к данным на уровне блочных устройств.

При настройке внешнего хранилища необходимо руководствоваться инструкциями производителя оборудования.

3.4.1. Настройка хранилищ с драйвером FS_LVM

3.4.1.1. Особенности использования драйвера FS_LVM

Исходные образы хранятся как обычные файлы, по умолчанию установлен следующий путь размещения в хранилище образов:
`/var/lib/one/datastores/<идентификатор_хранилища>`.

При создании ВМ образы дисков выгружаются в логические тома (LV). Виртуальные машины запускаются из LV на сервере виртуализации (см. рис. 3).

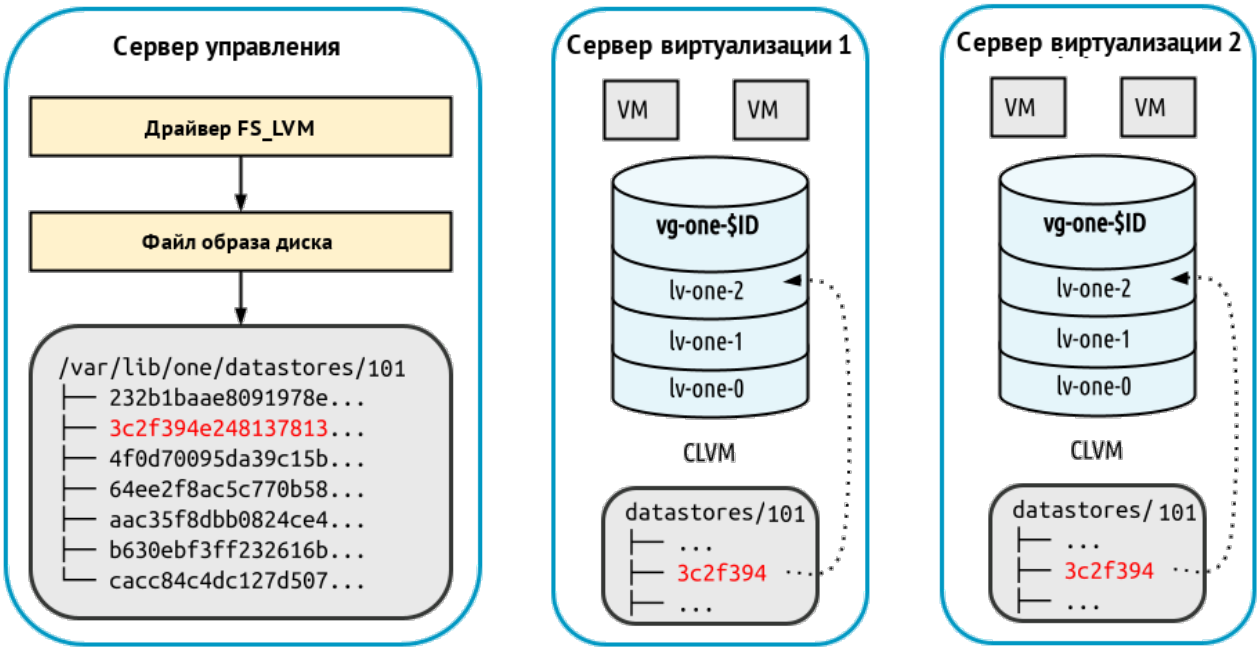

Рис. 3

Драйвер хранилища FS_LVM рекомендуется применять при наличии СХД высшего класса (high-end). В этом случае LUN можно экспортировать на все серверы виртуализации.

Для хранения образов дисков в виде файлов используется распределенная файловая система, такая как, например, NFS. При этом необходимо выполнить настройку каталогов хранилищ образов и точек монтирования так же, как и при использовании метода

совместной передачи (shared) в хранилище, построенном на базе файловой технологии хранения (см. 3.3). Рекомендуется сначала выполнить развертывание хранилища образов, построенного на базе файловой технологии хранения. А затем, убедившись в его корректной работе, заменить его на хранилище LVM.

ВНИМАНИЕ! Сетевая файловая система NFS не поддерживает использование меток безопасности. Если планируется использование этой файловой системы при построении хранилища, функционирующего в мандатном контексте, то для ВМ следует установить уровень целостности, назначаемый по умолчанию, равным 0 (см. 3.3.2).

3.4.1.2. Параметры хранилищ

При регистрации нового системного хранилища необходимо задать значения параметров в соответствии с таблицей 6

Таблица 6

Параметр	Значение
NAME	<Наименование_хранилища>
TYPE	SYSTEM_DS
TM_MAD	fs_lvm
BRIDGE_LIST	Список серверов виртуализации, разделенных пробелами, через которые осуществляется доступ к системе хранения данных (SAN). Не используется, если сервер управления имеет прямой доступ к системе хранения данных.

При регистрации нового хранилища образов необходимо задать значения параметров в соответствии с таблицей 7

Таблица 7

Параметр	Значение
NAME	<Наименование_хранилища>
TYPE	IMAGE_DS
DS_MAD	fs
TM_MAD	fs_lvm
DISK_TYPE	BLOCK
SAFE_DIRS	Перечень каталогов, разделенных символом пробела, в которых разрешается размещать образы. По умолчанию имеет значение «/var/tmp»
BRIDGE_LIST	Список серверов виртуализации, разделенных пробелами, через которые осуществляется доступ к системе хранения данных (SAN). Не используется, если сервер управления имеет прямой доступ к системе хранения данных.

3.4.1.3. Регистрация хранилищ

ВНИМАНИЕ! Действия по регистрации хранилищ в ПК СВ выполняются под учетной записью администратора ПК СВ.

Пример

Регистрация системного хранилища с использованием конфигурационного файла:

1) создать файл `systemds.txt` со следующим содержанием:

```
NAME = fs_lvm-system
TYPE  = SYSTEM_DS
TM_MAD  = fs_lvm
BRIDGE_LIST = "NODE1 NODE2"
```

2) выполнить команду:

```
onedatastore create systemds.txt
```

Пример вывода после выполнения команды:

```
ID: 100
```

Пример

Регистрация хранилища образов с использованием конфигурационного файла:

1) создать файл `imageds.txt` со следующим содержанием:

```
NAME  = fs_lvm-images
TYPE = IMAGE_DS
DS_MAD = fs
TM_MAD = fs_lvm
DISK_TYPE = "BLOCK"
SAFE_DIRS = "/var/tmp /tmp"
BRIDGE_LIST = "NODE1 NODE2"
```

2) выполнить команду:

```
onedatastore create imageds.txt
```

Пример вывода после выполнения команды:

```
ID: 101
```

3.4.1.4. Настройка ПК СВ для использования хранилищ

ВНИМАНИЕ! Действия по настройке ПК СВ для использования хранилищ выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности.

Необходимо обеспечить совместный доступ всех серверов виртуализации к каталогу хранилища образов. Для этого используется распределенная файловая система, такая как, например, NFS.

Кроме того, все серверы виртуализации должны иметь доступ к одним и тем же сетевым блочным устройствам.

Примечание. К серверу управления сетевые блочные устройства можно не

подключать. Сервер управления может получить доступ к системному хранилищу через узлы виртуализации (параметр `BRIDGE_LIST`).

На основе совместно используемых сетевых блочных устройств для каждого хранилища должна быть создана группа томов с именем вида:

`vg-one-<идентификатор_системного_хранилища>`

Примечание. Формирование групп томов достаточно выполнить только на одном из узлов виртуализации.

Пример

Формирование группы томов (состоит из одного тома `/dev/sda`) для системного хранилища с идентификатором «100»:

1) инициализировать блочное устройство для работы с LVM:

```
sudo pvcreate /dev/sda
```

Пример вывода после успешного выполнения команды:

```
Physical volume "/dev/sda" successfully created.
```

2) создать группу томов:

```
sudo vgcreate vg-one-100 /dev/sda
```

Пример вывода после успешного выполнения команды:

```
Volume group "vg-one-100" successfully created
```

3.4.2. Настройка хранилищ с драйвером LVM_LVM

3.4.2.1. Особенности использования драйвера LVM_LVM

Драйвер LVM_LVM позволяет организовать и хранилище образов, и системное хранилище в LVM. При этом, в отличие от использования драйвера FS_LVM, нет необходимости создавать общую сетевую файловую систему для образов.

При использовании драйвера хранилища LVM_LVM необходимо наличие на всех серверах виртуализации общих блочных устройств хранения данных.

Особенности функционирования драйвера хранилища LVM_LVM:

- предварительно необходимо создать отдельные группы LVM-томов для хранилища образов и системного хранилища;
- при загрузке образа диска ВМ в хранилище образов автоматически создается LVM-том, в который записывается загружаемый образ в формате `raw`;
- при развертывании ВМ в системном хранилище автоматически создается копия LVM-тома из хранилища образов.

Примечание. При копировании LVM-тома в системное хранилище происходит посекторное клонирование, что может занять длительное время. Учитывая эту особенность рекомендуется в хранилище образов создавать исходный образа диска ВМ минимально необходимого объема. А при развертывании ВМ увеличивать образ

диска до необходимого размера. Порядок увеличения объема дисков, выделенных для ВМ, представлен в документе РУСБ.10015-01 93 01 «Операционная система специального назначения «Astra Linux Special Edition». Руководство пользователя» из комплекта поставки.

ВНИМАНИЕ! В драйвере хранилища LVM_LVM не поддерживается создание снимков состояний образа диска и создание «тонких» дисков. Учитывая эту особенность для резервного копирования и восстановления ВМ рекомендуется использовать специализированные средства резервного копирования.

3.4.2.2. Параметры хранилищ

При регистрации нового системного хранилища необходимо задать значения параметров в соответствии с таблицей 8

Таблица 8

Параметр	Значение
NAME	<Наименование_хранилища>
TYPE	SYSTEM_DS
TM_MAD	lvm_lvm
DRIVER	raw

При регистрации нового хранилища образов необходимо задать значения параметров в соответствии с таблицей 9

Таблица 9

Параметр	Значение
NAME	<Наименование_хранилища>
TYPE	IMAGE_DS
DS_MAD	lvm
TM_MAD	lvm_lvm
DISK_TYPE	BLOCK
DRIVER	raw

3.4.2.3. Регистрация хранилищ

ВНИМАНИЕ! Действия по регистрации хранилищ в ПК СВ выполняются под учетной записью администратора ПК СВ.

Пример

Регистрация системного хранилища с использованием конфигурационного файла.

```
cat > system-ds.conf <<EOT
NAME="lvm-lvm-system"
```

```
TYPE="SYSTEM_DS"
TM_MAD="lvm_lvm"
DRIVER="raw"
EOT
onedatastore create system-ds.conf
```

Пример вывода после выполнения команды:

```
ID: 100
```

Пример

Регистрация хранилища образов с использованием конфигурационного файла.

```
cat > images-ds.conf <<EOT
NAME="lvm-lvm-images"
TYPE="IMAGE_DS"
DS_MAD="lvm"
TM_MAD="lvm_lvm"
DISK_TYPE="BLOCK"
DRIVER="raw"
EOT
onedatastore create images-ds.conf
```

Пример вывода после выполнения команды:

```
ID: 101
```

3.4.2.4. Настройка ПК СВ для использования хранилищ

ВНИМАНИЕ! Действия по настройке ПК СВ для использования хранилищ выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности.

ВНИМАНИЕ! Все компьютеры (выполняющие функцию сервера управления или сервера виртуализации) должны иметь доступ к одним и тем же сетевым блочным устройствам.

На одном из компьютеров (выполняющем функцию сервера управления или сервера виртуализации) необходимо создать отдельные группы LVM-томов для хранилища образов и системного хранилища.

Пример

Формирование группы томов (состоит из одного тома `/dev/sda`) для системного хранилища с идентификатором «100» и группы томов (состоит из одного тома `/dev/sdb`) для хранилища образов с идентификатором «101»:

1) инициализировать блочные устройства для работы с LVM:

```
sudo pvcreate /dev/sda
sudo pvcreate /dev/sdb
```

Пример вывода после успешного выполнения команд:

```
Physical volume "/dev/sda" successfully created.
```

2) создать группу томов:

```
sudo vgcreate vg-one-100 /dev/sda
sudo vgcreate vg-one-101 /dev/sdb
```

Пример вывода после успешного выполнения команд:

```
Volume group "vg-one-100" successfully created
```

3.4.3. Настройка хранилищ с драйвером LVM_THIN

3.4.3.1. Особенности использования драйвера LVM_THIN

Драйвер LVM_LVM позволяет организовать и хранилище образов, и системное хранилище в LVM. В отличие от драйвера LVM_LVM, при создании в системном хранилище нового логического тома LVM, его фактический размер соответствует объему имеющихся данных на исходном LVM-томе, и увеличивается по мере записи данных в этот том. Такой логический том LVM называют «тонким» LVM-томом. При этом для каждого сервера виртуализации в общем системном хранилище организуется индивидуальный ресурс — пул «тонких» LVM-томов.

ВНИМАНИЕ! «Тонкие» LVM-тома не могут совместно использоваться несколькими серверами виртуализации. В связи с этим, при использовании драйвера хранилища LVM_THIN не поддерживается миграция ВМ.

Особенности функционирования драйвера хранилища LVM_THIN:

- предварительно необходимо создать отдельные группы LVM-томов для хранилища образов;
- на каждом сервере виртуализации предварительно необходимо создать отдельную группу LVM-томов с привязкой к общему системному хранилищу;
- на каждом сервере виртуализации предварительно необходимо создать отдельный пул «тонких» LVM-томов;
- при загрузке образа диска в хранилище образов автоматически создается LVM-том, в который пишется загружаемый образ в формате `RAW`;
- при развертывании ВМ в системном хранилище из образа диска автоматически создается «тонкий» LVM-том в формате `QCOW2`.

3.4.3.2. Параметры хранилищ

При регистрации нового системного хранилища необходимо задать значения параметров в соответствии с таблицей 10

Таблица 10

Параметр	Значение
`NAME`	<Наименование_хранилища>

Окончание таблицы 10

Параметр	Значение
TYPE	SYSTEM_DS
TM_MAD	lvm_thin

При регистрации нового хранилища образов необходимо задать значения параметров в соответствии с таблицей 11

Таблица 11

Параметр	Значение
NAME	<Наименование_хранилища>
TYPE	IMAGE_DS
DS_MAD	lvm_thin
TM_MAD	lvm_thin
DISK_TYPE	BLOCK
DRIVER	raw

3.4.3.3. Регистрация хранилищ

ВНИМАНИЕ! Действия по регистрации хранилищ в ПК СВ выполняются под учетной записью администратора ПК СВ.

Примеры:

1. Регистрация системного хранилища с использованием конфигурационного файла:

```
cat > system-ds.conf <<EOT
NAME="lvm-thin-system"
TYPE="SYSTEM_DS"
TM_MAD="lvm_thin"
EOT
onedatastore create system-ds.conf
```

2. Регистрация хранилища образов с использованием конфигурационного файла:

```
cat > images-ds.conf <<EOT
NAME="lvm-thin-images"
TYPE="IMAGE_DS"
DS_MAD="lvm_thin"
TM_MAD="lvm_thin"
DISK_TYPE="BLOCK"
DRIVER="qcow2"
EOT
onedatastore create images-ds.conf
```

3.4.3.4. Настройка ПК СВ для использования хранилища образов

ВНИМАНИЕ! Действия по настройке ПК СВ для использования хранилищ выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности.

ВНИМАНИЕ! Все компьютеры (выполняющие функцию сервера управления или сервера виртуализации) должны иметь доступ к одним и тем же сетевым блочным устройствам.

На одном из компьютеров (выполняющем функцию сервера управления или сервера виртуализации) необходимо создать отдельную группу томов для хранилища образов, которая должна иметь наименование вида:

```
vg-one-<идентификатор_хранилища_образов>
```

Пример

Формирование группы томов (состоит из одного тома `/dev/sdc`) для хранилища образов с идентификатором «101»:

1) инициализировать блочное устройство для работы с LVM:

```
sudo pvcreate /dev/sdc
```

Пример вывода после успешного выполнения команды:

```
Physical volume "/dev/sdc" successfully created.
```

2) создать группу томов:

```
sudo vgcreate vg-one-101 /dev/sdc
```

Пример вывода после успешного выполнения команды:

```
Volume group "vg-one-101" successfully created
```

3.4.3.5. Настройка ПК СВ для использования системного хранилища

ВНИМАНИЕ! Действия по настройке ПК СВ для использования хранилищ выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности.

ВНИМАНИЕ! Все компьютеры (выполняющие функцию сервера управления или сервера виртуализации) должны иметь доступ к одним и тем же сетевым блочным устройствам.

На каждом сервере виртуализации необходимо выполнить следующие действия:

1) создать отдельную группу томов с именем вида:

```
vg-one-<идентификатор_системного_хранилища>-<имя_узла_виртуализации>
```

2) создать пул логических томов с именем вида:

```
vg-one-<идентификатор_системного_хранилища>-<имя_узла_виртуализации>/
      onethinpool
```

Пример

Настройка сервера виртуализации для использования системного хранилища с идентификатором «100»:

1) инициализировать блочное устройство для работы с LVM:

```
sudo pvcreate /dev/sda
```

Пример вывода после успешного выполнения команды:

```
Physical volume "/dev/sda" successfully created.
```

2) создать группу томов (в представленном примере группа состоит из одного тома):

```
sudo vgcreate vg-one-100-node1 /dev/sda
```

Пример вывода после успешного выполнения команды:

```
Volume group "vg-one-100-node1" successfully created
```

3) создать пул логических томов:

```
sudo lvcreate -T -L <размер>G vg-one-100-node1/onethinpool
```

где <размер> — размер пула логических томов в ГБ. Должен быть не больше размера локального блочного устройства (в представленном примере — /dev/sda).

Пример вывода после успешного выполнения команды:

```
Thin pool volume with chunk size 64,00 KiB can address at most 15,81 TiB of /
   data.
Logical volume "onethinpool" created.
```

При создании «тонкого» LVM-тома дополнительно к исходному LVM-тому создаются два скрытых тома под метаданные (информация о выделенных блоках). При исчерпании свободного места в пуле логических томов возникает потеря метаданных на скрытых томах. Это приводит к повреждению файловых систем на «тонких» томах, что проявляется как ошибка записи.

Потерянные метаданные возможно восстановить с помощью команды:

```
lvconvert --repair <наименование_группы>/<наименование_пула>
```

Драйвер LVM_THIN поддерживает автоматическое увеличение размера пула «тонких» логических томов при его заполнении. Для этого необходимо всегда оставлять свободное место в группе LVM-томов. Автоматическое увеличение размера томов по умолчанию выключено. Для того чтобы его включить, необходимо в конфигурационном файле /etc/lvm/lvm.conf скорректировать значения следующих параметров:

- «thin_pool_autoextend_threshold» — пороговое значение (в процентах от заданного размера «тонкого» LVM-тома) при котором автоматически будет увеличен размер этого тома. По умолчанию имеет значение «100», в этом случае автоматическое расширение тома не производится;
- «thin_pool_autoextend_percent» — объем дискового пространства (в процентах от заданного размера «тонкого» LVM-тома) на которое автоматически будет увеличен размер этого тома. По умолчанию имеет значение «20».

Пример

Автоматическое увеличение размера томов на 20%, когда объем дискового про-

странства, выделенный для «тонкого» LVM-тома заполнится на 70%.

```
thin_pool_autoextend_threshold = 70
thin_pool_autoextend_percent = 20
```

Например, был создан «тонкий» LVM-том размером 1 ГБ. Когда объем данных, размещенных на этом томе, достигнет размера 700 МБ, «тонкий» LVM-том будет автоматически расширен до 1,2 ГБ. После того как объем данных, размещенных на этом томе, достигнет размера 840 МБ, «тонкий» LVM-том будет автоматически расширен до 1,44 ГБ.

3.5. Хранилища Ceph

3.5.1. Особенности использования хранилища Ceph

Ceph — распределенная объектная сеть хранения, обеспечивающая файловый и блочный интерфейсы доступа. Она может использоваться на системах, состоящих как из нескольких серверов, так и из тысяч узлов, образовывающих кластер. Встроенные механизмы продублированной репликации данных обеспечивают высокую отказоустойчивость системы. При добавлении или удалении новых узлов кластера массив данных автоматически балансируется с учетом внесенных изменений. В Ceph обработка данных и метаданных разделена на различные группы узлов в кластере.

Образы и диски виртуальных машин хранятся в одном Ceph-пуле. Каждый образ в пуле имеет наименование вида «one-<идентификатор_образа>». Виртуальные машины будут использовать RBD-тома для своих дисков если образы помечены как «постоянный», в противном случае создаются новые снимки состояний образа с наименованием вида: one-<идентификатор_образа>-<идентификатор_ВМ>-<идентификатор_диска_ВМ>.

Допускается совместная работа хранилища образов, построенного на базе Ceph, и системного хранилища, построенного на базе файловой технологии хранения. При этом в качестве драйвера передачи данных между хранилищем образов и системным хранилищем используется метод совместной передачи (shared) — см. 3.3. В этом случае энергозависимые диски и диски подкачки создаются в виде обычных файлов в системном хранилище. А также кроме Ceph-кластера необходимо выполнить установку и настройку распределенной файловой системы, например, NFS.

ВНИМАНИЕ! Для использования хранилища Ceph необходимо, чтобы серверы виртуализации являлись Ceph-клиентами работающего Ceph-кластера.

3.5.2. Дополнительная настройка Ceph-кластера для использования в ПК СВ

ВНИМАНИЕ! Действия по настройке Ceph-кластера выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности.

Предварительно должен быть развернут Ceph-кластер. Порядок развертывания Ceph представлен в документе РУСБ.10015-01 95 01-1 «Операционная система специаль-

ного назначения «Astra Linux Special Edition». Руководство администратора. Часть 1» из комплекта поставки.

Дополнительно на административной рабочей станции от имени учетной записи администратора Ceph-кластера необходимо выполнить следующие настройки:

1) распределить конфигурационные файлы на узлы Ceph-кластера, например, с использованием инструмента командной строки `ceph-deploy`:

```
ceph-deploy --username <администратор_Ceph-кластера> config push \
      <узел_кластера-1> <узел_кластера-2> ... <узел_кластера-N>
```

2) создать пул для хранилищ, в качестве наименование пула указав `one`:

```
sudo ceph osd pool create one <количество_групп>
```

где `<количество_групп>` — количество групп в пуле, которое определяется по следующей формуле:

((Общее количество OSD * 100) / Уровень репликации) с округлением до ближайшей степени 2 в сторону увеличения.

Пример

В случае для 3 узлов ceph:

```
(3 OSD * 100) / 3 = 100 (округляется до 128)
```

Таким образом, количество групп в пуле должно быть равным 128.

3) вывести перечень пулов командой:

```
sudo ceph osd lspools
```

Пример вывода после выполнения команды:

```
1 device_health_metrics
2 one
```

4) настроить пул `one` на работу с RBD:

```
sudo ceph osd pool application enable one rbd
```

Пример вывода после успешного выполнения команды:

```
enabled application 'rbd' on pool 'one'
```

5) создать Ceph-пользователя, который будет иметь доступ к пулу хранилищ. Данный пользователь будет также использоваться службой libvirt для доступа к образам дисков. Пример создания пользователя с именем `libvirt`:

```
sudo ceph auth get-or-create client.libvirt \
      mon 'profile rbd' osd 'profile rbd pool=one'
```

Пример вывода после успешного выполнения команды:

```
[client.libvirt]
      key = AQAS8hJkyaa9FxAAnRqI2RTD1nqmOcJLxPRWNg==
```

Примечание. Префикс `client` означает, что команда выполняется в отношении логической сущности «пользователь».

6) получить копию ключа Ceph-пользователя для ее дальнейшей передачи на серверы виртуализации. Пример команды для пользователя с именем libvirt:

```
sudo ceph auth get-key client.libvirt | tee client.libvirt.key
```

Пример вывода после успешного выполнения команды:

```
AQAS8hJkyaa9FxAAnRqI2RTD1nqmOcJLxPRWNg==
```

7) экспортировать набор ключей Ceph-пользователя в файл ceph.client.libvirt.keyring командой:

```
sudo ceph auth get client.libvirt -o ceph.client.libvirt.keyring
```

Пример вывода после успешного выполнения команды:

```
exported keyring for client.libvirt
```

3.5.3. Настройка сервера управления для работы с Ceph-кластером

Для сервера управления не требуется специальная настройка. Сервер управления будет выполнять доступ к Ceph-кластеру через серверы виртуализации, настроенные на использование Ceph-кластера (параметр BRIDGE_LIST, который указывается при регистрации хранилища, — см. 3.5.5.1).

3.5.4. Настройка сервера виртуализации для работы с Ceph-кластером

ВНИМАНИЕ! Действия по настройке сервера виртуализации выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности.

Для настройки сервера виртуализации на использование Ceph-кластера необходимо на административной рабочей станции от имени учетной записи администратора Ceph-кластера выполнить следующие действия:

1) установить клиентские инструментальные средства на всех компьютерах, выполняющих функцию сервера виртуализации. Пример команды:

```
ceph-deploy --username <администратор_Ceph-кластера> \
      install --cli <сервер_виртуализации>
```

где <сервер_виртуализации> — сетевое имя или IP-адрес компьютера, на котором развернута служба сервера виртуализации;

2) скопировать ключ Ceph-пользователя, созданного ранее (см. 3.5.2), на все серверы виртуализации в каталог /var/lib/one/. Пример команды:

```
scp client.libvirt.key <администратор>@<сервер_виртуализации>:/tmp
ssh <администратор>@<сервер_виртуализации> \
      "sudo mv /tmp/client.libvirt.key /var/lib/one"
```

где <администратор> — учетная запись локального администратора компьютера, на котором развернута служба сервера виртуализации;

3) скопировать набор ключей Ceph-пользователя, созданного ранее (см. 3.5.2), на все серверы виртуализации в каталог /etc/ceph/. Пример команды:

```
scp ceph.client.libvirt.keyring <администратор>@<сервер_виртуализации>:/tmp
```

```
ssh <администратор>@<сервер_виртуализации> \
      "sudo mv /tmp/ceph.client.libvirt.keyring /etc/ceph"
```

4) сгенерировать универсальный уникальный идентификатор (UUID) и сохранить его в файл `secret.xml`:

```
UUID=$(uuidgen)
cat > secret.xml <<EOF
<secret ephemeral='no' private='no'>
  <uuid>$UUID</uuid>
  <usage type='ceph'>
        <name>client.libvirt secret</name>
  </usage>
</secret>
EOF
```

5) скопировать файл `secret.xml` на все серверы виртуализации в каталог `/var/lib/one`. Пример команды:

```
scp secret.xml <администратор>@<сервер_виртуализации>:/tmp
ssh <администратор>@<сервер_виртуализации> \
      "sudo mv /tmp/secret.xml /var/lib/one"
```

Примечание. Значение универсального уникального идентификатора (UUID) в дальнейшем потребуется для настройки хранилищ;

6) последовательно на всех серверах виртуализации задать закрытый ключ службы libvirt, используя файл `secret.xml`. Для этого на административной рабочей станции необходимо выполнить команду:

```
ssh <администратор>@<сервер_виртуализации> \
      "sudo virsh -c qemu:///system secret-define /var/lib/one/secret.xml"
```

Пример вывода после успешного выполнения команды:

```
Секрет c84b8321-6d49-4b43-8d1b-0efc1686edc4 создан
```

7) последовательно на всех серверах виртуализации связать закрытый ключ службы libvirt и ключ Ceph-пользователя. Для этого на административной рабочей станции необходимо выполнить команду:

```
ssh <администратор>@<сервер_виртуализации> \
      "sudo virsh -c qemu:///system secret-set-value \
      --secret $UUID --file /var/lib/one/client.libvirt.key"
```

Пример вывода после успешного выполнения команды:

```
Значение установлено
```

8) последовательно на всех серверах виртуализации убедиться в том, что Ceph-пользователь (с наименованием `libvirt`) имеет корректные настройки. Для этого на административной рабочей станции необходимо выполнить команду:

```
ssh <администратор>@<сервер_виртуализации> "sudo rbd ls -p one --id libvirt"
```

результатом выполнения команды должен быть пустой вывод без ошибок.

Примечание. После настройки сервера виртуализации необходимо убедиться в том, что на узлах Ceph-кластера выделено достаточно места для хранения вспомогательных файлов виртуальных машин, таких как context-диски, файлы развертывания и файлы контрольной точки.

3.5.5. Регистрация хранилищ

ВНИМАНИЕ! Действия по регистрации хранилищ в ПК СВ выполняются под учетной записью администратора ПК СВ.

3.5.5.1. Параметры хранилищ

Для использования Ceph-кластера в качестве системы хранения необходимо зарегистрировать системное хранилище и хранилище образов. При регистрации этих хранилищ указываются значения общих параметров конфигурации, приведенные в таблице 12, а также дополнительные параметры для каждого типа хранилища, представленные в таблицах 13 и 14.

Таблица 12

Параметр	Описание	Обязательный
NAME	Имя хранилища	ДА
POOL_NAME	Имя Ceph-пула	ДА
CEPH_USER	Имя Ceph-пользователя, используемое службами libvirt и rbd	ДА
CEPH_KEY	Полный путь файла закрытого ключа для пользователя, если не используется стандартный файл (/var/lib/one/client.libvirt.key)	НЕТ
CEPH_CONF	Нестандартный конфигурационный файл Ceph, если необходим	НЕТ
RBD_FORMAT	По умолчанию будет использоваться RBD-формат «2»	НЕТ
BRIDGE_LIST	Разделенный пробелами список серверов виртуализации, настроенных на использование Ceph-кластера	ДА
CEPH_HOST	Разделенный пробелами список узлов Ceph-кластера, с инициированной службой монитора (MON)	ДА
CEPH_SECRET	Универсальный уникальный идентификатор (UUID) закрытого ключа libvirt	ДА

При регистрации системного хранилища дополнительно к параметрам, приведенным в таблице 12, устанавливаются параметры, указанные в таблице 13.

Таблица 13

Параметр	Значение	Обязательный
TYPE	SYSTEM_DS	ДА
TM_MAD	ceph	ДА

При регистрации хранилища образов дополнительно к параметрам, приведенным в

таблице 12, устанавливаются параметры, указанные в таблице 14.

Таблица 14

Параметр	Значение	Обязательный
TYPE	IMAGE_DS	ДА
DS_MAD	ceph	ДА
TM_MAD	ceph	ДА
DISK_TYPE	RBD	ДА
STAGING_DIR	Каталог на компьютере, выполняющем функцию моста для сервера управления, (параметр BRIDGE_LIST) в котором будет временно размещен образ перед передачей его в хранилище. По умолчанию имеет значение /var/tmp	НЕТ

В конфигурационном файле /var/lib/one/remotes/datastore/ceph/ceph.conf могут быть установлены значения по умолчанию для следующих параметров хранилища Ceph:

- POOL_NAME;
- STAGING_DIR;
- RBD_FORMAT.

3.5.5.2. Регистрация системного хранилища

Пример

Создание хранилища с использованием конфигурационного файла:

1) создать файл systemds.txt со следующим содержанием:

```
NAME = ceph_system
TYPE = SYSTEM_DS
TM_MAD = ceph

POOL_NAME = one
CEPH_USER = libvirt
BRIDGE_LIST = "<сервер_виртуализации-1> <сервер_виртуализации-2> ... \
      <сервер_виртуализации-N>"
CEPH_HOST = "<узел_кластера-1> <узел_кластера-2> ... <узел_кластера-N>"
CEPH_SECRET = "<значение_UUID>"
```

2) выполнить команду:

```
onedatastore create systemds.txt
```

Пример вывода после выполнения команды:

```
ID: 100
```

Примечание. Также Ceph может работать с системным хранилищем, построенном на базе файловой технологии хранения с использованием метода совместной передачи

(shared) — см. 3.3. В этом случае энергозависимые диски и диски подкачки создаются в виде обычных файлов в системном хранилище. Кроме Ceph-кластера необходимо выполнить установку и настройку распределенной файловой системы, например, NFS.

Примечание. Особенности настройки NFS представлены в 3.3.2.

3.5.5.3. Регистрация хранилища образов

Пример

Создание хранилища с использованием конфигурационного файла:

1) создать файл `imageds.txt` со следующим содержанием:

```
NAME = "ceph_images"
TYPE = IMAGE_DS
DS_MAD = ceph
TM_MAD = ceph
DISK_TYPE = RBD

POOL_NAME = one
CEPH_USER = libvirt
BRIDGE_LIST = "<сервер_виртуализации-1> <сервер_виртуализации-2> ... \
      <сервер_виртуализации-N>"
CEPH_HOST = "<узел_кластера-1> <узел_кластера-2> ... <узел_кластера-N>"
CEPH_SECRET = "<значение_UUID>"
```

2) выполнить команду:

```
onedatastore create imageds.txt
```

Пример вывода после выполнения команды:

```
ID: 101
```

3.6. Хранилище образов Raw Device Mapping

3.6.1. Общие сведения

Технология Raw Device Mapping (RDM) обеспечивает возможность использования блочных устройств вместо обычных файлов образов диска в хранилище образов. В качестве диска ВМ выступает блочное устройство, подключенное к серверу виртуализации. При этом блочное устройство может быть, как локальным, так и сетевым (презентованным внешним хранилищем).

ВНИМАНИЕ! Образы, создаваемые в данном хранилище, должны быть помечены как «постоянный». В противном случае, появляется возможность использования данного устройства более чем одной ВМ, что может привести к возникновению проблем и повреждению данных.

Хранилище образов RDM используется совместно с системным хранилищем, построенным на базе файловой технологии хранения (см. 3.3).

При использовании технологии RDM обеспечивается быстрое развертывание ВМ, так как нет необходимости передачи файла образа диска из хранилища образов в системное хранилище. В хранилище образов только записывается регистрационная информация о блочном устройстве, используемом для развертывания ВМ.

3.6.2. Настройки ПК СВ для использования хранилища

Дополнительная настройка не требуется.

3.6.3. Регистрация хранилища

ВНИМАНИЕ! Действия по регистрации хранилищ в ПК СВ выполняются под учетной записью администратора ПК СВ.

Для регистрации хранилища необходимо указать значения параметров, указанные в таблице 15.

Таблица 15

Параметр	Значение
NAME	<наименование_хранилища>
TYPE	IMAGE_DS
DS_MAD	dev
TM_MAD	dev
DISK_TYPE	BLOCK

Пример

Создание хранилища с использованием конфигурационного файла:

1) создать файл `imageds.txt` со следующим содержанием:

```
NAME = rdm_datastore
TYPE = "IMAGE_DS"
DS_MAD = "dev"
TM_MAD = "dev"
DISK_TYPE = "BLOCK"
```

2) выполнить команду:

```
onedatastore create imageds.txt
```

Пример вывода после выполнения команды:

```
ID: 101
```

3.6.4. Регистрация блочного устройства в хранилище

ВНИМАНИЕ! Действия по регистрации блочного устройства в хранилище выполняются под учетной записью администратора ПК СВ.

В хранилище можно добавлять новые образы с указанием пути. При использовании инструмента командной строки нельзя применять сокращенные параметры, т.к. вначале

проверяется, существует ли файл и устройство на сервере управления.

Пример

Регистрация в хранилище `101` образа, которому соответствует диск `/dev/sdb`:

1) создать `image.tmpl` со следующим содержанием:

```
NAME=scsi_device
PATH=/dev/sdb
PERSISTENT=YES
```

2) выполнить команду:

```
oneimage create image.tmpl -d 101
```

3.7. Хранилище файлов

Хранилище файлов используется для хранения обычных файлов. Такими файлами могут быть резервные копии виртуальных машин или контекстные файлы. Например, в хранилище файлов можно поместить определенный init-скрипт и указать его в контекстуализации для ВМ. Этот файл будет размещен на контекстном CD-ROM, доступном в ОС этой ВМ. Таким образом можно настроить выполнение указанного init-скрипта при загрузке ОС виртуальной машины.

ВНИМАНИЕ! Если в ПК СВ для обеспечения отказоустойчивости сервера управления применяется технология Raft, хранилище файлов должно быть построено на базе файловой технологии хранения. При этом должна использоваться общая (распределенная) файловая система.

При использовании хранилища файлов применяются стандартные инструменты командной строки, например, `cp`, `ln`, `mv`, `tar`, `mkfs`, которые установлены в системе по умолчанию.

3.7.1. Настройка сервера управления

Большинство критериев настройки, используемых для хранилищ образов, применяются к хранилищу файлов.

3.7.2. Настройка сервера виртуализации

Используемый драйвер SSH для хранилища файлов не требует особой настройки. Достаточно убедиться в том, что на дисковом ресурсе, соответствующем этому хранилищу, достаточно места для размещения файлов ВМ на сервере управления и на серверах виртуализации.

3.7.3. Регистрация хранилища

ВНИМАНИЕ! Действия по регистрации хранилищ в ПК СВ выполняются под учетной записью администратора ПК СВ.

Для регистрации хранилища необходимо указать значения параметров, указанные в

таблице 16.

Таблица 16

Параметр	Значение
NAME	<Наименование_хранилища>
TYPE	FILE_DS
DS_MAD	fs
TM_MAD	ssh
SAFE_DIRS	Перечень каталогов, разделенных символом пробела, в которых разрешается размещать образы. По умолчанию имеет значение «/var/tmp»

Пример

Создание хранилища файлов с использованием конфигурационного файла:

1) создать файл files_ds.txt со следующим содержанием:

```
NAME = files
TYPE = FILE_DS
DS_MAD = fs
TM_MAD = ssh
SAFE_DIRS = /var/tmp/files
```

2) выполнить команду:

```
onedatastore create files_ds.txt
```

Пример вывода после выполнения команды:

```
ID: 103
```

Значения параметров DS и TM MAD можно впоследствии изменить командой onedatastore update. Подробные значения параметров хранилища можно просмотреть с помощью команды onedatastore show.

4. НАСТРОЙКА СЕТИ

Действия по настройке ПК СВ для использования виртуальных сетей выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности. Действия по созданию виртуальных сетей в ПК СВ выполняются под учетной записью администратора ПК СВ.

4.1. Общие сведения

При запуске новой ВМ сетевые интерфейсы этой ВМ, определяемые параметром NIC в настройках ВМ, подключаются к физическим устройствам сервера виртуализации в соответствии с настройками виртуальной сети. Это позволяет ВМ иметь доступ к публичным и частным сетям.

ПК СВ поддерживает четыре сетевых режима:

1) режим «Сетевой мост» — ВМ напрямую соединяется с существующим мостом на сервере виртуализации. Данный режим может быть настроен на использование групп безопасности и изоляции сети;

2) режим VLAN — для каждой сети создается мост, к которому подключается VLAN-тегированный сетевой интерфейс (VLAN-тегирование стандарта IEEE802.1Q);

3) режим VXLAN — для каждой сети создается мост, к которому подключается VXLAN-тегированный сетевой интерфейс. Используемый протокол VXLAN основан на UDP-инкапсуляции и групповой адресации IP;

4) режим Open vSwitch — аналогичен режиму VLAN, но использует программный коммутатор Open vSwitch (OVS) вместо сетевого моста. Группы безопасности данным режимом не поддерживаются.

Сетевой стек сети может объединяться с внешним диспетчером IP-адресов (IPAM). Для этого необходимо добавить связующий элемент.

4.2. Параметры сети

При создании виртуальной сети необходимо указать значения следующих параметров:

1) параметры физической сети, которая будет ее поддерживать, включая сетевой драйвер;

2) доступное адресное пространство. Адресами, связанными с виртуальной сетью, могут быть IPv4, IPv6, IPv4-IPv6 с двумя стеками или Ethernet;

3) необязательные параметры контекстуализации (сетевые настройки виртуальных машин, которые могут включать, например, маски сети, сервера DNS или шлюзы).

Примечание. Подробное описание параметров виртуальной сети представлено

в документе РДЦП.10001-02 95 01-2 «Программный комплекс «Средства виртуализации «Брест» (ПК СВ «Брест»). Руководство администратора. Часть 2».

4.3. Режим «Сетевой мост»

В данном сетевом режиме трафик ВМ напрямую передается через существующий сетевой мост на серверах виртуализации. При этом устанавливается один из режимов фильтрации трафика, применяемой в сети:

- режим «сетевой мост без фильтрации» (Bridged);
- режим «сетевой мост с группами безопасности» (Bridged with Security Groups, далее по тексту — Security Group) — устанавливаются правила iptables для внедрения правил групп безопасности;
- режим «сетевой мост с правилами ebtables» (Bridged with ebtables isolation, далее по тексту — Ebtables VLAN) — тоже что и для режима Security Group, но с дополнительными правилами ebtables для изоляции (L2) всех виртуальных сетей.

4.3.1. Особенности и ограничения

При фильтрации трафика необходимо учитывать следующее:

- в режимах Bridged и Security Group можно добавлять тегированные сетевые интерфейсы для обеспечения сетевой изоляции. Данный режим является рекомендуемой стратегией развертывания в работающих системах (не тестовых);
- режим Ebtables VLAN предназначен для небольших сред без соответствующей аппаратной поддержки для внедрения сетей VLANS. Данный режим ограничен сетями с длиной префикса 24 бита (/24) и IP-адреса не могут перекрываться в виртуальных сетях. Рекомендуется только для целей тестирования.

ВНИМАНИЕ! По умолчанию при удалении ВМ на сервере виртуализации также будет удален существующий сетевой мост, если он больше не используется ни одной ВМ.

Для того чтобы незадействованный сетевой мост не удалялся, необходимо в конфигурационном файле `/var/lib/one/remotes/etc/vnm/OpenNebulaNetwork.conf` установить следующее значение параметра `keep_empty_bridge`:

```
:keep_empty_bridge: true
```

4.3.2. Настройка сервера виртуализации

ВНИМАНИЕ! Действия по настройке ПК СВ для использования виртуальных сетей выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности.

Для настройки данного сетевого режима необходимо выполнение следующих требований:

- на серверы виртуализации необходимо установить пакет `bridge-utils`;

- если планируется использовать режим фильтрации Ebtables VLAN, на серверы виртуализации необходимо установить пакет `ebtables`, который по умолчанию обеспечивает изоляцию сети.

На сервере виртуализации необходимо создать сетевой мост для каждой сети, в которой будут работать виртуальные машины. При этом следует использовать одно имя сети на всех серверах виртуализации.

Пример

Содержание файла `/etc/network/interfaces` с настройками сетевого моста

```
auto eth0
iface eth0 inet manual
auto br0
iface br0 inet static
bridge_ports eth0
address 172.16.1.20
netmask 255.255.255.0
gateway 172.16.1.1
```

4.3.3. Настройка сервера управления

Режим Сетевой мост не требует специальных настроек.

4.3.4. Создание сети

ВНИМАНИЕ! Действия по созданию виртуальных сетей в ПК СВ выполняются под учетной записью администратора ПК СВ.

Для создания сети необходимо указать параметры физической сети, приведенные в таблице 17.

Таблица 17

Параметр	Значение	Обязательный
`NAME`	Имя сети	ДА
`VN_MAD`	`bridge` — для режима без фильтрации; `fw` — для режима фильтрации Security Group; `ebtables` — для режима фильтрации Ebtables VLAN	ДА
`BRIDGE`	Имя сетевого моста на серверах виртуализации	ДА

Примеры:

1. Создание сети с использованием конфигурационного файла. Будет создана сеть, работающая в режиме сетевой мост с использованием режима фильтрации Security Group:

   а) создать файл `new-net.conf` со следующим содержанием:

```
# параметры физической сети
```

```
NAME = "bridged_net"
VN_MAD = "fw"
BRIDGE = "vbr1"
# доступное адресное пространство
AR=[TYPE = "IP4", IP = "172.16.1.100", SIZE = "100" ]
# параметры контекстуализации
NETWORK_ADDRESS = "172.16.1.0"
NETWORK_MASK = "255.255.255.0"
DNS = "172.16.1.1"
GATEWAY = "172.16.1.1"
```

б) выполнить команду:

```
onevnet create new-net.conf
```

Пример вывода после выполнения команды:

```
ID: 1
```

2. Правила ebtables, которые создаются при необходимости отладки настройки:

```
# Игнорировать пакеты, которые не соответствуют MAC-адресу сети
-s ! <mac_address>/ff:ff:ff:ff:ff:0 -o <tap_device> -j DROP
# Предотвратить MAC-спуфинг
-s ! <mac_address> -i <tap_device> -j DROP
```

4.4. Сетевой режим VLAN

В данном сетевом режиме для каждой сети создается мост, к которому подключается VLAN- тегированный сетевой интерфейс (VLAN-тегирование стандарта IEEE802.1Q).

Идентификационный номер VLAN рассчитывается автоматически и будет одинаковым для всех интерфейсов в конкретной сети. Возможно также принудительно указать значение параметра `VLAN_ID` в настройках сети.

4.4.1. Настройка сервера виртуализации

ВНИМАНИЕ! Действия по настройке ПК СВ для использования виртуальных сетей выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности.

Для настройки сетевого режима VLAN необходимо выполнение следующих требований:

- модуль 802.1Q должен быть загружен в ядро;
- наличие сетевого коммутатора, способного направлять VLAN-тегированный трафик. Физические порты сетевого коммутатора должны быть каналами связи VLAN.

4.4.2. Настройка сервера управления

ВНИМАНИЕ! Действия по настройке ПК СВ для использования виртуальных сетей выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем

целостности.

Значение параметра VLAN_ID рассчитывается в соответствии с настройками, указанными в конфигурационном файле /etc/one/oned.conf (см. 5.2).

Изменением значения данного параметра можно зарезервировать некоторые сети VLAN, и они не будут назначаться сети. Можно также указать первый номер VLAN_ID. При создании новой изолированной сети определяется свободный номер VLAN_ID из пула VLAN. Этот пул является глобальным и совместно используется с сетевым режимом Open vSwitch.

В файле /var/lib/one/remotes/vnm/OpenNebulaNetwork.conf можно откорректировать параметр настройки validate_vlan_id. Установив значение true можно проверить, что другие сети VLAN не подсоединены к мосту.

4.4.3. Создание сети

ВНИМАНИЕ! Действия по созданию виртуальных сетей в ПК СВ выполняются под учетной записью администратора ПК СВ.

Для создания сети необходимо задать значения параметров физической сети, приведенных в таблице 18.

Таблица 18

Параметр	Значение	Обязательный
NAME	Имя сети	ДА
VN_MAD	802.1Q	ДА
PHYDEV	Имя физического сетевого устройства, которое будет подключено к сетевому мосту	ДА
BRIDGE	Имя сетевого моста, назначается по умолчанию onebr.<net_id> или onebr.<vlan_id>	НЕТ
VLAN_ID	Идентификационный номер сети VLAN. Будет сгенерирован, если не указан, а AUTOMATIC_VLAN_ID устанавливается на YES	ДА (если не AUTOMATIC_VLAN_ID)
AUTOMATIC_VLAN_ID	Обязательный и должен быть установлен на YES, если VLAN_ID определен	ДА (если не VLAN_ID)
MTU	Максимальный передаваемый модуль данных (MTU) для тегированного интерфейса и моста	НЕТ

Пример

Создание сети, работающей в режиме VLAN, с использованием конфигурационного файла:

1) создать файл new-net.conf со следующим содержанием:

```
# параметры физической сети
NAME = "hmnet"
VN_MAD = "802.1Q"
```

```
PHYDEV= "eth0"
VLAN_ID = 50
BRIDGE= "brhm"
# доступное адресное пространство
AR=[TYPE = "IP4", IP = "172.16.1.100", SIZE = "100" ]
# параметры контекстуализации
NETWORK_ADDRESS = "172.16.1.0"
NETWORK_MASK = "255.255.255.0"
DNS = "172.16.1.1"
GATEWAY = "172.16.1.1"
```

2) выполнить команду:

```
onevnet create new-net.conf
```

Пример вывода после выполнения команды:

```
ID: 1
```

В данном примере проверяется наличие моста `brhm`. Если он не существует, то будет создан. Сетевое устройство `eth0` будет тегировано (`eth0.50`) и подсоединено к `brhm`.

4.5. Сетевой режим VXLAN

В данном сетевом режиме для каждой сети создается мост, к которому подключается VXLAN-тегированный сетевой интерфейс.

Идентификационный номер VLAN рассчитывается автоматически и будет одинаковым для всех интерфейсов в конкретной сети. Возможно также принудительно указать значение параметра `VLAN_ID` в шаблоне виртуальной сети.

Кроме того, каждая сеть VLAN назначает групповой адрес для инкапсуляции транслирования L2 и группового трафика. Данный адрес назначается по умолчанию диапазону 239.0.0.0/8 в соответствии с RFC 2365 (административно назначаемая групповая адресация IP). В частности, групповой адрес получается добавлением `VLAN_ID` к основному адресу 239.0.0.0/8.

4.5.1. Особенности и ограничения

В данном сетевом режиме задействован стандартный UDP-порт сервера 8472.

Трафик VXLAN направляется на физическое устройство, которое может быть установлено как VLAN-тегированный интерфейс, но в этом случае необходимо убедиться в том, что тегированный интерфейс будет создан вручную изначально на всех серверах виртуализации.

4.5.2. Настройка сервера виртуализации

ВНИМАНИЕ! Действия по настройке ПК СВ для использования виртуальных сетей

выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности.

Для настройки сетевого режима VXLAN необходимо чтобы при подключении всех серверов виртуализации к одной подсети, групповой трафик не фильтровался правилами iptables на серверах виртуализации. Если групповой трафик должен проходить через маршрутизаторы, необходимо настроить в сети многоадресный протокол, например, IGMP.

4.5.3. Настройка сервера управления

ВНИМАНИЕ! Действия по настройке ПК СВ для использования виртуальных сетей выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности.

Значение параметра `VXLAN_ID` рассчитывается в соответствии с настройками, указанными в конфигурационном файле `/etc/one/oned.conf` (см. 5.2).

Параметры настройки, приведенные в таблице 19, можно откорректировать в файле `/var/lib/one/remotes/vnm/OpenNebulaNetwork.conf`.

Таблица 19

Параметр	Описание
`vxlan_mc`	Основной групповой адрес для каждой сети VLAN. Групповой адрес: `vxlan_mc + vlan_id`
`vxlan_ttl`	Время жизни (TTL) должно быть меньше 1 в маршрутизируемых многоадресных сетях (IGMP)
`validate_vlan_id`	Установить на `true` для проверки, что другие сети VLAN не подсоединены к мосту

4.5.4. Создание сети

ВНИМАНИЕ! Действия по созданию виртуальных сетей в ПК СВ выполняются под учетной записью администратора ПК СВ.

Для создания сети VXLAN необходимо задать значения параметров физической сети, приведенных в таблице 20.

Таблица 20

Параметр	Значение	Обязательный
`NAME`	Имя сети	ДА
`VN_MAD`	`vxlan`	ДА
`PHYDEV`	Имя физического сетевого устройства, которое будет подключено к мосту	ДА
`BRIDGE`	Имя сетевого моста, назначается по умолчанию `onebr.<net_id>` или `onebr.<vlan_id>`	НЕТ

Окончание таблицы 20

Параметр	Значение	Обязательный
VLAN_ID	Идентификационный номер сети VLAN. Будет сгенерирован, если не указан	НЕТ
MTU	Максимальный передаваемый модуль данных (MTU) для тегированного интерфейса и моста	НЕТ

Пример

Создание сети, работающей в режиме VXLAN, с использованием конфигурационного файла:

1) создать файл new-net.conf со следующим содержанием:

```
# параметры физической сети
NAME = "vxlan_net"
VN_MAD = "vxlan"
PHYDEV = "eth0"
VLAN_ID = 50 # optional
BRIDGE = "vxlan50" # optional
# доступное адресное пространство
AR=[TYPE = "IP4", IP = "172.16.1.100", SIZE = "100" ]
# параметры контекстуализации
NETWORK_ADDRESS = "172.16.1.0"
NETWORK_MASK = "255.255.255.0"
DNS = "172.16.1.1"
GATEWAY = "172.16.1.1"
```

2) выполнить команду:

```
onevnet create new-net.conf
```

Пример вывода после выполнения команды:

```
ID: 1
```

В данном примере драйвер проверяет наличие моста vxlan50. Если он не существует, то будет создан. Сетевое устройство eth0 будет тегировано (eth0.50) и подсоединено к vxlan50. Сетевое устройство eth0 может иметь 802.1Q тегированный интерфейс, если предполагается изолировать трафик сети VXLAN.

4.6. Сети Open vSwitch

Действия по настройке сети Open vSwitch выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности. Действия по по созданию виртуальных сетей в ПК СВ выполняются под учетной записью администратора ПК СВ.

Сети Open vSwitch создаются на базе программного коммутатора Open vSwitch.

Open vSwitch — программный многоуровневый коммутатор, обеспечивающий изоля-

цию сети с помощью сетей VLAN путем тегирования портов и фильтрацию базовой сети с помощью OpenFlow.

Архитектура OVS состоит из трех основных компонентов: базы данных, непосредственно программного коммутатора и управляющего контроллера. На каждом из физических серверов вместе с гипервизором располагаются собственные БД и коммутатор. Эти два компонента образуют отдельно стоящий коммутатор, информационно не связанный с другими программными коммутаторах на соседних физических серверах.

ВНИМАНИЕ! Группы безопасности данным сетевым режимом не поддерживаются.

4.6.1. Особенности конфигурирования

Конфигурация всех Open vSwitch коммутаторов, портов, настройки поддерживаемых протоколов хранятся в собственной базе данных OVS (OVSDB). В стандартной конфигурации в OVSDB существуют следующие таблицы:

- Open_vSwitch — Схема
- Bridge
- Port
- Interface
- Flow_Table — конфигурация OpenFlow
- QoS
- Mirror
- Controller — параметры подключения к контроллеру OpenFlow
- Manager — конфигурация OVSDB
- NetFlow
- SSL
- sFlow
- IPFIX
- Flow_Sample_Collector_Set

Изначально почти все таблицы пусты, так как конфигурация отсутствует. Утилита `ovs-vsctl` предоставляет интерфейс для внесения изменений в БД. Для внесения изменений используется команда вида:

```
sudo ovs-vsctl <команда> <таблица> <запись> <ключ=значение>
```

Для создания программного коммутатора с именем `ovs-sw0` необходимо выполнить следующую команду:

```
sudo ovs-vsctl add-br ovs-sw0
```

После появляется возможность подключения ВМ. При этом ВМ, подключенные к `ovs-sw0`, будут работать в изолированной сети. Для того, чтобы предоставить им доступ к внешней сети, необходимо подключить к `ovs-sw0` в качестве порта физический интерфейс

eth0, выполнив команду:

```
sudo ovs-vsctl add-port ovs-sw0 eth0
```

Для того чтобы разрешить порту eth0 пропускать во внешнюю сеть трафик из определенных VLAN, необходимо выполнить команду:

```
sudo ovs-vsctl set port eth0 trunks=10,20,30,40,50
```

Ниже представлен список вариантов команд с параметрами вызова:

- list <таблица> <запись>
- find <таблица> <условие>
- get <таблица> <запись> <ключ=значение>
- add <таблица> <запись> <ключ=значение>
- remove <таблица> <запись> <ключ=значение>
- clear <таблица> <запись> <ключ>
- create <таблица> <запись> <ключ=значение>
- destroy <таблица> <запись>
- wait-until <таблица> <запись> <ключ=значение>

Для просмотра записей, присутствующих в таблице, описывающей порты, выполнить команду:

```
sudo ovs-vsctl list port
```

Для вывода списка портов, включенных в VLAN, необходимо выполнить команду:

```
sudo ovs-vsctl find port tag=10
```

4.6.2. Агрегирование физических интерфейсов

Для повышения пропускной способности и уровня отказоустойчивости в Open vSwitch коммутатор могут быть включены несколько физических интерфейсов с задействованной на них агрегацией по протоколу LACP (Link Aggregation Control Protocol). Выполняется на канальном уровне путем создания объединенного интерфейса (Bonding).

Для создания объединенного интерфейса на базе физических интерфейсов eth0 и eth1 необходимо выполнить следующую команду:

```
sudo ovs-vsctl add-bond ovs-sw0 bond0 eth0 eth1
```

После следует включить lacp на созданном объединенном интерфейсе:

```
sudo ovs-vsctl set port bond0 lacp=active
```

На этом настройка отказоустойчивости сетевых интерфейсов завершена.

4.6.3. Зеркалирование портов

Open vSwitch позволяет направлять копию потока трафика из одного или нескольких интерфейсов в другой. Так же он может организовать перенаправление трафика из всей VLAN в конкретный порт или наоборот. Зеркалироваться может только входящий, только исходящий или оба типа трафика. Использование такой возможности позволит вести кон-

троль сетевого трафика, передаваемого между ВМ с целью обнаружения (предупреждения) компьютерных атак.

Пример

Зеркалирование трафика из интерфейса vnet2, принадлежащего одной ВМ, в специально созданный для прослушивания порт mirror0 с типом internal.

```
sudo ovs-vsctl -- set Bridge ovs-sw0 mirrors=@m -- \
    --id=@mirror0 get Port mirror0 -- --id=@vnet2 get Port vnet2 -- \
    --id=@m create Mirror name=mymirror select-dst-port=@vnet2 \
    select-src-port=@vnet2 output-port=@mirror0
```

где конструкцией –id=@<имя_переменной> определяется использование переменной;

командой set Bridge ovs-sw0 mirrors=@m создается зеркало, имя и параметры которого получаются из переменной @m (см. ниже);

командой –id=@mirror0 get Port mirror0 – –id=@vnet2 get Port vnet2 определяются значения переменных @mirror0, @vnet2 — записываются идентификаторы соответствующих портов;

командой –id=@m create Mirror name=mymirror select-dst-port=@vnet2 select-src-port=@vnet2 output-port=@mirror0 определяется значение переменной @m — записываются имя и параметры зеркала;

select-dst-port — зеркалирование входящего трафика;

select-src-port — зеркалирование исходящего трафика;

output-port — место перенаправления трафика.

С помощью консольной утилиты tcpdump, запущенной на сервере виртуализации, можно прослушивать весь трафик поступающий, например, на порт mirror0. Для этого необходимо выполнить команду:

```
tcpdump -i mirror0
```

Также можно организовать ретрансляцию всех пакетов, например, пришедших на порт eth0 или eth1 на порт eth2:

```
sudo ovs-vsctl -- set Bridge ovs-sw0 mirrors=@m \
    -- --id=@eth0 get Port eth0 -- --id=@eth1 get Port eth1 \
    -- --id=@eth2 get Port eth2 \
    -- --id=@m create Mirror name=mymirror -- select-dst-port=@eth0,@eth1 \
    select-src-port=@eth0,@eth1 output-port=@eth2
```

где конструкцией –id=@<имя_переменной> определяется использование переменной;

командой set Bridge ovs-sw0 mirrors=@m создается зеркало, имя и параметры которого получаются из переменной @m (см. ниже);

командой – –id=@eth0 get Port eth0 – –id=@eth1 get Port eth1 – –id=@eth2 get Port eth2 определяются значения переменных @eth0, @eth1 и @eth2;

командой –id=@m create Mirror name=mymirror select-dst-port=@eth0, @eth1 select-src-port=@eth0,@eth1 output-port=@eth2 определяется значение переменной @m — записываются имя и параметры зеркала;

select-dst-port — зеркалирование входящего трафика;

select-src-port — зеркалирование исходящего трафика;

output-port — место перенаправления трафика.

Для отмены зеркалирования выполнить команду:

```
sudo ovs-vsctl remove Bridge ovs-sw0 mirrors mymirror
```

4.6.4. Настройка сервера виртуализации

ВНИМАНИЕ! Действия по настройке ПК СВ для использования виртуальных сетей выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности.

4.6.4.1. Требования

Для настройки данного сетевого режима необходимо чтобы на каждом сервере виртуализации был установлен пакет openvswitch-switch (данный пакет размещен в базовом репозитории ОС СН).

4.6.4.2. Настройка

Для настройки необходимо создать программный коммутатор для каждой сети, в которой будут работать виртуальные машины. На всех серверах виртуализации необходимо использовать одно и тоже имя для программного коммутатора. Затем добавить физический сетевой интерфейс к этому программному коммутатору.

Пример

Сервер виртуализации, который направляет трафик виртуальных сетей через сетевой интерфейс enp0s8. Пример вывода после выполнения команды:

```
sudo ovs-vsctl show
c61ba96f-fc11-4db9-9636-408e763f529e Bridge "ovsbr0"
Port "ovsbr0"
Interface "ovsbr0" type: internal
Port "enp0s8"
Interface "enp0s8"
```

4.6.5. Общие настройки ПК СВ

ВНИМАНИЕ! Действия по настройке ПК СВ для использования виртуальных сетей выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности.

Значение параметра VLAN_ID рассчитывается в соответствии с настройками, указанными в конфигурационном файле /etc/one/oned.conf (см. 5.2).

Изменением данного параметра можно зарезервировать некоторые сети VLAN, и они не будут назначаться виртуальной сети. Можно также указать первый номер VLAN_ID. При создании новой изолированной сети находит свободный номер VLAN_ID из пула VLAN. Этот пул является глобальным, а также совместно используется с сетевым режимом 802.1Q VLAN.

В файле /var/lib/one/remotes/vnm/OpenNebulaNetwork.conf можно откорректировать параметр настройки arp_cache_poisoning, отвечающий за подключение правила предотвращения изменения кэша ARP (ARP Cache Poisoning).

ВНИМАНИЕ! После корректировки значения параметра arp_cache_poisoning необходимо выполнить команду onehost sync для применения изменений на всех серверах виртуализации.

4.6.6. Создание сети

ВНИМАНИЕ! Действия по созданию виртуальных сетей в ПК СВ выполняются под учетной записью администратора ПК СВ.

Для создания сети Open vSwitch необходимо задать значения параметров физической сети, приведенных в таблице 21.

Таблица 21

Параметр	Значение	Обязательный
NAME	Имя сети	ДА
VN_MAD	ovswitch	ДА
PHYDEV	Имя физического сетевого устройства, которое будет подключено к мосту	ДА
BRIDGE	Имя сетевого моста, назначается по умолчанию onebr.<net_id> или onebr.<vlan_id>	НЕТ
VLAN_ID	Идентификационный номер сети VLAN. Будет сгенерирован, если не указан и для параметра AUTOMATIC_VLAN_ID установлено значение YES	НЕТ
AUTOMATIC_VLAN_ID	Игнорируется, если параметр VLAN_ID определен. Следует установить значение YES, если необходимо в автоматическом режиме генерировать идентификационный номер сети VLAN	НЕТ

Окончание таблицы 21

Параметр	Значение	Обязательный
MTU	Максимальный передаваемый модуль данных (MTU) для сети Open vSwitch	НЕТ

Пример

Создание сети Open vSwitch с использованием конфигурационного файла:

1) создать файл new-net.conf со следующим содержанием:

```
# параметры физической сети
NAME = "ovswitch_net"
VN_MAD = "ovswitch"
BRIDGE = vbr1
VLAN_ID = 50 # optional
# доступное адресное пространство
AR=[TYPE = "IP4", IP = "172.16.1.100", SIZE = "100" ]
# параметры контекстуализации
NETWORK_ADDRESS = "172.16.1.0"
NETWORK_MASK = "255.255.255.0"
DNS = "172.16.1.1"
GATEWAY = "172.16.1.1"
```

2) выполнить команду:

```
onevnet create new-net.conf
```

Пример вывода после выполнения команды:

```
ID: 1
```

4.6.7. Многоканальные сети VLAN (VLAN транкинг)

ВНИМАНИЕ! Действия по настройке VLAN транкинга в ПК СВ выполняются под учетной записью администратора ПК СВ.

VLAN транкинг поддерживается путем добавления тега VLAN_TAGGED_ID: к элементу NIC в шаблоне ВМ или шаблоне виртуальной сети. Тег позволяет указать диапазон сетей VLAN, подлежащий тегированию, например, 1,10,30,32.

4.6.8. Правила OpenFlow

4.6.8.1. MAC-спуфинг

Данные правила предотвращают выход любого трафика с порта, если был изменен MAC-адрес.

Пример

```
in_port=<PORT>,dl_src=<MAC>,priority=40000,actions=normal
in_port=<PORT>,priority=39000,actions=normal
```

4.6.8.2. IP-захват

Данные правила предотвращают выход любого трафика с порта для IPv4, если не настроен IP-адрес для ВМ.

Пример

```
in_port=<PORT>,arp,dl_src=<MAC>priority=45000,actions=drop
in_port=<PORT>,arp,dl_src=<MAC>,nw_src=<IP>,priority=46000,actions=normal
```

4.6.8.3. Черные порты

Применяется одно правило на порт.

Пример

```
tcp,dl_dst=<MAC>,tp_dst=<PORT>,actions=drop
```

4.6.8.4. ICMP-игнорирование

С помощью данной настройки можно, например, заблокировать ping-запросы к ВМ.

Пример

```
icmp,dl_dst=<MAC>,actions=drop
```

5. ДОПОЛНИТЕЛЬНОЕ КОНФИГУРИРОВАНИЕ СЛУЖБЫ СЕРВЕРА УПРАВЛЕНИЯ

Действия по дополнительной настройке службы сервера управления выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности.

Служба сервера управления в ПК СВ реализована в виде системной службы `opennebula`. В качестве ядра службы сервера управления выступает инструмент командной строки `oned`.

Настройки службы сервера управления размещены в конфигурационном файле `/etc/one/oned.conf`.

ВНИМАНИЕ! Изменение значений параметров службы сервера управления производится в конфигурационных файлах каталога `/etc/one/one.d/`. Допускается править параметры в имеющихся файлах или добавлять новые параметры в виде отдельных файлов с расширением *.conf.

После внесения изменений необходимо перезапустить службу сервера управления командой:

```
sudo systemctl restart opennebula
```

После перезапуска в новый файл конфигурации `/etc/one/oned.conf` будут собраны значения параметров из всех файлов каталога `/etc/one/one.d/`.

5.1. Параметры настройки службы сервера управления

Файл конфигурации службы поддерживает настройку параметров, приведенных в таблице 22.

Таблица 22

Параметр	Описание
`MANAGER_TIMER`	Время в секундах, необходимое службе для оценки периодических функций
`MONITORING_INTERVAL_DATASTORE`	Время в секундах между циклами мониторинга хранилища. Параметр не может иметь значение меньше, чем параметр `MANAGER_TIMER`
`MONITORING_INTERVAL_MARKET`	Время в секундах между циклами мониторинга магазина приложений. Параметр не может иметь значение меньше, чем параметр `MANAGER_TIMER`
`MONITORING_INTERVAL_DB_UPDATE`	Время в секундах между циклами записи в БД информации мониторинга ВМ. Параметр не может иметь значение меньше, чем параметр `MANAGER_TIMER`. Чтобы запретить запись в БД информации мониторинга ВМ, необходимо установить значение «-1». Чтобы записывать в БД информацию мониторинга ВМ, получаемую при каждом цикле мониторинга, необходимо установить значение «0»

Окончание таблицы 22

Параметр	Описание
DS_MONITOR_VM_DISK	Количество интервалов времени MONITORING_INTERVAL_DATASTORE, по прошествии которых будет запущена процедура мониторинга дисков ВМ. Применяется только для хранилищ, построенных на базе файловой технологии хранения, или использующих драйвер хранилища FS_LVM. Чтобы отключить процедуру мониторинга дисков ВМ, необходимо установить значение «0»
SCRIPTS_REMOTE_DIR	Удаленный путь для хранения скрипта мониторинга и управления ВМ
PORT	Порт, на котором службы сервера управления будет принимать запросы xml-rpc
LISTEN_ADDRESS	IP-адрес для приема запросов xml-rpc (по умолчанию все IP-адреса)
DB	Блок настройки БД, по умолчанию в ПК СВ используется БД PostgreSQL: - BACKEND = "postgresql" (наименование БД), - SERVER — IP-адрес или сетевое имя компьютера, на котором запущена служба PostgreSQL-сервра, - PORT = 0 (порт для подключения к БД), - USER = "oneadmin" (имя пользователя БД), - PASSWD — пароль пользователя БД, - DB_NAME = "brest" (наименование БД)
VNC_PORTS	Пул портов VNC для автоматического назначения портов VNC, по возможности, устанавливать порт на START+VMID: - start — первый назначаемый порт; - reserved — список зарезервированных портов, разделенный запятыми. Два номера, разделенные двоеточием, указывают диапазон
VM_SUBMIT_ON_HOLD	Принудительное создание ВМ в состоянии удержания вместо состояния ожидания. Возможные значения YES (ДА) или NO (НЕТ)
LOG	Блок настройки системы регистрации: 1) SYSTEM — тип системы регистрации, возможные значения: - file (по умолчанию) — файловая система регистрации, - syslog — регистрация системных журналов, - std — регистрация в стандартный поток ошибок; 2) DEBUG_LEVEL — устанавливает уровень отладки зарегистрированных сообщений. Возможные значения: - 0 — ошибка, - 1 — предупреждение, - 2 — информация, - 3 — отладка

Пример

Значения параметров службы сервера управления, установленные по умолчанию

```
LOG = [
      SYSTEM = "file",
      DEBUG_LEVEL = 3
      ]
#MANAGER_TIMER = 15
MONITORING_INTERVAL_DATASTORE = 300
MONITORING_INTERVAL_MARKET = 600
MONITORING_INTERVAL_DB_UPDATE = 0
#DS_MONITOR_VM_DISK = 10
SCRIPTS_REMOTE_DIR=/var/tmp/one
PORT = 2633
LISTEN_ADDRESS = "0.0.0.0"
DB = [ BACKEND = "postgresql",
      SERVER = "localhost",
      PORT = 0,
      USER = "oneadmin",
      PASSWD = "<хэш_пароля>",
      DB_NAME = "brest"
      ]
VNC_PORTS = [
START = 5900,
RESERVED = "32768:65536"
# RESERVED = "6800, 6801, 6810:6820, 9869"
]
#VM_SUBMIT_ON_HOLD = "NO"
```

5.2. Параметры настройки сетей

Сети в ПК СВ поддерживают настройку параметров, приведенных в таблице 23.

Таблица 23

Параметр	Описание
NETWORK_SIZE	Определяет размер по умолчанию для виртуальных сетей
MAC_PREFIX	MAC-префикс по умолчанию, предназначенный для создания автоматически генерируемых MAC-адресов (может переписываться шаблоном виртуальной сети)

Окончание таблицы 23

Параметр	Описание
VLAN_IDS	Блок настройки пула идентификаторов для автоматического назначения VLAN_ID. Данный пул предназначен для сетей 802.1Q (Open vSwitch и драйверы 802.1Q). Первый идентификатор будет иметь значение [START (см. ниже) + VNET_ID]: - START — начальное значение для определения пула идентификаторов VLAN_ID; - RESERVED — перечень зарезервированных идентификаторов VLAN_ID, разделенных запятыми. Два номера, разделенные двоеточием, указывают диапазон
VXLAN_IDS	Блок настройки автоматического назначения идентификатора сети VXLAN (VNI). Используется для сетей VXLAN. START — первый VNI, который может использоваться. Резервирование идентификаторов не применяется.

Пример

Значения параметров сетей, установленные по умолчанию

```
NETWORK_SIZE = 254
MAC_PREFIX = "02:00"
VLAN_IDS = [
      START = "2",
      RESERVED = "0, 1, 4095"
      ]
VXLAN_IDS = [
      START = "2"
      ]
```

5.3. Параметры настройки хранилищ

В хранилищах и шаблонах ВМ (настройках, касающихся образов) можно настроить значения параметров, приведенных в таблице 24.

Таблица 24

Параметр	Описание
DATASTORE_LOCATION	Путь к хранилищам. Одинаков для всех серверов виртуализации и сервера управления. По умолчанию /var/lib/one/datastores
DATASTORE_CAPACITY_CHECK	Проверяет наличие достаточного пространства до создания нового образа. Значение по умолчанию «Yes»

Окончание таблицы 24

Параметр	Описание
DEFAULT_IMAGE_TYPE	Значение по умолчанию для поля «TYPE», если оно отсутствует в шаблоне. Возможные значения: - OS — файл образа, содержащий операционную систему; - CDROM — файл образа, содержащий CDROM; - DATABLOCK — файл образа, содержащий блок данных, создаваемый как пустой блок
DEFAULT_DEVICE_PREFIX	Значение по умолчанию для поля «DEV_PREFIX», если оно отсутствует в шаблоне. Отсутствующее поле «DEV_PREFIX» заполняется, когда создаются образы, поэтому изменение префикса не повлияет на существующие образы. Возможные значения: - префикс hd — для устройства IDE; - префикс sd — для устройства SCSI; - префикс vd — для устройства Virtio
DEFAULT_CDROM_DEVICE_PREFIX	Аналогично DEFAULT_DEVICE_PREFIX, но для устройств CDROM
DEFAULT_IMAGE_PERSISTENT	При клонировании или сохранении образа (командами oneimage clone и onevm disk-saveas) устанавливает атрибут образа «постоянный». Если этот параметр не определен, то атрибут образа наследуется из исходного образа
DEFAULT_IMAGE_PERSISTENT_NEW	При создании образа (командой oneimage create) устанавливает атрибут образа «постоянный». По умолчанию для создаваемых образов установлен атрибут «непостоянный»

Пример

Значения параметров хранилищ, установленные по умолчанию

```
#DATASTORE_LOCATION = /var/lib/one/datastores
DATASTORE_CAPACITY_CHECK = "yes"
DEFAULT_DEVICE_PREFIX = "sd"
DEFAULT_CDROM_DEVICE_PREFIX = "hd"
DEFAULT_IMAGE_TYPE = "OS"
#DEFAULT_IMAGE_PERSISTENT = ""
#DEFAULT_IMAGE_PERSISTENT_NEW = ""
```

5.4. Параметры настройки системы мониторинга

Для указания настроек системы мониторинга в конфигурационном файле используется блок IM_MAD, в котором указываются значения параметров, приведенных в таблице 25.

Таблица 25

Параметр	Описание
NAME	Имя службы
EXECUTABLE	Путь исполняемого модуля службы, может быть абсолютным или относительным (относительно каталога /usr/lib/one/mads/)
ARGUMENTS	Конфигурационный файл для службы, может быть абсолютным или относительным (относительно каталога /etc/one/)
THREADS	количество потоков обработки информации

Пример

Настройки системы мониторинга, установленные по умолчанию после инициализации программных компонентов ПК СВ

```
IM_MAD = [
      NAME = "monitord",
      EXECUTABLE = "onemonitord",
      ARGUMENTS = "-c monitord.conf",
      THREADS = 8 ]
```

5.5. Система хуков

Хуки в ПК СВ являются программами, выполняемыми при изменении состояния ВМ или серверов виртуализации. Хуки могут выполняться как локально, так и удаленно в сервере виртуализации, где работает ВМ. Для настройки системы хуков необходимо установить следующие значения в конфигурационном файле /etc/one/oned.conf:

- executable — путь исполняемого модуля драйвера хука, может быть абсолютным или относительным (относительно каталога /usr/lib/one/mads/);
- arguments — конфигурационный файл для исполняемого модуля драйвера хука, может быть абсолютным или относительным (относительно каталога /etc/one/).

Пример

```
HM_MAD = [
executable = "one_hm"
]
```

5.5.1. Хуки виртуальной машины (VM_HOOK)

Хуки ВМ определяются по следующим параметрами:

- name — имя хука;
- on — условия выполнения хука:
    - CREATE — при создании ВМ;
    - PROLOG — при нахождении ВМ в состоянии PROLOG;

- RUNNING — после успешной загрузки ВМ;
- UNKNOWN — при нахождении ВМ в неизвестном состоянии;
- SHUTDOWN — после отключения ВМ;
- STOP — после остановки ВМ (включая передачу образов ВМ);
- DONE — после удаления или отключения ВМ;
- CUSTOM — определяемое пользователем конкретный статус STATE и комбинация состояний LCM_STATE для запуска хука;

- command — путь может быть абсолютным или относительным (относительно каталога /usr/share/one/hooks);
- arguments — аргументы для хука. Можно использовать следующую информацию о ВМ:
  - $ID — идентификатор ВМ;
  - $TEMPLATE — шаблон ВМ в формате xml с кодированием base64;
  - $PREV_STATE — предыдущий статус ВМ;
  - $PREV_LCM_STATE предыдущее состояние ВМ.

  Примечание. Подробное описание статусов и состояний ВМ представлено в документе РДЦП.10001-02 95 01-2;
- remote — удаленное выполнение. Возможные значения:
  - YES — хук выполняется на сервере виртуализации, где установлена ВМ;
  - NO — хук выполняется на сервере управления. Является значением по умолчанию.

Пример

```
VM_HOOK = [
name = "advanced_hook",
on = "CUSTOM",
state = "ACTIVE", lcm_state = "BOOT_UNKNOWN", command = "log.rb",
arguments = "$ID $PREV_STATE $PREV_LCM_STATE"
]
```

5.5.2. Хуки сервера виртуализации (HOST_HOOK)

Хуки сервера виртуализации определяются по следующим параметрами:

- name — имя хука;
- on — условия выполнения хука:
  - CREATE — при создании сервера виртуализации (использование команды onehost create);
  - ERROR — при нахождении сервера виртуализации в состоянии сбоя;

- DISABLE — после отключения сервера виртуализации;

- command — путь может быть абсолютным или относительным (относительно каталога /usr/share/one/hooks);

- arguments — аргументы для хука. Можно использовать следующую информацию о сервере виртуализации:

  - $ID — идентификатор сервера виртуализации;

  - $TEMPLATE — шаблон сервера виртуализации в формате xml с кодированием base64;

- remote — удаленное выполнение. Возможные значения:

  - YES — хук выполняется на сервере виртуализации;

  - NO — хук выполняется на сервере управления. Является значением по умолчанию.

5.6. Особенности работы ПК СВ в условиях применения мандатного управления доступом

Для того чтобы обеспечить возможность управления ПК СВ с использованием инструментов командной строки (onevm, onehost и т. д.) в условиях применения мандатного управления доступом, необходимо:

1) на компьютере, выполняющим функции сервера управления, в файле /etc/parsec/privsock.conf добавить следующее строки:

```
#brest
/usr/bin/oned
```

2) перезагрузить компьютер, выполняющий функции сервера управления.

6. МОНИТОРИНГ И УЧЕТ

6.1. Мониторинг

В ПК СВ используется распределенная система мониторинга, которая реализована в виде выделенного процесса `onemonitord`, являющегося составной частью службы сервера управления.

Система мониторинга собирает следующую информацию, касающуюся серверов виртуализации и виртуальных машин:

- состояние сервера виртуализации;
- основные показатели производительности сервера виртуализации;
- состояние ВМ;
- вычислительные ресурсы, потребляемые ВМ.

Информация мониторинга формируется в результате выполнения ряда тестовых программ на серверах виртуализации и транслируется по сети на сервер управления (по умолчанию используется TCP/UDP-порт 4124).

ВНИМАНИЕ! Межсетевой экран сервера управления должен разрешать получение пакетов по прослушиваемому порту.

Схема работы системы мониторинга приведена на рис. 4.

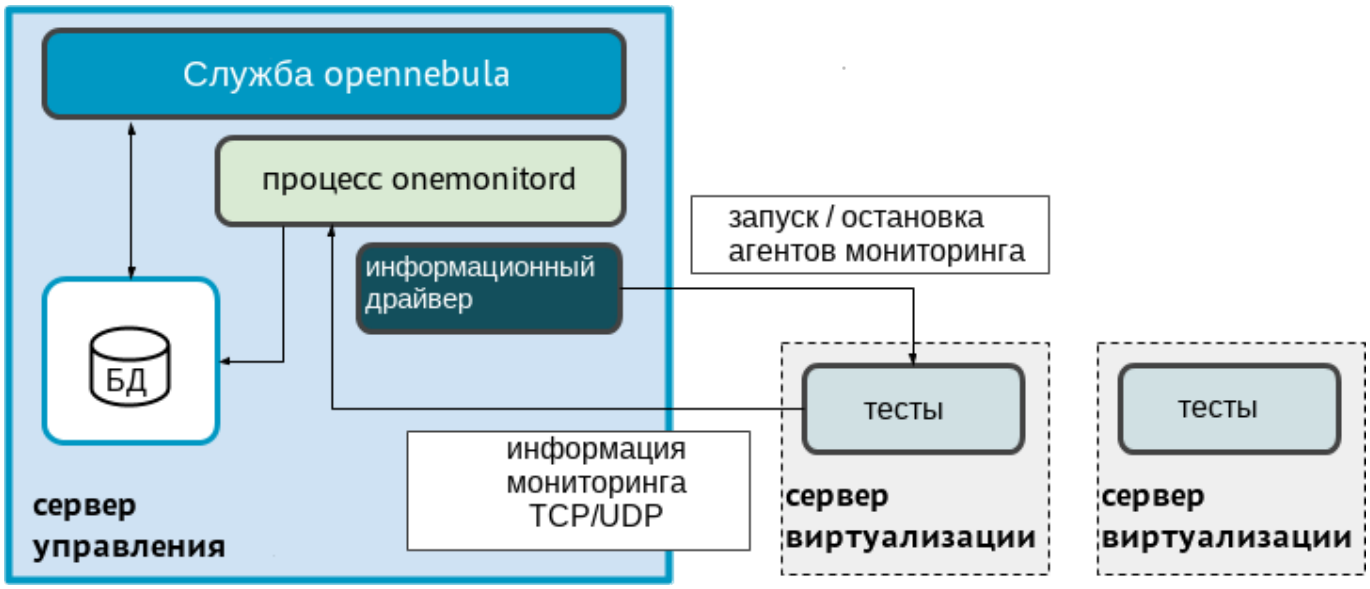

Рис. 4

При первичном запуске система мониторинга посредством специализированного информационного драйвера подключается к серверу виртуализации по ssh и запускает на нем службу агента мониторинга. Агент мониторинга выполняет тесты и затем отсылает собранные данные на сервер управления в систему мониторинга. Затем агент мониторинга с заданной периодичностью выполняет тесты и отсылает собранные данные. В связи с этим системе мониторинга не требуется выполнять новые ssh-соединения для получения данных.

В случае, если в заданный промежуток времени в систему мониторинга не поступили данные от агента мониторинга, производится повторное подключение и перезапуск агента.

6.1.1. Настройка системы мониторинга

Действия по настройке системы мониторинга выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности.

Настройки системы мониторинга размещены в конфигурационном файле `/etc/one/monitord.conf`, в котором можно задать значения параметров, приведенных в таблице 26.

Таблица 26

Параметр	Описание
`MANAGER_TIMER`	Время в секундах, необходимое для оценки периодических функций
`MONITORING_INTERVAL_HOST`	Время ожидания данных от агента мониторинга (в секундах). Если за указанное время данные не получены, то выполняется повторное подключение и перезапуск агента мониторинга
`HOST_MONITORING_EXPIRATION_TIME`	Время в секундах, по истечении которого информация мониторинга сервера виртуализации устаревает. Если необходимо отключить мониторинг, следует установить значение «0»
`DB`	Блок настроек подключения к БД. Основные настройки подключения к БД задаются в конфигурационном файле `/etc/one/one.d/db.conf`. В файле `/etc/one/monitord.conf` указывается только значение параметра `CONNECTIONS` — количество одновременных подключений к БД
`LOG`	Блок параметров для настройки регистрации событий системы мониторинга. Содержит следующие параметры: 1) `SYSTEM` — тип системы регистрации, возможные значения: - `file` — регистрация в файл `/var/log/one/monitor.log` (установлено по умолчанию); - `syslog` — регистрация в системный журнал; - `std` — регистрация в стандартный поток ошибок; 2) `DEBUG_LEVEL` — уровень протоколирования, возможные значения: - «0» — регистрировать сообщения об ошибках; - «1» — регистрировать предупреждения; - «2» — регистрировать информационные сообщения; - «3» — регистрировать общие отладочные сообщения (установлено по умолчанию)

Окончание таблицы 26

Параметр	Описание
NETWORK	Блок настроек сетевого соединения. Указываются значения следующих параметров: 1) ADDRESS — IP-адрес, на котором принимать информацию мониторинга (на заданный TCP/UDP-порт); 2) MONITOR_ADDRESS — IP-адрес сервера управления, на который агенты мониторинга отправляют информацию мониторинга. Если используется технология Raft, то необходимо указать плавающий IP-адрес кластера; 3) PORT — TCP/UDP-порт, на котором принимать информацию мониторинга; 4) THREADS — количество потоков обработки информации мониторинга; 5) PUBKEY — абсолютный путь для открытого ключа. Не указывается, если кодирование не применяется; 6) PRIKEY — абсолютный путь для закрытого ключа. Не указывается, если кодирование не применяется
PROBES_PERIOD	Блок настроек тестов. Указываются значения следующих параметров: 1) BEACON_HOST — время в секундах, по прошествии которого на сервер виртуализации отправляется тестовый пакет, для проверки его работоспособности; 2) SYSTEM_HOST — время в секундах, по прошествии которого, должна быть получена информация о состоянии и конфигурации сервера виртуализации; 3) MONITOR_HOST — время в секундах, по прошествии которого, должна быть получена информация мониторинга сервера виртуализации (о вычислительных ресурсах и сетевой нагрузке); 4) STATE_VM — время в секундах, по прошествии которого, должна быть получена информация о состоянии ВМ; 5) MONITOR_VM — время в секундах, по прошествии которого, должна быть получена информация о вычислительных ресурсах, потребляемых ВМ; 6) SYNC_STATE_VM — время ожидания информации мониторинга ВМ. Если за указанное время информация не получена, то направляется полный отчет о ВМ

После внесения изменений в конфигурационный файл необходимо перезапустить службу сервера управления командой:

```
sudo systemctl restart opennebula
```

Пример

Значения параметров системы мониторинга, установленные по умолчанию

```
#MANAGER_TIMER = 15
MONITORING_INTERVAL_HOST = 30
```

```
#HOST_MONITORING_EXPIRATION_TIME = 43200
#VM_MONITORING_EXPIRATION_TIME = 43200

DB = [
CONNECTIONS = 15
]
LOG = [
SYSTEM = "file",
DEBUG_LEVEL = 3
]
NETWORK = [
ADDRESS = "0.0.0.0",
MONITOR_ADDRESS = "auto",
PORT = 4124,
THREADS = 8,
PUBKEY = "",
PRIKEY = ""
]
PROBES_PERIOD = [
BEACON_HOST = 30,
SYSTEM_HOST = 600,
MONITOR_HOST = 120,
STATE_VM = 5,
MONITOR_VM = 30,
SYNC_STATE_VM = 180
]
```

Для указания настроек информационного драйвера в конфигурационном файле `/etc/one/monitord.conf` используется блок `IM_MAD`, в котором указываются значения параметров, приведенных в таблице 27.

Таблица 27

Параметр	Описание
`NAME`	Наименование информационного драйвера
`SUNSTONE_NAME`	Тип гипервизора, установленного на сервере виртуализации
`EXECUTABLE`	Путь исполняемого модуля драйвера, может быть абсолютным или относительным (относительно каталога `/usr/lib/one/mads/`)

Окончание таблицы 27

Параметр	Описание
ARGUMENTS	Параметры настройки функционирования информационного драйвера 1) r — количество перезапусков агента мониторинга, выполняемых в случае отсутствия информации мониторинга в заданный период времени; 2) t — количество агентов мониторинга, которым одновременно будут направлены внешние команды (по ssh); 3) w — таймаут (в секундах) до повторного выполнения внешних команд (по ssh)
THREADS	количество потоков обработки информации мониторинга

Пример

Настройки информационного драйвера для сервера виртуализации с гипервизором KVM, установленные по умолчанию

```
IM_MAD = [
      NAME = "kvm",
      SUNSTONE_NAME = "KVM",
      EXECUTABLE = "one_im_ssh",
      ARGUMENTS = "-r 3 -t 15 -w 90 kvm",
      THREADS = 0
      ]
```

6.1.2. Отчет системы мониторинга

По умолчанию отчеты системы мониторинга сохраняются в файл /var/log/one/monitor.log.

Пример

Результаты мониторинга сервера виртуализации с идентификатором «0» (host: 0) и виртуальной машины с идентификатором «10» (VM: 10)

```
Thu Jun 23 12:35:28 2022 [Z0][DrM][I]: Loading drivers.
Thu Jun 23 12:35:28 2022 [Z0][DrM][I]: Loading driver: kvm
Thu Jun 23 12:35:28 2022 [Z0][DrM][I]:  Driver loaded: kvm
Thu Jun 23 12:35:28 2022 [Z0][DrM][I]: Loading driver: qemu
Thu Jun 23 12:35:28 2022 [Z0][DrM][I]:  Driver loaded: qemu
Thu Jun 23 12:35:28 2022 [Z0][DrM][I]: Loading driver: lxd
Thu Jun 23 12:35:28 2022 [Z0][DrM][I]:  Driver loaded: lxd
Thu Jun 23 12:35:28 2022 [Z0][DrM][I]: Loading driver: lxc
Thu Jun 23 12:35:28 2022 [Z0][DrM][I]:  Driver loaded: lxc
Thu Jun 23 12:35:28 2022 [Z0][DrM][I]: Loading driver: firecracker
Thu Jun 23 12:35:28 2022 [Z0][DrM][I]:  Driver loaded: firecracker
Thu Jun 23 12:35:28 2022 [Z0][DrM][I]: Loading driver: vcenter
```

```
Thu Jun 23 12:35:28 2022 [Z0][DrM][I]:  Driver loaded: vcenter
Thu Jun 23 12:35:32 2022 [Z0][HMM][I]: Raft status: SOLO
Thu Jun 23 12:35:41 2022 [Z0][HMM][I]: Successfully monitored VM: 10
Thu Jun 23 12:36:17 2022 [Z0][HMM][D]: Monitoring host fn.brest.local(0)
Thu Jun 23 12:36:23 2022 [Z0][HMM][I]: Successfully monitored VM: 10
Thu Jun 23 12:36:23 2022 [Z0][HMM][I]: Successfully monitored host: 0
Thu Jun 23 12:36:23 2022 [Z0][HMM][D]: Start monitor success, host: 0
Thu Jun 23 12:36:24 2022 [Z0][HMM][I]: Successfully monitored host: 0
Thu Jun 23 12:36:24 2022 [Z0][HMM][I]: Successfully monitored VM: 10
Thu Jun 23 12:36:55 2022 [Z0][HMM][I]: Successfully monitored VM: 10
Thu Jun 23 12:37:25 2022 [Z0][HMM][I]: Successfully monitored VM: 10
Thu Jun 23 12:38:02 2022 [Z0][HMM][D]: Monitoring host fn.brest.local(0)
```

Кроме того, в файле `/var/log/one/oned.log` также фиксируются сообщения, относящиеся к системе мониторинга.

Пример

```
Thu Jun 23 12:35:40 2022 [Z0][InM][D]: Monitoring datastore images-ds (100)
Thu Jun 23 12:35:40 2022 [Z0][InM][D]: Monitoring datastore system-ds (101)
Thu Jun 23 12:35:40 2022 [Z0][InM][D]: Monitoring datastore default (1)
Thu Jun 23 12:35:40 2022 [Z0][InM][D]: Monitoring datastore files (2)
...
Thu Jun 23 12:36:23 2022 [Z0][InM][D]: Host fn.brest.local (0)
    successfully monitored.
Thu Jun 23 12:36:26 2022 [Z0][InM][D]: Host fn.brest.local (0)
    successfully monitored.
Thu Jun 23 12:37:29 2022 [Z0][InM][D]: VM_STATE update from host: 0.
    VM id: 10, state: RUNNING
```

6.1.3. Настройка и расширение

6.1.3.1. Кодирование информации мониторинга

В ПК СВ можно включить кодирование сообщений, которые агенты мониторинга направляют на сервер управления. Для этого необходимо выполнить следующие действия:

1) на сервере управления войти в ОС СН под учетной записью администратора с уровнем целостности равным 127;

2) создать открытый и закрытый ключи, сохранив их, например, в каталог `/etc/one/`, командой:

```
sudo ssh-keygen -f /etc/one/onemonitor
```

Для всех параметров оставлять значения по умолчанию (сразу нажимать клавишу

<Enter>;

3) создать новый файл открытого ключа в формате PKCS#1 командой:

```
sudo ssh-keygen -f /etc/one/onemonitor.pub -e -m pem | \
    sudo tee /etc/one/onemonitor_pem.pub
```

4) в конфигурационном файле /etc/one/monitord.conf, в блоке настроек сетевого соединения указать абсолютные пути открытого и закрытого ключей;

Пример

```
NETWORK = [
...
    PUBKEY = "/etc/one/onemonitor_pem.pub",
    PRIKEY = "/etc/one/onemonitor"
    ]
```

5) перезапустить службу opennebula командой:

```
sudo systemctl restart opennebula
```

6) перезапустить агенты мониторинга на серверах виртуализации командой:

```
sudo -u oneadmin onehost sync -f
```

Пример вывода после выполнения команды:

```
* Adding fn.brest.local to upgrade
[========================================] 1/1 fn.brest.local
All hosts updated successfully.
```

Если для обеспечения отказоустойчивости службы сервера управления применяется технология Raft, то открытый и закрытый ключи, а также конфигурационный файл /etc/one/monitord.conf необходимо скопировать на другие экземпляры сервера управления. Для этого следует выполнить следующие действия:

1) скопировать файл закрытого ключа командой:

```
sudo scp /etc/one/onemonitor <сервер_управления>:/etc/one/
```

где <сервер_управления> — сетевое имя экземпляра сервера управления. Допускается вместо сетевого имени указать IP-адрес;

2) скопировать файл открытого ключа в формате PKCS#1 командой:

```
sudo scp /etc/one/onemonitor_pem.pub <сервер_управления>:/etc/one/
```

3) скопировать конфигурационный файл командой:

```
sudo scp /etc/one/monitord.conf <сервер_управления>:/etc/one/
```

4) на другом экземпляре сервера управления перезапустить запустить службу сервера управления командой:

```
sudo systemctl restart opennebula
```

6.1.3.2. Тесты

Тесты представляют собой специальные программы, которые обеспечивают получение контрольных показателей мониторинга. Конфигурационные файлы тестов определяются для каждого гипервизора. Для гипервизора KVM используется конфигурационный файл `/var/lib/one/remotes/etc/im/kvm-probes.d/probe_db.conf`. Следующие параметры доступны для корректировки значений:

1) `obsolete` — период времени (в минутах), по истечению которого информация о статусе ВМ считается устаревшей и будет удалена;

2) `times_missing` — количество тестов, завершившихся неудачей, после которых для ВМ устанавливается статус «недоступна».

Пример

Настройки теста для сервера виртуализации с гипервизором KVM, установленные по умолчанию

```
:obsolete: 720
:times_missing: 5
```

После внесения изменений в конфигурационные файлы тестов необходимо перезапустить агенты мониторинга на серверах виртуализации командой:

```
sudo -u oneadmin onehost sync -f
```

6.1.4. Получение информации о потреблении ресурсов

Для вывода информации о потреблении ресурсов сервера виртуализации используется команда:

```
onehost monitoring <идентификатор_сервера_виртуализации> \
      <параметр_мониторинга> <вид_отображения>
```

Описание параметров мониторинга приведено в таблице 28.

Таблица 28

Параметр	Описание
`FREE_CPU`	Количество свободных ЦП
`FREE_MEMORY`	Объем свободной памяти
`USED_CPU`	Количество ЦП, выделенных для работы всех ВМ
`USED_MEMORY`	Объем памяти, выделенной для работы всех ВМ
`NETRX`	Объем входящего сетевого трафика
`NETTX`	Объем исходящего сетевого трафика

Если не указывать вид отображения, то информация мониторинга будет выведена в виде графика (в ОС СН должен быть установлен пакет `gnuplot`). Кроме того, в качестве вида отображения информации мониторинга можно указать следующее:

- «--table» — табличный вид отображения;
- «--csv <символ_разделителя>» — отображение в формате csv.

Дополнительно можно указать следующие параметры отображения:

- «--n <количество>» — отображать указанное количество последних записей;
- «--unit <единицы_измерения>» — отображение в заданных единицах измерения (например, «G» — в гигабайтах);
- «--start <дата>» — отображать записи, начиная с указанной даты;
- «--end <дата>» — отображать записи, до указанной даты.

Примеры:

1. Отображения количества свободных ЦП в виде графика (в ОС СН должен быть установлен пакет gnuplot). Пример команды:

```
onehost monitoring 0 FREE_CPU --n 10 --unit G
```

Пример вывода после выполнения команды:

```
gnuplot 5.2 patchlevel 6
Host 0 FREE_CPU from 07/07/2022 10:00 to 07/07/2022 12:11
400 +-------------------------------------------------------------+
    |        +      **        +        +        +       +        |
395 |-+           ** *                 A        A              +-|
    |            *   *               ***       **               |
390 |-+         *    *              *  *      * *              +-|
    |          *     *            **   *     *  *               |
385 |-+       *      *           *     *    *   *              +-|
    |       **       *         **      *    *   *               |
380 |-+    *         *        *        *   *    *              +-|
375 |-+   *          *      **         *  *     *              +-|
    |    *           *     *           * *      *               |
370 |-+ *            *   **            **       *              **|
    | **             *  *              A        *        ******  |
365 |*+              ***                       *  ******      +-|
    |                A                         A**              |
360 |-+                                                       +-|
    |        +       +        +        +        +       +        |
355 +-------------------------------------------------------------+
12:04    12:05   12:06    12:07    12:08    12:09   12:10    12:11
```

2. Пример команды для отображения в виде таблицы:

```
onehost monitoring 0 FREE_CPU  --table --n 10 --unit G
```

Пример вывода после выполнения команды:

```
Host 0 FREE_CPU from 07/07/2022 10:00 to 07/07/2022 12:06
TIME VALUE
11:59 396
11:59 360
12:01 396
12:01 360
12:02 400
12:02 356
12:04 396
12:04 364
12:06 400
12:06 364
```

3. Пример команды для отображения в формате csv:

```
onehost monitoring 0 FREE_CPU  --csv ';' --n 10 --unit G
```

Пример вывода после выполнения команды:

```
TIME;VALUE
11:59;396
11:59;360
12:01;396
12:01;360
12:02;400
12:02;356
12:04;396
12:04;364
12:06;400
12:06;364
```

6.2. Логирование

6.2.1. Настройка системы регистрации

В ПК СВ обеспечивается ведение журналов для большинства ресурсов. Поддерживается три системы регистрации: файловая система регистрации, регистрация системных журналов и регистрация в стандартный поток ошибок. Для настройки системы регистрации используется блок настроек `LOG` в конфигурационном файле `/etc/one/oned.conf` (см. раздел 5).

При использовании файловой регистрации создаются отдельные файлы журналов для каждого активного компонента, при этом все они хранятся в каталоге `/var/log/one`. В качестве таких активных компонент могут выступать:

- служба `oned`, регистрационная информация которой выгружается в файл `/var/log/one/oned.log`;
- процесс системы мониторинга `onemonitord`, регистрационная информация кото-

рой выгружается в файл /var/log/one/monitor.log;

- виртуальные машины — информация, относящаяся к ВМ, будет выгружаться в файл журнала /var/log/one/<идентификатор_ВМ>.log.

6.2.2. Регистрационный формат

Сообщения для файловой системы регистрации имеют следующую структуру:

```
<дата> [Z<zone_id>][<module>][<log_level>]: <текст_сообщения>
```

где <zone_id> — идентификатор зоны при объединении экземпляров ПК СВ в единый ЦОХД (служебный режим «федерация»), для независимого экземпляра ПК СВ имеет значение «0»;

<module> — краткое наименование составной части ПК СВ (VMM — для ВМ, InM — для информационного драйвера, TM — для драйвера передачи данных и т.д.);

<log_level> — представляет собой отдельный символ, указывающий уровень регистрации: I — для информации, D — для отладки и т.д.

Пример

Сообщения для файловой системы регистрации представленные в файле /var/log/one/oned.log

```
Thu Jul 7 16:29:34 2022 [Z0][TrM][D]: Message received: TRANSFER SUCCESS 26 -/
    1 1
Thu Jul 7 16:29:34 2022 [Z0][VMM][I]: Successfully execute transfer manager /
   driver operation: tm_context.
Thu Jul 7 16:29:35 2022 [Z0][VMM][I]: ExitCode: 0
Thu Jul 7 16:29:35 2022 [Z0][VMM][I]: Successfully execute network driver /
   operation: pre.
Thu Jul 7 16:29:35 2022 [Z0][VMM][I]: Successfully execute virtualization /
   driver operation: /bin/mkdir -p.
Thu Jul 7 16:29:35 2022 [Z0][VMM][I]: Successfully execute virtualization /
   driver operation: /bin/cat - >/var/lib/one/vms/26/vm.xml.
Thu Jul 7 16:29:35 2022 [Z0][VMM][I]: Successfully execute virtualization /
   driver operation: /bin/cat - >/var/lib/one/vms/26/ds.xml.
Thu Jul 7 16:29:35 2022 [Z0][VMM][I]: Successfully execute virtualization /
   driver operation: deploy.
...
Thu Jul 7 16:30:25 2022 [Z0][InM][D]: Host fn.brest.local (0) successfully /
   monitored.
Thu Jul 7 16:30:27 2022 [Z0][InM][D]: Host fn.brest.local (0) successfully /
   monitored.
```

Сообщения для регистрации системных журналов имеют следующую структуру:

```
<дата> <имя_компьютера> process[<pid>]: [Z<zone_id>][module][log_level]:
```

```
   <текст_сообщения>
```

При этом сообщения о состоянии ВМ для регистрации системных журналов имеют следующую структуру:

```
<дата> <имя_компьютера> process[<pid>]: [<идентификатор_ВМ>][Z<zone_id>]
   [module][log_level]: <текст_сообщения>
```

Пример

Сообщения ПК СВ, представленные в файле /var/log/syslog

```
Jul 7 16:40:49 fn oned[25658]: [VM 26][Z0][VM][I]: New state is ACTIVE
Jul 7 16:40:49 fn oned[25658]: [VM 26][Z0][VM][I]: New LCM state is /
   BOOT_POWEROFF
Jul 7 16:40:49 fn oned[25658]: [VM 26][Z0][VMM][I]: Generating deployment /
   file: /var/lib/one/vms/26/deployment.1
...
Jul 7 16:40:50 fn oned[25658]: [Z0][VMM][I]: Successfully execute transfer /
   manager driver operation: tm_context.
Jul 7 16:40:50 fn oned[25658]: [Z0][VMM][I]: ExitCode: 0
Jul 7 16:40:50 fn oned[25658]: [Z0][VMM][I]: Successfully execute network /
   driver operation: pre.
Jul 7 16:40:50 fn oned[25658]: [Z0][VMM][I]: Successfully execute /
   virtualization driver operation: /bin/mkdir -p.
Jul 7 16:40:50 fn oned[25658]: [Z0][VMM][I]: Successfully execute /
   virtualization driver operation: /bin/cat - >/var/lib/one/vms/26/vm.xml.
Jul 7 16:40:50 fn oned[25658]: [Z0][VMM][I]: Successfully execute /
   virtualization driver operation: /bin/cat - >/var/lib/one/vms/26/ds.xml.
Jul 7 16:40:51 fn oned[25658]: [Z0][VMM][I]: Successfully execute /
   virtualization driver operation: deploy.
Jul 7 16:40:52 fn oned[25658]: [Z0][VMM][I]: ExitCode: 0
Jul 7 16:40:52 fn oned[25658]: [Z0][VMM][I]: Successfully execute network /
   driver operation: post.
Jul 7 16:40:52 fn oned[25658]: [VM 26][Z0][VM][I]: New LCM state is RUNNING
```

Сообщения для регистрации в стандартный поток ошибок имеют следующую структуру:

```
<дата> [Z<zone_id>][<module>][<log_level>]: <текст_сообщения>
<дата> [<идентификатор_ВМ>][Z<zone_id>][<module>][<log_level>]:
   <текст_сообщения>
```

Пример

Сообщения регистрации в стандартный поток ошибок:

```
Thu Jul 7 17:02:46 2022 [Z0][VMM][I]: ExitCode: 0
Thu Jul 7 17:02:46 2022 [Z0][VMM][I]: Successfully execute network driver /
   operation: clean.
Thu Jul 7 17:02:46 2022 [Z0][IPM][D]: Message received: SHUTDOWN SUCCESS 26 -/
```

```
    0 0
Thu Jul 7 17:02:46 2022 [VM 26][Z0][VM][I]: New state is POWEROFF
Thu Jul 7 17:02:46 2022 [VM 26][Z0][VM][I]: New LCM state is LCM_INIT
Thu Jul 7 17:03:06 2022 [Z0][InM][D]: Host fn.brest.local (0) successfully /
   monitored.
```

6.2.3. Вывод информации о виртуальной машине

Для получения информации о ВМ необходимо выполнить команду:

```
onevm show <идентификатор_ВМ>
```

Пример

Вывод информации о ВМ с идентификатором «0»:

```
VIRTUAL MACHINE 0 INFORMATION
ID : 0
NAME : tmp-for-install-os
USER : brest-admin
GROUP : brestadmins
STATE : DONE
LCM_STATE : LCM_INIT
LOCK : None
RESCHED : No
START TIME : 06/21 13:02:01
END TIME : 06/21 14:53:10
DEPLOY ID : 12ba00af-4eda-49a1-bd29-7efc1df27b77
...
USER TEMPLATE
AUTOSTARTVM="0"
HOT_RESIZE=[
CPU_HOT_ADD_ENABLED="NO",
MEMORY_HOT_ADD_ENABLED="NO" ]
HYPERVISOR="kvm"
INPUTS_ORDER=""
MEMORY_UNIT_COST="MB"
SCHED_DS_REQUIREMENTS="ID=\"0\""
SCHED_MESSAGE="Thu Jun 23 17:18:34 2022: Cannot dispatch VM to any Host. /
   Possible reasons: Not enough capacity in Host or System DS, dispatch limit/
    reached, or limit of free leases reached."
SERVICEUSERVM="0"
```

Ошибка, приведенная в примере (поле SCHED_MESSAGE), указывает на то, что было невозможно разместить ВМ на сервере виртуализации, возможно недостаточно свободных вычислительных ресурсов.

6.2.4. Вывод информации об сервере виртуализации

Для получения информации об сервере виртуализации необходимо выполнить команду:

```
onehost show <идентификатор_сервера_виртуализации>
```

Пример

Вывод информации об сервере виртуализации с идентификатором «0»:

```
HOST 0 INFORMATION
ID : 0
NAME : fn.brest.local
CLUSTER : default
STATE : MONITORED
IM_MAD : kvm
VM_MAD : kvm
LAST MONITORING TIME : 07/07 14:57:49

HOST SHARES
RUNNING VMS : 2
MEMORY
      TOTAL : 5.8G
      TOTAL +/- RESERVED : 5.8G
      USED (REAL) : 3.3G
      USED (ALLOCATED) : 4G
CPU
      TOTAL : 400
      TOTAL +/- RESERVED : 400
      USED (REAL) : 44
      USED (ALLOCATED) : 50

LOCAL SYSTEM DATASTORE #0 CAPACITY
TOTAL: : 61.8G
USED: : 24.2G
FREE: : 34.5G
...

VIRTUAL MACHINES

ID USER  GROUP NAME STAT CPU MEM HOST TIME
25 brest-ad brestadm ALSE runn 0.25 2G fn.brest.local 13d 02h22
24 brest-ad brestadm ALCE runn 0.25 2G fn.brest.local 13d 02h31
```

7. ИНТЕГРАЦИЯ В ЕДИНЫЙ ЦОХД («ФЕДЕРАЦИЯ»)

7.1. Общие сведения

Несколько экземпляров ПК СВ могут быть объединены в единый центр обработки и хранения данных (ЦОХД), который называется «федерация». В этом случае каждый экземпляр ПК СВ называется зоной. Один из экземпляров ПК СВ настраивается как ведущий, остальные — ведомые.

«Федерация» позволяет конечным пользователям использовать ресурсы, распределенные Администраторами единого ЦОХД, независимо от места их нахождения. Интеграция проходит комплексно, то есть пользователю, авторизованному в веб-интерфейсе определенной зоны, не придется выходить из системы и вводить адрес другой зоны. веб-интерфейс ПК СВ позволяет изменять активную зону в любое время, а также автоматически перенаправляет запросы в ПК СВ в целевой зоне.

Служебный режим «федерация» является интеграцией с непосредственными связями. Все экземпляры ПК СВ имеют общую конфигурацию (общие таблицы БД) учетных записей пользователей, групп и полномочий. Доступ возможно ограничить до конкретных зон, а также до конкретных кластеров внутри данной зоны. Только ведущая зона ПК СВ имеет права на внесение записей в общие таблицы, у ведомых зон хранится локальная копия для чтения. Это гарантирует целостность данных без ущерба для скорости действий по считыванию.

Синхронизация выполняется путем настройки конфигурации ПК СВ для репликации только определенных таблиц. Репликация способна работать при соединениях на больших расстояниях и при нестабильных соединениях. В случае сбоя ведущей зоны и ее длительной перезагрузки ведомые зоны могут продолжать работать в нормальном режиме, за исключением нескольких действий, например, создание нового пользователя или обновление паролей.

Новые ведомые зоны можно добавлять к существующей «федерации» в любой момент. Кроме того, администратор ПК СВ может добавить абсолютно новый экземпляр ПК СВ или импортировать существующую развертку в «федерацию», сохранив действующих пользователей, групп, конфигурацию и виртуальные ресурсы.

Что касается обновлений ПК СВ, БД разработана таким образом, чтобы различные версии ПК СВ являлись частью одной и той же «федерации». При необходимости обновить локальные таблицы (ВМ, Образ, объекты VNet) новые версии сохранят совместимость с общими таблицами. На практике это означает, что в случае выхода новой версии ПК СВ можно обновить каждую зону в разное время без каких-либо последствий для «федерации».

Служба веб-интерфейса ПК СВ ведущей зоны подключена ко всем экземплярам

службы `oned` в «федерации», что позволяет пользователям менять зоны. Возможно использовать один веб-интерфейс ПК СВ для всей «федерации» или в каждой зоне использовать свой веб-интерфейс ПК СВ (рис. 5).

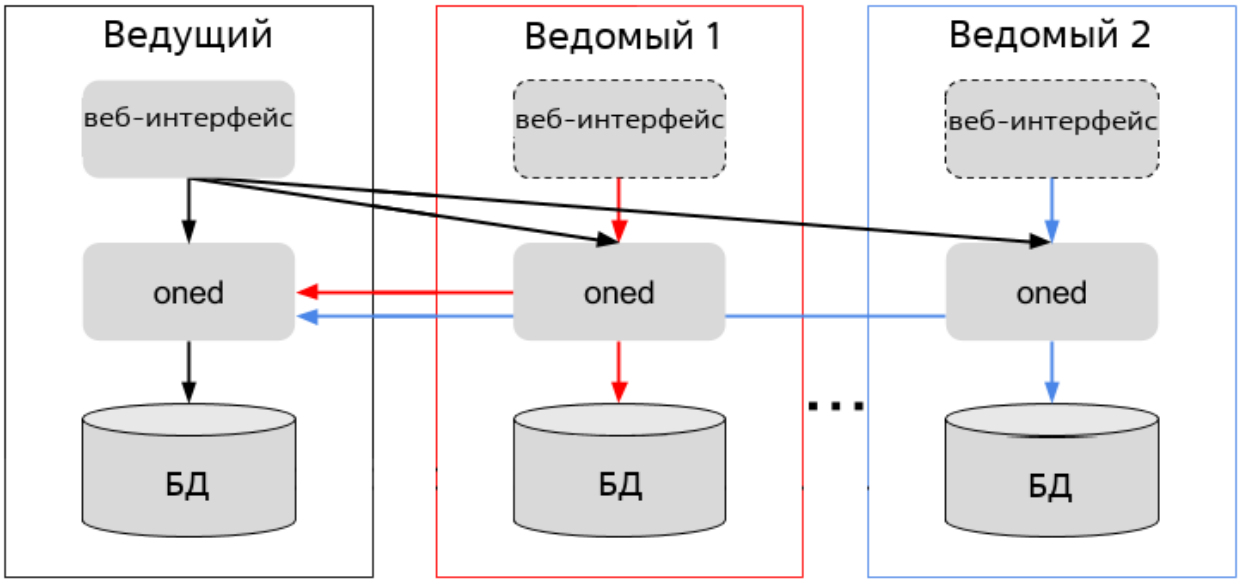

Рис. 5

ВНИМАНИЕ! Несмотря на то, что одна служба веб-интерфейса ПК СВ может подключаться к различным зонам, все остальные службы ПК СВ будут работать только с локальными ресурсами зоны.

В «федерации» зарегистрирован уникальный пользователь `oneadmin`, обладающий правами администратора ПК СВ и являющийся администратором «федерации». В безопасной среде администратор каждой зоны включается в группу `oneadmin`. В других сценариях администратор «федерации» может создать специальную административную группу с полными правами доступа только для одной зоны.

Администраторы могут совместно использовать устройства в зонах благодаря службе «Магазин приложений».

7.2. Настройка «федерации»

Особенности использования служебного режима «федерация»:

- на всех серверах и во всех зонах в конфигурационном файле `/etc/one/one.d/db.conf`:
  - имя пользователя пользователя БД должно иметь значение `oneadmin`;
  - наименования БД должны совпадать;
- во всех экземплярах ПК СВ не должен использоваться алгоритм RAFT (поддерживается только один экземпляр сервера управления на зону).

ВНИМАНИЕ! Действия по настройке «федерации» выполняются в ОС сервера

управления каждой зоны под учетной записью администратора ОС СН с высоким уровнем целостности.

Предварительно необходимо настроить беспарольный доступ для пользователя root. Для этого следует выполнить следующие действия:

1) на каждом экземпляре сервера управления создать ssh-ключ от имени пользователя root командой:

```
sudo ssh-keygen -t rsa
```

Для всех параметров оставлять значения по умолчанию (сразу нажимать клавишу **<Enter>**;

2) на каждом экземпляре сервера управления выполнить обмен ключами командами:

```
KEY=$(sudo cat /root/.ssh/id_rsa.pub)
sudo ssh <имя_администратора>@<имя_ведущего_сервера> \
    "sudo bash -c \"echo $KEY >>    /root/.ssh/authorized_keys\""
sudo ssh <имя_администратора>@<имя_ведомого_сервера_1> \
    "sudo bash -c \"echo $KEY >> /root/.ssh/authorized_keys\""
...
sudo ssh <имя_администратора>@<имя_ведомого_сервера_N> \
   "sudo bash -c \"echo $KEY >> /root/.ssh/authorized_keys\""
```

где <имя_ведущего_сервера> — сетевое имя (hostname) сервера управления ведущей зоны. Допускается вместо имен указывать IP-адреса;

имя_ведомого_сервера_N — сетевое имя (hostname) сервера управления ведомой зоны. Допускается вместо имен указывать IP-адреса;

<имя_администратора> — имя локального администратора компьютера, заданное при установке ОС СН;

а) при появлении приглашения для ввода вида:

```
Are you sure you want to continue connecting (yes/no)?
```

ввести «yes» и нажать клавишу **<Enter>**;

б) ввести пароль локального администратора компьютера, заданный при установке ОС СН.

ВНИМАНИЕ! В том числе необходимо выполнить обмен ключами «сам на себя»;

3) проверить обмен ключами, для этого:

а) в терминале сервера управления ведущей зоны выполнить вход по ssh «сам на себя» командой:

```
sudo ssh <имя_ведущего_сервера>
```

б) выполнить вход по ssh на один из экземпляр сервера управления командой:

```
sudo ssh <имя_ведомого_сервера_N>
```

в) последовательно закрыть сессии ssh командами:

```
exit
exit
```

4) аналогичным образом проверить беспарольный доступ на остальных экземплярах сервера управления.

Для автоматической настройки «федерации» можно воспользоваться скриптом `brestcloud-federation-configure`, который запускается на сервере управления ведущей зоны от имени администратора ОС СН с высоким уровнем целостности командой:

```
sudo  brestcloud-federation-configure
```

Далее необходимо следовать указаниями мастера настройки.

Примечание. В списке серверов необходимо указывать только ведомые сервера (ведущий сервер добавляется первым в список автоматически).

ПЕРЕЧЕНЬ ТЕРМИНОВ

Администратор ОС СН — пользователь ОС СН, входящий в группу `astra-admin`, которому предоставляются права для выполнения действий по настройке ОС, требующих привилегий суперпользователя `root`.

Администратор ПК СВ — пользователь, реализующий роль администратора средства виртуализации.

Примечание. Описание ролей пользователей представлено в документе РДЦП.10001-02 97 01 «Программный комплекс «Средства виртуализации «Брест». Руководство по КСЗ».

Администратор Ceph-кластера — пользователь ОС СН, которому предоставляются права для выполнения действий по настройке и управлению Ceph-кластером.

Примечание. Порядок создания учетной записи администратора Ceph-кластера представлен в документе РУСБ.10015-01 95 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1».

Закрытый ключ — сохраняемый в тайне ключ из ключевой пары.

Примечание. Не предназначен для защиты информации в контексте использования по предназначению ПК СВ. К ключам не предъявляются требования по источнику псевдослучайных чисел, криптографической стойкости, времени действия и т.п.

Ключ — параметр в виде последовательности псевдослучайных чисел.

Примечание. Не предназначен для защиты информации в контексте использования по предназначению ПК СВ. К ключам не предъявляются требования по источнику псевдослучайных чисел, криптографической стойкости, времени действия и т.п.

Ключевая пара — упорядоченная пара математически однозначно связанных ключей, определяющих взаимосвязанные защитные преобразования.

Кодирование — защитное преобразование с помощью кода.

Локальный администратор компьютера — администратор ОС СН, установленной на компьютере.

Открытый ключ — ключ из ключевой пары, который может быть сделан общедоступным.

Примечание. Не предназначен для защиты информации в контексте использования по предназначению ПК СВ. К ключам не предъявляются требования по источнику псевдослучайных чисел, криптографической стойкости, времени действия и т.п.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД — база данных
ВМ — виртуальная машина
ОС — операционная система
ОС СН — операционная система специального назначения «Astra Linux Special Edition»
ПК СВ — программный комплекс «Средства виртуализации «Брест»
ФС — файловая система
ЦОХД — центр обработки и хранения данных
ЦП — центральный процессор

CLVM — Clustered Logical Volume Manager (кластерное управление логическими томами)
CPU — Central Processing Unit (центральный процессор)
iSCSI — Internet Small Computer System Interface (протокол на базе TCP/IP для взаимодействия и управления системам хранения данных, серверов и клиентов)
KVM — Kernel-based Virtual Machine (программное решение, обеспечивающее виртуализацию в среде Linux на платформе, которая поддерживает аппаратную виртуализацию на базе Intel VT (Virtualization Technology) либо AMD SVM (Secure Virtual Machine))
LUN — Logical Unit Number (номер объекта внутри цели (target))
LV — Logical Volume (логический том)
LVM — Logical Volume Manager (менеджер логических томов)
MON — Monitor (системный процесс, отслеживающий состояние кластера Ceph)
NFS — Network File System (сетевая файловая система)
OSD — Object Storage Device (основное устройстве хранения объектов Ceph, обычно связанное с одним физическим диском, в котором хранятся фактические данные пользователя)
OVS — Open vSwitch (программный многоуровневый коммутатор для работы в гипервизорах и на компьютерах с виртуальными машинами)
OVSDB — база данных OVS
QEMU — Quick Emulator (средства эмуляции аппаратного обеспечения)
RADOS — Reliable Autonomic Distributed Object Store (хранилище, отвечающее за хранение объектов кластера Ceph независимо от их типа данных)
RBD — Rados block device (блочное хранилище кластера Ceph, которое может отображаться, форматироваться и монтироваться в точности как любой другой диск в сервере)
RDM — Raw Device Mapping (используется для прямого подключения к виртуальной

машине существующих блочных устройств сервера виртуализации)

SAN — Storage Area Network (сеть хранения данных)

SCSI — Small Computer System Interface (системный интерфейс малых компьютеров)

SSH — Secure Shell Protocol (протокол защищенной передачи информации)

TM — Transfer Manager (драйвер передачи)

UDP — User Datagram Protocol (протокол пользовательских дейтаграмм)

UUID — Universally Unique Identifier (универсальный уникальный идентификатор)

VLAN — Virtual Local Area Network (виртуальная локальная вычислительная сеть)

VNC — Virtual Network Computing (система удаленного доступа к рабочему столу компьютера)

VXLAN — Virtual Extensible Local Area Network (виртуальная масштабируемая локальная вычислительная сеть)

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					
1		Все				РДЦП.03-22 от 03.11.2022			
2		Все				РДЦП.06-23 от 22.09.2023			