УТВЕРЖДЕН

ДСБР.30001-01 34 01-ЛУ

ОБЛАЧНАЯ ПЛАТФОРМА «SPACEVM»

Руководство оператора

ДСБР.30001-01 34 01

Листов 399

2022

Литера

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

АННОТАЦИЯ

Данный документ является руководством оператора для облачной платформы «SpaceVM», которая предназначена для создания и администрирования виртуальной инфраструктуры для аппаратных платформ на базе процессоров x86 с аппаратной поддержкой виртуализации, далее по тексту – SpaceVM или программа.

Документ описывает назначение, условия и порядок функционирования SpaceVM, а также действия оператора при запуске и во время выполнения программы. Документ не содержит рисунков и является дополнением к действиям оператора на ПЭВМ, поэтому работа с ним должна сопровождаться аналогичными операциями в оконном интерфейсе SpaceVM.

Настоящее руководство оператора входит в состав эксплуатационной документации и рассчитано на пользователя, имеющего навыки работы на ПЭВМ в операционной системе (ОС) Linux.

СОДЕРЖАНИЕ

Лист

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. SpaceVM предназначена для создания и администрирования виртуальной инфраструктуры для аппаратных платформ на базе процессоров x86 с аппаратной поддержкой виртуализации.

1.2. SpaceVM обеспечивает создание и администрирование виртуальной инфраструктуры как на отдельной серверной платформе, так и на кластерной системе (группе серверных платформ).

1.3. SpaceVM обеспечивает возможность автоматической настройки нового физического сервера в момент добавления его в кластер.

1.4. SpaceVM обеспечивает создание и управление следующими типами объектов:

– физический сервер;

– виртуальная машина (ВМ);

– виртуальная сеть;

– пул хранения данных;

– виртуальный диск;

– образ оптического диска;

– шаблон виртуальной машины.

1.5. SpaceVM поддерживает запуск гостевых операционных систем (ОС) для архитектуры x86_64.

1.6. SpaceVM обеспечивает возможность инсталляции ОС внутри ВМ с образа оптического диска в формате ISO 9660 и UDF.

1.7. SpaceVM обеспечивает создание, хранение и импорт шаблонов ВМ для автоматического развертывания ВМ.

1.8. SpaceVM обеспечивает создание шаблона ВМ из виртуальной машины, инсталлированной с образа оптического диска.

1.9. SpaceVM обеспечивает для платформ, имеющих аппаратную поддержку виртуализации, возможность монополизации виртуальными машинами физических компонентов аппаратной платформы, подключенных к интерфейсам SATA, PCI, PCI-E, USB, Serial.

1.10. SpaceVM обеспечивает использование в качестве пулов хранения данных:

– необщие хранилища;

– общие хранилища.

1.11. SpaceVM обеспечивает использование локальных групп логических томов (LVM – Logical Volume Manager) на вычислительных узлах в качестве локальных хранилищ данных.

1.12. SpaceVM обеспечивает использование внешних систем хранения данных, подключаемых по протоколу NFS, в качестве общих хранилищ.

1.13. SpaceVM обеспечивает использование распределенных хранилищ данных в качестве общих хранилищ.

1.14. SpaceVM обеспечивает возможность переноса ВМ между физическими серверами, объединенными в кластер, находящимся под управлением одного экземпляра SpaceVM.

1.15. SpaceVM обеспечивает поддержку переноса виртуальных дисков между пулами хранения данных.

1.16. SpaceVM при помощи средств интерфейса управления обеспечивает выполнение следующих операций:

– создание ВМ из шаблона;

– уничтожение ВМ (с сохранением ее виртуального жесткого диска и без него);

– редактирование параметров ВМ;

– создание шаблона ВМ;

– запуск ВМ;

– остановка ВМ;

– перезагрузка ВМ;

– клонирование ВМ;

– создание копии состояния ВМ (снэпшот ВМ);

– восстановление состояния текущей ВМ из копии;

– создание новой ВМ из копии состояния.

1.17. SpaceVM при создании ВМ обеспечивает возможность задания следующих параметров:

– имя ВМ;

– описание ВМ;

– количество виртуальных процессоров;

– количество оперативной памяти;

– количество дискового пространства;

– количество сетевых интерфейсов и их сопоставление с виртуальными сетями;

– имя шаблона (при создании из шаблона);

– вычислительный узел для запуска ВМ (из состава кластера);

– выбор существующего или создание нового виртуального диска;

– пул для хранения виртуального диска.

1.18. SpaceVM обеспечивает возможность опционально задавать количество виртуальных процессоров при создании ВМ.

1.19. SpaceVM при помощи средств интерфейса управления обеспечивает выполнение следующих операций над виртуальными дисками:

– создание;

– уничтожение;

– клонирование;

– перенос виртуального диска в другой пул хранения данных;

– подключение диска к ВМ;

– отключение диска от ВМ.

1.20. SpaceVM при создании виртуального диска обеспечивает возможность задать следующие параметры:

– имя виртуального диска;

– пул хранения для размещения виртуального диска;

– количество дисковой памяти.

1.21. SpaceVM обеспечивает возможность работы ВМ в режиме высокой доступности. Работа ВМ в режиме высокой доступности осуществляется путем автоматического перезапуска на резервном вычислительном узле виртуальных машин, которые были запущены на отказавшем вычислительном узле.

Примечания:

1. Работа ВМ в режиме высокой доступности возможна только при хранении виртуальных дисков данной ВМ на общем хранилище.

2. Высокая доступность обеспечивается только при объединении физических серверов в кластерную систему.

1.22. SpaceVM обеспечивает время запуска процедуры восстановления работы ВМ, запущенной в режиме высокой доступности, не более 5 мин.

1.23. SpaceVM обеспечивает возможность создания изолированных виртуальных сетей между ВМ.

1.24. SpaceVM для управления использует Web-ориентированный графический интерфейс и REST-API.

1.25. SpaceVM обеспечивает возможность шифрования канала управления средствами протокола HTTPS.

1.26. SpaceVM обеспечивает вывод в интерфейс управления информации о текущем состоянии каждого физического сервера в кластере. Информация о каждом физическом сервере содержит:

– имя хоста;

– описание хоста;

– текущее состояние (доступен, недоступен);

– время последнего изменения состояния;

– количество запущенных ВМ;

– загрузка процессора (в процентах);

– количество свободной оперативной памяти;

– загрузка дисковой подсистемы;

– состояние локально подключенных дисков и количество свободного места на них;

– загрузка сетевых интерфейсов.

1.27. SpaceVM обеспечивает вывод в интерфейс управления следующей информации о каждой ВМ:

– имя ВМ;

– описание ВМ;

– текущее состояние;

– время последнего изменения состояния;

– время с момента включения;

– время создания ВМ;

– время последнего запуска (остановки) ВМ;

– пользователь, создавший ВМ;

– загрузка процессоров ВМ (в процентах);

– загрузка сетевых интерфейсов ВМ;

– загрузка дисковой подсистемы ВМ.

1.28. SpaceVM обеспечивает возможность создания нескольких типов учетных записей с различным уровнем привилегий.

1.29. SpaceVM обеспечивает занесение в журнал записей о следующих событиях:

– авторизация пользователя в интерфейсе управления;

– ошибка аутентификации пользователя;

– запуск контроллера;

– изменение состояния физического сервера;

– добавление нового физического сервера;

– удаление физического сервера;

– время создания ВМ;

– запуск ВМ;

– остановка ВМ;

– уничтожение ВМ;

– миграция ВМ;

– создание копии состояния ВМ (снэпшот ВМ);

– клонирование ВМ.

1.30. SpaceVM обеспечивает возможность настройки IP-адреса или доменного имени файлового хранилища.

1.31. SpaceVM обеспечивает добавление:

– пользователей к организации;

– виртуальных сетей к организации.

1.32. SpaceVM обеспечивает настройку и вызов задач по расписанию для создания резервной копии базы данных контроллера.

1.33. SpaceVM обеспечивает создание политики фильтрации при создании виртуальной сети, на основе выбранной из существующих.

1.34. SpaceVM обеспечивает групповое добавление ВМ в виртуальную сеть из меню виртуальной сети.

1.35. SpaceVM обеспечивает выбор физического подключения через виртуальный коммутатор или внешнюю сеть.

1.36. SpaceVM обеспечивает добавление внутреннего интерфейса при создании внешней сети.

1.37. SpaceVM обеспечивает возможность:

– группового переноса виртуальных дисков;

– группового удаления ZFS-пулов;

– группового переноса дисков включенной ВМ;

– групповой миграции ВМ с выбором кластера.

1.38. SpaceVM обеспечивает возможность настройки переподписки vCPU на ядро для ВМ.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. SpaceVM функционирует на базе средств вычислительной техники с характеристиками:

– процессор – не менее двух ядер, частота – не менее 2 ГГц;

– оперативная память – не менее 20 Гбайт;

– постоянное запоминающее устройство – не менее 32 Гбайт (рекомендуется 120 Гбайт);

– интерфейсы сетевые – не менее одного интерфейса 1 Гбит Ethernet.

Примечание. Расчет необходимого места под хранение журналов и статистики на контроллере можно произвести согласно руководству системного программиста ДСБР.30001-01 32 01.

2.2. SpaceVM предназначена для использования на серверных платформах с архитектурой x86–64.

2.3. Аппаратные требования к физическому серверу:

– материнская (процессорная) плата и процессор должны поддерживать технологию аппаратной виртуализации – VT-d и VT-x для Intel, AMD-v для AMD или другую аналогичную технологию;

– каждый процессор должен иметь не менее четырех вычислительных потоков;

– объем установленной оперативной памяти должен быть не менее 20 Гбайт;

– каждый сервер должен иметь возможность установки не менее одного накопителя на жестком магнитном диске (НЖМД) с интерфейсом SATA/SAS;

– объем каждого установленного НЖМД должен быть не менее 120 Гбайт;

– при установке более одного НЖМД все установленные НЖМД должны быть однотипными;

– каждый сервер должен иметь интерфейс управления Intelligent Platform Management Interface (IPMI);

– каждый имеющийся в системе сетевой интерфейс (кроме IPMI) должен поддерживать технологии не менее 1 Гбит Ethernet и Jumbo Frame;

– каждый сервер должен иметь не менее одного полноценного интерфейса PCIe для установки дополнительного сетевого адаптера.

2.4. Для установки SpaceVM на физический сервер необходимо, чтобы данный сервер обладал портом или устройством в соответствии с выбранным методом установки:

– для установки с CD/DVD-диска должен быть внутренний или внешний CD/DVD-привод, а также возможность выбора в BIOS сервера загрузки с диска;

– для установки с USB-накопителя должен быть USB-порт, а также возможность выбора в BIOS сервера загрузки с USB;

– для установки по сети должен быть сетевой интерфейс с поддержкой загрузки по протоколу PXE (Preboot Execution Environment), а также возможность выбора в BIOS сервера загрузки по сети;

– для установки через IPMI-интерфейс в IPMI-интерфейсе должна быть поддержка подключения ISO-образа для загрузки.

2.5. Программные (функциональные) требования к физическому серверу:

– для работы в штатном режиме используется кластер серверов, состоящий не менее чем из трех физических серверов для среды выполнения ВМ;

– допускается эксплуатация SpaceVM в составе двух физических серверов с (без) сетью хранения данных с применением ограниченного функционала управления.

Примечание. Ограниченный функционал управления заключается в переводе в ручной режим управляющих механизмов миграции ВМ, отказоустойчивости и распределения ВМ по серверам.

2.6. Для корректной и полноценной работы SpaceVM необходимо:

– не менее одного выделенного интерфейса IPMI;

– не менее одного интерфейса 1 Гбит Ethernet;

– не менее одного интерфейса 10 Гбит Ethernet.

Примечание. Допускается использование двух интерфейсов 1 Гбит Ethernet с ограничением скорости работы операций миграции и дисковых операций ВМ, диски которых находятся на внешних (общих) хранилищах.

2.7. Для дисковых подсистем серверов общего назначения, применяемых для хранения данных ВМ, применяются те же требования, что и для сервисов, исполняемых внутри самих ВМ.

2.8. Для выбора памяти на серверах кластера SpaceVM необходимо учитывать, что для одной ВМ может быть выделено виртуальной памяти не более, чем установленной физической памяти.

ВНИМАНИЕ! В случае необходимости использования технологий VT-d/AMD-Vi (Intel IOMMU, AMD IOMMU) для проброса PCI-устройств либо виртуальных функций (SR-IOV, vGPU, GVT-g) следует убедиться, что в системе отсутствуют либо не используются PCI-e NVMe/SATA контроллеры на чипах Marvell 88SE9120, 88SE9123, 88SE9125, 88SE9128, 88SE9130, 88SE9143, 88SE9172, 88SE9215, 88SE9220, 88SE9230, 88SE9485, PCI-X контроллеры на чипе 88SX6081. В случае крайней необходимости использования этих контроллеров следует убедиться, что в BIOS машины отключена технология VT-d/AMD-Vi (SR-IOV в DELL BIOS). В противном случае устройства, подключенные к данным контроллерам, могут быть недоступны, данные на них могут быть повреждены, и система может работать нестабильно.

2.9. Для установки SpaceVM не требуется отдельной установки базовой ОС общего назначения. Установка модулей SpaceVM производится с дистрибутива непосредственно на физический сервер без предварительной установки дополнительного программного обеспечения (ПО).

2.10. Для работы в Web-интерфейсе необходимо наличие ПЭВМ (клиента) и браузера со следующими характеристиками:

– браузер поддерживает протоколы HTTP/HTTPS;

– браузер поддерживает исполнение HTML5, TypeScript и JavaScript кода;

– браузер позволяет интерфейсу управления открывать дополнительные окна (вкладки).

Примечание. Необходимо обеспечить связь между сервером SpaceVM и клиентом (например, при помощи Ethernet-соединения, локальной сети, сети Интернет).

2.11. Физические границы SpaceVM приведены на рис. 1.

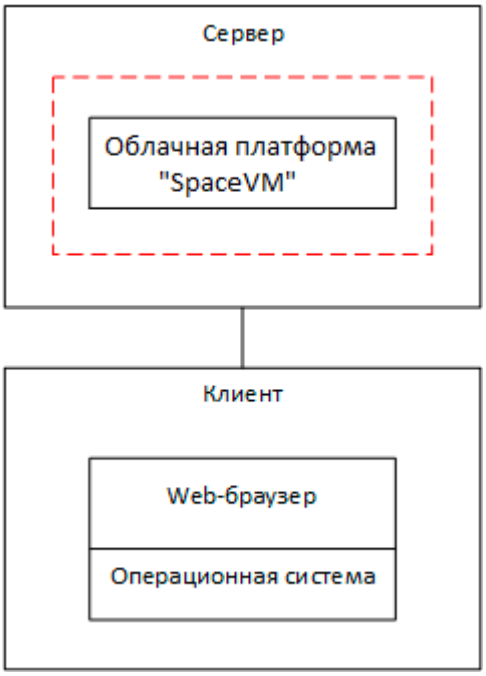

Рис. 1

2.12. В состав программного обеспечения (ПО) SpaceVM входят все компоненты, которые необходимы для его корректного функционирования. При соблюдении требования установки (обновления) ПО только с репозиториев разработчика гарантируется корректное функционирование SpaceVM. При необходимости использования дополнительного (стороннего) ПО необходимо связаться со службой технической поддержки разработчика.

2.13. Специалист, производящий установку SpaceVM, должен обладать знаниями, соответствующими специализации «Администратор Linux», «Администратор сетей передачи данных» в областях:

– установка ОС Linux семейства Debian/Ubuntu;

– настройка ОС Linux семейства Debian/Ubuntu;

– настройка и эксплуатация систем на базе Linux KVM;

– основы построения сетей передачи данных TCP/IP, VLAN, настройка поддержки Jumbo Frame, LACP, VLAN на коммутаторах.

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Подготовка к работе

3.1.1. Перед началом работы пользователю необходимо у администратора системы виртуализации получить параметры авторизации (имя учетной записи и пароль), с которыми он в дальнейшем будет работать.

3.1.2. Если учетная запись не была создана, то необходимо воспользоваться учетной записью администратора.

3.1.3. Если не производилась первоначальная настройка кластера, то ее необходимо выполнить в следующем порядке:

– установить SpaceVM на все серверы. Установка выполняется в соответствии с разделом 3 руководства системного программиста ДСБР.30001-01 32 01;

– добавить все серверы в кластер, используя Web-интерфейс (3.6.2 данного руководства);

– подключить сетевые (общие) хранилища (3.9.9 данного руководства);

– при необходимости использования высокой доступности (ВД) или другого функционала, недоступного для базового кластера, создать дополнительный кластер и перенести в него серверы (3.6.2 данного руководства);

– при управлении одним контроллером группами серверов, сети управления которых отличаются (находятся в разных центрах обработки данных (ЦОД)), внести в разделе «Сети» – «Сетевые настройки» для сети управления контроллера статические маршруты до сетей управления остальных групп серверов. Настройка маршрутизации для серверов другой сети управления производится из Command Line Interface (CLI) серверов группы перед их добавлением к контроллеру (3.10.2.6 данного руководства);

– при необходимости использования второго (резервного) контроллера произвести настройку репликации данных (из CLI). Более полное описание приведено в руководстве системного программиста ДСБР.30001-01 32 01;

– при необходимости создать и настроить дополнительные коммутаторы, группы интерфейсов (3.10.2.6 данного руководства);

– для формирования L2-сетевой связанности между локациями настроить туннель (3.10.2.6 данного руководства);

– создать и настроить виртуальные машины (3.8.1 данного руководства).

3.2. Общие правила при работе с программой

3.2.1. При работе с программой ВАЖНО знать:

– ряд объектов кластера помимо функции штатного удаления имеют опцию форсированного удаления;

– форсированное удаление объектов кластера должно производиться только компетентным сотрудником. При форсированном удалении не выполняется проверка состояния и связанности удаляемого объекта с другими объектами кластера. Фактически данная операция удаляет запись об объекте из базы данных (БД) кластера, что может нарушить работу связанных объектов и (или) привести к потере данных;

– восстановление объектов кластера, удаленных таким образом, невозможно, так как все объекты кластера имеют уникальный идентификатор, генерируемый при создании объекта. Созданный заново объект будет иметь новый идентификатор.

3.2.2. При создании объектов кластера рекомендуется ознакомиться с предельными значениями, приведенными в приложении 1 данного руководства.

3.2.3. Все действия выполняются одинарным нажатием левой клавиши графического манипулятора (далее по тексту – нажатием клавиши) на объект (его изображение или название), на который в данный момент указывает курсор. При этом открываются окна с информацией о состоянии (свойствах) любого объекта кластера, для которого такое окно предусмотрено. Если открытие окна не произошло, значит оно не предусмотрено для этого объекта.

3.2.4. Для комфортной работы с интерфейсом программы рекомендуется разрешение экрана 1920*1080. При меньшем разрешении экрана часть элементов интерфейса может быть скрыта.

3.3. Включение программы

3.3.1. Включение программы происходит с помощью запуска сервера (впоследствии ВМ) контроллера кластера, на котором располагается менеджер конфигурации (МК). В процессе запуска контроллера автоматически запускаются все службы и сервисы, необходимые для его работы, и становится доступным интерфейс системы управления МК.

3.3.2. Для начала работы пользователю необходимо авторизоваться в системе управления. Для этого необходимо выполнить следующие действия:

1) проверить следующие возможности браузера, установленного на автоматизированном рабочем месте (АРМ), для нормального функционирования интерфейса управления:

– браузер поддерживает протоколы HTTP/HTTPS;

– браузер поддерживает исполнение HTML5, TypeScript и JavaScript кода;

– браузер позволяет интерфейсу управления открывать дополнительные окна (вкладки);

2) осуществить доступ к Web-интерфейсу управления кластером. Для этого пользователю необходимо ввести в строке адреса браузера адрес МК, который был настроен при установке SpaceVM.

Примечания:

1. Если было использовано значение «по умолчанию», то IP-адрес интерфейсу управления назначается автоматически.

2. После установки доступ к Web-интерфейсу автоматически перенаправляется на протокол HTTP.

3. Первоначально для доступа по HTTPS используется самоподписанный сертификат, созданный автоматически в процессе установки ПО. Для корректной работы необходимо заменить HTTPS-сертификат на валидируемый локальным или глобальным центром сертификации;

3) в Web-интерфейсе управления кластером ввести имя учетной записи и пароля, а также отметить необходимость использования LDAP и выбрать язык (из списка);

4) после первой авторизации в системе в Web-интерфейсе необходимо ввести лицензионный ключ. Для этого необходимо перейти в раздел «Настройки» – «Лицензирование» и в окне управления лицензиями нажать на кнопку «Выбрать файл лицензии». В стандартном окне загрузки файлов выбрать нужную лицензию и нажать на кнопку «Открыть».

Более подробная информация приведена в разделе 3 руководства системного программиста ДСБР.30001-01 32 01;

5) после успешной авторизации пользователь переходит в основное окно интерфейса. При установке автоматически создается базовая локация «default location» с базовым кластером «default cluster».

3.4. Окно интерфейса

3.4.1. Основное окно

3.4.1.1. В основном окне интерфейса содержится сетевая инфраструктура базовой локации, включающая информацию об объектах, существующих в системе:

– кластеры;

– серверы;

– виртуальные машины;

– пулы данных;

– файловые сетевые хранилища;

– блочные сетевые хранилища;

– контроллеры.

Также в этом окне имеются графики, отображающие основные показатели загрузки в реальном времени. Отображаемая загрузка процессоров и памяти кластера указана в процентах от общего количества физических процессоров и памяти в кластере. Индивидуальная загрузка для каждого сервера отображается во вкладке информации о сервере.

При нажатии кнопки  происходит автоматическое обновление графиков.

При нажатии кнопки  в открывшемся окне существует возможность:

– задать начало и конец графика путем выбора даты и времени в открывающемся календаре;

– задать интервал между точками;

– сброса – выполняется автоматически при нажатии кнопки «Сбросить»;

– применения настроек – выполняется автоматически при нажатии кнопки «Применить».

3.4.1.2. Для того чтобы сразу перейти к объектам инфраструктуры, необходимо нажать на верхнюю строчку с названием объекта и кнопкой  .

3.4.1.3. В верхней части окна интерфейса также есть кнопка открытия дерева инфраструктуры  . В виде дерева расположены объекты в следующем порядке:

– локации;

– кластеры;

– серверы;

– виртуальные машины.

Слева, двигаясь по дереву, можно раскрывать объекты, нажимая на «+». Если нажать на имя объекта, то справа в рабочей области откроется окно состояния объекта.

Вернутся к структуре дерева можно, нажав на  . Справа в рабочей области в древовидной структуре при наведении на объект можно получить информацию о его типе и статусе.

Также в верхней части окна интерфейса есть кнопка  перехода к настройкам ping (открытия окна тестирования прохождения ICMP-запросов). Для выполнения ping необходимо заполнить следующие поля:

– сервер (выбор из раскрывающегося списка);

– цели для пинг-запросов;

– протокол (выбор из раскрывающегося списка);

– количество раундов для пинга;

– MTU;

– размер данных для Payload;

– сетевой интерфейс.

После заполнения полей необходимо нажать на кнопку «ОК».

3.4.2. Основное меню

3.4.2.1. В левой части окна интерфейса находится основное меню, позволяющее управлять системой и содержащее разделы – «Локации», «Кластеры», «Серверы», «Виртуальные машины», «Шаблоны ВМ», «Пулы ресурсов», «Хранилища», «Сети», «Журнал», «Безопасность» и «Настройки». Разделы основного меню «Хранилища», «Сети», «Журнал», «Безопасность» и «Настройки» содержат подразделы.

3.4.2.2. При переходе от одного раздела (подраздела) к другому в основной рабочей области окна интерфейса изменяется список объектов, относящийся к данному разделу (подразделу). Общую информацию о состоянии объекта можно получить, нажав на его название.

3.4.2.3. Для того чтобы из любого раздела (подраздела) основного меню вернуться к окну с сетевой инфраструктурой, необходимо нажать на надпись «SpaceVM» или кнопку  , расположенную в верхней строке интерфейса.

3.4.2.4. При работе с окнами существует возможность их сворачивания с помощью кнопки  в правом верхнему углу окна. Если окно занимает всю рабочую поверхность, то окно будет выведено на передний план с возможностью его перемещения. В окне при нажатии на кнопку  происходит разворачивание окна на весь экран, при нажатии на кнопку  происходит сворачивание окна в верхнюю панель, при нажатии на кнопку  происходит закрытие окна.

3.4.3. События

3.4.3.1. В нижней части окна содержится информация о событиях. В случае регистрации в системе ошибок или предупреждений при выполнении операций в нижней строчке окна интерфейса слева появляются соответствующие индикаторы. Цифра рядом с индикатором указывает на количество соответствующих событий.

Имеется возможность просмотра и получения информации:

– о событиях с предупреждением  и с ошибками  ;

– о задачах в процессе  , успешных  , с ошибками  , потерянных  , частичных  и отмененных  .

Более подробная информация об этом и о работе с журналами описана в 3.11 данного руководства.

3.4.4. Документация

3.4.4.1. В правой верхней части окна интерфейса содержится ссылка на встроенную документацию. Нажав на ссылку «Документация» открывается новое окно, содержащее справочные и эксплуатационные документы для работы с данным ПО.

3.4.5. Профиль пользователя

3.4.5.1. В правом верхнем углу окна интерфейса отображается имя пользователя, авторизовавшегося в системе, с возможностью посмотреть свой профиль и выйти из системы. При нажатии на имя пользователя открывается окно профиля пользователя.

3.4.5.2. В окне профиля пользователя содержится основная информация пользователя. Кнопка «Изменить пароль» позволяет изменить свой пароль, указав текущий.

3.4.5.3. Информация о пользователе разделена на следующие группы:

– информация;

– настройки;

– роли и разрешения;

– сессии;

– теги.

3.4.5.4. Во вкладке «Информация» отображаются следующие сведения:

1) логин;

2) имя (редактируемый параметр);

3) фамилия (редактируемый параметр);

4) электронная почта (редактируемый параметр);

5) состояние (редактируемый параметр);

6) активность:

– текущее количество неуспешных авторизаций;

– общее количество неуспешных авторизаций;

– дата и время последней неуспешной авторизации;

– дата и время последней успешной авторизации.

3.4.5.5. Во вкладке «Настройки» отображается следующая информация:

– часовой пояс;

– дата окончания действия пользователя;

– дата окончания действия пароля;

– суточный период пользователя;

– время начала суточного периода;

– время окончания суточного периода;

– посылать ошибки на электронную почту;

– двухфакторная аутентификация;

– максимальное количество одновременных сеансов;

– время неактивности для деактивации пользователя в днях (редактируемый параметр).

3.4.5.6. Во вкладке «Роли и разрешения» отображаются:

– роли пользователя;

– разрешения пользователя.

3.4.5.7. Во вкладке «Сессии» для каждой сессии отображаются IP-адрес клиента, агент клиента, статус («текущая» или нет), дата создания сессии, дата последнего использования.

3.4.5.8. Управление пользователями подробно описано в 3.12.1 данного руководства.

3.5. Локации и кластеры

Локации и кластеры – логические группы, которые представляют собой организационные единицы (OE), предназначенные для группирования серверов и применения к ним групповых настроек.

Локации и кластеры предназначены для группировки серверов с целью разделения серверов по сетям (сетевым настройкам), исполняемым задачам и расположению в ЦОД.

Группы физических серверов и внешних систем хранения данных, находящихся на географически удаленных друг от друга площадках, называются локации.

Группа физических серверов и внешних систем хранения данных, реализующих отдельные функции, называются кластеры.

В SpaceVM реализована возможность включения серверов в локации или кластеры.

3.5.1. Локации

3.5.1.1. Локации представляют собой сущности, предназначенные для группирования кластеров. Изначально предполагается, что каждая локация – это отдельный ЦОД или его часть.

Кластеры, серверы, сетевые хранилища и другие единицы из состава одной локации должны находиться в одной локальной вычислительной сети (ЛВС), а скорость сетевого соединения между ними должны быть не менее 1 Гбит/с с сетевыми задержками не более 400 мс.

В рамках одной локации допускается использование одного общего сетевого хранилища для всех кластеров, перенос серверов между кластерами.

Также присутствуют ограничения на построение туннелей и катастрофоустойчивой ВМ. Эти единицы кластера могут быть настроены только между разными локациями.

Список всех локаций, включая для каждой из них ее название, количество процессоров (CPU), объем памяти (RAM), количество кластеров, файловых и блочных хранилищ, а также статус локации, можно посмотреть, выбрав раздел «Локации» основного меню.

3.5.1.2. Существует возможность обновить, добавить, найти или просмотреть уже существующие локации более подробно.

3.5.1.3. Для добавления локации необходимо в разделе «Локации» основного меню нажать кнопку «Создать» и в открывшемся окне заполнить название (обязательное поле) и описание локации. После этого необходимо нажать кнопку «ОК».

3.5.1.4. Для изменения уже существующей локации необходимо в разделе «Локации» нажать на ее название.

3.5.1.5. В окне локации имеется следующая информация, разграниченная по группам:

1) «Информация» – содержит сведения о локации:

– график загрузки «cpu_percent» (общая загрузка процессорных ресурсов (Central Processing Unit, далее CPU)) и «memory_percent» (общая загрузка оперативной памяти (Random Access Memory, далее RAM);

– название (редактируемый параметр);

– описание (редактируемый параметр);

– процессоры;

– оперативная память;

– дата и время создания;

– дата и время изменения;

2) «Кластеры» – содержит список кластеров, входящий в состав локации, включая для каждого из них:

– название кластера;

– сведения о CPU, RAM;

– количество серверов;

– статус.

При нажатии на кластер открывается окно, подробное описание которого приведено в 3.5.2 данного руководства;

3) «Хранилища» – отображаются общие сетевые хранилища (файловые и блочные) для этой локации;

4) «События» – отображаются системные события для этой локации;

5) «Теги» – отображаются применяемые к локации метки (теги).

Примечание. При добавлении серверов необходимо указывать локацию, в которую добавляется сервер. Процедура добавления сервера описана в 3.6.2 данного руководства.

3.5.1.6. В окне локации можно обновить информацию, просканировать хранилища локации или удалить локацию.

3.5.1.7. Кнопка «Сканировать хранилища локации» запускает сканирование и синхронизацию на всех серверах локации следующих хранилищ:

– сетевых хранилищ;

– блочных сетевых хранилищ;

– пулов zfs;

– кластерных транспортов;

– пулов данных.

Примечание. Поиск пулов данных будет осуществлен на всех (на уже известных и на найденных) хранилищах. Все пулы данных, включая найденные, будут просканированы на предмет содержащихся на них образов, дисков и файлов.

3.5.2. Кластеры

3.5.2.1. Общие сведения

3.5.2.1.1. Кластеры представляют собой сущности, предназначенные для группировки серверов.

Изначально предполагается, что каждый кластер – это группа серверов, объединенных ЛВС со скоростью передачи данных более или равно 1 Гбит/с с сетевыми задержками не более 100 мс. Сетевые СХД, подключенные к серверам кластера, используются для хранения дисков ВМ. Для каждого кластера можно настроить параметры высокой доступности ВМ и динамического распределения нагрузки. Также для каждого кластера можно настроить индивидуальные сетевые параметры, применяемые ко всем серверам кластера. В рамках одного кластера можно настроить распределенный виртуальный коммутатор.

Базовый кластер, в состав которого входит контроллер SpaceVM имеет ограничение на включение поддержки кластерной файловой системы (ФС) и предназначен для применения к добавляемому серверу организационных операций. Это связано с тем, что большинство кластерных ФС требуют сохранения кворума серверов-клиентов и, в случае отсутствия кворума, серверы могут отключаться для предотвращения повреждения данных. При этом сервер, выполняющий роль контроллера, не может быть огражден для предотвращения потери управления системой.

ВНИМАНИЕ! При установке «по умолчанию» создается базовая локация и кластер. Удалять их ЗАПРЕЩЕНО. При создании новых локаций их базовые кластеры создаются автоматически. При удалении локаций удаляются и их базовые кластеры.

3.5.2.1.2. Список всех кластеров можно посмотреть в разделе «Кластеры» основного меню. В этом же окне имеется возможность обновления кластеров, добавление нового кластера, а также поиск кластера.

3.5.2.2. Создание кластера

3.5.2.2.1. Создать кластер в составе локации для добавления нераспределенных серверов можно в разделе «Кластеры» основного меню, нажав кнопку «Создать». Далее в открывшемся окне необходимо ввести уникальное название создаваемого кластера и выбрать локацию, в которую будет включен данный кластер.

ВНИМАНИЕ! Перемещение уже добавленного сервера между кластерами в составе разных локаций невозможно.

3.5.2.3. Информация о кластере

3.5.2.3.1. Для просмотра или изменения уже существующего кластера необходимо в разделе «Кластеры» нажать на его название.

3.5.2.3.2. В открывшемся окне можно обновить информацию, просканировать хранилища кластера или удалить кластер. Кнопка «Сканировать хранилища кластера» запускает сканирование и синхронизацию на всех серверах кластера следующих хранилищ:

– сетевых хранилищ;

– блочных сетевых хранилищ;

– пулов zfs;

– кластерных транспортов;

– пулов данных.

Примечание. Поиск пулов данных будет осуществлен на всех (на уже известных и на найденных) хранилищах. Все пулы данных, включая найденные, будут просканированы на предмет содержащихся на них образов, дисков и файлов.

3.5.2.3.3. В окне кластера имеется следующая информация:

1) графики загрузки CPU и RAM кластера. При наличии данных будет сформированы обновляемые в реальном времени графики использования CPU и RAM в процентах.

Для удобства анализа использования аппаратных мощностей кластера можно настроить отображение графиков, нажав слева от графиков на кнопку  «Задать интервал» и в открывшемся окне настроить интервал.

Для увеличения определенного интервала можно нажать на кнопку  «Масштабировать» и в миниатюрном изображении графиков под основными графиками выделить область для просмотра;

2) название (редактируемый параметр). Название – уникальное имя кластера. Чтобы его изменить, необходимо нажать кнопку  «Изменение названия кластера» и в открывшемся окне ввести новое уникальное имя кластера, после чего нажать кнопку «Сохранить»;

3) описание кластера (редактируемый параметр). Чтобы его изменить, необходимо нажать кнопку  «Изменение описания кластера» и в открывшемся окне ввести описание, после чего нажать кнопку «Сохранить»;

4) локация – это локация, в которую входит кластер;

5) процессоры – общее количество потоков всех узлов кластера;

6) оптимальный тип процессора для ВМ определяется по наименьшему совпадению функций (флагов) процессоров всех узлов кластера. При отсутствии совпадения выводит тип определения «default»;

7) оперативная память – общий объем доступной оперативной памяти всех узлов кластера;

8) кворум кластера (включить или выключить). Данный параметр показывает, включен ли механизм поддержания состояния кворума на контроллере. Включение данного параметра необходимо для реализации механизма «Высокой доступности». Чтобы изменить состояние кворума кластера, необходимо нажать кнопку  «Настройки кворума» и в открывшемся окне подтвердить действие;

9) дата и время создания – показывает, когда был создан данный кластер;

10) дата и время изменения – показывает, когда были внесены изменения в конфигурацию кластера.

3.5.2.4. Серверы в составе кластера

3.5.2.4.1. Вкладка «Серверы» – содержит список физических серверов в табличном виде, включая информацию о каждом из них:

– название;

– IP-адрес;

– сведения о CPU и RAM;

– количество ВМ (включенных и всего);

– статус.

3.5.2.4.2. Перемещение сервера между кластерами в составе одной локации возможно только после перевода сервера в «Сервисный режим». Перевод в сервисный режим осуществляется в окне «Серверы» – <имя сервера>.

3.5.2.4.3. Добавление сервера в состав кластера производится в разделе «Серверы» основного меню при выполнении операции «Добавить».

3.5.2.4.4. Более подробное описание сервера и операции с ним приведены в подразделе 3.6 данного руководства.

3.5.2.5. Пулы ресурсов в составе кластера

3.5.2.5.1. Вкладка «Пулы ресурсов» – содержит список пулов ресурсов в табличном виде, включая информацию о каждом из них:

– название;

– ВМ;

– ограничение памяти;

– ограничение CPU.

3.5.2.5.2. Также имеется возможность создания нового пула ресурсов.

3.5.2.5.3. Более подробное описание пулов ресурсов и операции с ним приведены в подразделе 3.7 данного руководства.

3.5.2.6. Виртуальные машины в составе кластера

3.5.2.6.1. Вкладка «Виртуальные машины» – содержит список ВМ кластера, включая информацию о каждой из них:

– название;

– сервер;

– IP-адрес;

– количество виртуальных процессоров и загруженность vCPU;

– объем виртуальной оперативной памяти и загруженность vRAM;

– количество виртуальных дисков vDisk;

– количество виртуальных сетевых интерфейсов vNIC;

– количество сетевых адаптеров vFunc;

– количество mediated-устройств vGPU;

– приоритет;

– статус.

3.5.2.6.2. Более подробное описание ВМ и операции с ней приведены в подразделе 3.8 данного руководства.

3.5.2.7. Хранилища в составе кластера

3.5.2.7.1. В состав каждого кластера могут входить различные хранилища данных и кластерные транспорты.

3.5.2.7.2. Вкладка «Хранилища» включают следующие объекты:

– «Пулы данных»;

– «ZFS пулы»;

– «Файловые хранилища»;

– «Блочные хранилища»;

– «Кластерные транспорты»;

– «Тома».

3.5.2.7.3. «Пулы данных» содержит список пулов данных в табличном виде, включая информацию о каждом из них:

– название;

– тип пула данных;

– количество серверов, к которым подключен конкретный пул данных;

– количество виртуальных дисков, находящихся на конкретном пуле данных;

– количество ISO-образов, находящихся на конкретном пуле данных;

– количество файлов, находящихся на конкретном пуле данных;

– использованный и общий объем пула данных;

– приоритет;

– статус.

Также имеется возможность создания нового пула данных и поиска пула с применением фильтра.

Более подробное описание пула данных и операции с ним приведены в 3.9.3 данного руководства.

3.5.2.7.4. Вкладка «ZFS пулы» содержит информацию обо всех ZFS-пулах кластера в табличном виде, а именно:

– название;

– сервер, на котором развернуто конкретное ZFS-хранилище;

– тип ZFS-хранилища;

– размер хранилища ZFS;

– состояние (Health) хранилища ZFS;

– количество локальных устройств хранения данных, используемых для организации ZFS-хранилища;

– количество внешних устройств хранения данных, используемых для организации ZFS-хранилища;

– статус.

Также имеется возможность создания нового ZFS-пула и поиска ZFS-пула с применением фильтра.

Более подробное описание ZFS-хранилища и операции с ним приведены в 3.9.8 данного руководства.

3.5.2.7.5. Вкладка «Файловые хранилища» содержит информацию обо всех файловых хранилищах кластера в табличном виде, а именно:

– название;

– тип подключения файлового хранилища;

– использованный и общий объем конкретного пула данных;

– количество созданных пулов данных на файловом хранилище;

– количество серверов кластера, к которым подключено файловое хранилище;

– статус.

Также имеется возможность добавить файловое хранилище.

Более подробное описание файлового хранилища и операции с ним приведены в 3.9.9.1 данного руководства.

3.5.2.7.6. Вкладка «Блочные хранилища» содержит информацию обо всех блочных хранилищах кластера в табличном виде, а именно:

– название;

– тип подключения блочного хранилища;

– статус.

Также имеется возможность добавить блочное хранилище.

Более подробное описание блочного хранилища и операции с ним приведены в 3.9.9.2 данного руководства.

3.5.2.7.7. Вкладка «Кластерные транспорты» содержит информацию обо всех кластерных транспортах кластера в табличном виде, а именно:

– название;

– кластер, к которому подключен кластерный транспорт;

– тип кластерного транспорта;

– статус.

Также имеется возможность добавить кластерный транспорт.

Более подробное описание кластерного транспорта и операции с ним приведены в 3.9.11.1 данного руководства.

3.5.2.7.8. Вкладка «Тома» содержит список подключенных к кластеру томов в табличном виде, включая информацию о каждом из них:

– название;

– используемый кластерный транспорт;

– тип тома;

– использованный и общий объем тома;

– Gluster статус;

– статус тома.

Также имеется возможность создания нового тома.

Более подробное описание тома и операции с ним приведены в 3.9.11.2 данного руководства.

3.5.2.8. Высокая доступность

3.5.2.8.1. Высокая доступность – это набор механизмов управления, позволяющий восстанавливать работоспособность ВМ без риска повреждения данных при прекращении работы узла кластера.

Механизмы ВД для платформы виртуализации SpaceVM позволяют повысить отказоустойчивость вычислительной инфраструктуры за счет возможности автоматического восстановления ВМ на резервном физическом сервере в случае сбоя или отказа сервера, на которой она выполнялась. Механизмы ВД возможно активировать на кластере до 96 физических серверов.

ВД SpaceVM отличается от аналогичных решений тем, что позволяет организовывать инфраструктуру автоматизированного восстановления ВМ на кластере из двух серверов и более (до 96), а также позволяет сохранять работоспособность при отказе более половины серверов виртуализации.

Это достигается тем, что ВД SpaceVM имеет централизованную архитектуру, встроенную в программный контроллер SpaceVM. Вследствие чего кворум (согласованность) поддерживается централизованно арбитром контроллера, а не распределенными равнозначными между собой физическими серверами. Только на тех узлах, которые находятся в состоянии кворума возможна попытка восстановления ВМ на своих вычислительных ресурсах.

Механизм поддержания состояния кворума необходим для предотвращения проблемы с запуском нескольких экземпляров ВМ при потере связности между работоспособными узлами, так как это может повлечь за собой, например, повреждение данных в следствие одновременного выполнения операции записи двух экземпляров ВМ в один участок дисковой памяти. Данная проблема известна под названием «Расщепление» или «Split Brain».

Например, достаточность количества работоспособных узлов при распределенном поддержании кворума определяется по формуле n > N/2, где n – количество работоспособных узлов, N – общее количество узлов в кластере. То есть узлы считают, что находятся в состоянии кворума, если количество «видимых» узлов превышает половину от общего количества.

Таким образом, в случае отказа более половины серверов, кластер теряет кворум и не предпринимает попыток восстановить на работоспособных серверах отказавшие ВМ.

В SpaceVM по причине поддержания кворума контроллером кластер может сохранять работоспособность, если отказало больше половины серверов. В таком случае контроллер продолжит восстановление отказавших ВМ на работоспособных серверах. В случае отказа сервера с контроллером возможно активировать резервный контроллер и механизмы ВД SpaceVM продолжат работу.

3.5.2.8.2. Основной частью отказоустойчивости является настройка высокой доступности (ВД) ВМ в составе кластера. Важным моментом защиты ВМ, предотвращающим восстановление ВМ на новом сервере до полного останова ее копии на аварийном оборудовании, является управление сервером по IPMI.

Поэтому без получения от сервера сигнала об ограждении (отключении питания или перезагрузке), ВМ не будет перезапущена на новом сервере. Для серверов, не оборудованных IPMI, предусмотрена возможность признания сервера выключенным автоматически, что теоретически может привести к повреждению диска ВМ из-за попыток записи данных на один диск двумя экземплярами ОС ВМ.

Реализация механизмов по типу ограждения IPMI основывается на соблюдении ряда требований:

– серверы в составе кластера должны поддерживать управление по протоколу IPMI v2 (LanPlus) по выделенному сетевому интерфейсу.

Если IP-адреса управления находятся в сети, отделенной от сети управления SpaceVM, то в разделе «Сети» – «Сетевые настройки» основного меню для контроллера SpaceVM необходимо прописать маршрут для доступа к IP-адресам IPMI-интерфейсов. Также допускается настройка виртуального внутреннего интерфейса для контроллера с доступом в сеть управления IPMI. Это необходимо для возможности опроса серверов в составе кластера на предмет состояния питания сервера;

– на основании состояния питания сервера («Power On/Off», «Cycle») принимается решение о возможности запуска ВМ на другом сервере. Это связано с тем, что, если сервер, на котором выполняется ВМ, не был гарантированно выключен, то возможно, что восстановление работы ВМ на новом сервере начнется до окончания ее функционирования на сервере, где произошел сбой.

Реализация механизмов в случае наличия кластерного транспорта типа «gfs2» основывается на том, что кворум серверов «gfs2» может самостоятельно принимать решение об ограждении узлов. Подробное описание приведено в 3.9.11.1.

3.5.2.8.3. Настройка высокой доступности, применяемая на весь кластер, выполняется в разделе «Кластеры» основного меню. Для каждого кластера доступно применение индивидуальных настроек. ВД может применяться как для всего кластера целиком (для всех ВМ кластера), так и выборочно для конкретной виртуальной машины (машин).

Примечание. Необходимо учитывать, что индивидуальные настройки ВМ (при включенной ВД) перекрывают настройки кластера. Настройка ВД для ВМ содержится в 3.8.19 данного руководства.

Для управления ВД существуют следующие настройки:

1) «Высокая доступность». Для включения (отключения)) «Высокой доступности» необходимо перевести переключатель «Высокая доступность» в соответствующее положение. «По умолчанию» – выключено.

Включение ВД для всего кластера означает, что для всех ВМ, параметры которых позволяют применить к ним ВД, будет активирована данная опция;

2) «Автоматический выбор сервера для восстановления ВМ». Для включения (отключения) автоматического выбора сервера необходимо перевести переключатель «Автоматический выбор сервера для восстановления ВМ» в соответствующее положение. «По умолчанию» – «Выключено».

Включение автоматического выбора сервера для кластера означает, что автоматическое восстановление ВМ будет осуществлено на наименее загруженный сервер кластера. Определяется на основе параметра DRS «Тип собираемых метрик». Подробнее в 3.5.2.9;

3) «Количество попыток восстановления ВМ». В некоторых случаях запуск ВМ не удается. Причин может быть множество, например, нет доступа к виртуальному диску или сбой СХД. Количество попыток – это изменяемое число попыток запуска ВМ, по истечении которых система считает, что восстановление ВМ невозможно, прекращает попытки запуска ВМ и выключает ВД для этой ВМ. «По умолчанию» – «5»;

4) «Интервал между попытками восстановления ВМ» – это пауза (в секундах), применяемая между попытками перезапуска ВМ. «По умолчанию» – «60»;

5) «Признак полной загрузки ВМ». Для обеспечения правильной очередности включения ВМ (например, до полной загрузки ВМ, обеспечивающей сервис DNS, нет смысла включать другие ВМ, которые не могут работать без DNS) в SpaceVM предусмотрены два настраиваемых признака:

– «Истечение заданного времени» – время (в секундах), по истечению которого, предполагается, что ВМ будет способна осуществлять свои функции. Очередь автоматического восстановления ВМ приостанавливается на время ожидания. «По умолчанию» – «0»;

– «Запуск гостевого агента ВМ» – очередь автоматического восстановления ВМ приостанавливается на время ожидания ответа от гостевого агента ВМ.

В случае, если агент по каким-либо причинам не отвечает, предусмотрено максимальное время ожидания (в секундах), по истечению которого, очередь восстановления будет продолжена, вне зависимости от того, получен ли ответ от гостевого агента. Нулевое значение признака означает, что наличие ответа гостевого агента не требуется. «По умолчанию» – «0».

Примеры значений:

а) ответ от гостевого агента ВМ не требуется. Значение – «0» (задержка очереди составляет 0 секунд);

б) требуется ответ от гостевого агента и максимальное время ожидания 2 минуты. Значение – «120».

Существует два основных варианта развития событий:

– гостевой агент дал ответ через 50 секунд (к примеру) после включения ВМ и очередь восстановление немедленно продолжена (задержка очереди составляет 50 секунд);

– ответ от гостевого агента не получен за 2 минуты и очередь восстановления продолжена (задержка очереди составляет 2 минуты).

Примечание. Если заданы оба признака готовности ВМ, приоритет будет у того признака, у которого время ожидания больше;

6) таблица серверов, используемых для ВД, позволяет ограничивать список серверов, на которых будут восстанавливаться ВМ. Данная опция недоступна при включенном автоматическом выборе целевого сервера для восстановления ВМ.

Примечание. При использовании ограниченного списка серверов, участвующих в ВД, добавляемые в кластер новые серверы попадают в список «Нераспределенные серверы».

Если были внесены изменения в настройки ВД, то становится доступна кнопка «Сохранить». После изменений настроек ВД важно их сохранить. В противном случае все изменения будут утеряны!

При нажатии кнопки «Групповая настройка ВМ» откроется диалоговое окно с таблицей всех ВМ кластера. В таблице выведены все параметры ВД для каждой ВМ кластера. Последний столбец таблицы «Статус» определяется автоматически на основе текущих параметров ВД ВМ и имеет три значения:

– SUCCESS (настройки ВД корректны и ВМ может быть восстановлена автоматически);

– FAILED (настройки ВД не корректны и ВМ не может быть восстановлена автоматически);

– DISABLED (ВД отключена). Для редактирования параметров ВД ВМ необходимо в таблице выделить нужные ВМ и в верхней части заполнить форму настроек.

Ниже приведен пример использования высокой доступности ВМ кластера.

Сотрудники организации используют виртуальные рабочие столы, службу каталогов (LDAP) и сервер доменных имен (DNS). Служба каталогов, сервер доменных имен и все ВМ сотрудников расположены на сервере «А», а сервер «Б» – резервный. Серверы объединены в кластер «В».

Высокая доступность кластера «В» включена с настройками «по умолчанию» и автоматическим выбором сервера для восстановления ВМ. Выполнены все условия для успешной миграции и восстановления ВМ в рамках кластера «В» (см. 3.5.2.8.4). Все виртуальные машины подлежат восстановлению в случае аварийной остановки любого сервера.

Для корректного восстановления работы данной инфраструктуры следует в первую очередь перезапустить сервер доменных имен, так как и служба каталогов, и ВМ сотрудников используют этот сервис. Следующей ВМ в очереди на восстановлении должна быть служба каталогов, так как сотрудники должны пройти аутентификацию на своих ВМ через LDAP. Далее, одновременно, должны быть восстановлены все ВМ сотрудников.

Таким образом, очередь восстановления должна быть следующей:

1) сервер доменных имен;

2) служба каталогов;

3) все ВМ сотрудников («999» – номер в очереди «по умолчанию»).

Далее следует настроить признак готовности для сервера DNS и службы LDAP. Предположим, опытным путем выяснено, что ВМ с сервером DNS запускается 2 мин, а служба каталогов – 3 мин. В данном случае удобно использовать признак готовности «Истечение заданного времени»:

– для сервера DNS – 120 с;

– для службы LDAP – 180 с.

Примечание. Как правило, признак «Истечение заданного времени» используется для тяжелых сервисов, загрузка которых занимает некоторое время уже после старта операционной системы. Если необходима полная загрузка только операционной системы ВМ, то следует использовать признак «Запуск гостевого агента ВМ» – при получении ответа от агента, очередь восстановления будет продолжена немедленно.

Теперь, в случае потери связи между контроллером и сервером «А», будет запущено автоматическое восстановление ВМ на сервере «Б» в следующем порядке:

– запуск сервера доменных имен;

– ожидание загрузки сервера доменных имен 120 с;

– запуск службы каталогов;

– ожидание загрузки службы каталогов 180 с;

– параллельный запуск всех ВМ сотрудников.

3.5.2.8.4. Методика демонстрации работы ВД (настройка и проверка ВД) заключается в следующем:

– добавить IPMI-настройки для каждого сервера в кластере;

– выставить тип ограждения IPMI на кластер или отдельно на каждый сервер (крайне желательно, чтобы это была отдельная сеть от «management»);

– создать пул данных одного из типов – «nfs», «cifs», «glusterfs», «gluster», «gfs2», доступный для всех узлов данного кластера;

– создать ВМ с дисками на этом пуле данных;

– включить ВД целиком на кластер или отдельно на каждую ВМ;

– отключить сетевой кабель «management» сети (или отключить питание сервера, или отключить супервизор узла) из какого-то сервера в кластере;

– наблюдать процесс, как сервер переходит через 30 секунд в статус ERROR («Ошибка» – узел недоступен), затем в статус HERMIT («Ограждается» – узел недоступен продолжительное время и его необходимо оградить для перезапуска виртуальных машин на других узлах, возможен мгновенный переход от ERROR в FAILED), затем в статус FAILED (узел был недоступен и его оградили (fence), виртуальные машины могут быть перезапущены на других узлах);

– наблюдать в журнале задач, как ВМ перезапускаются на других узлах поочередно (имя задачи «Восстановление виртуальной машины {domain_name} на узле {node_name}»).

Примечания:

1. Если ВД на двух серверах (узел и узел на контроллере), то восстановление ВМ возможно только в одну сторону – с узла на узел на контроллере.

2. Если все попытки восстановления ВМ завершились неудачей, то высокая доступность выключается для этой ВМ, что можно проследить по журналу событий.

3.5.2.9. DRS

3.5.2.9.1. DRS (система распределения ресурсов) настраивается на кластер и выполняет роль «выравнивателя» выбранного ресурса по всем его узлам.

3.5.2.9.2. В начале каждого цикла работы сервиса DRS через заданный интервал («Тайм-аут между проверками и попытками переезда виртуальных машин») происходит группировка узлов кластера в зависимости от «Типа собираемых метрик».

Далее считается среднеквадратичное (стандартное) отклонение нагрузки узлов кластера в процентах. Если оно меньше или равно «Пределу среднеквадратичного отклонения для начала работы DRS», то никаких действий не происходит до следующего цикла. Если отклонение больше заданного значения, то создается карта использования ресурсов кластера, суммированная по узлам, и выбирается наиболее нагруженный сервер. После чего происходит выбор ВМ, миграция которой удовлетворит требования к нагрузке на все узлы кластера.

Для этого для всех включенных ВМ наиболее нагруженного узла последовательно симулируется изменение нагрузки на серверы после миграции на все остальные узлы кластера с последующим расчетом возможного среднеквадратичного отклонения нагрузки кластера.

В качестве целевой ВМ и целевого узла для «живой» миграции выбирается та комбинация, после выполнения которой среднеквадратичное отклонение нагрузки на серверы кластера будет минимальным.

Если ВМ для миграции или узел назначения не найдены, то ничего не происходит до следующего цикла.

После отработки механизма предсказания нагрузки система определяет ВМ для миграции, узел-источник и узел назначения.

Далее, если в «Режиме создания виртуальных машин и воздействий» задан режим «SOFT», то появляется подсказка с предложением миграции ВМ, если же задан режим «HARD», то происходит попытка выполнения миграции целевой ВМ на узел назначения.

3.5.2.9.3. Вкладка «DRS» содержит информацию о параметрах динамического управления ресурсами. DRS настраивается на кластер и выполняет роль сервиса, который выравнивает нагрузку по всем узлам, входящих в кластер.

Для изменения настроек имеются следующие параметры:

1) включение (отключение) DRS. Для включения (отключения) DRS необходимо перевести переключатель DRS в соответствующее положение. «По умолчанию» – «Выключено»;

2) тайм-аут между проверками и попытками миграции ВМ – это интервал проверки загруженности узлов кластера. В случае выявления отклонения выше заданного параметра осуществляется попытка выравнивания нагрузки на узлы путем выдачи предупреждений или «живой» миграции ВМ, в зависимости от режима работы. «По умолчанию» – 180 секунд;

3) предел среднеквадратичного отклонения для начала работы DRS. В начале каждого цикла сервис проверяет отклонение нагрузки на каждый узел кластера от среднего по всем узлам, и, если отклонение превышает заданный предел («предел среднеквадратичного отклонения для начала работы DRS»), пытается привести нагрузку на узлы путем «живой» миграции ВМ к значениям, удовлетворяющим данный параметр. «По умолчанию» – 2 %;

4) типы собираемых метрик для начала работы DRS (выбор из раскрывающегося списка). Это типы загрузки хостов кластера, по которым каждый цикл происходит выявление отклонений нагрузки. Возможные варианты – CPU, MEMORY или CPU_MEMORY. Для типа CPU_MEMORY рассчитывается среднее отклонение для двух других метрик CPU и MEMORY. «По умолчанию» – MEMORY;

5) режим создания ВМ и воздействий (выбор из раскрывающегося списка). Это варианты действий при выявлении отклонения выше заданного параметра «предела среднеквадратичного отклонения для начала работы DRS». Возможные варианты – SOFT (ручной) или HARD (автоматический). При типе SOFT будут выдаваться предупреждения (рекомендации) о миграции определенной ВМ. При типе HARD будет выполнена «живая» миграция ВМ. «По умолчанию» – SOFT.

Если были внесены изменения в настройки DRS, то для их сохранения необходимо нажать кнопку «Сохранить».

3.5.2.10. Связность и ограждение

3.5.2.10.1. Вкладка «Связность и ограждение» содержит информацию о типах ограждения и связности.

3.5.2.10.2. Имеется возможность настроить ограждение и связность, нажав на кнопку «Изменить настройки».

3.5.2.10.3. Тип ограждения может принимать значения:

– AUTO;

– IPMI;

– VIRTUAL;

– SSH;

– NODE.

3.5.2.10.4. Тип связности может принимать значения:

– AUTO;

– KERNEL;

– KERNEL_IPMI;

– KERNEL_STORAGE.

3.5.2.11. Кворум

3.5.2.11.1. Во вкладке «Кворум кластера» содержится список всех участников кворума в табличном виде, включая информацию о каждом из них:

– IP-адрес – IP-адрес участника кворума и порт для поддержания связи в рамках кворума;

– ID участника кворума;

– лидер кворума – показан текущий активный лидер кворума;

– сервер;

– версия протокола;

– Voter.

3.5.2.12. Пределы ресурсов

3.5.2.12.1. Во вкладке «Пределы ресурсов» отображается информация о состоянии динамического управления ресурсами. Данные настройки предназначены для ограничения загруженности серверов кластера. При изменении базовых настроек необходимо учитывать возможную пиковую нагрузку на сервер. Также данные настройки влияют на распределение ВМ по серверам при срабатывании механизмов ВД и DRS.

3.5.2.12.2. Информация содержит уровни загрузки процессора и памяти (в процентах):

– верхний аварийный уровень загрузки процессора (редактируемый параметр). Это уровень загрузки процессора, при котором происходит выключение ВМ. «По умолчанию» – «85»;

– верхний предупредительный уровень загрузки процессора (редактируемый параметр). Это уровень загрузки процессора, при котором появляется предупреждение о высоком уровне загрузки процессора узла (узлов) кластера. «По умолчанию» – «80»;

– верхний аварийный уровень загрузки памяти (редактируемый параметр). Это уровень загрузки оперативной памяти, при котором происходит выключение ВМ. «По умолчанию» – «85»;

– верхний предупредительный уровень загрузки памяти (редактируемый параметр).

Уровень загрузки оперативной памяти, при котором появляется предупреждение о высоком уровне загрузки памяти узла (узлов) кластера. «По умолчанию» – «80».

Если были внесены изменения в настройки ресурсов, то становится доступна кнопка «Сохранить».

3.5.2.13. События

3.5.2.13.1. Во вкладке «События» содержится список последних событий для кластера с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.5.2.14. Теги

3.5.2.14.1. Во вкладке «Теги» содержится список присвоенных кластеру меток. Существует возможность создать, применить тег и обновить список назначенных кластеру тегов.

3.5.2.14.2. Для создания тега необходимо нажать кнопку «Создать тег» и в открывшемся окне указать уникальное название тега и выбрать цвет.

3.5.2.14.3. Для применения тега к кластеру необходимо нажать кнопку «Применить» и выбрать существующий тег.

3.5.2.14.4. Настройки тегирования выполняются при нажатии кнопки «Настройки». При включении опций тегирования кластера теги, установленные на ВМ и узлы этого кластера, будут влиять на работу механизмов ВД и DRS.

При включении опции «Разрешение на использование тегов узлов и ВМ при миграции, HA, DRS» при выборе доступных узлов для миграции и восстановления ВМ будут браться только те узлы, у которых стоит такой же тег, как и у ВМ.

При включении дополнительно опции «Дополнительное разрешение на использование тегов узлов и ВМ при миграции, HA, DRS, при котором ВМ мигрируют только на те узлы, на которых нет ВМ с таким же тегом» при выборе доступных узлов для миграции и восстановления ВМ будут браться только те узлы, у которых стоит такой же тег, как и у ВМ, и на которых нет ВМ с таким же тегом.

Для сохранения изменений необходимо нажать кнопку «Сохранить».

3.6. Серверы

3.6.1. Общая информация

3.6.1.1. Физические серверы могут добавляться в кластер и удаляться из него. Физические серверы – это основная среда исполнения ВМ.

ПО, устанавливаемое на сервер, формирует слой абстрагирования реального аппаратного обеспечения от ресурсов, предоставляемых ВМ. Это позволяет распределять физические ресурсы между ВМ и создавать виртуальные ресурсы (диски, сетевые карты и прочее) для обеспечения корректной работы ВМ и их взаимодействия.

3.6.1.2. На физических серверах могут размещаться файловые и блочные хранилища для дисков виртуальных машин, хранилища образов CD/DVD-дисков.

3.6.1.3. Физические серверы также могут предоставлять ресурсы для распределенных хранилищ.

3.6.1.4. Физические сетевые интерфейсы серверов участвуют в работе виртуальных и распределенных коммутаторов. Настройка интерфейсов описана в 3.6.11 данного руководства. Важной частью настройки физического сервера является настройка виртуальных и распределенных коммутаторов. На основании этих настроек обеспечивается сетевая связанность внутри кластера и доступ к сетям вне кластера. При добавлении сервера автоматически создается набор базовых сетевых настроек – базовый коммутатор и сетевой интерфейс.

3.6.1.5. В разделе «Серверы» основного меню содержится список серверов, включая для каждого их них его название, IP-адрес, сведения о CPU и RAM, количество ВМ (включенных и всего) и статус. Также имеется возможность обновления списка серверов, добавление нового сервера и выбора определенного сервера с применением фильтра.

3.6.1.6. Для поиска определенного сервера с применением фильтра необходимо в разделе «Серверы» нажать на кнопку «Фильтр» в верхней строчке окна. В открывшемся окне содержатся следующие поля для фильтрации:

– «Имя сервера» – имя искомого сервера;

– «Статус» – выбор из раскрывающегося списка («Без фильтра», «Исправно», «Нет соединения» или «Произошла ошибка»);

– «Файловое хранилище» – выбор из раскрывающегося списка;

– «Пул данных» – выбор из раскрывающегося списка;

– «Кластеры» – выбор из раскрывающегося списка;

– «Локации» – выбор из раскрывающегося списка;

– «Пулы ресурсов» – выбор из раскрывающегося списка;

– «Теги» – выбор из раскрывающегося списка.

После настройки фильтра необходимо нажать «Применить» или «Сбросить все».

3.6.2. Информация о сервере

3.6.2.1. Для просмотра или изменения информации о добавленном сервере в кластере необходимо в разделе «Серверы» основного меню выбрать целевой сервер, после чего в открывшемся окне во вкладке «Информация» отобразятся следующие сведения:

– название – уникальное имя сервера. Чтобы его изменить, необходимо нажать кнопку «Изменение названия сервера» и в открывшемся окне ввести новое уникальное имя сервера, после чего нажать кнопку «Сохранить»;

– описание – описание сервера. Чтобы его изменить, необходимо нажать кнопку «Изменение описания сервера» и в открывшемся окне ввести описание, после чего нажать кнопку «Сохранить»;

– локация – локация, в которую входит сервер;

– кластер – кластер, в который входит сервер;

– IP-адрес – IP-адрес сервера;

– тип установки – тип установленной SpaceVM на сервер. Может быть «controller + server» и «server». «controller + server» соответствует установке «Controller+Node», а «server» – «Node»;

– дата создания показывает, когда был добавлен данный сервер;

– дата изменения показывает, когда были внесены изменения в конфигурацию сервера;

– время беспрерывной работы – время работы сервера после последнего старта;

– дата запуска – дата и время последнего запуска сервера;

– системное время – дата и время сервера;

– часовой пояс – часовой пояс на сервере. Чтобы его изменить, необходимо нажать кнопку «Изменение часового пояса» и в открывшемся окне выбрать необходимый часовой пояс, после чего нажать кнопку «ОК».

3.6.3. Мониторинг

3.6.3.1. Для просмотра используемых ресурсов сервера необходимо в разделе «Кластеры» основного меню выбрать целевой сервер, после чего в открывшемся окне во вкладке «Мониторинг» отобразится следующая информация:

1) графики загрузки CPU и RAM сервера. При наличии данных будут сформированы обновляемые в реальном времени графики использования CPU и RAM в процентах.

Для удобства анализа использования аппаратных мощностей кластера можно настроить отображение графиков, нажав на кнопку слева от графиков «Задать интервал» и в открывшемся окне настроить интервал.

Для увеличения определенного интервала можно нажать на кнопку «Масштабировать» и в миниатюрном изображении графиков под основными графиками выделить область для просмотра;

2) использование CPU и RAM:

– суммарная текущая частота – рабочая частота CPU сервера;

– текущая нагрузка – текущая нагрузка CPU;

– оперативная память – общий объем RAM;

– объем занятой памяти под кэш – объем RAM, занятый под кэширование данных;

– текущая нагрузка оперативной памяти – общий занятый объем RAM;

3) среднее значение загрузки. Среднее значение загрузки в SpaceVM показывает среднее отношение имеющихся запросов на вычислительные ресурсы к количеству этих самых ресурсов за заданный промежуток времени (1 минута, 5 минут и 15 минут).

Среднее значение загрузки системы за 1 минуту показывает среднее значение загрузки за последнюю минуту.

Среднее значение загрузки системы за 5 минут показывает среднее значение загрузки за последние 5 минут.

Среднее значение загрузки системы за 15 минут показывает среднее значение загрузки за последние 15 минут.

Если среднее значение загрузки:

– меньше числа ядер (потоков) CPU, то это означает, что на выполнение всех текущих запросов тратится такое количество тиков, которое меньше доступного количества тиков CPU;

– равно числу ядер (потоков) CPU, то это означает, что на выполнение всех текущих запросов тратится такое количество тиков, которое равно доступному количеству тиков CPU;

– больше числа ядер (потоков) CPU, то это означает, что на выполнение всех текущих запросов тратится такое количество тиков, которое больше доступного количества тиков CPU (часть запросов ожидают выполнение и не могут быть выполнены своевременно).

Ожидание выполнения запросов может происходить не только по причине загрузки CPU, но и из-за дисковой нагрузки ввода/вывода (запрос не может быть выполнен, пока не будут получены данные с диска и так далее).

4) нагрузка ВМ:

– нагрузка процессора ВМ – нагрузка на CPU, которую создают ВМ;

– нагрузка памяти ВМ – используемый ВМ объем RAM;

– количество памяти ВМ – объем RAM, выданный ВМ.

3.6.4. Web-интерфейс узла

3.6.4.1. Общая информация

3.6.4.1.1. Просматривать и управлять узлом Node и его сущностями можно также в Web-интерфейсе узла.

Примечание. Если узел подключен к контроллеру, то часть функционала Web-интерфейса узла становится недоступным.

3.6.4.1.2. Переход к Web-интерфейсу узла можно выполнить двумя способами:

– через Web-интерфейса контроллера;

– через браузер.

3.6.4.1.3. Для перехода к Web-интерфейсу узла необходимо в Web-интерфейсе контроллера SpaceVM в окне «Серверы» – <имя сервера> нажать кнопку «Web-интерфейс». После нажатия на указанную кнопку произойдет открытие Web-интерфейса узла в новой вкладке браузера.

3.6.4.1.4. Для перехода к Web-интерфейсу узла в адресной строке браузера необходимо ввести IP-адрес узла *http://<ip_адрес>*. Произойдет открытие Web-интерфейса узла в новой вкладке браузера.

3.6.4.1.5. Для входа в Web-интерфейс узла необходимо ввести имя и пароль учетной записи пользователя узла. У каждого узла SpaceVM свой список пользователей, независимый от контроллера или других узлов. Подробная информация о пользователях Web-интерфейса узла содержится в 3.6.4.10 данного руководства.

3.6.4.1.6. Пользователь «по умолчанию»:

– имя пользователя – admin;

– пароль – veil.

3.6.4.1.7. Ниже приведен краткий список доступных в Web-интерфейсе узла функций:

1) кластер:

– просмотр информации о кластере;

– просмотр серверов, которые входят в кластер;

– просмотр ВМ кластера;

2) сервер:

– просмотр информации о сервере;

– просмотр ресурсов сервера;

– просмотр загруженности сервера;

– доступ к терминалу сервера;

– получение данных с датчиков сервера;

– управление сервером через IPMI;

– просмотр детальной информации о CPU сервера;

– просмотр детальной информации о RAM сервера;

– просмотр детальной информации о HDD сервера;

– проверка наличия обновлений;

3) операции с ВМ:

– получение списка ВМ сервера и их статус;

– удаление и создание ВМ;

– получение общей информации о ВМ;

– управление питанием ВМ сервера (включение, выключение, пауза);

– доступ к ВМ по протоколу SPICE и VNC;

– настройки удаленного доступа к ВМ;

– получение информации о конфигурации ВМ (опции загрузки, устройство шин и прочее);

– детальная информация и настройка CPU ВМ;

– детальная информация и настройка RAM ВМ;

– добавление и отключение виртуальных дисков к ВМ;

– монтирование и размонтирование ISO-образов к ВМ;

4) операции с пулами данных:

– получение списка подключенных пулов данных и информации о них;

– создание пулов данных;

– просмотр существующих и загрузка новых файлов;

– просмотр существующих и загрузка новых ISO-образов;

– просмотр и удаление существующих, а также создание новых виртуальных дисков;

– просмотр существующих LUN;

– просмотр и подключение файловых хранилищ;

5) сетевые настройки:

– просмотр информации о внутренних интерфейсах;

– просмотр информации о физических интерфейсах;

– просмотр информации о свободных интерфейсах;

– просмотр таблицы маршрутизации;

– просмотр сетевых настроек интерфейсов;

– просмотр, создание и удаление виртуальных сетей;

6) безопасность:

– просмотр существующих пользователей;

– создание новых пользователей;

– просмотр журнала событий и задач сервера.

3.6.4.1.8. В Web-интерфейсе узла недоступны следующие функции, доступные в Web-интерфейсе контроллера:

1) общие функции:

– управление кластерами SpaceVM, в том числе, объединение узлов в кластер;

– управление локациями SpaceVM;

– управление другими серверами;

– создание и изменение задач по расписанию;

– создание групповых задач;

– обновление узла;

– изменение названия и описания узла;

– настройка сетевых интерфейсов;

2) операции с ВМ:

– управление ВМ, которые расположены на других узлах кластера;

– создание и применение «Снимков», а также создание «Резервных копий ВМ»;

– управление и создание «Шаблонов»;

3) операции с пулами данных:

– удаление данных с пулов данных;

– загрузка и конвертирование виртуальных дисков;

– сканирование пулов данных;

– управление пулами данных, в том числе удаление;

– добавление блочных СХД;

4) безопасность:

– управление доступом к терминалу;

– управление доступом по протоколу SSH;

– резервное копирование узла;

– управление настройками NTP серверов и времени.

3.6.4.2. Информация о сервере

3.6.4.2.1. В Web-интерфейсе узла в разделе «Информация» содержатся следующие сведения:

1) уровень загрузки узла. В правом углу интерфейса содержится информация о загрузки системы, а именно:

– CPU – текущая нагрузка на CPU в процентах;

– всего RAM – общий объем оперативной памяти узла в гигабайтах;

– используется RAM – общий занятый объем RAM;

– свободно – незанятый объем RAM;

– буфферизовано – объем RAM, занятый под буфферизацию данных;

– кэшировано – объем RAM, занятый под кэширование данных;

2) идентификационная информация:

– название – уникальное имя сервера;

– описание – описание сервера;

– ID узла – уникальный идентификационный номер узла, который генерируется автоматически контроллером;

3) IP-адрес сервера и контроллера:

– адрес управления узла – IP-адрес сервера;

– адрес управления контроллера – IP-адрес контроллера;

4) прочая информация:

– статус – статус сервера;

– тип ограждения – выбранный тип получения подтверждения того, что аварийный сервер перешел в состояние, не допускающее повреждения ВМ при аварийных ситуациях;

– тип связности – выбранный метод принятия решения о том, что на сервере произошла авария.

Примечание. Подробная информация о доступных типах ограждения и типах связанности содержится в 3.6.12 данного руководства;

– наличие кворума – параметр, который показывает состояние кворума кластера SpaceVM;

– статус связи с контроллером – параметр, который показывает наличие или отсутствие связи узла с контроллером SpaceVM;

– версия ПО – версия установленного ПО SpaceVM;

5) пределы ресурсов:

– верхний аварийный уровень загрузки процессора – при достижении CPU данной отметки будет выведено событие с предупреждением, что достигнут аварийный уровень загрузки системы;

– верхний предупредительный уровень загрузки процессора – при достижении CPU данной отметки будет выведено событие с предупреждением, что достигнут предупредительный уровень загрузки системы;

– верхний аварийный уровень загрузки памяти – при достижении RAM данной отметки будет выведено событие с предупреждением, что достигнут аварийный уровень загрузки системы;

– верхний предупредительный уровень загрузки памяти – при достижении RAM данной отметки будет выведено событие с предупреждением, что достигнут предупредительный уровень загрузки системы.

Примечание. Подробная информация о механизме DRS содержится в 3.5.2.9 данного руководства.

3.6.4.3. Информация о кластере

3.6.4.3.1. В разделе «Кластер» Web-интерфейса узла содержится информация о кластере SpaceVM, в состав которого включен данный узел.

3.6.4.3.2. Во вкладке «Информация» раздела «Кластер» содержится название кластера SpaceVM, в который включен данный узел.

Во вкладке «Серверы» раздела «Кластер» содержится список серверов, которые входят в кластер.

Во вкладке «ВМ» раздела «Кластер» содержится список виртуальных машин, которые существуют в пределах кластера.

Во вкладке «Кворум» раздела «Кластер» содержится список серверов, которые поддерживают кворум кластера.

3.6.4.4. Терминал

3.6.4.4.1. Некоторые действия при работе с SpaceVM можно выполнять в терминале (CLI) узла.

3.6.4.4.2. Получить доступ к CLI можно в Web-интерфейсе узла в разделе «Терминал».

ВНИМАНИЕ! Невозможно выполнить подключение к терминалу через Web-интерфейс при использовании механизма NAT.

3.6.4.4.3. Для входа в CLI SpaceVM после получения доступа необходимо ввести логин и пароль SSH-пользователя.

Примечание. В SpaceVM при установке в автоматическом режиме «по умолчанию» создается пользователь со следующими учетными данными:

– логин – «root»;

– пароль – «bazalt».

3.6.4.5. Оборудование

3.6.4.5.1. В разделе «Оборудование» Web-интерфейса узла содержится информация о подключенном к узлу оборудовании, разделенная на группы:

– процессоры;

– память;

– IOMMU;

– IPMI;

– датчики;

– статистика HDD.

3.6.4.5.2. Для просмотра информации об установленных CPU на сервере необходимо перейти в подраздел «Процессоры». В открывшемся окне будет указана следующая информация:

1) модель – оптимальная модель vCPU для установленных процессоров, которая будет использоваться «по умолчанию»;

2) производитель –производитель физического процессора;

3) детальная информация.

В табличном виде содержится детальная информация о каждом установленном физическом процессоре:

– ID – идентификатор процессора;

– семейство – семейство процессора;

– производитель – производитель физического процессора;

– версия – версия (точная модель) процессора;

– максимальная частота – максимальная рабочая частота процессора;

– максимальное количество потоков – максимальное возможное количество потоков;

4) сокеты, ядра и потоки.

Сверху в правом углу окна содержится следующая информация о сокетах, ядрах и потоках установленных процессоров:

– количество сокетов – количество процессорных сокетов на материнской плате сервера, в которые установлены физические процессоры;

– количество ядер на сокет – количество процессорных ядер, приходящихся на один сокет;

– количество потоков на ядро – количество потоков, приходящихся на один сокет;

– общее количество потоков – количество потоков на сервер;

– количество NUMA узлов – количество NUMA узлов на сервер;

– архитектура – архитектура установленных физических процессоров на сервер;

– частота процессоров – текущая рабочая частота процессоров;

– доступные функции – раскрывающийся список доступных функций и инструкций физического процессора.

3.6.4.5.3. Для получения информации об оперативной памяти сервера перейти в подраздел «Память». В открывшемся окне будет указана следующая информация:

1) Swappiness:

– минимальный размер незанятой памяти под кэш;

– процент свободной оперативной памяти в процентах – процент оперативной памяти от общего числа, которая не используется под кэширование данных;

– nr_hugepages;

– уровень выделяемой памяти под кэш в условных единицах;

2) дедупликации:

– количество полных сканирований (Full scans);

– max_page_sharing;

– режим дедуплицирования памяти между NUMA nodes на узле (Merge across nodes);

– использующиеся дедуплицированные страницы памяти (Pages shared);

– страницы памяти для проверки (Pages to scan);

– недедуплицированные страницы памяти (Pages to scan);

– быстро меняющиеся страницы памяти для дедуплицирования (Pages volatile);

– работа сервиса (Run);

– время ожидания между сканированиями (Sleep millisecs);

– stable_node_chains;

– stable_node_chains_prune_millisecs;

– stable_node_dups;

– use_zero_pages.

3.6.4.5.4. Для просмотра информации, настройки и управления сервером по протоколу IPMI необходимо в разделе «Оборудование» перейти во вкладку «IPMI».

ВНИМАНИЕ! Если аппаратная платфора не имеет IPMI, то управление сервером по протоколу IPMI будет недоступным.

Чтобы отправить серверу команду на выполнение по протоколу IPMI необходимо нажать кнопку «Команды», в открывшемся окне выбрать нужную команду и нажать кнопку «ОК».

Для того чтобы выполнить настройку IPMI сервера, необходимо нажать кнопку «Настройки». В открывшемся окне необходимо настроить следующие поля:

– IP – это IP-адрес платы управления IPMI;

– пользователь – это имя (логин) учетной записи IPMI, от имени которой будут выполняться все дальнейшие действия;

– пароль – это пароль используемой учетной записи IPMI.

После заполнения всех полей необходимо нажать кнопку «Применить».

Примечание. Перед изменением IPMI-настроек убедитесь через Web-интерфейс, что в BMC сервера включена поддержка запросов по сети (например, опция «IPMI over Lan» в iDRAC). Проверить доступность IPMI можно командой *ipmitool -I lanplus -H [ipmi_ip] -U [ipmi_username] -P [ipmi_password] power status*. Если при изменении настроек IPMI появляется ошибка «Интерфейс IPMI на указанном адресе недоступен с указанными параметрами», то можно посмотреть детальную ошибку в журнале контроллера в CLI командой *log controller*.

3.6.4.5.5. В подразделе «Датчики» Web-интерфейса узла содержится список датчиков аппаратной платформы и их статус. Список датчиков и их статус может отличаться в зависимости от аппаратной платформы.

3.6.4.5.6. В подразделе «Статистика HDD» Web-интерфейса узла содержится список подключенных к серверу дисках и следующая информация о них:

– устройство – идентификатор диска в системе;

– драйвер – имя устройства в системе;

– тип подключения – тип подключения диска.

Также существует возможность получить подробную информацию о диске, такую как идентификационную информацию и результаты SMART-диагностики при ее поддержки диском. Для этого следует раскрыть информацию, нажав на знак «v». После нажатия отобразится следующая информация:

1) идентификационная информация:

– производитель диска;

– модель диска;

– серийный номер диска;

– доступная емкость диска;

– максимальная скорость вращения шпинделя жесткого диска (HDD) или тип диска для твердотельных накопителей (SSD);

– форм-фактор диска;

– поддержка SMART;

Примечание. Необходимо учитывать, что подключенные по iSCSI и FC (Fiber Channel) блочные устройства LUN определяются гипервизором как локальные устройства. В этом случае в модели устройства IDENTIFY в поле «Vendor» (производитель диска) будет указан поставщик LUN;

2) результаты самодиагностики.

В зависимости от типа диска и производителя информация, содержащаяся в результате самопроверки диска, может отличаться. Пример входящей информации в результаты SMART-диагностики:

– количество переназначенных секторов;

– общее время работы диска;

– количество полных циклов включения-выключения диска;

– текущая температура диска;

– состояние пула резервных блоков;

– общее количество ошибок, происходящих при записи сектора;

– число секторов, являющихся кандидатами на замену.

3.6.4.6. Виртуальные машины

3.6.4.6.1. Для получения списка ВМ, расположенных на узле, и их управления необходимо перейти в раздел «Виртуальные машины».

В разделе «Виртуальные машины» представлен список ВМ в табличном виде, включающий следующую информацию:

– название;

– IP-адрес;

– состояние – показывает в каком состоянии находится ВМ в данный момент (включена, выключена, на паузе);

– vCPU – количество выделенных vCPU ВМ;

– vRAM – объем выделенной ВМ оперативной памяти;

– загруженность vRAM.

3.6.4.6.2. В Web-интерфейсе узла существует возможность создания и удаления ВМ:

1) создание ВМ.

Для создания ВМ необходимо в разделе «Виртуальные машины» нажать кнопку «Создать» и в открывшемся окне заполнить следующую информацию:

– название – имя создаваемой ВМ;

– диск – имеющийся на узле виртуальный диск. Если требуется использовать новый виртуальный диск, необходимо его сначала создать. Подробная информация о создании виртуальных дисков содержится в 3.8.1.2 (шаг 2) данного руководства;

– образ ISO – ISO-образ диска, который будет подключен к ВМ после создания;

– размер RAM (МБ) – объем выделяемой для ВМ оперативной памяти;

– количество vCPU – количество выделенных vCPU ВМ;

– максимальное количество vCPU – максимальное количество потоков CPU;

– пароль SPICE;

– тип ОС;

– версия ОС;

– описание.

После чего нажать кнопку «Создать»;

2) удаление ВМ.

Для удаления ВМ необходимо в разделе «Виртуальные машины» выбрать целевую ВМ и в открывшемся окне нажать кнопку «Удалить», после чего подтвердить действие, нажав кнопку «Удалить».

3.6.4.6.3. Для просмотра детальной информации о ВМ необходимо в разделе «Виртуальные машины» выбрать целевую ВМ и в открывшемся окне во вкладке «Информация» будут содержаться следующие сведения:

– название – название ВМ;

– id – UUID ВМ в системе;

– описание – описание ВМ;

– память (ОЗУ) – объем выделяемой ВМ RAM;

– операционная система – семейство операционной системы, установленной на ВМ;

– версия операционной системы – версия установленной на ВМ ОС;

– агент – состояние агента ВМ;

– шаблон – параметр, указывающий на то, является ли ВМ шаблоном или нет;

– всегда включен – параметр, указывающий на то, включен ли автозапуск ВМ;

– статус службы гостевого агента;

– версия гостевого агента;

– имя хоста;

– IP-адрес;

– дата создания – дата создания ВМ;

– время активности.

3.6.4.6.4. В Web-интерфейсе узла можно управлять питанием ВМ, для этого нужно в разделе «Виртуальные машины» выбрать целевую ВМ, и в открывшемся окне нажать кнопку «Управление» и выбрать одно из следующих действий:

– запуск;

– пауза;

– перезагрузка;

– принудительная перезагрузка;

– выключение;

– выключение питание.

Для получения доступа к ВМ по протоколу SPICE из Web-интерфейса необходимо в Web-интерфейсе узла в разделе «Виртуальные машины» выбрать целевую ВМ и нажать кнопку «Терминал SPICE».

Примечание. Если возникли проблемы с «мышкой» при подключении по SPICE:

– попробуйте сменить графический адаптер на qxl (потребуется выключение ВМ);

– попробуйте обновить spice-vdagent до более актуальной версии.

Для запуска «Терминала SPICE» в полноэкранном режиме в правом верхнем углу «Терминала SPICE» раскрыть меню дополнительных функций и нажать кнопку «Полноэкранный режим».

Для того чтобы отправить сочетание клавиш, необходимо в правом верхнем углу «Терминала SPICE» раскрыть меню дополнительных функций, нажать кнопку «Отправить комбинацию клавиш» и выбрать требуемую комбинацию клавиш.

Для получения доступа к ВМ по протоколу VNC из Web-интерфейса необходимо в Web-интерфейсе узла в разделе «Виртуальные машины» выбрать целевую ВМ и нажать кнопку «Терминал noVNC».

Для запуска «Терминала noVNC» в полноэкранном режиме с левой стороны «Терминала noVNC» раскрыть меню дополнительных функций и нажать кнопку «Fullscreen».

Для того чтобы отправить сочетание клавиш «Ctrl+Alt+Del», необходимо с левой стороны «Терминала noVNC» раскрыть меню дополнительных функций, нажать кнопку «Show Extra Keys» и нажать кнопку «Send Ctrl-Alt-Del».

3.6.4.6.5. Для просмотра детальной информации о процессорах ВМ необходимо в разделе «Виртуальные машины» выбрать целевую ВМ и в открывшемся окне перейти в раздел «Процессоры».

В разделе «Процессоры» указана следующая информация:

– сокеты – количество сокетов ВМ;

– ядер на сокет – количество ядер на сокет ВМ;

– потоков на ядро – количество потоков на ядро ВМ;

– общее количество потоков;

– максимальное количество потоков – максимальное количество потоков ВМ;

– режим определения – режим эмулирования CPU;

– модель – эмулируемая модель процессора;

– приоритет vCPU ВМ – приоритет виртуальных процессоров.

Настройку процессоров можно выполнить с помощью кнопки «Настройки», которая при открытии окна позволяет изменить следующие параметры:

– количество vCPU и максимальное количество vCPU.

При нажатии кнопки «Количество» в открывшемся окне необходимо указать количество и максимальное количество процессоров, после чего подтвердить операцию, нажав кнопку «Сохранить»;

– топология процессоров. При нажатии кнопки «Топология» в открывшемся окне необходимо задать количество сокетов, ядер на сокет и потоков, после чего подтвердить операцию, нажав кнопку «Сохранить»;

– модель процессора. При нажатии кнопки «Модель» необходимо выбрать из раскрывающегося списка режим определения процессора, после чего подтвердить операцию, нажав кнопку «Сохранить»;

– приоритеты выделения процессорного времени ВМ. При нажатии кнопки «Приоритет» в открывшемся окне необходимо выбрать из раскрывающегося списка базовый приоритет процессора, детальный приоритет процессора, гарантированное количество vCPU, после чего подтвердить операцию, нажав кнопку «Сохранить».

Параметр «Максимальное количество vCPU» стоит ставить больше при планировании увеличивать количество vCPU при включенной ВМ. При изменении «max_cpu_count» топология подстраивается под этот параметр, то есть включенная ВМ видит именно «max_cpu_count vCPU», но при этом только на «cpu_count vCPU» подключается питание, а «(max_cpu_count – cpu_count) vCPU» видятся неактивными (без питания).

Изменение топологии процессора предназначено для удовлетворения требований ОС ВМ. Некоторые ОС не умеют работать с многоядерными процессорами, некоторые ограничивают количество сокетов CPU, а некоторые ОС ограничивают количество ядер на сокет.

Модель процессора может влиять на функциональность ОС ВМ и на возможность миграции ВМ внутри кластера.

Доступные функции узла можно посмотреть во вкладке узла «Оборудование» – «Процессоры».

Модель (архитектура) CPU виртуальной машины может быть:

– default – назначаются виртуальные процессоры. Если ОС ВМ чувствительна к набору инструкций центрального процессора, то использование виртуальных процессоров может не удовлетворять требованиям ОС ВМ. Доступные функции берутся из модели процессора qemu64;

– host-model – модель, аналогичная физическому, с незначительными ограничениями. Доступные функции берутся из узла, где находится ВМ;

– host-passthrough – фактическая трансляция полного комплекта инструкций и модели физического процессора. Доступные функции берутся из узла, где находится ВМ;

– custom – выбор модели процессора из списка. Необходимо учитывать предоставляемые наборы инструкций выбираемой модели и ограничения для ОС ВМ перед сменой типа процессора на custom. Доступные функции берутся из известного набора инструкций для каждого процессора, определенного в гипервизоре.

Привязка процессоров ВМ к физическим ядрам сильно ограничивает производительность сервера. Эту опцию рекомендуется применять только к высоко нагруженным ВМ, миграция которых невозможна. Физическое ядро, привязанное к CPU виртуальной машины, будет использоваться только для этой ВМ.

Приоритет выделения процессорного времени ВМ может понизить или повысить приоритет выделения ресурсов для ВМ.

3.6.4.6.6. Для просмотра детальной информации о выделяемой оперативной памяти ВМ необходимо в разделе «Виртуальные машины» выбрать целевую ВМ и в открывшемся окне перейти в раздел «Память».

В разделе «Память» указана следующая информация:

– оперативная память – объем выделяемой оперативной памяти ВМ;

– приоритет памяти ВМ – приоритет выделяемой памяти ВМ;

– максимальное значение памяти;

– минимально гарантированная память – параметр для учета при работе сервиса распределения памяти «ballooning» и при распределении ресурсов узлов.

Настройку процессоров можно выполнить с помощью кнопки «Настройки», которая при открытии окна позволяет изменить параметры. Для сохранения настроек необходимо нажать кнопку «Сохранить».

В SpaceVM реализовано добавление ОЗУ в процессе работы ВМ («на лету»). Добавляется кратно 256 Мбайт, и ВМ изнутри видит ее как дополнительную DIMM планку памяти.

Примечание. Для корректной работы добавления ОЗУ «на лету» необходимо перед этим установить комплект virtio драйверов.

3.6.4.6.7. Для просмотра подключенных виртуальных дисков к ВМ необходимо в разделе «Виртуальные машины» выбрать целевую ВМ и в открывшемся окне перейти в раздел «Диски».

В разделе «Диски» содержится следующая информация о подключенных к ВМ виртуальных дисках:

– source – расположение виртуального диска;

– устройство;

– target_bus – тип виртуальной шины подключения;

– driver_cache – тип кэширования;

– vdisk – UUID виртуального диска в системе.

Для того чтобы добавить виртуальный диск к ВМ необходимо нажать кнопку «Добавить» и в открывшемся окне выбрать имеющийся на узле виртуальный диск. Если требуется использовать новый виртуальный диск, его сначала необходимо создать. Подробная информация о создании виртуальных дисков содержится в 3.8.1.2 (шаг 2) данного руководства.

Для того чтобы отключить виртуальный диск от ВМ, необходимо выбрать отключаемый виртуальный диск и в его строке нажать кнопку «Отключить», далее подтвердить действие, нажав кнопку «Отключить».

3.6.4.6.8. Для просмотра информации о виртуальных приводах ВМ необходимо в разделе «Виртуальные машины» выбрать целевую ВМ и в открывшемся окне перейти в раздел «CD-Rom», где будет отображена следующая информация:

– cdrom – UUID привода, через который примонтирован образ диска;

– устройство;

– действие (удалить CD-ROM);

– iso – UUID образа диска;

– source – расположение образа диска;

– действие (отмонтировать ISO).

Для того чтобы добавить CD-ROM к ВМ, необходимо нажать на кнопку «Добавить CD-ROM».

Для того чтобы выполнить монтирование ISO-образа, необходимо нажать кнопку «Монтировать ISO».

Для того чтобы выполнить размонтирование ISO-образа от ВМ, необходимо выбрать отключаемый образ диска и в его строке нажать кнопку «Отключить», далее подтвердить действие, нажав кнопку «Отключить».

3.6.4.6.9. Для просмотра подключенных к ВМ LUN необходимо в разделе «Виртуальные машины» выбрать целевую ВМ и в открывшемся окне перейти в раздел «LUN».

3.6.4.6.10. Для просмотра подключенных к ВМ виртуальных сетевых интерфейсов необходимо в разделе «Виртуальные машины» выбрать целевую ВМ и в открывшемся окне перейти в раздел «Интерфейсы».

В разделе «Интерфейсы» содержится следующая информация о подключенных к ВМ виртуальных интерфейсах:

– MAC-адрес виртуального интерфейса;

– виртуальная сеть, к которой подключен данный виртуальный интерфейс;

– драйвер.

Для того чтобы добавить виртуальный интерфейс к ВМ, необходимо нажать кнопку «Подключить» и в открывшемся окне выбрать виртуальную сеть, к которой будет подключена ВМ через создаваемый интерфейс, при необходимости указать MAC-адрес, а также выбрать NIC драйвер, после чего подтвердить действие, нажав кнопку «Подключить».

Для того чтобы отключить виртуальный интерфейс от ВМ необходимо выбрать отключаемый виртуальный интерфейс и в его строке нажать кнопку «Отключить», далее подтвердить действие, нажав кнопку «Отключить».

3.6.4.6.11. Для просмотра конфигурации видео ВМ необходимо в разделе «Виртуальные машины» выбрать целевую ВМ и в открывшемся окне перейти в раздел «Видео».

В разделе «Видео» содержится следующая информация:

– тип виртуального видеоадаптера;

– память – объем выделяемой оперативной памяти узла под видеопамять ВМ в Гбайтах.

– количество мониторов – количество виртуальных мониторов, подключенных к ВМ.

3.6.4.6.12. Для просмотра конфигурации звука ВМ необходимо в разделе «Виртуальные машины» выбрать целевую ВМ и в открывшемся окне перейти в раздел «Звук».

В разделе «Звук» содержится следующая информация:

– модель виртуального звукового адаптера;

– кодек виртуального звукового адаптера.

3.6.4.6.13. Для просмотра опций высокой доступности ВМ необходимо в разделе «Виртуальные машины» выбрать целевую ВМ и в открывшемся окне перейти в раздел «Высокая доступность».

В разделе «Высокая доступность» содержится следующая информация:

– синхронизация с настройками кластера;

– количество попыток восстановления ВМ;

– интервал между попытками восстановления ВМ (с);

– номер в очереди на восстановление;

– признак полной загрузки ВМ – истечение заданного времени (с);

– признак полной загрузки ВМ – запуск гостевого агента ВМ. Задается максимальное время ожидания (с);

– высокая доступность;

– автоматический выбор сервера для восстановления ВМ.

3.6.4.6.14. Для просмотра опций загрузки ВМ необходимо в разделе «Виртуальные машины» выбрать целевую ВМ и в открывшемся окне перейти в раздел «Опции загрузки».

В разделе «Опции загрузки» содержится следующая информация:

– автозапуск ВМ при активации узла;

– загрузочное меню;

– тип загрузки – тип используемого для виртуализации загрузчика;

– время ожидания – время ожидания до начала загрузки ВМ.

Также здесь имеется информация о нераспределенных и используемых в загрузке устройствах.

3.6.4.6.15. Для просмотра настроек удаленного доступа к ВМ необходимо в разделе «Виртуальные машины» выбрать целевую ВМ и в открывшемся окне перейти в раздел «Удаленный доступ».

В разделе «Удаленный доступ» содержится следующая информация о настройках удаленного доступа к ВМ:

– удаленный доступ – состояние удаленного доступа (включено или выключено);

– порт доступа – сетевой порт узла, который может быть использован для подключения к ВМ по протоколу SPICE;

– пароль для доступа – пароль, который должен быть использован для подключения по протоколу SPICE к ВМ через указанный порт доступа.

Для того чтобы изменить «Пароль для доступа» необходимо нажать кнопку «Настройка», в открывшемся окне ввести новый пароль и нажать кнопку «Изменить».

3.6.4.6.16. Для просмотра устройства шин (виртуальных контроллеров) ВМ необходимо в разделе «Виртуальные машины» выбрать целевую ВМ и в открывшемся окне перейти в раздел «Устройства шин».

В данном разделе содержится следующая информация о системных шинах ВМ, разделенная на подразделы по типам устройств (IDE, PCI, SATA, USB, Virtio-serial), в табличном виде:

– модель виртуального контроллера;

– порядок.

3.6.4.7. Хранилища

3.6.4.7.1. Для просмотра информации о пулах данных, подключенных к узлу, необходимо перейти в раздел «Хранилища», далее «Пулы данных», где будет отображена следующая информация в табличном виде:

– название пула данных;

– тип пула данных;

– путь – относительный путь к пулу данных на узле;

– свободно – незанятый объем пула данных;

– размер – общий размер пула данных.

Для того чтобы создать пул данных, необходимо нажать кнопку «Создать», где в открывшемся окне ввести следующие данные:

– название создаваемого пула данных;

– тип создаваемого пула данных;

– путь – относительный путь к создаваемому пулу данных на узле;

– описание создаваемого пула данных (необязательно).

После чего подтвердить действие, нажав кнопку «Создать».

3.6.4.7.2. Для просмотра информации о виртуальных дисках, расположенных на узле, необходимо перейти в раздел «Хранилища», далее «Диски», где будет отображена следующая информация в табличном виде:

– название виртуального диска;

– тип виртуального диска;

– путь – относительный путь к виртуальному диску;

– размер – размер виртуального диска.

Для того чтобы создать виртуальный диск, необходимо нажать кнопку «Создать», где в открывшемся окне ввести следующие данные:

– название виртуального диска создаваемого пула данных;

– пул данных, на котором будет создан виртуальный диск;

– размер виртуального диска – доступный ВМ размер создаваемого виртуального диска в Гбайтах;

– предварительно выделить место – отметить, стоит ли предварительно выделить место. Если предварительно выделить место под виртуальный диск, то занимаемый им объем будет равен размеру виртуального диска.

В противном случае занимаемый виртуальным диском объем будет равен используемому ВМ объему данного диска.

После чего подтвердить действие, нажав кнопку «Создать».

Для того чтобы удалить виртуальный диск, необходимо выбрать удаляемый виртуальный диск, после чего в открывшемся окне нажать кнопку «Удалить» и подтвердить действие, нажав кнопку «Далее».

Примечание. Перед удалением виртуального диска его следует отключить от всех ВМ. Подробная информация об этом содержится в 3.6.4.6.7 данного руководства.

3.6.4.7.3. Для просмотра информации об образах ISO, расположенных на узле, необходимо перейти в раздел «Хранилища», далее «Образы ISO», где будет отображена следующая информация в табличном виде:

– название ISO-образа;

– путь – относительный путь к ISO-образу;

– размер – размер ISO-образа.

Для того чтобы загрузить ISO-образ из файловой системы, необходимо нажать кнопку «Загрузить» и в открывшемся окне выбрать требуемый ISO-образ и пул данных.

Для того чтобы загрузить ISO-образ по URL, необходимо нажать кнопку «Загрузить по url» и в открывшемся окне ввести URL-адрес.

Для того чтобы удалить ISO-образ, необходимо выбрать удаляемый ISO-образ, после чего в открывшемся окне нажать кнопку «Удалить» и во вновь открывшемся окне подтвердить действие, нажав кнопку «Далее».

Примечание. Перед удалением ISO-образа его следует отключить от всех ВМ. Подробная информация об этом содержится в 3.6.4.6.8 данного руководства.

3.6.4.7.4. Для просмотра информации о файлах, расположенных на узле, необходимо перейти в раздел «Хранилища», далее «Файлы», где будет отображена следующая информация в табличном виде:

– название файла;

– путь –относительный путь к файлу;

– тип файла;

– размер – размер файла.

Для того чтобы загрузить файл из файловой системы, необходимо нажать кнопку «Загрузить» и в открывшемся окне выбрать требуемый файл и пул данных.

Для того чтобы загрузить файл по URL, необходимо нажать кнопку «Загрузить по url» и в открывшемся окне ввести URL-адрес.

3.6.4.7.5. Для просмотра информации о подключенных к узлу блочных устройствах, необходимо перейти в раздел «Хранилища», далее «Блочные устройства».

3.6.4.7.6. Для просмотра информации о подключенных к узлу LUN, расположенных на узле, необходимо перейти в раздел «Хранилища», далее «LUNs», где будет отображена следующая информация в табличном виде:

– путь – iSCSI имя;

– серийный номер;

– размер;

– устройство – путь к устройству в системе;

– статус устройства.

3.6.4.7.7. Для просмотра информации о подключенных к узлу ZFS-хранилищах, расположенных на узле, необходимо перейти в раздел «Хранилища», далее «ZFS», где будет отображена следующая информация в табличном виде:

– название ZFS-хранилища;

– тип ZFS-хранилища;

– размер;

– health – состояние;

– точка монтирования – относительный путь точки монтирования хранилища.

Чтобы посмотреть детальную информацию о конкретном ZFS-хранилище, необходимо нажать на название соответствующего ZFS-хранилища и в открывшемся окне отобразится следующая информация:

– название ZFS-хранилища;

– тип ZFS-хранилища;

– размер;

– свободное пространство;

– health – состояние;

– точка монтирования – относительный путь точки монтирования хранилища.

В таблице приведены локальные устройства, участвующие в организации ZFS-хранилища и следующая информация о них:

– название – локальное устройство, участвующее в организации ZFS-хранилища;

– размер – объем локального устройства;

– health – состояние;

– spare – является ли устройство устройством горячего резервирования;

– cache – используется ли устройство для кэширования данных ZFS-хранилища;

– log – используется ли устройство для ведения целевого журнала ZFS.

3.6.4.7.8. Для просмотра информации о подключенных к узлу сетевых файловых хранилищах, необходимо перейти в раздел «Хранилища», далее «Файловые хранилища».

3.6.4.7.9. Для просмотра информации о подключенных к узлу сетевых блочных хранилищах, необходимо перейти в раздел «Хранилища», далее «Блочные хранилища».

3.6.4.8. Сеть

3.6.4.8.1. Для того чтобы посмотреть текущие настройки сетевых интерфейсов, необходимо перейти в раздел «Сеть», далее «Сетевые настройки».

В подразделе «Доменные имена» содержатся значения текущих настроек DNS, а именно:

– DHCP – параметр, отвечающий за то, получает ли узел настройки DNS по протоколу DHCP;

– домен – имя домена, в который входит узел;

– интерфейс, к которому применима данная настройка. Если пустой, то ко всем;

– DNS серверы – список DNS серверов, к которым обращается сервер;

– поддомены.

В подразделе «Шлюз» содержатся значения текущих настроек основных шлюзов, а именно:

– DHCP – параметр, отвечающий за то, получает ли узел адрес основного шлюза по протоколу DHCP;

– шлюз – основной шлюз;

– интерфейс, к которому применима данная настройка.

В подразделе «Маршруты» отображается таблица маршрутизации, в которую входят следующие данные:

– назначение маршрута. Если маска сети не указана, то используется «/32»;

– интерфейс, на котором используется данный маршрут. Если пусто, то может использоваться на любом интерфейсе;

– шлюз – IP-адрес узла сети, через который осуществляется доступ в подсеть назначения;

– метрика – значение, описывающее приоритет маршрута. Чем ниже значение, тем более приоритетный маршрут.

3.6.4.8.2. В Web-интерфейсе узла предусмотрена возможность получения информации о сетевых сущностях.

Также для некоторых сетевых сущностей реализована возможность управления этими сетевыми сущностями. К сетевым сущностям узла относятся:

1) виртуальные сети (см. 3.6.4.8.4);

2) коммутаторы (см. 3.6.4.8.4);

3) интерфейсы:

– физические интерфейсы (см. 3.6.4.8.4);

– внутренний интерфейсы (см. 3.6.4.8.6);

– агрегированные интерфейсы.

3.6.4.8.3. Для просмотра существующих виртуальных сетей сервера необходимо в разделе «Сеть» – «Сетевые сущности» перейти во вкладку «Виртуальные сети».

Для того чтобы получить подробную информацию о виртуальной сети, необходимо выбрать целевую виртуальную сеть, и в открывшемся окне будет отображена следующая информация, разделенная на группы:

1) информация – название виртуальной сети;

2) физические подключения – название интерфейса подключения;

3) подключенные ВМ к виртуальной сети.

В табличном виде приведены подключенные к данной сети/коммутатору ВМ:

– ВМ – название ВМ;

– MAC – MAC-адрес виртуального интерфейса ВМ, с помощью которого осуществляется подключение к данной сети/коммутатору;

– switch – дублирование названия сети/коммутатора;

– target_dev – интерфейс на хосте, который отдан ВМ.

Для того чтобы выполнить удаление, необходимо выбрать виртуальную сеть (коммутатор) и в открывшемся окне нажать кнопку «Удалить», после чего подтвердить действие, нажав кнопку «Удалить».

Для того чтобы создать виртуальную сеть (коммутатор) необходимо нажать кнопку «Создать» и в открывшемся окне ввести следующие данные:

– название виртуальной сети (коммутатора);

– подключение, через которое будет выполнено подключение сети к серверу;

– MTU – максимальный размер полезного блока данных одного пакета;

– VLAN – тег виртуальной сети согласно стандарту 802.1Q;

– VNI сетевого идентификатора VXLAN.

После ввода данных необходимо нажать кнопку «Создать».

3.6.4.8.4. Для просмотра существующих коммутаторов сервера необходимо в разделе «Сеть» – «Сетевые сущности» перейти во вкладку «Коммутаторы».

3.6.4.8.5. Для просмотра физических интерфейсов сервера необходимо в разделе «Сеть»-«Сетевые сущности» перейти во вкладку «Интерфейсы», выбрать «Физические», далее отобразится следующая информация в табличном виде:

– название интерфейса;

– модель интерфейса;

– состояние линка;

– состояние порта;

– неразборчивый режим – включен ли неразборчивый режим;

– MTU – текущий максимальный размер полезного блока данных одного пакета;

– MAC-адрес интерфейса;

– включен в агрегацию;

– поддержка SR-IOV;

– включен SR-IOV;

– подключение (vswitch).

Для того чтобы получить подробную информацию о физическом интерфейсе, необходимо выбрать целевой физический интерфейс, и в открывшемся окне будет отображена следующая информация:

– название;

– MAC-адрес;

– pci_info;

– изготовитель;

– модель;

– драйвер;

– версия драйвера;

– состояние линка;

– поддержка SR-IOV;

– включен SR-IOV;

– vf_count;

– включен в агрегацию;

– подключение (vswitch);

– неразборчивый режим – включен ли неразборчивый режим;

– max MTU – максимально возможный размер полезного блока данных одного пакета;

– MTU – текущий максимальный размер полезного блока данных одного пакета.

3.6.4.8.6. Для просмотра внутренних интерфейсов сервера необходимо в разделе «Сеть»-«Сетевые сущности» перейти во вкладку «Интерфейсы», выбрать «Внутренние», далее отобразится следующая информация в табличном виде:

– название интерфейса;

– модель интерфейса;

– MAC-адрес интерфейса;

– MTU – максимальный размер полезного блока данных одного пакета.

Для того чтобы получить подробную информацию о внутреннем интерфейсе, необходимо выбрать целевой внутренний интерфейс, и в открывшемся окне будет отображена следующая информация:

– название;

– MAC-адрес;

– IP-адрес узла в сети;

– маска подсети;

– DHCP – параметр, показывающий использует ли сервер протокол DHCP для получения сетевых настроек этого интерфейса;

– режим VLAN;

– тег VLAN;

– транки;

– MTU – текущий максимальный размер полезного блока данных одного пакета.

3.6.4.8.7. Для просмотра агрегированных интерфейсов сервера необходимо в разделе «Сеть»-«Сетевые сущности» перейти во вкладку «Интерфейсы» и выбрать «Агрегированные».

3.6.4.9. Журнал

3.6.4.9.1. Для просмотра журнала событий сервера необходимо в разделе «Журнал» перейти во вкладку «События», где отобразится следующая информация в табличном виде:

– сообщение – описание совершившегося события;

– тип события;

– дата создания записи о событии.

Для того чтобы получить детальную информацию о событии, необходимо нажать на интересующее событие, и в открывшемся окне будет отображена следующая информация:

– сообщение – описание совершившегося события;

– пользователь, от имени которого было зафиксировано событие;

– тип события;

– дата создания записи о событии.

3.6.4.9.2. Для просмотра журнала задач сервера необходимо в разделе «Журнал» перейти во вкладку «Задачи», где отобразится следующая информация в табличном виде:

– сообщение – название задачи;

– статус задачи;

– дата создания задачи.

Для того чтобы получить детальную информацию о задаче, необходимо нажать на интересующую задачу, и в открывшемся окне будет отображена следующая информация:

– название задачи;

– результат выполнения задачи;

– пользователь, от имени которого было зафиксировано событие;

– время выполнения задачи в секундах;

– дата создания задачи;

– дата завершения задачи;

– статус задачи;

– список событий, относящихся к данной задаче в табличном виде.

3.6.4.10. Пользователи

3.6.4.10.1. Для просмотра пользователей Web-интерфейса узла необходимо перейти в раздел «Пользователи», где будет отображена следующая информация о существующих пользователях в табличном виде:

– пользователь – имя пользователя;

– статус пользователя.

Для того чтобы создать нового пользователя, необходимо нажать кнопку «Создать» и в открывшемся окне ввести следующие данные:

– пользователь – имя пользователя;

– пароль;

– группы – роли, назначенные пользователю.

Для того чтобы получить детальную информацию о пользователях, необходимо нажать на интересующего пользователя, и в открывшемся окне будет отображена следующая информация:

– пользователь – имя пользователя;

– статус.

Также имеется возможность изменить статус пользователя, нажав кнопку «  », и изменить пароль, нажав кнопку «Изменить пароль».

3.6.4.11. Версия ПО

3.6.4.11.1. В разделе «Версия ПО» содержится информация о версиях модулей:

– версия CLI;

– версия окружения CLI;

– версия узла;

– версия окружения узла;

– версия веб-интерфейса;

– версия утилит;

– версия сборки.

3.6.4.12. NTP-серверы

3.6.4.13. В разделе «NTP серверы» можно настроить список NTP-серверов, с которым будет синхронизироваться контроллер. При нажатии кнопки «Установка NTP» в открывшемся окне необходимо задать адреса NTP-серверов из раскрывающегося списка и нажать кнопку «Добавить». После этого сохранить изменения, нажав кнопку «Установить».

3.6.4.14. Сервисы

3.6.4.14.1. В разделе «Сервисы» отображается список сервисов и их состояние:

– node-engine;
– node-web-api;
– node-web-proxy;
– node-web-uploader;
– node-statistics;
– iscsi;
– multipath;
– postgresql;
– nginx;
– ntp;
– redis;
– beanstalkd;
– ttyd;
– snmp;
– gluster;
– corosync;
– dlm;
– watchdog;
– linstor-satellite;
– tg-agent;
– consul.

3.6.5. Управление физическими серверами

3.6.5.1. Добавление сервера

3.6.5.1.1. Добавление сервера происходит в разделе «Серверы» основного меню при нажатии в верхней строчке окна кнопки «Добавить» и заполнения в открывшемся окне следующей информации:

1) IP-адрес контроллера, который будет использован для управления платформой. Для его выбора необходимо раскрыть список и выбрать соответствующий контроллер;

2) локация, из состава которой будет добавлен сервер (выбор из списка ранее созданных);

3) кластер, куда будет добавлен сервер (выбор из списка ранее созданных);

4) уникальное название сервера, которое будет отображаться в интерфейсе;

5) данные сервера. Для добавления сервера необходимо указать следующие данные – IP-адрес сервера, SSH-пользователь, SSH-порт и SSH-пароль:

– IP-адрес сервера необходимо указать в соответствующем поле. Форма записи IP-адреса – «192.168.1.1».

Примечание. IP-адрес, используемый для управления кластером, должен выбираться исходя из настроек IP-адресов, присвоенных интерфейсам управления серверов. Интерфейс, не являющийся интерфейсом управления, может быть ограничен встроенным межсетевым экраном (МСЭ) и не пропускать трафик с управляющими командами;

– SSH-пользователь, «по умолчанию» – «root». Если политика безопасности запрещает использовать «root», то следует предварительно создать другого пользователя с необходимым набором прав. Для того чтобы задать SSH-пользователя, его имя необходимо ввести в соответствующее текстовое поле;

– SSH-порт – порт для входящих SSH-подключений, «по умолчанию» – «22». Если политика запрещает использовать порт «22» для входящих SSH-подключений, его следует предварительно сменить на сервере. Для того чтобы задать SSH-порт, необходимо ввести его в соответствующее поле;

– SSH-пароль – пароль от пользователя, введенного в поле «SSH-пользователь». При автоматической установке пароль от учетной записи «root» – «bazalt»;

6) проверка соединения. После того как все данные были введены, рекомендуется выполнить проверку соединения. Для этого необходимо нажать кнопку «Проверить соединение». В случае, если не удалось выполнить тестовое соединение, необходимо проверить корректность введенных данных сервера и его доступность по сети контроллеру;

7) дополнительные настройки:

– описание – это любой текст, который будет отображаться в соответствующем поле сервера;

– можно указать опцию «Форсированное добавление». Форсированное добавление используется, если сервер уже участвовал ранее в составе (в том числе другого) кластера SpaceVM или ранее был удален из состава кластера форсировано. Эта операция принудительно заменяет привязку сервера к контроллеру.

Для применения настроек необходимо нажать кнопку «ОК».

3.6.5.1.2. В процессе добавления на сервере настраиваются базовые объекты, необходимые для включения в состав кластера. Процесс добавления выполняется в фоновом режиме, а пользователь возвращается к списку серверов.

3.6.5.1.3. В процессе создания статус сервера в общем списке серверов – «создается». После успешного добавления сервера статус сервера изменится на «исправно». В случае возникновения ошибки необходимо проверить вводимые данные и обратиться к журналам для выявления неисправности.

Примечания:

1. Поля «Описание» и «SSH порт» являются необязательными.

2. После добавления сервера к контроллеру управление сервером идет по шифрованному каналу с ключом RSA длиной 1024.

3. После добавления сервера к контроллеру выбранный при установке hostname узла сменится на системный ID. Общение между контроллером и узлом происходит именно по нему, поэтому ручная корректировка его в «hosts» НЕ ДОПУСКАЕТСЯ. Следует учитывать, что файл «hosts» одинаковый на всех узлах системы. При необходимости ручной корректировки надо зайти в CLI контроллера и добавить новый файл в каталог «/etc/hosts.d/» с необходимым сопоставлением имени и IP-адреса, после чего ввести команду «*sudo /usr/local/sbin/veil-hosts –c*». После этого можно проверить файл «hosts».

3.6.5.2. Сервисный/стандартный режим

3.6.5.2.1. Сервисный режим в окне «Серверы» – <имя сервера> предназначен для проведения обслуживания сервера или миграции его в другой кластер. Перевод сервера в сервисный режим возможен только после выключения или миграции всех ВМ этого сервера.

3.6.5.2.2. После активации сервисного режима становится доступна операция перевода узла в другой кластер и перевод в стандартный (активный) режим.

3.6.5.2.3. Для перевода в сервисный режим необходимо нажать в окне «Серверы» – <имя сервера> кнопку «Сервисный режим». При переводе в сервисный режим есть две опции:

– автоматическая миграция всех ВМ;

– выключение сервера.

При включенной опции «Автоматическая миграция всех ВМ узла» перед переводом сервера в сервисный режим будет выполнена попытка миграции всех ВМ на другие серверы в рамках кластера.

ВНИМАНИЕ! Все ВМ, которые не имеют возможности мигрировать, а также другие сущности, расположенные на этом сервере, перейдут в состояние «failed».

При включенной опции «Выключение сервера через 1 минуту после перехода» сервер после успешного перехода в сервисный режим будет выключен через 1 минуту.

3.6.5.2.4. Для того чтобы сервер из сервисного режима перевести в стандартный, необходимо в окне «Серверы» – <имя сервера> нажать кнопку «Стандартный режим».

Примечание. Перед переводом сервера в стандартный (активный) режим необходимо во вкладке «ПО и Сервисы» – «Сервисы» запустить проверку по кнопке «Проверка агента», чтобы убедиться, что сетевая связность между сервером и контроллером присутствует, и он готов к работе.

3.6.5.2.5. При переводе в сервисный режим есть опция выключения сервера.

3.6.5.3. Автотестирование узла

3.6.5.3.1. Автотестирование узла используется для автоматического выявления сбоев в работе и нарушений конфигураций сервера.

3.6.5.3.2. Во время автотестирования узла система автоматически исправит выявленные неисправности. Если выявленную неисправность система не может автоматически исправить, то она сообщит о наличии такой неисправности.

ВНИМАНИЕ! В случае, если сервер недоступен контроллеру или на узле не запущена служба «node-engine», то задача автотестирования на узле завершится со статусом LOST.

3.6.5.3.3. Для того чтобы запустить автотестирование узла, необходимо в окне нажать кнопку «Автотестирование узла», после чего подтвердить действие в открывшемся окне.

3.6.5.4. Перезагрузка сервера

3.6.5.4.1. Перезагрузку сервера можно выполнить несколькими способами:

– в CLI;

– в Web-интерфейсе.

ВНИМАНИЕ! Перед перезагрузкой необходимо выключить или перенести все ВМ, расположенные на сервере, после чего перевести его в «Сервисный режим».

3.6.5.4.2. Для того чтобы выполнить перезагрузку в CLI, необходимо получить доступ к CLI и выполнить команду *reboot.*

3.6.5.4.3. Для того чтобы выполнить перезагрузку в Web-интерфейсе, необходимо в окне «Сервер» – <имя сервера> – «Оборудование» – «IPMI» нажать кнопку «Перезагрузить сервер»  или кнопку «Принудительно перезагрузить сервер»  .

Примечание. Для работы IPMI необходимо, чтобы аппаратная платформа имела поддержку и были сделаны соответствующие настройки в SpaceVM. Информация о том, как настроить IPMI в SpaceVM, содержится в 3.6.5.8.

3.6.5.5. Выключение сервера

3.6.5.5.1. Выключение сервера можно выполнить несколькими способами:

– в CLI;

– в Web-интерфейсе.

ВНИМАНИЕ! Перед выключением сервера необходимо выключить или перенести все ВМ, расположенные на сервере, после чего перевести его в «Сервисный режим».

3.6.5.5.2. Для того чтобы выполнить выключение сервера в CLI, необходимо получить доступ к CLI и выполнить команду *shutdown*.

ВНИМАНИЕ! После выключения через консоль без доступа к IPMI сервера может потребоваться физический доступ к серверу для его включения.

3.6.5.5.3. Для того чтобы выполнить выключение сервера в Web-интерфейсе, необходимо во вкладке «Сервер» – <имя сервера> – «Оборудование» – «IPMI» нажать кнопку «Выключить»  .

Примечание. Для работы IPMI необходимо, чтобы аппаратная платформа имела поддержку и были сделаны соответствующие настройки в SpaceVM. Информация о том, как настроить IPMI в SpaceVM, содержится в 3.6.5.8.

3.6.5.6. Перемещение сервера в другой кластер

3.6.5.6.1. В SpaceVM реализовано перемещение узлов между кластерами в пределах одной локации.

ВНИМАНИЕ! При переводе сервера в другой кластер необходимо убедиться в том, что он не участвует в кластерных транспортах.

3.6.5.6.2. Для перемещения сервера в другой кластер необходимо в окне «Серверы» – <имя сервера> перевести его в «Сервисный режим» (см. 3.6.5.2), нажать появившуюся кнопку «Переместить» (появляется рядом с кнопкой удаления сервера) и выполнить операцию переноса, выбрав целевой кластер.

3.6.5.6.3. После перемещения сервера необходимо перевести сервер в стандартный режим. Для этого необходимо в этом окне нажать кнопку «Стандартный режим» (см. 3.6.5.2).

3.6.5.7. Терминал

3.6.5.7.1. Некоторые действия при работе с SpaceVM можно выполнять в терминале (CLI) узлов как с типом установки «controller + server», так и «server». Получить доступ к CLI можно несколькими способами:

– подключившись к узлу по протоколу SSH;

– в Web-интерфейсе;

– напрямую, используя IPMI сервера или подключенные клавиатуру и «мышь».

Примечание. Для получения доступа к терминалу узел должен быть включен!

Для входа в CLI SpaceVM после получения доступа необходимо ввести логин и пароль SSH-пользователя.

Примечание. В SpaceVM при установке в автоматическом режиме «по умолчанию» создается пользователь со следующими учетными данными:

– логин – «root»;

– пароль – «bazalt».

3.6.5.7.2. Для получения доступа к терминалу в Web-интерфейсе необходимо в окне «Серверы» – <имя сервера> нажать кнопку «Терминал». После нажатия кнопки окно терминала откроется в новой вкладке браузера.

Примечание. Также возможно получить доступ к терминалу через Web-интерфейс узла. Информацию о том, как это сделать см. в 3.6.4.4.

ВНИМАНИЕ! Невозможно выполнить подключение к терминалу через Web-интерфейс при использовании механизма NAT.

3.6.5.7.3. Для получения доступа к терминалу по протоколу SSH необходимо в приложении, которое имеет функционал подключения по протоколу SSH, например, Putty, выполнить подключение и ввести учетные данные SSH-пользователя.

ВНИМАНИЕ! Если в настройках сервера «Статус SSH» – «Выключен», то подключение к терминалу доступно только в Web-интерфейсе.

3.6.5.8. IPMI

3.6.5.8.1. В случае, если аппаратная платформа сервера, на которую установлена SpaceVM, поддерживает управление сервером по IPMI, можно перейти к IPMI из Web-интерфейса SpaceVM.

3.6.5.8.2. Для того чтобы появилась возможность перехода к IPMI сервера, необходимо выполнить настройку IPMI. Описание настройки смотрите в 3.6.7.2.

3.6.5.8.3. Для получения доступа к IPMI в Web-интерфейсе необходимо в разделе «Серверы» основного меню выбрать целевой сервер и нажать кнопку «IPMI». После нажатия на указанную кнопку произойдет открытие IPMI в новой вкладке браузера.

3.6.5.8.4. Для управления питанием сервера необходимо перейти в в раздел «Серверы» основного меню, выбрать целевой сервер, далее перейти во вкладку «Оборудование» и в раскрывшемся списке выбрать «IPMI».

В открывшемся окне будут доступны следующие действия:

– запуск сервера. Для того чтобы выполнить запуск сервера, необходимо нажать кнопку «»;

– приостановка работы сервера. Для того чтобы приостановить работу сервера, необходимо нажать кнопку «»;

– перезагрузка сервера. Для того чтобы выполнить перезагрузку сервера, необходимо нажать кнопку «»;

– принудительная перезагрузка сервера. Для того чтобы выполнить принудительную перезагрузку сервера, необходимо нажать кнопку «»;

– выключение сервера. Для того чтобы выполнить выключение сервера, необходимо нажать кнопку «».

ВНИМАНИЕ! Перед управлением питанием сервера необходимо перевести его в «Сервисный режим», нажав кнопку «Сервисный режим». После окончания работ, связанных с управлением питанием сервера, необходимо перевести его в «Стандартный режим», нажав кнопку «Стандартный режим». Подробная информация о «сервисном»/«стандартном» режимах приведена в 3.6.5.2.

3.6.6. Удаление сервера

3.6.6.1. В окне состояния выбранного сервера имеется возможность удаления сервера.

3.6.6.2. Для удаления сервера из кластера необходимо:

1) нажать кнопку «Удалить сервер» и в открывшемся окне заполнить поля о сервере:

– SSH-пользователь;

– SSH-пароль;

– SSH-порт.

Если использовались параметры «по умолчанию», то необходимо заполнить поля следующим образом:

– SSH-пользователь – «root»;

– SSH-пароль, который был задан при установке ОС сервера;

– SSH-порт – «22»;

2) после заполнения подтвердить удаление, нажав кнопку «Удалить».

ВНИМАНИЕ!

1. Перед удалением сервера из кластера необходимо проверить, все ли данные объекты от него отключены или удалены, так как в составе кластера с сервером связаны многие другие объекты кластера.

2. Штатное удаление проводит проверку на связанность удаляемого объекта с другими в составе кластера. Предупреждение о наличии связанных объектов будет отображаться при попытке удаления.

3. С сервером могут быть связаны:

– файловые (локальные), блочные и распределенные хранилища;

– виртуальные машины, их шаблоны, виртуальные диски, резервные копии;

– образы CD/DVD-дисков;

– физические сетевые интерфейсы, привязанные к ВМ или ВК.

4. Если сервер находится в аварийном состоянии (недоступен для управления), и связанные с данным сервером объекты не нужны или не могут быть отключены или удалены из кластера штатным образом, то удаление сервера будет произведено форсировано.

5. Если сервер принадлежит кластеру, на котором поднят кластерный транспорт типа Gluster, то следует убедиться, что ни одному тому Gluster не принадлежат в качестве разделов какие-либо ZFS-пулы сервера, даже удаленные на данный момент. В противном случае удаление сервера завершится ошибкой.

3.6.7. «Серверы» – <имя сервера> – «Оборудование»

В окне «Серверы» – <имя сервера> – «Оборудование» содержится следующая информация, разделенная на группы:

– процессоры;

– IPMI;

– сведения о HDD;

– остальное оборудование;

– память;

– пределы ресурсов.

В данном окне для всех групп имеется возможность обновления информации о ресурсах. Обновление информации о ресурсах производится после изменения аппаратной конфигурации сервера – изменения количества, типа процессоров, памяти, дисков.

Примечание. После изменения конфигурации оборудования необходимо обновить ресурсы в базе данных контроллера по кнопке «Обновить информацию о ресурсах».

3.6.7.1. Процессоры

3.6.7.1.1. Для просмотра информации об установленных CPU на сервер необходимо в разделе «Серверы» основного меню выбрать целевой сервер, после чего в открывшемся окне во вкладке «Оборудование» – «Процессоры» отобразится следующая информация о CPU:

1) сокеты, ядра и потоки:

– количество сокетов – количество процессорных сокетов на материнской плате сервера, в которые установлены физические процессоры;

– количество ядер на сокет – количество процессорных ядер, приходящихся на один сокет;

– количество потоков на ядро – количество потоков, приходящихся на один сокет;

– общее количество потоков – количество потоков на сервер;

– количество NUMA узлов – количество NUMA узлов на сервер;

2) физические процессоры:

– архитектура – архитектура установленных физических процессоров в сервер;

– общая максимальная частота – суммарная частота всех потоков сервера;

– модель – оптимальная модель vCPU для установленных процессоров, которая будет использоваться «по умолчанию»;

3) детальная информация о физических процессорах.

Процессоры – раскрывающийся список, в котором установленные процессоры упорядочены по их идентификатору. Для просмотра детальной информации необходимо выбрать интересующий процессор. В раскрывающемся меню приведена следующая информация:

– семейство – семейство процессора;

– производитель – производитель физического процессора;

– максимальная частота – максимальная рабочая частота процессора;

– версия – версия процессора;

– статус – текущий статус процессора;

4) занятые ВМ процессоры.

Занятые виртуальной машиной процессоры – раскрывающийся список индивидуально присвоенных ВМ ядер (потоков) физических процессоров. Настройка присвоения ядер (потоков) влияет на конечную производительность ВМ и описана в 3.8.7;

5) доступные функции – раскрывающийся список доступных функций и инструкций физического процессора;

6) тип процессора.

3.6.7.2. IPMI

3.6.7.2.1. IPMI-управление сервером необходимо для операций ограждения (при авариях) и управления электропитанием серверов в составе кластера в режиме динамического управления питанием в кластере.

Также на основании ответа Baseboard Management Controller (BMC) сервера принимается решение о запуске ВМ на другом сервере кластера.

3.6.7.2.2. Настройка доступа по IPMI-интерфейсу сервера необходима для использования типа ограждения «IPMI» при настройке связности узла (в окне «Серверы» – <имя сервера> – «Настройка связанности»). При нажатии кнопки «Настройки» – «Получить IP» происходит опрос BMC сервера на предмет текущих сетевых настроек первого канала управления IPMI. Если IP-адрес не отобразился, то стоит проверить работоспособность BMC платы сервера или ввести адрес вручную.

Примечание. Есть ли «жизнь» без IPMI? Есть, но с некоторыми ограничениями в плане ограждения сервера.

3.6.7.2.3. Для управления питанием сервера необходимо перейти в Web-интерфейсе в раздел «Серверы» основного меню, выбрать целевой сервер, далее перейти во вкладку «Оборудование» и в раскрывшемся списке выбрать «IPMI». В открывшемся окне будут доступны следующие действия:

– запуск сервера. Для того чтобы выполнить запуск сервера, необходимо нажать кнопку «  »;

– приостановка работы сервера. Для того чтобы приостановить работу сервера, необходимо нажать кнопку «»;

– перезагрузка сервера. Для того чтобы выполнить перезагрузку сервера, необходимо нажать кнопку «»;

– принудительная перезагрузка сервера. Для того чтобы выполнить принудительную перезагрузку сервера, необходимо нажать кнопку «»;

– выключение сервера. Для того чтобы выполнить выключение сервера, необходимо нажать кнопку «».

ВНИМАНИЕ! Перед управлением питанием необходимо перевести сервер в «Сервисный режим», нажав кнопку «Сервисный режим». После окончания работ, связанных с управлением питанием сервера, необходимо перевести сервер в «Стандартный режим», нажав кнопку «Стандартный режим». Подробная информация о «Сервисном»/«стандартном» режимах приведена в 3.6.5.2.

3.6.7.2.4. Для получения списка датчиков IPMI и их показаний необходимо нажать кнопку (запросить состояние датчиков).

3.6.7.2.5. Для того чтобы выполнить настройку IPMI сервера, необходимо перейти в Web-интерфейсе в раздел «Серверы» основного меню, выбрать целевой сервер, далее перейти во вкладку «Оборудование», в раскрывшемся списке выбрать «IPMI» и нажать кнопку «Настройки». В открывшемся окне необходимо настроить следующие поля:

– IP-адрес IPMI – это IP-адрес платы управления IPMI. Его можно получить автоматически, нажав кнопку «Получить IP». Если автоматическое получение IP-адреса не работает или полученный IP-адрес некорректный, то необходимо проверить работоспособность BMC платы или ввести его вручную в соответствующее поле;

– имя пользователя IPMI – это имя (логин) учетной записи IPMI, от имени которой будут выполняться все дальнейшие действия;

– пароль IPMI – это пароль от используемой учетной записи IPMI.

После заполнения всех полей необходимо нажать кнопку «Сохранить».

Примечание. Перед изменением IPMI настроек необходимо убедиться (в Web-интерфейсе), что в BMC сервера включена поддержка запросов по сети (например, опция «IPMI over Lan» в iDRAC). Проверить доступность IPMI можно командой

ipmitool -I lanplus -H [ipmi_ip] -U [ipmi_username] -P [ipmi_password] power status

Если при изменении настроек IPMI появляется ошибка «Интерфейс IPMI на указанном адресе недоступен с указанными параметрами», то следует посмотреть детальную ошибку в журнале контроллера в CLI командой

log controller

3.6.7.2.6. Ниже приведены варианты использования IPMI:

– для удобного мониторинга состояния датчиков материнской платы;

– для связности контроллера с сервером и его ограждения. Подробное описание приведено в 3.6.12 данного руководства;

– для использования кластерного транспорта типа «gfs2». Подробное описание приведено в 3.9.11.1 данного руководства;

– для «watchdog». Подробное описание приведено в 3.9.11.1 данного руководства.

3.6.7.3. Сведения о HDD

3.6.7.3.1. В SpaceVM поддерживаются диски и созданные на них блочные тома объемом до 100 Тбайт.

3.6.7.3.2. Для просмотра информации об установленных HDD на сервер необходимо в разделе «Серверы» основного меню выбрать целевой сервер, после чего в открывшемся окне во вкладке «Оборудование» – «Сведения о HDD» отобразится следующая информация о всех установленных HDD на сервер:

1) основная информация о диске:

– ID диска – уникальный ID диска;

– CONN_TYPE – тип подключения диска;

– DRIVE_NAME – имя устройства в системе;

2) идентификационная информация.

IDENTIFY – раскрывающийся список идентификационной информации, который может отличаться в зависимости от модели и производителя диска. Как правило, идентификационная информация содержит следующие данные:

– производитель диска;

– модель диска;

– серийный номер диска;

– доступная емкость диска;

– максимальная скорость вращения шпинделя жесткого диска (HDD) или тип диска для твердотельных накопителей (SSD);

– форм-фактор диска;

– поддержка SMART.

Примечание. Необходимо учитывать, что подключенные по iSCSI и FC (Fiber Channel) блочные устройства LUN определяются гипервизором как локальные устройства. В этом случае в модели устройства IDENTIFY в поле «Vendor» (производитель диска) будет указан поставщик LUN;

3) результаты самодиагностики.

SMART – при поддержке технологии SMART раскрывающийся список, который содержит результаты самопроверки диска. В зависимости от типа диска и производителя информация, содержащаяся в результате самопроверки диска, может отличаться.

Пример входящей информации:

– количество переназначенных секторов;

– общее время работы диска;

– количество полных циклов включения-выключения диска;

– текущая температура диска;

– состояние пула резервных блоков;

– общее количество ошибок, происходящих при записи сектора;

– число секторов, являющихся кандидатами на замену;

4) статус.

STATUS – раскрывающийся список, который содержит текущее состояние диска.

3.6.7.3.3. Для формирования графика использования дисков необходимо в поле «Выбрать устройства для вывода метрик» выбрать целевой диск (можно выбрать несколько).

При наличии данных будут выведены следующие графики для каждого выбранного диска:

– read – скорость чтения (Мбит/с);

– write – скорость записи (Мбит/с);

– r_await – среднее время (миллисекунды) на обработку запросов на чтение (включает время, потраченное в очереди на обработку и время на обработку запроса);

– w_await – среднее время (миллисекунды) на обработку запросов на запись (включает время, потраченное в очереди на обработку и время на обработку запроса);

– wrqms – обобщенное количество запросов на запись в секунду;

– rrqms – обобщенное количество запросов на чтение в секунду;

– rs – количество запросов на чтение в секунду;

– ws – количество запросов на запись в секунду;

– io_now – текущее число выполняемых операций ввода-вывода;

– util – процент процессорного времени, в течение которого диску были отправлены запросы ввода-вывода;

– avgrq – средний размер (в секторах) запросов к диску;

– avgqu – средний размер очереди запросов к диску.

3.6.7.3.4. Для удобства анализа использования аппаратных мощностей кластера можно настроить отображение графиков, нажав на кнопку слева от графиков «Задать интервал» и в открывшемся окне настроить интервал.

3.6.7.3.5. Для увеличения определенного интервала можно нажать на кнопку «Масштабировать» и в миниатюрном изображении графиков под основными графиками выделить область для просмотра.

3.6.7.4. Остальное оборудование

3.6.7.4.1. В окне «Серверы» – <имя сервера> – «Оборудование» – «Остальное оборудование» отображаются все устройства системы, фактически повторяя вывод результата работы утилиты Linux «lshw». Для того чтобы получить информацию об оборудовании, необходимо в левой верхней части окна раскрыть список, нажав на знак «+», после чего в открывшемся окне отобразится следующая информация:

– bus (раскрывающийся многоуровневый список) – основная шина PCI express;

– power – информация о блоках питания;

– network – активные системные сетевые интерфейсы.

3.6.7.5. Память

3.6.7.5.1. Для получения информации об используемой сервером оперативной памяти необходимо перейти в окно «Серверы» – <имя сервера> – «Оборудование» – «Память».

3.6.7.5.2. В открывшемся окне «Память» содержится следующая информация:

1) оперативная память (Мбайт);

2) состояние механизма очистки памяти «Ballooning» (вкл/выкл);

3) настройки «Swappiness» (раскрывающийся список). При нажатии на кнопку редактирования в открывшемся окне отображаются следующие параметры с возможностью их изменения:

– процент свободной оперативной памяти;

– уровень выделяемой памяти под кэш в условных единицах (меняется от «0» до «100»);

4) настройки «Дедупликации» (раскрывающийся список):

– состояние дедупликации;

– количество полных сканирований (Full scans);

– Max page sharing;

– режим дедуплицирования памяти между NUMA nodes на узле (Merge across nodes);

– использующиеся дедуплицированные страницы памяти (Pages shared);

– дедуплицированные страницы памяти (Pages sharing);

– страницы памяти для проверки (Pages to scan);

– недедуплицированные страницы памяти (Pages unshared);

– быстро меняющиеся страницы памяти для дедуплицирования (Pages volatile);

– работа сервиса (Run);

– время ожидания между сканированиями (Sleep millisecs);

– Stable node chains;

– Stable node chains prune millisecs;

– Stable node dups;

– Use zero pages.

В окне также имеется возможность обновления информации о ресурсах и настройка параметров системы сжатия и дедупликации страниц памяти.

3.6.7.5.3. Обновление информации о ресурсах производится после изменения аппаратной конфигурации сервера – изменения количества и (или) типа процессоров, памяти, дисков.

3.6.7.5.4. Включение и настройки механизма дедупликации производится с помощью кнопки редактирования, при нажатии на которую в открывшемся окне можно настроить:

1) управление работой системы (раскрывающийся список) Может принимать значения:

– выключить с сохранением имеющихся дупликацированных страниц;

– включить;

– выключить и сбросить все дедупликацированные страницы;

2) режим доступности дедуплицированных страниц между NUMA (Non-Uniform Memory Access) узлами (раскрывающийся список). Может принимать значения:

– страницы памяти становятся общими в рамках одного NUMA узла;

– страницы памяти становятся общими для всех NUMA узлов;

3) время перерыва между сканированиями страниц памяти;

4) количество страниц памяти для сканирования за один цикл.

Для сохранения изменений необходимо нажать кнопку «Изменить».

Для закрытия окна «Изменение параметров системы сжатия и дедупликации страниц памяти» необходимо нажать кнопку «Закрыть» или  .

Настройка сжатия и дедупликации страниц памяти сервера управляет механизмами контроля выделения страниц памяти NUMA узлам и появления дубликатов страниц при их перераспределении. Включение данных механизмов предотвращает возможность доступа к «теневым копиям» страниц памяти сервера, ищет и убирает дублирующие страницы памяти, но негативно влияет на производительность системы.

3.6.7.6. Пределы ресурсов

3.6.7.6.1. Для получения информации о пределах ресурсов необходимо перейти в окно «Серверы» – <имя сервера> – «Оборудование» – «Пределы ресурсов».

В данном окне отображается информация о состоянии динамического управления ресурсами:

– верхний аварийный уровень загрузки процессора – при достижении CPU данной отметки будет выведено событие с предупреждением о том, что достигнут аварийный уровень загрузки системы. Также в случае, если включен DRS, выбран режим создания виртуальных машин и воздействий HARD и выбраны типы собираемых метрик CPU или CPU_MEMORY, SpaceVM предпримет попытки живой миграции ВМ с целью понизить нагрузку на данный сервер;

– верхний предупредительный уровень загрузки процессора – при достижении CPU данной отметки будет выведено событие с предупреждением о том, что достигнут предупредительный уровень загрузки системы;

– верхний аварийный уровень загрузки памяти – при достижении RAM данной отметки будет выведено событие с предупреждением о том, что достигнут аварийный уровень загрузки системы. Также в случае, если включен DRS, выбран режим создания виртуальных машин и воздействий HARD и выбраны типы собираемых метрик MEMORY или CPU_MEMORY, SpaceVM предпримет попытки живой миграции ВМ с целью понизить нагрузку на данный сервер;

– верхний предупредительный уровень загрузки памяти – при достижении RAM данной отметки будет выведено событие с предупреждением о том, что достигнут предупредительный уровень загрузки системы.

Подробная информация о механизме DRS содержится в 3.5.2.9.

Данные настройки предназначены для ограничения загруженности сервера. При изменении базовых настроек необходимо учитывать возможную пиковую нагрузку на сервер. Также данные настройки влияют на распределение ВМ по серверам при срабатывании механизмов ВД при автоматическом распределении ВМ.

Для применения настроек необходимо нажать на кнопку «Сохранить» (доступно, если вносились изменения).

3.6.8. «Серверы» – <имя сервера> – «Пулы ресурсов»

3.6.8.1. В окне «Серверы» – <имя сервера> – «Пулы ресурсов» содержится список относящихся к серверу пулов ресурсов, включая для каждого из них:

– название – название пула ресурса, в который входит данный сервер;

– ВМ – количество ВМ, которые созданы в рамках данного пула ресурсов;

– ограничение памяти – ограничение RAM, указанное в настройках данного пула ресурсов;

– ограничение CPU – ограничение CPU, указанное в настройках данного пула ресурсов.

Также в этом окне существует возможность создания нового пула по кнопке «Создать пул ресурсов» и выбора определенного пула с применением фильтра по кнопке «Фильтр».

3.6.8.2. Подробное описание пулов ресурсов приведено в 3.7 данного руководства.

3.6.9. «Серверы» – <имя сервера> – «Хранилища»

Для управления подсистемой хранения необходимо перейти в окно «Серверы» – <имя сервера> – «Хранилища».

В окне управления хранилищами содержится:

– информация о настроенных на сервере пулах данных;

– информация о ZFS-пулах;

– информация о подключенных к серверу файловых сетевых хранилищах;

– информация о подключенных к серверу блочных сетевых хранилищах;

– управление блочными устройствами (локальными томами LVM);

– управление кластерными транспортами;

– управление томами.

3.6.9.1. Пулы данных

3.6.9.1.1. Для просмотра информации о подключенных к серверу пулах данных необходимо в разделе «Серверы» основного меню выбрать целевой сервер, после чего в открывшемся окне во вкладке «Хранилища» – «Пулы данных» отобразится таблица, содержащая следующую информацию:

– название – название подключенного пула данных к серверу;

– тип – тип пула данных;

– серверы – количество серверов, к которым подключен данный пул данных;

– диски – количество содержащихся виртуальных дисков на данном пуле данных;

– образы – количество содержащихся образов ISO на данном пуле данных;

– файлы – количество содержащихся файлов на данном пуле данных;

– использовано/всего – занятый и общий объем пула данных;

– приоритет;

– статус – статус пула данных.

3.6.9.1.2. Также в окне «Серверы» – <имя сервера> – «Хранилища» – «Пулы данных» имеется возможность:

– создание нового пула. Для этого необходимо нажать кнопку «Создать» и в открывшемся окне ввести необходимые данные;

– фильтр списка пулов данных. Для этого необходимо нажать кнопку «Фильтр»;

– сканирование подключенных пулов данных к серверу. Для этого необходимо нажать кнопку «Сканировать»;

– сбор статистики работы пула данных. Для этого необходимо нажать кнопку «Статистика I/O». При нажатии открывается окно выбора параметров сбора с заданными значениями «по умолчанию». Сбор происходит с сервера в верхней директории всех активных пулов данных типа «файловый» с размером блока 4K.

3.6.9.1.3. Подробное описание пулов данных приведено в 3.9.3 данного руководства.

3.6.9.2. ZFS-пулы

3.6.9.2.1. Для просмотра информации о подключенных к серверу ZFS-пулах необходимо в разделе «Серверы» основного меню выбрать целевой сервер, после чего в открывшемся окне во вкладке «Хранилища» – «ZFS-пулы» отобразится таблица, содержащая следующую информацию:

– название – название подключенного ZFS-пула к серверу;

– сервер – имя сервера, к которому подключен данный ZFS-пул;

– тип – тип ZFS-пула;

– размер – объем ZFS-пула;

– health – состояние ZFS-пула;

– локальные устройства – количество локальных дисковых устройств, используемых для создания данного ZFS-пула;

– LUNs – количество сетевых дисковых устройств, используемых для создания данного ZFS-пула;

– статус – статус пула данных.

3.6.9.2.2. Также в окне «Серверы» – <имя сервера> – «Хранилища» – «ZFS пулы» имеется возможность:

– создание нового ZFS-пула. Для этого необходимо нажать кнопку «Добавить ZFS» и в открывшемся окне ввести необходимые данные;

– фильтр списка пулов данных. Для этого необходимо нажать кнопку «Фильтр»;

– сканирование подключенных ZFS-пулов к серверу. Для этого необходимо нажать кнопку «Сканировать».

3.6.9.2.3. Подробное описание ZFS-пулов приведено в 3.9.8 данного руководства.

3.6.9.3. Файловые хранилища

3.6.9.3.1. Для просмотра информации о подключенных к серверу файловых хранилищах необходимо в разделе «Серверы» основного меню выбрать целевой сервер, после чего в открывшемся окне во вкладке «Хранилища» – «Файловые хранилища» отобразится таблица, содержащая следующую информацию:

– название – название подключенного файлового хранилища;

– тип подключения – тип подключения файлового хранилища;

– использовано/всего – занятый и общий объем файлового хранилища;

– пулы данных – количество пулов данных, использующих данное файловое хранилище;

– серверы – количество серверов, к которым подключен данный пул данных;

– статус – статус пула данных.

3.6.9.3.2. Также в окне «Серверы» – <имя сервера> – «Хранилища» – «Файловые хранилища» имеется возможность:

– добавить новое файловое хранилище. Для этого следует нажать кнопку «Добавить» и ввести необходимые данные в открывшемся окне;

– сканировать подключенные к серверу файловые хранилища. Для этого необходимо нажать кнопку «Сканировать».

3.6.9.3.3. Подробное описание файловых хранилищ приведено в 3.9.9.1 данного руководства.

3.6.9.4. Блочные хранилища

3.6.9.4.1. Для просмотра информации о подключенных к серверу блочных хранилищах необходимо в разделе «Серверы» основного меню выбрать целевой сервер, после чего в открывшемся окне во вкладке «Хранилища» – «Блочные хранилища» отобразится таблица, содержащая следующую информацию:

– название – название подключенного блочного хранилища;

– тип подключения – тип подключения блочного хранилища;

– статус – статус пула данных.

3.6.9.4.2. В окне «Серверы» – <имя сервера> – «Хранилища» – «Блочные хранилища» имеется возможность:

– сканирование SCSI Hosts. Для этого необходимо нажать кнопку «Сканировать SCSI HOSTS»;

– сканирование подключенных к серверу блочных хранилищ. Для этого необходимо нажать кнопку «Сканировать»;

– редактирование подключенных WWNS-хранилищ. Для этого необходимо нажать кнопку «WWNS»;

– получение локальных WWNS-хранилищ. Для этого необходимо нажать кнопку «Локальные WWNS»;

– получение iSCSI инициатора узла с возможностью его изменения. Для этого необходимо нажать кнопку «Имя инициатора iscsi»;

– добавление нового блочного хранилища. Для этого необходимо нажать кнопку «Добавить» и в открывшемся окне ввести соответствующие данные.

3.6.9.4.3. Подробное описание блочных хранилищ приведено в 3.9.9.2 данного руководства.

3.6.9.5. Блочные устройства

3.6.9.5.1. Для управления дисковой подсистемой сервера в окне «Серверы» – <имя сервера> – «Хранилища» – «Блочные устройства» существуют возможности управления блочными устройствами (группами логических разделов, группами томов LVM).

3.6.9.5.2. В окне «Управление блочными устройствами» содержится информация об имеющихся блочных устройствах, включая название группы, общий и свободный объем, возможность расширения и удаления.

Управление блочными устройствами позволяет изменять конфигурацию дисковой подсистемы (добавлять и удалять физические диски, управляемые менеджером LVM), без необходимости обращаться к консоли сервера.

В окне «Управление блочными устройствами» предусмотрена возможность создания, расширения и удаления новых групп логических разделов на физических дисках, не используемых в системном разделе.

Примечание. Создание, расширение и удаление новых групп логических разделов на съемных устройствах невозможно.

Дополнительные группы томов LVM могут использоваться для формирования пулов данных форматов LVM и thin-LVM (далее *LVM) в окне «Серверы» – <имя сервера> – «Хранилища – «Пулы данных». Пулы данных форматов *LVM используются для размещения виртуальных дисков ВМ на логических разделах в рамках группы. Таким образом, в ВМ в качестве жесткого диска предоставляется не файл формата «qcow2», а блочное устройство, являющееся логическим разделом физического жесткого диска (раздел LVM).

Тома LVM, размещенные в группах LVM на физических дисках сервера, имеют более высокую производительность, но возможности по операциям над ними ограничены.

ВНИМАНИЕ! Будьте осторожны при операциях с системным разделом диска.

Примечание. При использовании хранилищ форматов *LVM необходимо понимать принцип работы механизмов самого LVM и предоставления логического раздела в качестве НЖМД для ВМ.

3.6.9.5.3. Для создания группы необходимо в окне «Управление блочными устройствами»:

– нажать кнопку «Создать группу VG»;

– если в дисковой подсистеме сервера есть неиспользуемое (неразмеченное) дисковое пространство, то в открывшемся окне необходимо ввести название группы логических томов и выбрать блочные устройства для включения в группу;

– если неиспользуемого пространства нет, то появится надпись «нет доступных блочных устройств»;

– для сохранения изменений нажать кнопку «Сохранить».

После успешного создания группы она отобразится в списке блочных устройств.

Примечание. В списке доступных блочных устройств показываются только устройства без разметки (разделов). Чтобы очистить требуемое устройство от ранее созданной разметки, следует воспользоваться командой CLI *wipefs [-h] [drive ...]*, после этого устройство появится в списке. В случае устройств LUN, возможно, потребуется отключить и заново присоединить устройство.

3.6.9.5.4. В окне «Управление блочными устройствами» для свободного устройства существует возможность:

– расширения. При нажатии на кнопку «Расширить» в открывшемся окне необходимо выбрать из раскрывающегося списка дополнительные блочные устройства, после чего подтвердить операцию, нажав кнопку «Расширить»;

– очистки дисков узла (полная очистка). Доступно для незадействованного устройства. Выполняется при нажатии на кнопку «Очистка дисков узла». В открывшемся окне необходимо выбрать из раскрывающегося списка блочное устройство, после чего подтвердить операцию, нажав кнопку «Сохранить».

3.6.9.5.5. Управление связанными объектами производится в разделе «Хранилища» основного меню и соответствующих подразделах интерфейса. Более подробное описание приведено в 3.9.10 данного руководства.

3.6.9.6. Кластерные транспорты

3.6.9.6.1. Для просмотра информации о подключенных к серверу кластерных транспортах необходимо в разделе «Серверы» основного меню выбрать целевой сервер, после чего в открывшемся окне во вкладке «Хранилища» – «Кластерные транспорты» отобразится таблица, содержащая следующую информацию:

– название – название подключенного кластерного транспорта;

– кластер – кластер, к которому подключен данный кластерный транспорт;

– тип – тип кластера;

– статус – статус кластерного транспорта.

3.6.9.6.2. Для добавления хранилища необходимо нажать кнопку «Создать». В открывшемся окне заполнить следующие поля:

– название хранилища;

– его описание;

– кластер, в котором расположено хранилище (выбор из раскрывающегося списка);

– тип хранилища (выбор из раскрывающегося списка);

– LUN (выбор из раскрывающегося списка);

– определиться с выбором внешней сети.

Для подтверждения операции необходимо нажать кнопку «Создать».

3.6.9.6.3. Более подробное описание приведено в 3.9.11.1 данного руководства.

3.6.9.7. Тома

3.6.9.7.1. Для просмотра информации о подключенных к серверу томах необходимо в разделе «Серверы» основного меню выбрать целевой сервер, после чего в открывшемся окне во вкладке «Хранилища» – «Тома» отобразится таблица, содержащая следующую информацию:

– название – название подключенного тома;

– кластерный транспорт – название кластерного транспорта, используемого для подключения;

– тип – тип транспорта для тома;

– использовано/всего – занятый и общий объем тома;

– gluster статус;

– статус – статус кластерного транспорта.

3.6.9.7.2. Для добавления тома необходимо нажать кнопку «Создать». В открывшемся окне заполнить следующие поля:

– название хранилища;

– его описание;

– тип тома (выбор из раскрывающегося списка);

– кластерные транспорты (выбор из раскрывающегося списка);

– разделы (ZFS пулы);

– размер записи (выбор из раскрывающегося списка);

– значение репликации тома;

– наличие раздела арбитра в реплицированном томе (вкл/выкл);

– определиться с созданием пула данных (вкл/выкл).

Для подтверждения операции необходимо нажать кнопку «ОК».

3.6.9.7.3. Более подробное описание приведено в 3.9.11.2 данного руководства.

3.6.10. «Серверы» – <имя сервера> – «Виртуальные машины»

3.6.10.1. Для получения списка ВМ и шаблонов необходимо перейти в окно «Серверы» – <имя сервера> – «Виртуальные машины». В данном окне существует два подраздела «Виртуальные машины» и «Шаблоны». В каждом из подразделов представлен список объектов, размещенных на данном сервере.

3.6.10.2. Управление ВМ в составе данного сервера производится в окне «Серверы» – <имя сервера> – «Виртуальные машины» – «Виртуальные машины».

3.6.10.3. Управление шаблонами ВМ в составе данного сервера производится в окне «Серверы» – <имя сервера> – «Виртуальные машины» – «Шаблоны».

3.6.10.4. Для ВМ и шаблонов ВМ на выбранном сервере в окне управления ВМ предусмотрены следующие операции:

– включение всех ВМ сервера. Для этого необходимо нажать кнопку «Включение всех ВМ» и в открывшемся окне подтвердить операцию, нажав кнопку «Да»;

– выключение всех ВМ сервера. Для этого необходимо нажать кнопку «Выключение всех ВМ» и в открывшемся окне выставить тайм-аут ожидания выключения питания ВМ, после чего подтвердить операцию, нажав кнопку «ОК»;

– порядок загрузки всех ВМ сервера при работе ВД. При нажатии соответствующей кнопки открывается информационное окно с очередностью загрузки существующих ВМ. Окно закрывается с помощью кнопки «Закрыть» или  ;

– миграция всех ВМ сервера на доступные серверы. Для этого необходимо нажать кнопку «Миграция всех ВМ» и в открывшемся окне подтвердить операцию, нажав кнопку «Да»;

– сканирование ВМ. При нажатии соответствующей кнопки открывается информационное окно с выявленными незарегистрированными ВМ. Окно закрывается с помощью кнопки «Закрыть» или  .

3.6.10.5. Для выбора определенной ВМ из списка с применением фильтра необходимо нажать на кнопку «Фильтр» и в открывшемся окне заполнить следующие поля:

– «Имя виртуальной машины» – название искомой ВМ;

– «Состояние питания» – выбор из раскрывающегося списка («Без фильтра», «включена» или «Выключена»);

– «Серверы» – выбор из раскрывающегося списка;

– «Пул данных» – выбор из раскрывающегося списка;

– «Кластеры» – выбор из раскрывающегося списка;

– «Локация» – выбор из раскрывающегося списка;

– «Пулы ресурсов» – выбор из раскрывающегося списка;

– «Виртуальные сети» – выбор из раскрывающегося списка;

– «Теги» – выбор из раскрывающегося списка.

После настройки фильтра необходимо нажать «Применить» или «Сбросить все».

3.6.10.6. В окне управления ВМ содержится список виртуальных машин, существующих в системе и привязанных к данному серверу, включая для каждой из них ее название, сервер, IP-адрес, количество виртуальных процессоров vCPU, объем виртуальной оперативной памяти vRAM, количество виртуальных дисков vDisk и сетевых адаптеров vNIC, количество виртуальных функций vFunc и статус.

3.6.10.7. Подробное описание ВМ приведено в 3.8 данного руководства.

3.6.10.8. В окне «Серверы» – <имя сервера> – «Виртуальные машины» – «Шаблоны» содержится информация о шаблонах, включая для каждого из них его название, сервер, IP-адрес, сведения о vCPU, vRAM, vDisk, vNIC и статус.

Работа с шаблонами ВМ происходит аналогично работе с ВМ.

3.6.10.9. SpaceVM поддерживает установку всех антивирусных программных средств в ВМ с гостевыми ОС семейств Windows и Linux, в том числе, специализированных, работающих в сочетании с уровнем виртуализации, например, «Kaspersky Security для виртуальных сред. Легкий агент».

3.6.11. «Серверы» – <имя сервера> – «Сети»

3.6.11.1. Виртуальные сети

3.6.11.1.1. Для просмотра информации о виртуальных сетях сервера необходимо в разделе «Серверы» основного меню выбрать целевой сервер, после чего в открывшемся окне во вкладке «Сети» – «Виртуальные сети» отобразится таблица, содержащая следующую информацию:

– название – название виртуальной сети;

– связанность – тип связанности в виртуальной сети;

– подсеть – подсеть виртуальной сети;

– VLAN ID – тег по стандарту 802.1Q, который присваивается всему трафику данной сети;

– используется брандмауэр – параметр, который указывает, используется ли межсетевой экран для данной сети;

– статус – статус виртуальной сети.

3.6.11.1.2. Подробная о виртуальных сетях содержится в 3.10.5.

3.6.11.2. Виртуальные коммутаторы

3.6.11.2.1. Виртуальные коммутаторы (ВК) – это коммутаторы уровня сервера (узла), предназначенные для управления физическими сетевыми интерфейсами сервера, внутренними интерфейсами сервера и обеспечения L2-связанности распределенных коммутаторов.

3.6.11.2.2. Для просмотра информации о виртуальных коммутаторах сервера необходимо в разделе «Серверы» основного меню выбрать целевой сервер, после чего в открывшемся окне во вкладке «Сети» – «Виртуальные коммутаторы» отобразится таблица, содержащая следующую информацию:

– название – название виртуального коммутатора;

– сервер – название сервера, на котором находится виртуальный коммутатор;

– тип – тип виртуального коммутатора;

– статус – статус виртуального коммутатора.

3.6.11.2.3. Также в окне управления ВК («Серверы» – <имя сервера> – «Сети» – «Виртуальные коммутаторы») имеется возможность добавить новый ВК, используя кнопку «Добавить виртуальный коммутатор». При нажатии на эту кнопку открывается окно, в котором необходимо заполнить следующие поля:

– название ВК;

– описание ВК (при необходимости);

– тип (выбрать из раскрывающегося списка).

Для подтверждения операции необходимо нажать кнопку «ОК».

3.6.11.2.4. Информацию по коммутатору можно получить, нажав на его название в списке коммутаторов.

3.6.11.2.5. Дополнительная информация и управление ВК приведены в 3.10.2.1 и 3.10.3.4 данного руководства.

3.6.11.3. Внутренние интерфейсы

3.6.11.3.1. Внутренние интерфейсы – это виртуальные интерфейсы уровня гипервизора, подключаемые в порт-группы виртуального коммутатора. Основным внутренним интерфейсом является «mgmt», через который происходит взаимодействие между серверами в составе кластера.

За счет настройки дополнительных внутренних интерфейсов можно отделить от сети управления сеть передачи данных (доступ к NFS и iSCSI), сеть доступа к интерфейсу управления, сеть управления серверами по IPMI и другие сети.

3.6.11.3.2. Для просмотра информации о внутренних интерфейсах сервера необходимо в разделе «Серверы» основного меню выбрать целевой сервер.

После этого в открывшемся окне во вкладке «Сети» – «Внутренние интерфейсы» отобразится таблица, содержащая следующую информацию:

– название – название внутреннего интерфейса;

– IP-адрес – IP-адрес внутреннего интерфейса в сети;

– маска подсети – маска подсети сети, к которой подключен внутренний интерфейс;

– DHCP – параметр, который указывает, включено ли на внутреннем интерфейсе автоматическое получение сетевых настроек;

– MAC-адрес – MAC (физический адрес) внутреннего интерфейса;

– подключение к виртуальному коммутатору – название внутреннего ВК, к которому подключен внутренний интерфейс;

– статус – статус внутреннего интерфейса.

3.6.11.3.3. Информацию о конкретном внутреннем интерфейсе можно получить, нажав на его название в списке интерфейсов.

3.6.11.3.4. Также в окне управления внутренними интерфейсами («Серверы» – <имя сервера> – «Сети» – «Внутренние интерфейсы») имеется возможность добавить интерфейс, используя кнопку «Добавить». При нажатии на эту кнопку открывается окно, в котором необходимо заполнить следующие поля:

– название интерфейса;

– описание интерфейса (при необходимости);

– ВК (выбрать из раскрывающегося списка);

– порт-группа (выбрать из раскрывающегося списка);

– протокол DHCP (включить или выключить);

– IP-адрес;

– маска подсети;

– MAC-адрес.

Для подтверждения операции необходимо нажать кнопку «ОК».

3.6.11.3.5. Дополнительная информация приведена в 3.10.2.5 и 3.10.3.4 данного руководства.

3.6.11.4. Агрегированные интерфейсы

3.6.11.4.1. Агрегированные интерфейсы – это список групповых сетевых интерфейсов. Каждый агрегированный интерфейс представляет собой группу физических интерфейсов сервера со своей политикой объединения.

Политики объединения могут быть как для резервирования, так и для увеличения пропускной способности каналов связи.

Необходимо учитывать, что при группировании интерфейсов для увеличения пропускной способности с балансировкой нагрузки и применением протокола LACP, порты физического коммутатора, к которым подключена данная группа физических интерфейсов, также должны быть собраны в группу, и на них должна быть включена поддержка LACP.

Попытка агрегировать несколько портов с использованием уже настроенных ранее может привести к временной потере сетевого соединения. Это связано с тем, что перед агрегацией ранее настроенный порт должен быть отсоединен от своих старых связей. При удалении агрегированного порта (высвобождении сетевых интерфейсов из объединения) их настройки (VLAN, MTU) сбрасываются.

3.6.11.4.2. В окне «Серверы» – <имя сервера> – «Сети» – «Агрегированные интерфейсы» содержится список агрегированных интерфейсов сервера, включая для каждого из них его режим агрегации и LACP, LACP time, переключение в режим, состояние и статус.

3.6.11.4.3. Для агрегации нескольких интерфейсов необходимо в окне управления агрегированными интерфейсами сервера нажать кнопку «Добавить».

В открывшемся окне необходимо заполнить необходимые поля:

1) название агрегированного интерфейса;

2) описание агрегированного интерфейса (при необходимости);

3) ВК (выбрать из раскрывающегося списка);

4) порт-группа (выбрать из раскрывающегося списка);

5) физические интерфейсы (выбрать из раскрывающегося списка), которые будут объединены (агрегированы). Если при создании агрегированного интерфейса в раскрывающемся списке написано «нет доступных интерфейсов», это означает отсутствие на узле доступных для добавления устройств;

6) тип агрегации (выбрать из раскрывающегося списка). Настройка типа агрегации выбирается исходя из потребностей и возможностей сетевого оборудования:

– «active-backup» – режим резервирования. Резервный канал не используется;

– «balance-tcp» – режим балансировки с использованием LACP;

– «balance-slb» – режим простой балансировки на основе MAC и VLAN.

Для правильного выбора режима необходимо обратиться к своему сетевому администратору;

7) связь протокола управления агрегацией каналов (выбрать из раскрывающегося списка);

8) включение агрегированного интерфейса после создания.

Для подтверждения операции необходимо нажать кнопку «ОК».

Примечание. Для использования «balance-tcp» необходимо предварительно включить поддержку LACP у физического коммутатора, к которому подключены агрегируемые порты. Порты, агрегируемые по этому типу, должны быть подключены в порты коммутатора, объединенные в порт-группу. Порт-группа физического коммутатора с включенным LACP не будет пропускать трафик пока не увидит, что порты сервера прошли агрегацию. Это необходимо учитывать при настройке и, если агрегация данного типа будет применяться для сети управления, ее необходимо делать из CLI-интерфейса сервера и при наличии доступа к интерфейсу управления коммутатором. При отсутствии поддержки LACP со стороны коммутатора сформируется сетевая петля, что приведет к срабатыванию защиты от петель.

3.6.11.4.4. Информацию по агрегированному интерфейсу можно получить, нажав на его название в списке интерфейсов.

Во вкладке «Информация» содержатся следующие сведения:

1) название;

2) описание (редактируемый параметр);

3) дата и время создания;

4) статус;

5) конфигурация управления агрегацией каналов (раскрывающийся список):

– связь протокола управления;

– тип агрегации (режим связи);

– резервный вариант протокола управления;

– время протокола управления;

– интервал ребаланса;

6) интерфейсы с возможностью их добавления по кнопке  . Каждый из интерфейсов содержит:

– состояние связи;

– скорость соединения;

– дуплексный режим;

– MTU;

– MAC-адрес.

Интерфейс можно удалить, нажав на «Удалить» в строке интерфейса;

7) сообщения о работе агрегированного интерфейса с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений.

3.6.11.4.5. Также в окне состояния выбранного агрегированного интерфейса предусмотрены следующие операции:

– обновление информации по кнопке  ;

– изменение параметров. Для этого необходимо нажать кнопку «Изменение параметров» и в открывшемся окне выбрать из раскрывающегося списка тип агрегации (режим связи) и связь протокола управления агрегацией каналов. Для сохранения изменений необходимо нажать кнопку «ОК»;

– включение (выключение) экземпляра. При нажатии кнопки «Включение (up)» или «Выключение (down)» в открывшемся окне необходимо подтвердить операцию, нажав на кнопку «Да»;

– удаление интерфейса. При нажатии кнопки «Удалить» в открывшемся окне необходимо определится с возможностью сохранения физического интерфейса после удаления соединения. Если опция «Оставить физический интерфейс» включена, осуществить выбор из раскрывающегося списка физического интерфейса и определится с возможностью включения агрегированного интерфейса после подключения. Далее необходимо подтвердить операцию, нажав кнопку «ОК».

3.6.11.5. Физические интерфейсы

3.6.11.5.1. В окне «Серверы» – <имя сервера> – «Сети» – «Физические интерфейсы» содержится список физических интерфейсов сервера, включая для каждого из них его название, поддержку SR-IOV, включен или выключен режим SR-IOV, включен или выключен неразборчивый режим, MTU, MAC-адрес, агрегацию, состояние, наличие физического подключения к серверу и статус (исправно или ошибка). Данные о состоянии интерфейсов берутся от гипервизора.

3.6.11.5.2. Информацию о состоянии физического интерфейса и его загруженности можно получить, нажав на название интерфейса в его окне управления.

В открывшемся окне состояния доступны следующие операции с физическим интерфейсом:

– обновление информации по кнопке  ;

– включение (выключение) интерфейса. При нажатии на кнопку «Включение (up)» («Выключение (down)») экземпляра» в открывшемся окне необходимо подтвердить операцию, нажав на кнопку «Да»;

– подключение (отключение) интерфейса. При нажатии на кнопку «Подключение» в открывшемся окне необходимо выбрать из раскрывающегося списка ВК и порт-группу, после чего подтвердить операцию, нажав кнопку «ОК». Для варианта с подключенным интерфейсом при нажатии на кнопку «Отключение (vswitch)» в открывшемся окне необходимо подтвердить операцию, нажав на кнопку «Да»;

– переподключение интерфейса. При нажатии на кнопку «Переподключение (vswitch)» в открывшемся окне необходимо выбрать из раскрывающегося списка ВК и порт-группу, после чего подтвердить операцию, нажав кнопку «ОК»;

– включение режима SR-IOV. При нажатии на кнопку «Включение SR-IOV» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «Да»;

– настройка длительности индикации светодиода. При нажатии на кнопку «LED» в открывшемся окне необходимо задать длительность индикации, после чего подтвердить операцию, нажав кнопку «ОК».

3.6.11.5.3. Также в окне состояния выбранного интерфейса содержится следующая информация:

1) графики загрузки «receive» и «transmit»;

2) название физического интерфейса;

3) его описание (редактируемый параметр);

4) дополнительная информация. Раскрывающаяся информация содержит:

– изготовитель;

– модель;

– драйвер;

– версия драйвера;

– PCI-устройство;

– неразборчивый режим (редактируемый параметр). Позволяет включить или выключить режим «Promisc»;

– MTU (редактируемый параметр);

– max MTU;

5) MAC-адрес;

6) включен в агрегацию («Да»/ «Нет»);

7) статус;

8) скорость соединения;

9) дуплексный режим;

10) состояние связи («Активен»/«Неактивен»);

11) состояние порта («Включен»/«Выключен»);

12) сообщения о работе интерфейса с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

ВАЖНО помнить, что физический интерфейс, настроенный при установке SpaceVM участвует в обеспечении работоспособности кластера. Все операции над этим интерфейсом необходимо проводить с учетом того, что при потере его настроек связь с управляемым сервером будет потеряна. Восстановление работоспособности сети будет возможно только через консоль сервера.

3.6.11.6. SR-IOV

3.6.11.6.1. В данном разделе описана возможность использования одного физического сетевого интерфейса несколькими ВМ с применением технологии SR-IOV.

3.6.11.6.2. Для использования технологии SR-IOV необходимо включить на целевом сервере поддержку IOMMU.

Примечание. Поделить интерфейс «InfiniBand» на виртуальные функции разрешается, но «прокинуть» функцию в ВМ на данный момент невозможно, так как ее MAC-адрес состоит из 20 байт, а не из 6, что вызывает ошибку гипервизора. Виртуальные функции можно «прокинуть» в ВМ через проброс PCI-устройств.

3.6.11.6.3. Для перевода физического интерфейса в режим SR-IOV необходимо выбрать нужный интерфейс с поддержкой SR-IOV и включить его в окне управления.

3.6.11.6.4. В окне «Серверы» – <имя сервера> – «Сети» – «SR-IOV» содержатся данные о режимах SR-IOV. Информацию о состоянии физического интерфейса и его запущенного режима SR-IOV можно получить, нажав на название интерфейса в его окне управления SR-IOV.

3.6.11.6.5. В окне состояния доступны следующие операции с физическим интерфейсом в режиме SR-IOV:

– обновление информации по кнопке  ;

– выключение SR-IOV. При нажатии на кнопку «Выключение SR-IOV» в открывшемся окне необходимо подтвердить операцию, нажав на кнопку «Да».

3.6.11.6.6. В окне состояния содержатся следующие сведения:

1) название (физического интерфейса);

2) описание;

3) дополнительная информация (раскрывающийся список):

– изготовитель;

– модель;

– драйвер;

– версия драйвера;

– PCI-устройства;

4) MAC-адрес;

5) включен в агрегацию («Да»/ «Нет»);

6) статус («ACTIVE»/«IN ACTIVE»);

7) скорость соединения;

8) дуплексный режим;

9) состояние связи;

10) состояние порта;

11) сообщения (список задач, отсортированный по дате).

3.6.11.6.7. Проверка использования одного физического сетевого интерфейса несколькими ВМ с применением технологии SR-IOV осуществляется следующим образом:

– необходимо включить SR-IOV на физическом интерфейсе. Перейти в раздел «Серверы» основного меню, выбрать целевой сервер, перейти во вкладку «Сети» – «Физические интерфейсы», выбрать целевой физический интерфейс с поддержкой технологии SR-IOV, нажать кнопку «Включение SR-IOV».

Таким образом, на физическом сетевом интерфейсе будут созданы виртуальные функции – виртуальные сетевые интерфейсы;

– далее необходимо создать ВМ. Проверка возможна при загрузке в режиме Live CD, поэтому создание диска и последующая установка операционной системы необязательны. После создания ВМ перейти в раздел «Виртуальные машины» основного меню, выбрать созданную ВМ, перейти во вкладку «Виртуальные функции», нажать кнопку «Добавить функцию», в раскрывающемся списке выбрать виртуальную функцию и нажать кнопку «ОК»;

– повторить предыдущий пункт необходимое количество раз, но не больше, чем количество доступных виртуальных функций, так как одна виртуальная функция может быть подключена к одной ВМ;

– включить созданные ВМ, после завершения загрузки. Если целевой физический сетевой интерфейс подключен к внешней сети с доступным DHCP-сервером, убедиться, что ВМ получили IP-адреса от DHCP сервера;

– проверить доступность ВМ между собой, выборочно выполнив команду

ping {IP-адрес другой ВМ} -c 1

– если целевой физический сетевой интерфейс подключен к внешней сети с доступом к сети Интернет, проверить доступность публичных DNS-серверов, выполнив на ВМ команду

ping 77.88.8.1 -c 1

3.6.12. «Серверы» – <имя сервера> – «Связность и ограждение»

3.6.12.1. Общая информация

3.6.12.1.1. Настройки связанности и ограждения – это определение механизмов контроля доступности сервера и управления его питанием.

3.6.12.1.2. Для обеспечения целостности данных ВМ может работать только на одном узле или любой другой службе кластера в одно и тоже время. Применение в конфигурации оборудования выключателей электропитания дает узлу возможность выполнять цикл выключения-включения питания другого узла до перезапуска служб ВД этого узла во время процесса отказов. Это предотвращает от одновременного доступа двух узлов к одним и тем же данным и к их разрушению. Ограждающие (fence) устройства используются для обеспечения гарантии целостности данных при сбоях в любых условиях.

3.6.12.1.3. В окне «Серверы» – <имя сервера> – «Связность и ограждение» можно получить информацию о текущих настройках:

– тип ограждения;

– тип связности;

– пулы данных.

Также существует возможность изменения настроек. При нажатии на кнопку «Изменить настройки» в открывшемся окне выбрать из раскрывающегося списка тип ограждения и тип связности, после чего подтвердить операцию, нажав кнопку «ОК».

Дополнительно можно и рекомендуется изменять настройки целиком на весь кластер в окне «Кластеры» – <имя кластера> – «Связность и ограждение».

3.6.12.2. Связность

3.6.12.2.1. Тип связанности отвечает за метод принятия решения о том, что на сервере произошла авария.

3.6.12.2.2. Тип связности может быть следующим:

– KERNEL – контролирует исполнение модулей системы управления на сервере. Контроллер открывает поток данных (grpc stream) до каждого узла по его UUID (hostname) и отправляет узлу свой IPv4-адрес. Узел при открытом потоке данных сверяет присланный ему адрес контроллера с адресом из его конфигурации и при совпадении раз в 1 секунду посылает через поток данных heartbeat. Контроллер при каждом получении heartbeat обновляет две метки с временем жизни 30 секунд (error label) и 60 секунд (hermit label) о доступности узла;

– KERNEL IPMI – дополнительно раз в 5 секунд проверяется доступность IPMI интерфейса сервера с контроллера (см. 3.6.7.2 данного руководства);

– KERNEL STORAGE – дополнительно раз в 5 секунд проверяется метаданные пула данных сервера на общем с контроллером файловом сетевом хранилище;

– AUTO – кроме проверки KERNEL связи при наличии настроек IPMI проверяется его доступность, при наличии общего пула данных проверяется и последний.

3.6.12.3. Ограждение

3.6.12.3.1. Ограждение – процесс получения подтверждения того, что аварийный сервер перешел в состояние, не допускающее повреждения ВМ («по умолчанию» – выключен). Тип ограждения может принимать несколько значений и, в соответствии с этим, определяется каким образом система управления будет пытаться оградить сервер при обнаружении аварии. Сервис ограждения циклически пытается оградить узлы, находящиеся в статусе HERMIT («Ограждается») в соответствии с настройками.

3.6.12.3.2. Тип ограждения может быть следующим:

– IPMI – использует управляющие команды BMC для выключения;

– VIRTUAL – признает сервер выключенным через 30 с после наступления аварии («по умолчанию»);

– SSH – использует подключение SSH для передачи команд выключения;

– NODE – использует вызов управляющих команд через систему управления кластером;

– AUTO – использует все возможные варианты последовательно.

3.6.12.3.3. В окне «Настройки» – «Контроллер» в «Настройках ограждения» есть редактируемые поля:

– начальный тайм-аут между попытками ограждения узлов («по умолчанию» – 15 с);

– максимальный тайм-аут между попытками ограждения узлов («по умолчанию» – 600 с);

– множитель увеличения тайм-аута между попытками («по умолчанию» – «2»).

3.6.12.3.4. Ниже приведен пример ограждения с типом ограждения узла IPMI и настройками ограждения контроллера «по умолчанию».

Сразу после перехода узла в статус HERMIT («Ограждается») производится первая попытка ограждения узла с контроллера. В случае удачного выключения узла он переходит в статус FAILED («Ошибка»). Если первая попытка не удалась, то через 15 с (начальный тайм-аут между попытками ограждения узлов) попытка повторяется. Если вторая попытка не удалась, то через интервал, равный «15 с * 2» («2» – множитель увеличения тайм-аута между попытками) попытка повторяется.

Если третья попытка не удалась, то через интервал, равный «15 с * 4» попытка повторяется. Тайм-аут будет увеличиваться до 600 с (максимальный тайм-аут между попытками ограждения узлов) и продолжаться до бесконечности, пока либо оператор не оградит узел вручную, либо ограждение закончится успешно.

3.6.12.4. Оптимальный выбор типов связности и ограждения

3.6.12.4.1. Оптимальным считается использование типа ограждения IPMI и типа связанности AUTO. Тип ограждения IPMI позволяет получить однозначное подтверждение о том, что сервер был огражден, а контроль модулей управления сервером реагирует также на проблемы в работе гипервизора.

3.6.12.5. Статусы узла и переходы между ними

3.6.12.5.1. Возможны следующие статусы узла:

– CREATING («Создается») – узел находится в процессе инсталляции;

– ACTIVE («Исправно») – узел активен и работает;

– FAILED («Ошибка») – узел был недоступен и его оградили (fence), виртуальные машины могут быть перезапущены на других узлах;

– ERROR («Ошибка») – узел недоступен;

– HERMIT («Ограждается») – узел недоступен продолжительное время и его необходимо оградить для перезапуска виртуальных машин на других узлах;

– DELETING («Удаляется») – узел находится в процессе удаления из кластера;

– SERVICE («Сервисный режим») – узел находится на техобслуживании.

3.6.12.5.2. При установке узел сначала находится в статусе CREATING («Создается») и после успешного добавления переходит в статус ACTIVE («Исправно»). В случае неуспешного добавления переходит в статус FAILED («Ошибка»). В этом случае рекомендуется посмотреть в журнале задач ошибку задачи добавления, разобраться с ошибкой, форсированно удалить узел и добавить его снова.

3.6.12.5.3. При потере связи контроллера с узлом последний переходит из статуса ACTIVE («Исправно») сначала в статус ERROR («Ошибка»), далее по истечению дополнительного времени и отсутствии связи в статус FAILED («Ошибка»), если узел на контроллере, или в статус HERMIT («Ограждается») для всех остальных узлов. Подробности ограждения описаны выше (см. 3.6.12.3).

При переходе узла в статус ERROR («Ошибка») контроллер пытается подключиться по SSH к узлу и перезапустить супервизор контроллера.

3.6.12.5.4. Контроллер постоянно циклически пытается опросить все известные ему узлы. Если узел в статусе НЕ ACTIVE и НЕ SERVICE и связь с ним появляется, то он переходит автоматически в статус ACTIVE («Исправно»).

3.6.12.5.5. Пользователь для перевода узла на техобслуживание должен перевести узел в статус SERVICE («Сервисный режим»). При этом все принадлежащие узлы сущности и связи узла переходят в статус FAILED («Ошибка»). ВМ узла перед переводом должны быть выключены.

3.6.12.5.6. При запуске задачи удаления узел сначала переходит в статус DELETING («Удаляется»), далее после успешного последовательного выполнения всех внутренних операций очистки узла от привязок к контроллеру он удаляется из базы системы управления. После неуспешного удаления переходит в статус FAILED («Ошибка»). В этом случае рекомендуется посмотреть в журнале задач ошибку задачи удаления, разобраться с ошибкой на будущее и форсированно удалить узел.

В случае, если узел не находится в статусе ACTIVE («Исправно»), его можно удалить форсированно, то есть исключительно из базы системы управления.

3.6.13. «Серверы» – <имя сервера> – «Профили»

3.6.13.1. В окне «Серверы» – <имя сервера> – «Профили» содержится список имеющихся профилей, включая для каждого из них название, имя пула данных и статус.

Также в этом окне существует возможность создания нового профиля по кнопке «Создать» и синхронизации настроек с другим узлом напрямую по кнопке «Синхронизировать».

3.6.13.2. При нажатии на название профиля открывается окно состояния профиля, содержащее следующую информацию:

– ballooning;

– drs_settings (раскрывающийся список);

– description;

– cluster;

– shared_storages;

– storages_transport.

В окне состояния профиля доступны следующие операции:

– обновление информации по кнопке  ;

– отсоединение. При нажатии кнопки «Отвязать» открывается окно «Отвязка профиля узла» с вопросом «Отвязать файл профиля узла?». Для подтверждения операции отсоединения необходимо нажать кнопку «ОК».

3.6.14. «Серверы» – <имя сервера> – «SSH»

3.6.14.1. Настройки SSH

3.6.14.1.1. Для просмотра и изменения настроек доступа по протоколу SSH к серверу необходимо в разделе «Серверы» основного меню выбрать целевой сервер, после чего в открывшемся окне во вкладке «SSH» – «Настройки» отобразятся следующие настройки:

– статус SSH – параметр, который показывает, включен ли доступ по SSH к серверу. «По умолчанию» – включен;

– количество одновременных подключений каждого пользователя – параметр, который указывает предельное количество одновременных подключений к терминалу по SSH от имени каждого пользователя. «По умолчанию» – «1»;

– общее количество одновременных подключений – параметр, который указывает предельное общее количество одновременных подключений по протоколу SSH. «По умолчанию» – «10»;

– количество мультиплексированных сеансов SSH в течение одного сеанса SSH - параметр, указывающий на предельное количество сеансов в рамках одного TCP соединения. «По умолчанию» – «10»;

– период неактивности пользователя в секундах, по истечению которого он будет отключен – параметр, указывающий временной интервал после последней активности (выполнение команд, ввод символов и так далее). «По умолчанию» – «7200»;

– количество периодов неактивности, по истечению которых пользователь будет отключен – количество периодов бездействия, по истечению которых будет произведено завершение сессии. «По умолчанию» – «1»;

– количество неудачных попыток входа – количество неудачных попыток входа подряд, после которых пользователь будет заблокирован.

3.6.14.2. Пользователи SSH

3.6.14.2.1. Для просмотра текущих пользователей SSH, а также добавления, удаления и изменения пользователей необходимо в разделе «Серверы» основного меню выбрать целевой сервер, после чего в открывшемся окне во вкладке «SSH» – «Пользователи» отобразится список пользователей, которым доступно SSH-подключение.

3.6.14.2.2. Для управления SSH-пользователями доступны следующие действия:

– блокировка (разблокировка) пользователя при помощи кнопки  . В открывшемся окне «Управление доступом по SSH» необходимо выбрать действие (заблокировать или разблокировать), определиться со способом выбора пользователей (ручной выбор пользователей или заблокировать всех), выбрать пользователей (при ручном способе выбора пользователей) и нажать кнопку «ОК»;

– добавления пользователя при помощи кнопки  . В открывшемся окне «Добавить пользователя» необходимо нажать кнопку «Добавить». В открывшемся окне добавления пользователей SSH необходимо ввести имя пользователя и пароль, после чего подтвердить операцию, нажав кнопку «Добавить».

Имя пользователя появится в списке добавленных пользователей. Нажатие кнопки «ОК» завершает операцию добавления новых пользователей;

– удаление пользователя при помощи кнопки  . В открывшемся окне «Удалить пользователя» необходимо выбрать пользователя и нажать кнопку «ОК».

3.6.14.2.3. У каждого пользователя имеется возможность изменить пароль доступа SSH при помощи кнопки  . В открывшемся окне «Изменения пароля» необходимо ввести пароль доступа SSH для выбранного пользователя и нажать кнопку «ОК».

3.6.14.3. Ключи шифрования

3.6.14.3.1. Для просмотра подключенных ключей шифрования, подключения новых и удаления необходимо в разделе «Серверы» основного меню выбрать целевой сервер, после чего в открывшемся окне во вкладке «SSH» – «Ключи шифрования» отобразится список подключенных ключей шифрования.

3.6.14.3.2. Доступны следующие действия:

– подключение нового ключа шифрования осуществляется при помощи кнопки «Подключение SSH ключа». В открывшемся окне необходимо выбрать ключ, пользователя SSH и нажать кнопку «ОК»;

– отключение конкретного ключа шифрования осуществляется при помощи кнопки «Отключить» в таблице ключей;

– отключение всех ключей шифрования осуществляется при помощи кнопки «Отключить все ключи SSH».

3.6.14.3.3. Более подробная информация описана в 3.12.6 данного руководства.

3.6.15. «Серверы» – <имя сервера> – «События»

3.6.15.1. В окне «Серверы» – <имя сервера> – «События» отображается список последних событий для данного сервера с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные».

Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.6.15.2. Более подробная информация описана в 3.11.2 данного руководства.

3.6.16. «Серверы» – <имя сервера> – «Резервное копирование»

3.6.16.1. В окне «Серверы» – <имя сервера> – «Резервное копирование» содержится список имеющихся резервных копий, включая для каждой из них название, имя пула данных, размер и статус.

3.6.16.2. В данной вкладке можно создавать резервные копии ОС с помощью кнопки «Создать резервную копию». В открывшемся окне необходимо выбрать пул данных для сохранения. Если его не указывать, то резервная копия будет создана на базовом пуле данных узла. Также в этом окне имеется текстовое поле «Описание», в которое можно внести дополнительную информацию, помогающую более точно идентифицировать файл резервной копии при восстановлении. Это описание можно будет в дальнейшем посмотреть при открытии файла через Web-интерфейс или непосредственно из posix shell.

3.6.16.3. При создании резервной копии, корневая файловая система резервируемого узла «замораживается», поэтому все операции на узле становятся не возможны. При создании резервной копии узла, на котором расположен контроллер, будет также приостановлена работа Web-интерфейса.

3.6.16.4. Правильным будет создавать резервные копии на сетевых хранилищах NFS, что в дальнейшем сильно упростит восстановление из них, используя «Live Mode» загрузку с установочного DVD.

3.6.16.5. Для загрузки резервной копии из файловой системы необходимо нажать кнопку «Загрузка из файловой системы» и в открывшемся окне выбрать файл (через стандартное окно загрузки файла) и пул (из раскрывающегося списка). После этого подтвердить операцию, нажав кнопку «ОК».

3.6.16.6. При открытии файла резервной копии, кроме обычных для файла кнопок («Обновить», «Копировать», «Скачать», «Удалить»), имеется кнопка «Описание», при нажатии на которую отобразится окно с описанием, внесенном при создании резервной копии. Берется из файла резервной копии, поэтому оно будет доступно, даже если файл был загружен.

3.6.16.7. При нажатии на название резервной копии открывается окно состояния резервной копии, содержащее следующую информацию:

– название;

– описание (с возможностью редактирования);

– расположение;

– название пула данных;

– дата и время создания;

– дата и время изменения;

– сообщения, выдаваемые при работе с резервными копиями с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.6.17. «Серверы» – <имя сервера> – «Теги»

3.6.17.1. В окне «Серверы» – <имя сервера> – «Теги» отображается список присвоенных серверу меток. Также имеется возможность обновления, создания и применения тега. Более подробная информация описана в 3.13.4 данного руководства.

3.6.18. «Серверы» – <имя сервера> – «ПО и Сервисы»

3.6.18.1. ПО (X.Y.Z)

3.6.18.1.1. Версия SpaceVM соответствует классической версии нумерации X.Y.Z:

– X – мажорная версия. Меняется при крупных релизах. Может не быть обратно совместима с прежними релизами;

– Y – минорная версия. Меняется при промежуточных релизах. Обязательно должна быть обратная совместимость;

– Z – версия патча. Меняется при исправлении ошибок промежуточных релизов.

3.6.18.1.2. В окне «Серверы» – <имя сервера> – «ПО и Сервисы» – «ПО (X.Y.Z)» отображается список компонентов SpaceVM, установленных на данном сервере и их текущие версии.

Также имеется возможность проверки наличия обновлений для компонентов системы. При нажатии кнопки «Проверить обновление ПО» в открывшемся окне отобразится информация о компонентах, текущих версиях и доступных для обновления версиях, после чего необходимо подтвердить обновление, нажав на кнопку «Обновить все пакеты ПО».

3.6.18.2. Сервисы

3.6.18.2.1. В окне «Серверы» – <имя сервера> – «ПО и Сервисы» –«Сервисы» отображается список сервисов и статус.

3.6.18.2.2. При нажатии кнопки «Действия над сервисами узла» отобразится мастер «Действия над сервисами узла», в котором можно выбрать «Сервис» из раскрывающего списка:

1) для контроллера:

– controller-engine;

– controller-web-api;

– controller-web-proxy;

– controller-web-uploader;

– controller-log-sender ;

– controller-websocket;

– elasticsearch;

– prometheus;

– linstor-controller;

– node-engine;

– node-statistics;

– iscsi;

– multipath;

– postgresql;

– nginx;

– ntp;

– redis;

– beanstalkd;

– ttyd;

– snmp;

– gluster;

– corosync;

– dlm;

– watchdog;

– linstor-satellite;

– td-agent;

– consul;

2) для узла:

– node-engine;

– node-web-api;

– node-web-proxy;

– node-web-uploader;

– node-statistics;

– iscsi;

– multipath;

– postgresql;

– nginx;

– ntp;

– redis;

– beanstalkd;

– ttyd;

– snmp;

– gluster;

– corosync;

– dlm;

– watchdog;

– linstor-satellite;

– td-agent;

– consul.

Над всеми сервисами можно выполнить следующие действия:

– start;

– stop;

– restart.

Для сохранения параметров необходимо нажать на кнопку «ОК».

3.6.18.2.3. Также имеется возможность проверки состояния супервизора системы управления сервером. При нажатии на кнопку «Проверка связи с супервизором узла» в открывшемся окне отобразится статус супервизора.

3.6.19. «Серверы» – <имя сервера> – «Задачи по расписанию»

3.6.19.1. В окне «Серверы» – <имя сервера> – «Задачи по расписанию» отображается список задач, запланированных на данном сервере, включая для каждой из них ее название, действие, статус, дату и время последнего и следующего запуска. Также в данном окне имеется возможность обновления и добавления задачи.

3.6.19.2. Для создания задачи по расписанию необходимо нажать кнопку «Добавить». В открывшемся окне заполнить следующие поля:

– название задачи;

– действие (выбор из раскрывающегося списка). Может принимать значение «upgrade» или «bacup_os»;

– периодичность выполнения (выбор из раскрывающегося списка);

– дата и время первого запуска;

– описание;

– для задачи создания резервной копии («bacup_os») можно выбрать пул данных, на котором будет создана резервная копия (если не выбран, то это базовый пул данных узла). Надо учитывать, что пул данных должен быть доступен на данном узле при создании задачи и ее выполнении.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

3.6.19.3. При нажатии на название задачи открывается окно состояния задачи, в котором предусмотрены следующие операции с выбранной задачей:

– обновление информации;

– запуск задачи. При нажатии кнопки «Запуск» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «Да»;

– удаление. При нажатии кнопки «Удалить» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «Да».

Также в окне состояния задачи содержится следующая информация:

– название (редактируемый параметр);

– описание (редактируемый параметр);

– периодичность (редактируемый параметр);

– действие;

– дата и время первого запуска задачи (редактируемый параметр);

– дата и время следующего запуска задачи;

– дата и время последнего запуска задачи;

– статус последнего запуска задачи;

– дата и время создания задачи;

– дата и время изменения задачи;

– сообщение об ошибке;

– сообщения о работе планировщика задач с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений.

3.7. Пулы ресурсов

3.7.1. Описание

3.7.1.1. Пул ресурсов – это логическая абстракция для гибкого управления ресурсами.

3.7.1.2. Пулы ресурсов позволяют делегировать управление ресурсами узла (или кластера), и преимущества очевидны, когда администратор использует пулы ресурсов для разделения всех ресурсов в кластере. Необходимо создать несколько пулов ресурсов и настроить их. Затем можно делегировать контроль над пулами ресурсов другим лицам или организациям.

3.7.1.3. Использование пулов ресурсов может привести к следующим преимуществам:

– гибкая иерархическая организация – добавление, удаление, реорганизация пулов ресурсов или изменение распределения ресурсов по мере необходимости;

– изоляция между пулами, совместное использование внутри пулов – администраторы верхнего уровня могут сделать пул ресурсов доступным для администратора организации. Изменения распределения, которые являются внутренними для одного пула ресурсов, не оказывают влияния на другие несвязанные пулы ресурсов;

– контроль доступа – когда администратор верхнего уровня делает пул ресурсов доступным администратору уровня организации, этот администратор может затем выполнять все операции по созданию и управлению ВМ в пределах ресурсов, на которые пул ресурсов имеет право в соответствии с настройками «shares», «guarantee» и «limit». Делегирование обычно выполняется в сочетании с настройками разрешений;

– отделение ресурсов от физически существующих. Это означает, что администраторы могут выполнять управление ресурсами независимо от фактических серверов, которые вносят свой вклад в ресурсы. Можно заменить три узла по 2 Гбайт на два узла по 3 Гбайт и для этого не нужно будет вносить изменения в распределение ресурсов.

Такое разделение позволяет администраторам больше думать о совокупной вычислительной мощности и меньше об индивидуальных серверах;

– управление наборами ВМ. Не нужно устанавливать ресурсы на каждой ВМ. Вместо этого можно управлять совокупным распределением ресурсов для набора ВМ, изменяя настройки их пула ресурсов.

Далее приведен пример использования. Предположим, что узел имеет пять ВМ. Отдел бухгалтерии использует три ВМ, а отдел программистов – две ВМ.

Поскольку отделу программистов требуется больший объем vCPU и памяти, администратор создает пул ресурсов для каждой группы. Администратор устанавливает «vcpu_shares» и «memory_shares» на более высокий уровень для пула отделов программистов, чтобы пользователи отдела программистов могли выполнять автоматические тесты и на средний для пула отделов бухгалтерии.

Второй пул ресурсов с меньшим количеством ресурсов vCPU и памяти достаточен для более легкой нагрузки персонала бухгалтерии. Всякий раз, когда отдел программистов не полностью использует свои ресурсы, отдел бухгалтерии может использовать доступные ресурсы.

Примечание. Условное соотношение vCPU на одно ядро процессора равно «4».

3.7.1.4. У каждого кластера по умолчанию существует базовый пул ресурсов, которому принадлежат все узлы и пулы данных этого кластера. Базовый пул ресурсов кластера является родительским для всех созданных пользователем пулов ресурсов в этом кластере. Его нельзя удалить, а также убирать из него узлы и пулы данных.

3.7.1.5. В разделе «Пулы ресурсов» основного меню содержится список имеющихся пулов ресурсов, включая для каждого из них его название, количество подключенных ВМ, ограничение памяти и CPU. В этом разделе производится основное управление пулом ресурсов.

3.7.1.6. Также в этом окне существует возможность создания нового пула по кнопке «Создать пул ресурсов».

3.7.2. Создание

3.7.2.1. При нажатии кнопки «Создать пул ресурсов» открывается окно для создания пула с соответствующими полями:

– название пула ресурсов;

– его описание;

– кластер – выбор из раскрывающегося списка;

– сервер – выбор из раскрывающегося списка или выбрать все;

– опция «Выбрать все серверы»;

– приоритет CPU пула относительно других пулов (значение «по умолчанию» – «1024», минимум – «2», максимум – «10000»);

– приоритет памяти пула относительно других пулов (значение «по умолчанию» – «1024», минимум – «2», максимум – «10000»);

– количество зарезервированных процессоров (минимум – «0», максимум – свободное количество vCPU выбранных узлов);

– количество зарезервированной памяти (Мбайт) (минимум – «0», максимум – свободное количество памяти выбранных узлов);

– ограничение сверху по процессорам vCPU;

– ограничение сверху по памяти (Мбайт).

После заполнения полей необходимо нажать «ОК».

3.7.3. Информация

3.7.3.1. При нажатии на название пула ресурсов открывается окно состояния, в котором информация разделена на следующие группы:

– информация;

– серверы;

– виртуальные машины;

– пулы данных;

– процессор;

– память;

– события;

– теги.

Также существует возможность обновления информации с помощью кнопки  и удаления пула с помощью кнопки «Удалить пул ресурсов».

В окне состояния пула имеется виджет используемого места с возможностью его обновления.

3.7.3.2. В окне «Пулы ресурсов» – <имя пула ресурсов> – «Информация» содержатся следующие сведения:

– название (редактируемый параметр);

– описание (редактируемый параметр);

– признак базового пула кластера («Да» или «Нет»);

– дата и время создания;

– дата и время изменения (обновления).

3.7.4. Серверы

3.7.4.1. В окне «Пулы ресурсов» – <имя пула ресурсов> – «Серверы» содержится список серверов, присутствующих в системе, включая для каждого из них его название, IP-адрес, CPU и RAM, количество ВМ (включенных и всего), статус и возможность подключения (отключения) для небазовых пулов.

Примечание. При отключении узла отключатся принадлежащие только ему пулы данных, а его ВМ перейдут в базовый пул ресурсов кластера этого узла.

Имеется возможность выбора определенного сервера с применением фильтра по кнопке «Фильтр» в верхней строчке окна. В открывшемся окне содержатся следующие поля для фильтрации:

– «Имя сервера»;

– «Статус» – выбор из раскрывающегося списка («Без фильтра», «Исправно», «Нет соединения» или «Произошла ошибка»);

– «Файловое хранилище» – выбор из раскрывающегося списка;

– «Пул данных» – выбор из раскрывающегося списка;

– «Кластеры» – выбор из раскрывающегося списка;

– «Локации» – выбор из раскрывающегося списка;

– «Пулы ресурсов» – выбор из раскрывающегося списка;

– «Теги» – выбор из раскрывающегося списка.

После настройки фильтра необходимо нажать «Применить» или «Сбросить все».

3.7.5. Виртуальные машины

3.7.5.1. В окне «Пулы ресурсов» – <имя пула ресурсов> – «Виртуальные машины» – «Виртуальные машины» содержится список ВМ, присутствующих в системе, включая для каждой из них ее название, сервер, IP-адрес, vRAM, vDisk, vNIC, vFunc и статус.

Для ВМ имеется возможность:

– добавления их в пул ресурсов по кнопке «Добавить ВМ»;

– применить параметры пула ресурсов к ВМ;

– поиска ВМ по названию с помощью поля «Найти » и кнопки .

3.7.6. Шаблоны

3.7.6.1. В окне «Пулы ресурсов» – <имя пула ресурсов> – «Виртуальные машины» – «Шаблоны» содержится список имеющихся шаблонов ВМ.

Для шаблонов ВМ (аналогично ВМ) имеется возможность:

– добавления их в пул ресурсов по кнопке «Добавить шаблон ВМ»;

– применить параметры пула ресурсов к ВМ;

– поиска шаблона ВМ по названию с помощью поля «Найти » и кнопки .

Примечания:

1. При добавлении шаблона в пул добавятся все его тонкие клоны.

2. При добавлении тонкого клона в пул добавятся его шаблон и все тонкие клоны этого шаблона.

3. После изменения параметров процессоров и памяти необходимо применить их ко всем ВМ пула, нажав кнопку «Применения параметров пула ресурсов».

3.7.7. Пулы данных

3.7.7.1. В окне «Пулы ресурсов» – <имя пула ресурсов> – «Пулы данных» содержится список имеющихся пулов, включая для каждого из них его название, тип, количество подключенных серверов, дисков, образов, файлов, использование памяти, его статус и возможность подключения (отключения) для небазовых пулов.

Имеется возможность выбора определенного пула с применением фильтра по кнопке «Фильтр» в верхней строчке окна. В открывшемся окне содержатся следующие поля для фильтрации:

– «Имя пула»;

– «Серверы» – выбор из раскрывающегося списка;

– «Кластеры» – выбор из раскрывающегося списка;

– «Локации» – выбор из раскрывающегося списка;

– «Пулы ресурсов» – выбор из раскрывающегося списка;

– «Файловые хранилища» – выбор из раскрывающегося списка;

– «Кластерные хранилища» – выбор из раскрывающегося списка;

– «Разделы (ZFS пулы)» – выбор из раскрывающегося списка;

– «Статус» – выбор из раскрывающегося списка («Без фильтра», «Исправно», «Нет соединения» или «Произошла ошибка»);

– «Тип пула» – выбор из раскрывающегося списка;

– «Теги» – выбор из раскрывающегося списка.

После настройки фильтра необходимо нажать «Применить» или «Сбросить все».

3.7.8. Процессор

3.7.8.1. В окне «Пулы ресурсов» – <имя пула ресурсов> – «Процессор» содержится информация о настройках процессора:

1) приоритет vCPU пула (раскрывающаяся информация):

– приоритет vCPU пула относительно других пулов (редактируемый параметр);

– средний приоритет vCPU по всем ВМ пула;

2) резервирование (раскрывающаяся информация):

– количество зарезервированных vCPU (редактируемый параметр);

– количество зарезервированных vCPU на 1 ВМ (количество vCPU/количество ВМ);

– среднее количество зарезервированных vCPU на 1 ВМ (пользователь может изменить параметр у самой ВМ);

3) ограничение (раскрывающаяся информация):

– максимальное количество vCPU (редактируемый параметр);

– количество vCPU серверов;

– количество vCPU ВМ.

3.7.9. Память

3.7.9.1. В окне «Пулы ресурсов» – <имя пула ресурсов> – «Память» содержится информация о настройках памяти:

1) приоритет памяти пула (раскрывающаяся информация):

– приоритет памяти пула относительно других пулов (редактируемый параметр);

– средний приоритет памяти по всем ВМ пула (пользователь может изменить приоритет у самой ВМ);

2) резервирование (раскрывающаяся информация):

– количество зарезервированной памяти (редактируемый параметр);

– количество зарезервированной памяти на 1 ВМ (количество памяти/количество ВМ);

– среднее количество зарезервированной памяти на 1 ВМ (пользователь может изменить параметр у самой ВМ);

3) ограничение (раскрывающаяся информация):

– максимальное количество памяти (редактируемый параметр);

– количество памяти серверов;

– количество памяти ВМ.

3.7.10. События

3.7.10.1. В окне «Пулы ресурсов» – <имя пула ресурсов> – «События» содержится список последних событий для этого пула с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные».

Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.7.11. Теги

3.7.11.1. В окне «Пулы ресурсов» – <имя пула ресурсов> – «Теги» содержится список присвоенных пулу тегов. Существует возможность создать, применить тег и обновить список назначенных пулу тегов.

3.8. Виртуальные машины

В разделе «Виртуальные машины» основного меню содержится информация обо всех ВМ и шаблонах ВМ. В этом разделе производится основное управление жизненным циклом ВМ.

В основном окне перечислен список ВМ, созданных в кластере, включая для каждой из них ее название, сервер, IP-адрес, количество виртуальных процессоров vCPU, объем виртуальной оперативной памяти vRAM, количество виртуальных дисков vDisk и сетевых адаптеров vNIC, количество виртуальных функций vFunc, количество mediated-устройств vGPU и статус.

3.8.1. Создание ВМ

3.8.1.1. Имеются следующие возможности:

– создать ВМ «с нуля»;

– создать ВМ на базе ранее созданного шаблона.

3.8.1.2. Процедура создания ВМ «с нуля» запускается с помощью нажатия кнопки «Добавить ВМ», расположенной в верхней части окна над списком ВМ. В процессе создания производится первоначальная настройка ВМ, необходимая для ее корректного запуска. Для создания ВМ необходимо выполнить следующие шаги:

1) первый шаг – настройка параметров ВМ:

– выбрать из раскрывающегося списка локацию и кластер;

– выбрать из раскрывающегося списка сервер при ручном выборе или в автоматическом режиме будет предложен наименее загруженный сервер первоначального размещения;

– указать название ВМ;

– выбрать из раскрывающегося списка режим определения процессора (оптимальный процессор определяется по наименьшему совпадению функций (флагов) процессоров всех узлов кластера);

– указать количество vCPU;

– указать максимальное количество vCPU;

– выбрать из раскрывающегося списка приоритет предоставления ресурсов CPU – «LOW», «MEDIUM» или «HIGH»;

– указать количество выделяемой оперативной памяти;

– выбрать из раскрывающегося списка тип ОС – «Windows», «Lunix» или «Other»;

– выбрать из раскрывающегося списка версию ОС;

– выбрать чипсет – «pc», «q35»;

– выбрать видео карту:

а) тип эмулируемого видео адаптера из раскрывающегося списка – «vga», «cirrus», «gxl» или «virtio»;

б) объем памяти из раскрывающегося списка – «16», «32», «64», «128», «256» или «512»;

в) количество мониторов из раскрывающегося списка – «1», «2», «3» или «4»;

– выбрать звуковую карту:

а) тип эмулируемой аудио карты из раскрывающегося списка – «es1370», «sb16», «ac97», «ich6» или «usb»;

б) кодек из раскрывающегося списка – «micro» или «duplex»;

в) включить (выключить) звуковой адаптер ВМ;

– выбрать тип загрузчика – «LegacyMBR» или «UEFI»;

– заполнить описание (при необходимости).

ВНИМАНИЕ! Не рекомендуется превышать количество ресурсов, физически присутствующих на узле (сервере), на котором создается ВМ. Необходимо учитывать, что при переносе (миграции) на целевом узле должно быть не меньше физических ресурсов, чем присвоено ВМ. В противном случае ВМ не будет запускаться до исправления ошибки. Если на целевом сервере будет недостаточно свободных ресурсов для запуска ВМ, то она также не запустится.

Для сохранения изменений необходимо нажать кнопку «ОК» и ВМ с заданными параметрами будет создана, но мастер создания ВМ не закроется.

Следующими шагами мастера по созданию ВМ будут:

– создание нового или подключение ранее созданного виртуального диска ВМ;

– монтирование в виртуальный CD-ROM образ CD/DVD-диска, загруженного в хранилище;

– создание виртуального сетевого адаптера ВМ и подключение его к виртуальной сети, к ранее созданному распределенному коммутатору в созданную на нем группу интерфейсов.

Примечание. Каждый из этих шагов можно пропустить или закрыть мастер создания ВМ. В таком случае, все настройки ВМ, которые были пропущены, возможно произвести в окне управления ВМ.

При последовательной настройке ВМ с помощью мастера создания ВМ необходимо перейти к шагу 2;

2) второй шаг – подключение дисков.

Имеется две возможности:

– создать новый виртуальный диск;

– добавить существующий.

Для создания нового диска необходимо:

– нажать кнопку «Создать новый»;

– выбрать из раскрывающегося списка тип пула данных и пул размещения (из списка доступных);

– указать отображаемое название диска;

– указать описание виртуального диска;

– определить необходимость предварительного выделения места;

– указать при необходимости тип выделения места («falloc» «по умолчанию»);

– выбрать из раскрывающегося списка тип шины диска («virtio», «ide», «scsi» или «sata») и тип кэширования чтения или записи («default», «none», «writethrough» или «writeback»). Для обеспечения нормальной миграции ВМ требуется отключить кэширование («none») и рекомендуется выбрать шину «virtio». При использовании ВМ, данные которой будут храниться в LVM-хранилище или в LUN, напрямую предоставляемым с СХД, этот шаг можно пропустить;

– для сохранения изменений нажать кнопку «ОК»;

– после создания диска нажать кнопку «Дальше» и перейти к шагу 3.

При включении опции предварительного выделения места оно будет выделено режимом «falloc» (falloc mode preallocates space for image by calling posix_fallocate()).

Если опция не включена, то используется режим «off».

Возможные режимы – «off», «metadata», «falloc», «full».

Статью с описанием производительности выделения места методом «falloc» можно посмотреть по ссылке *https://kashyapc.wordpress.com/2011/12/02/little-more-disk-io-perf-improvement-with-fallocateing-a-qcow2-disk/.*

Для подключения уже существующего диска, не используемого другими ВМ, необходимо:

– нажать кнопку «Добавить существующий»;

– выбрать из раскрывающегося списка тип пула данных и пул размещения (из списка доступных);

– выбрать диск, подключаемый к ВМ. Если в списке нет доступных для подключения дисков, значит необходимо создать новый, так как в выбранном пуле данных нет свободных дисков. Создание нового виртуального диска описано выше;

– выбрать из раскрывающегося списка тип шины диска («virtio», «ide», «scsi» или «sata») и тип кэширования чтения или записи («default», «none», «writethrough», «writeback», «directsync» или «unsafe»).

Если в раскрывающемся списке «Выбрать виртуальный диск» нет ни одного диска, значит в этом хранилище нет свободных дисков. Привязанные к ВМ диски в списке также не отображаются. В такой ситуации необходимо создать новый диск;

– для сохранения изменений нажать кнопку «ОК»;

– после добавления диска нажать кнопку «Дальше» и перейти к шагу 3;

3) третий шаг – подключение ISO-образа.

Для подключения ISO-образа необходимо:

– нажать на название диска или на изображение «компакт-диска» в столбце «Подключение»;

– в открывшемся окне состояния CD-ROM необходимо нажать кнопку «Монтировать образ»;

– в окне «Монтирование iso-образа» необходимо выбрать из раскрывающегося списка тип хранилища (тип пула данных), хранилище (пул данных) и ISO-образ.

Если в списке нет доступных для монтирования образов, значит в выбранный пул данных они не загружались (см. 3.9.3.1 данного руководства);

– смонтировать образ с помощью кнопки «Монтировать»;

– закрыть окно состояния CD-ROM по кнопке  ;

– нажать кнопку «Дальше» для перехода к шагу 4;

4) четвертый шаг – создание сетевых интерфейсов.

Для создания сетевого интерфейса необходимо нажать кнопку «Добавить» и в открывшемся окне «Добавить виртуальный интерфейс» заполнить следующие поля:

– виртуальная сеть (выбор из раскрывающегося списка);

– MAC-адрес. Поле «MAC-адрес» является необязательным для заполнения. Если не указывать MAC-адрес, то он будет сгенерирован автоматически;

– сетевая карта (выбор из раскрывающегося списка). В качестве модели сетевой карты можно выбрать «virtio», «e1000», «rtl8139» или «vmxnet3», в зависимости от поддерживаемых вариантов в устанавливаемой ОС;

– описание виртуального интерфейса (при необходимости).

Для сохранения изменений необходимо нажать кнопку «ОК». Для перехода к шагу 5 нажать кнопку «Дальше»;

5) пятый шаг – включение.

На пятом шаге следует выбрать опции запуска ВМ после создания (включить или не включить питание ВМ). Для подтверждения операции необходимо нажать кнопку «Готово».

После этого происходит возврат в окно со списком ВМ.

3.8.1.3. Можно создать ВМ на базе ранее созданного шаблона.

Для этого в разделе «Виртуальные машины» основного меню существует две возможности:

1) создать тонкий клон, нажав на кнопку «Добавить тонкий клон». После этого в открывшемся окне:

– указать название ВМ;

– выбрать шаблон ВМ из раскрывающегося списка ранее созданных ВМ (при необходимости отредактировать параметры);

– выбрать количество создаваемых ВМ (максимально 100);

– при необходимости активировать опцию «Включить после создания» (произойдет после создания всех ВМ);

– нажать кнопку «ОК»;

2) создать ВМ из шаблона, нажав на кнопку «Добавить ВМ из шаблона». После этого в открывшемся окне:

– указать название ВМ;

– выбрать сервер из раскрывающегося списка;

– выбрать пул данных из раскрывающегося списка;

– выбрать шаблон ВМ из раскрывающегося списка ранее созданных ВМ;

– выбрать количество создаваемых ВМ (максимально 100);

– при необходимости активировать опцию «Включить после создания» (произойдет после создания всех ВМ);

– нажать кнопку «ОК».

После создания ВМ она (они) появятся в общем списке ВМ.

3.8.1.4. При нажатии на уже существующую ВМ открывается окно, в котором содержится информация о ней. Работа с окнами ВМ подробно описана в 3.8.4 – 3.8.26 данного руководства.

3.8.2. Шаблоны ВМ

3.8.2.1. В разделе «Шаблоны» основного меню отображается информация о всех ВМ, которые переведены в режим шаблона.

3.8.2.2. Шаблон – это копия ВМ с упорядоченными папками и управляемая разрешениями для доступа к ней. Они полезны, потому что выступают как защищенные версии модели ВМ, которая может быть использована при создании новой ВМ. Так как шаблон – это оригинальный и совершенный образ определенной ВМ, он не может быть запущен как самостоятельная ВМ.

3.8.2.3. Шаблоны могут существенно сократить время развертывания новых ВМ, потому что позволяют клонировать новые ВМ из шаблона без необходимости настройки новой ВМ и установки ОС на ВМ.

3.8.2.4. При развертывании сервиса виртуальных рабочих станций (VDI) шаблон может использоваться как эталонная ВМ. Использование эталонных ВМ позволяет сохранять исходный образ ВМ неизменным. При использовании в сервисе VDI полных клонов каждое новое рабочее место является копией шаблона, а изменения, вносимые пользователем, хранятся только в копии шаблона.

Также на использовании эталонных ВМ работает технология тонких клонов, когда система сохраняет только изменения, являющиеся результатом работы пользователя. При этом статические данные, необходимые для работы ОС ВМ, берутся из шаблона, а динамические данные, необходимые для работы ВМ, пишутся в отдельный файл.

3.8.2.5. При нажатии на название уже существующего шаблона ВМ открывается окно, в котором содержится информация о шаблоне ВМ. Работа с шаблоном аналогична работе с ВМ (см. 3.8 данного руководства).

3.8.2.6. Также существует возможность перевода шаблона в режим ВМ и обратно. Находясь в окне состояния шаблона, при нажатии кнопки «В режим ВМ» или «В режим шаблона» в открывшемся окне «Переключение режима» необходимо подтвердить действие, нажав на кнопку «Да».

Примечания:

1. Для создания тонких клонов из шаблона диски в шаблоне должны находиться на пулах данных типа директория, то есть всех, кроме блочных (LVM, thin-LVM, LVM_shared).

2. При наличии у шаблона mediated-устройств при создании тонкого клона будет автоматически произведен поиск устройств того же типа на выбранном узле. При отсутствии устройство не добавится, и задача создания прервется на этом шаге.

3.8.2.7. Для создания тонкого клона или восстановления из резервной копии (часть шагов опциональна) необходимо выполнить следующие шаги:

– восстановление дисков;

– восстановление образов;

– создание пустой ВМ;

– копирование базовых параметров;

– создание интерфейсов;

– создание виртуальных функций;

– создание CD-ROM;

– создание дисков;

– добавление дисков;

– добавление хранилищ;

– добавление образов;

– добавление USB-устройств узла;

– добавление PCI-устройств узла;

– добавление mediated-устройств узла;

– восстановление снимков;

– добавление тегов;

– установка владельцев;

– старт.

3.8.3. Операции с ВМ

Окно состояния ВМ открывается по нажатию на название ВМ. В окне состояния для всех ВМ доступны следующие операции:

– управление ВМ (набор управляющих кнопок зависит от состояния ВМ);

– клонирование;

– перенос на другой сервер;

– удаление;

– изменить шаблон (доступна для ВМ, являющихся тонким клоном).

Данные операции выполняются с помощью соответствующих кнопок в верхней части окна.

В левом верхнем углу под именем ВМ показан ID ВМ. Он является также UUID материнской платы.

В окне состояния ВМ имеется виджет используемого места с возможностью его обновления.

В левой части окна состояния ВМ находится панель вкладок:

– «Информация»;

– «Мониторинг»;

– «ВМ/Шаблон»;

– «Процессоры»;

– «Память»;

– «Диски»;

– «CD-ROM»;

– «USB-устройства»;

– «PCI-устройства»;

– «Mediated-устройства»;

– «Снимки»;

– «Интерфейсы»;

– «Виртуальные функции»;

– «Контроллеры»;

– «LUNs»;

– «Высокая доступность»;

– «Опции загрузки»;

– «Резервное копирование»;

– «Удаленный доступ»;

– «Настройка безопасности»;

– «События»;

– «Теги»;

– «Задачи по расписанию».

В каждой вкладке перечислены специализированные настройки ВМ.

3.8.3.1. Управление питанием

3.8.3.1.1. В зависимости от состояния ВМ набор управляющих кнопок разный:

– обновление информации о ВМ  ;

– запуск ВМ  ;

– пауза  (только для включенной);

– выключение ВМ  ;

– перезагрузка ВМ  (только для включенной);

– принудительная перезагрузка ВМ  (только для включенной);

– выключение питания  .

3.8.3.1.2. Остановка ВМ без изменения конфигурации доступна только для ВМ с установленной ОС, так как остановка осуществляется с помощью передачи управляющим процессам ОС ACPI-команды на выключение. При этом процесс работы ВМ не останавливается полностью, и при повторном запуске конфигурация ВМ не изменяется. Данный процесс аналогичен «спящему режиму» для ноутбуков. Это необходимо учитывать при внесении изменений в конфигурацию ВМ.

3.8.3.2. Клонирование

3.8.3.2.1. Операция клонирования ВМ выполняется при нажатии кнопки «Клонировать». В открывшемся окне «Клонирование ВМ» необходимо заполнить название ВМ, выбрать из раскрывающегося списка сервер и пул данных, количество клонов, включить опции «Конвертировать в шаблон», «Включить после клонирования», «Управление памятью и процессорами ВМ», после чего подтвердить операцию, нажав кнопку «ОК».

Примечание. При клонировании шаблона можно выбрать опцию «Конвертации» его в ВМ и наоборот.

3.8.3.3. Перенос (миграция)

3.8.3.3.1. При нажатии кнопки «Перенести» в открывшемся окне необходимо выбрать автоматический или ручной перенос, после чего подтвердить операцию, нажав кнопку «Мигрировать».

3.8.3.3.2. «По умолчанию» для миграций ВМ используется сеть управления серверов, то есть миграция идет через коммутаторы «default», внутренние интерфейсы «mgmt» и через тот физический или агрегированный интерфейс, куда они соответственно подключены. То есть адресом назначения миграции является IP-адрес внутреннего интерфейса «mgmt» сервера, куда будет переноситься ВМ.

В SpaceVM можно использовать внешние сети для миграции ВМ и переноса дисков.

3.8.3.3.3. При автоматическом выборе ВМ переносится на наименее нагруженный первый сервер из кластера. Выбор нагруженности происходит исходя из настройки «Типы собираемых метрик» DRS-кластера. Например, если стоит «memory», то выбирается самый ненагруженный узел кластера по оперативной памяти.

3.8.3.3.4. При миграции с переносом дисков недоступные на целевом узле виртуальные диски переносятся на выбранный пользователем пул данных.

3.8.3.3.5. Причины отсутствия узла для миграции следующие:

– нет активных узлов в кластере;

– подключенные PCI- устройства;

– подключенные mediated-устройства;

– включен безопасный режим и ВМ включена;

– есть неактивные виртуальные интерфейсы;

– виртуальная сеть, в которую включен интерфейс, недоступна на узле;

– есть виртуальные диски с типом кэширования не «none»;

– есть неактивные виртуальные диски;

– пул данных диска недоступен на узле;

– пул данных снимка недоступен на узле;

– есть неактивные LUN;

– есть LUN с типом кэширования не «none»;

– LUN недоступен на узле;

– оперативная память на узле меньше или равна памяти ВМ;

– нет вхождения списка функций процессора ВМ в список функций процессора узла;

– нет свободной памяти на узле (если ВМ включена);

– количество гарантированной памяти ВМ больше свободной памяти узла (если ВМ включена);

– количество используемой памяти ВМ больше свободной памяти узла (если ВМ включена);

– количество используемой частоты процессора ВМ больше свободной частоты процессора узла (если ВМ включена);

– на узле нет свободных vCPU;

– количество гарантированных vCPU ВМ больше свободных vCPU узла (если ВМ включена);

– при включенных опциях использования тегов у кластера проверяются совпадения и несовпадения тегов ВМ и тегов узла и его ВМ.

3.8.3.3.6. Процесс миграции при выключенной ВМ заключается в следующем:

– если диски на общем хранилище, то ВМ просто сменяет родительский узел на узел назначения в базе контроллера;

– если не все диски на общем хранилище, то дополнительно происходит перенос дисков на новый узел.

3.8.3.3.7. Процесс миграции при включенной ВМ заключается в следующем:

– генерируется временный SSH-ключ на узле назначения;

– при использовании внешних сетей для миграции берется IP-адрес внутреннего интерфейса узла назначения из первой внешней сети, куда включен этот сервер. Если не используются внешние сети, то адресом назначения миграции является IP-адрес внутреннего интерфейса «mgmt» узла назначения;

– на узле-источнике, где находится ВМ, запускается процесс миграции, состоящий из адаптации конфигурации ВМ, переносов недоступных дисков при необходимости и, собственно, самого процесса миграции.

При миграции сначала копируется состояние памяти, сети, дисков ВМ, после чего она выключается на узле источнике, происходит докопирование изменившихся блоков состояния, и ВМ продолжает работу уже на узле назначения;

– удаляется временный SSH-ключ на узле назначения;

– адаптируются сетевые настройки ВМ на узле назначения;

– ставится приоритет ВМ на узле назначения относительно других ВМ.

3.8.3.3.8. Факторы, максимально влияющие на скорость миграции:

– максимальная производительность и загруженность сетевого канала, используемого для миграции;

– объем оперативной памяти ВМ и уровень ее использования ВМ;

– производительность и загруженность дисковой подсистемы при переносе дисков.

3.8.3.4. Удаление

3.8.3.4.1. Удаление ВМ выполняется с помощью кнопки «Удалить». При нажатии кнопки «Удалить» в открывшемся окне «Удаление виртуальной машины» необходимо определить потребность удаления дисков, подключенных к ВМ (удалять только ВМ или ВМ с дисками), после чего подтвердить операцию, нажав кнопку «Удалить».

3.8.4. «Виртуальные машины» – <имя ВМ> – «Информация»

3.8.4.1. При открытии окна состояния ВМ сразу открывается вкладка «Информация». В окне слева вверху находится id ВМ, который является также UUID материнской платы.

3.8.4.2. В данном окне содержится информация, разделенная на группы:

1) сводка. Содержит следующие параметры и харатеристики:

– доступ к терминалу;

– название (редактируемый параметр);

– описание (редактируемый параметр);

– тип ОС ВМ (редактируемый параметр);

– версия ОС ВМ (редактируемый параметр);

– сервер, на котором располагается ВМ;

– пул ресурсов;

– приоритет;

– виджеты используемых ресурсов;

2) информация о ВМ:

– конфигурация ВМ:

а) состояние (вкл/выкл) «watchdog» устройства (редактируемый параметр);

б) планшет (вкл/выкл) (редактируемый параметр);

в) оптимизация для vGPU (вкл/выкл) (редактируемый параметр);

г) TPM устройство (вкл/выкл) (редактируемый параметр);

д) возможности гипервизора (редактируемый параметр);

е) аргументы Qemu (редактируемый параметр);

ж) устройство рендеринга GL (редактируемый параметр);

з) консоли (редактируемый параметр;

и) высокая доступность (вкл/выкл);

– статусы служб агента. Если гостевой агент включен, то в статусах служб гостевых агентов содержится следующая информация о нем:

а) OEMU (вкл/выкл);

б) версия гостевого агента;

в) имя хоста;

г) IP-адрес;

– консоли. Содержит количество консолей (редактируемый параметр);

– история ВМ:

а) дата и время создания;

б) дата и время изменения (обновления);

в) дата и время последней успешной миграции;

г) время активности;

д) время активности на текущем сервере.

3) конфигурация оборудования:

– ЦП:

а) количество сокетов;

б) количество ядер на сокет;

в) общее количество потоков;

– ОЗУ:

а) оперативная память;

б) приоритет памяти ВМ;

в) максимальное значение памяти;

г) минимально гарантированная память;

– другое:

а) чипсет;

б) графический адаптер (редактируемый параметр);

в) звуковой адаптер (вкл/выкл) (редактируемый параметр);

4) использование процессора – информация в виде графика «cpu»;

5) использование оперативной памяти – информация в виде графика «memory».

3.8.4.3. Для запущенных ВМ становится возможным доступ к терминалу (консоли) по протоколу SPICE или VNC. Для перехода в терминал необходимо нажать кнопку «spice» или «vnc».

При нажатии на «spice» в окне терминала предусмотрены следующие операции:

1) обновление окна терминала ВМ;

2) отправка комбинаций клавиш на ВМ (выбор из раскрывающегося списка). Например, комбинация «Ctrl+Alt+Del» посылает действие «Ctrl+Alt+Del» на ВМ;

3) кнопка «Полноэкранный режим» разворачивает окно терминала на весь экран (выход из полноэкранного режима с помощью «Esc»);

4) кнопка «Открыть в новой вкладке» открывает окно в новой вкладке и закрывает его в текущей;

5) кнопка «Извлечь ISO» отмонтирует все подключенные к ВМ ISO-образы.

Решения проблем при работе с терминалом:

1) проблемы с «мышкой» при подключении по SPICE. В такой ситуации следует попробовать:

– сменить графический адаптер на «qxl» (потребуется выключение ВМ);

– обновить «spice-vdagent» до более актуальной версии;

2) если терминал ничего не показывает, то следует попробовать следующие действия:

– сменить графический адаптер на «qxl» (потребуется выключение ВМ);

– доставить нужные драйвера в ВМ.

Через буфер обмена работает перенос файлов между АРМ оператора и ВМ.

Интервал портов для терминала по протоколу SPICE и VNC следующий:

– нижняя граница – «5900»;

– верхняя граница – «32767».

При включении удаленного доступа автоматически берется первый случайный свободный порт из указанного выше интервала.

Для доступа к консоли, подключенной к последовательному порту ВМ, служит команда в CLI-интерфейсе

vm console <id>

3.8.5. «Виртуальные машины» – <имя ВМ> – «Мониторинг»

3.8.5.1. В окне «Виртуальные машины» – <имя ВМ> – «Мониторинг» содержатся графики загрузки:

– «cpu» (загрузка процессоров);

– «memory» (загрузка памяти);

– «read» и «write» (загрузка дисков, образов и LUNs);

– «transmit» и «receive» (загрузка сетевых интерфейсов).

3.8.6. «Виртуальные машины» – <имя ВМ> – «ВМ/Шаблон»

3.8.6.1. В окне «Виртуальные машины» – <имя ВМ> – «ВМ/Шаблон» имеется возможность перевести ВМ в режим шаблона и обратно. Когда виртуальная машина находится в режиме ВМ, то отображается следующая информация:

– шаблон ВМ – имя шаблона, на основе которого создана данная ВМ;

– тонкий клиент – является ли данная ВМ тонким клоном (да/нет).

3.8.6.2. Для ВМ предусмотрены следующие операции:

– обновление окна информации о ВМ;

– переключение ВМ в режим шаблона по кнопке «В режим шаблона». Если это шаблон ВМ, то переключение в режим ВМ по кнопке «В режим ВМ». В открывшемся окне необходимо подтвердить переключение, нажав на кнопку «Да»;

– управление SysPrep. При нажатии на кнопку «SysPrep» открывается окно настроек SysPrep, где необходимо указать использовать (не использовать) файл XML с настройками SysPrep, который будет скопирован на ВМ и применен. Можно дополнительно выбрать опции из раскрывающегося списка. Для подтверждения операции необходимо нажать «ОК»;

– управление VirtSysPrep. При нажатии на кнопку «VirtSysPrep» открывается окно настроек VirtSysPrep, где необходимо выбрать виртуальный загрузочный диск ВМ, который будет подготовлен, и опции из раскрывающегося списка. Для подтверждения операции необходимо нажать «ОК»;

– управление Hostname. При нажатии на кнопку «Hostname» открывается окно настроек Hostname, где необходимо выбрать имя и выбрать опции задания Hostname для конкретной ОС из раскрывающегося списка. Для подтверждения операции необходимо нажать «ОК»;

– добавление SSH-ключа. При нажатии на кнопку «Добавить SSH-ключ» добавляется SSS-ключ для выбранного пользователя (только для ОС Linux, для выключенной ВМ или для включенной с активным гостевым агентом);

– ввод в домен. При нажатии на кнопку «Ввод в домен» открывается окно настроек ввода ВМ в AD (только для ОС Windows);

– вывод из домена. При нажатии на кнопку «Вывод из домена» открывается окно настроек выведения ВМ из AD (только для ОС Windows).

3.8.6.3. В режиме шаблона в окне отображается список ВМ – «наследников» шаблона, созданных в кластере, включая их названия, сервер, сведения о vCPU, vRAM, vDisk, vNIC, vFunc и статус.

3.8.7. «Виртуальные машины» – <имя ВМ> – «Процессоры»

3.8.7.1. В окне «Виртуальные машины» – <имя ВМ> – «Процессоры» содержится следующая информация о процессорах ВМ:

– количество сокетов;

– количество ядер на сокет;

– количество потоков на ядро;

– общее количество потоков;

– максимальное количество потоков;

– режим определения;

– модель;

– приоритет vCPU ВМ;

– количество минимально гарантированных vCPU;

– приоритет виртуальных процессоров vCPU;

– приоритет виртуальных процессоров;

– дополнительные функции vCPU.

3.8.7.2. При нажатии на кнопку «Настройки» в открывшемся окне «Настройки процессоров» существует возможность изменения следующих параметров:

1) количество процессоров. При нажатии кнопки «Количество» в открывшемся окне «Количество процессоров» необходимо указать количество vCPU и максимальное количество vCPU, после чего подтвердить операцию, нажав кнопку «ОК»;

2) топология процессоров. При нажатии кнопки «Топология» в открывшемся окне «Топология процессора» необходимо задать количество сокетов, ядер на сокет и потоков на ядро, после чего подтвердить операцию, нажав кнопку «ОК»;

3) модель процессора. При нажатии кнопки «Модель» в открывшемся окне «Модель процессора» необходимо выбрать из раскрывающегося списка режим определения процессора – «default», «host-model», «host-passthrough» или «custom», после чего подтвердить операцию, нажав кнопку «ОК»;

4) привязка виртуальных процессоров к физическим ядрам. При нажатии кнопки «Привязка» в открывшемся окне «Привязка процессора» необходимо заполнить поле «Привязать виртуальные процессоры ВМ к физическим», после чего подтвердить операцию, нажав кнопку «ОК;

5) приоритет выделения процессорного времени ВМ. При нажатии кнопки «Приоритет» в открывшемся окне «Приоритет процессора» необходимо:

– выбрать из раскрывающегося списка базовый приоритет vCPU – «LOW», «MEDIUM» или «HIGH»;

– указать детальный приоритет vCPU ВМ;

– указать количество минимально гарантированных vCPU.

После внесения изменений необходимо подтвердить операцию, нажав кнопку «Сохранить»;

6) дополнительные функции vCPU. При нажатии кнопки «Дополнительные функции vCPU» в открывшемся окне необходимо указать дополнительные функции (флаги), после чего подтвердить операцию, нажав кнопку «Сохранить».

Параметр «Максимальное количество vCPU» рекомендуется ставить больше при планировании в дальнейшем увеличивать количество vCPU при включенной ВМ. При изменении максимального количества vCPU топология подстраивается под этот параметр, то есть включенная ВМ видит именно максимальное количество vCPU, но при этом только на указанном количестве vCPU подключается питание, а остальные vCPU видятся неактивными (без питания).

3.8.7.3. Изменение топологии процессора предназначено для удовлетворения требований ОС ВМ. Некоторые ОС не умеют работать с многоядерными процессорами, некоторые ограничивают количество сокетов CPU, а некоторые ОС ограничивают количество ядер на сокет.

3.8.7.4. Модель процессора может влиять на функциональность ОС ВМ и на возможность миграции ВМ внутри кластера.

Доступные функции узла можно посмотреть в окне «Сервер» – <имя сервера> – «Оборудование» – «Процессоры».

Модель (архитектура) CPU виртуальной машины может быть:

– «default» – назначаются виртуальные vCPU. Если ОС ВМ чувствительна к набору инструкций центрального процессора, то использование vCPU может не удовлетворять требованиям ОС ВМ. Доступные функции берутся из модели процессора qemu64;

– «host-model» – модель, аналогичная физическому, с незначительными ограничениями. Доступные функции берутся из узла, где находится ВМ;

– «host-passthrough» – фактическая трансляция полного комплекта инструкций и модели физического процессора. Доступные функции берутся из узла, где находится ВМ;

– «custom» – выбор модели процессора из списка. Необходимо учитывать предоставляемые наборы инструкций выбираемой модели и ограничения для ОС ВМ перед сменой типа процессора на «custom».

Доступные функции берутся из известного набора инструкций для каждого процессора, определенного в гипервизоре.

3.8.7.5. Привязка процессоров ВМ к физическим ядрам сильно ограничивает производительность сервера. Эту опцию рекомендуется применять только к высоконагруженным ВМ, миграция которых невозможна. Физическое ядро, привязанное к CPU виртуальной машины, будет использоваться только для этой ВМ.

3.8.7.6. Приоритет выделения процессорного времени ВМ может понизить или повысить приоритет выделения ресурсов для ВМ.

3.8.8. «Виртуальные машины» – <имя ВМ> – «Память»

3.8.8.1. Данный раздел отвечает за настройку выделяемой оперативной памяти.

3.8.8.2. В окне «Виртуальные машины» – <имя ВМ> – «Память» содержится следующая информация:

– оперативная память (редактируемый параметр);

– приоритет памяти ВМ (редактируемый параметр);

– максимальное значение памяти (редактируемый параметр);

– минимально гарантированная память (редактируемый параметр) – параметр, который учитывается при работе сервиса распределения памяти «ballooning» и при распределении ресурсов узлов.

3.8.8.3. В SpaceVM реализовано добавление ОЗУ в процессе работы («на лету»). Добавляется кратно 256 Мбайт, и ВМ изнутри видит ее как дополнительную DIMM планку памяти.

Для корректной работы добавления ОЗУ «на лету» необходимо перед этим установить комплект «virtio» драйверов.

3.8.9. «Виртуальные машины» – <имя ВМ> – «Диски»

3.8.9.1. В окне «Виртуальные машины» – <имя ВМ> – «Диски» содержится список дисков, подключенных в ВМ, включая для каждого из них его название, пул данных, размер и статус.

3.8.9.2. Создание нового диска и подключение существующего с помощью соответствующих кнопок полностью повторяет аналогичные операции при создании ВМ (см. 3.8.1.2 (шаг 2) данного руководства).

3.8.9.3. Для перехода в окно состояния диска необходимо нажать на его название, и в открывшемся окне будет отображаться информация о диске и кнопки управления.

3.8.9.4. Управление дисками допускает следующие операции:

1) обновление окна состояния диска по кнопке  ;

2) консолидация. Выполняется автоматически при нажатии кнопки «Консолидировать», кнопка присутствует на панели, если в списке есть диски, которые возможно консолидировать;

3) копирование. При нажатии кнопки «Копировать» в открывшемся окне «Копирование диска» необходимо выбрать из раскрывающегося списка пул данных, заполнить название и описание нового диска, после чего подтвердить операцию, нажав кнопку «Копировать»;

4) перенос диска. При нажатии кнопки «Перенос диска» в открывшемся окне необходимо выбрать из раскрывающегося списка пул данных для переноса, после чего подтвердить операцию, нажав кнопку «Перенести»;

5) подключение (отключение) диска от ВМ. При нажатии кнопки «Подключить» («Отключить») в открывшемся окне необходимо подтвердить операцию, нажав кнопку «Да»;

6) скачивание. Выполняется автоматически при нажатии кнопки «Скачать»;

7) настройки параметров ввода (вывода). При нажатии кнопки «Настройка I/O» в открывшемся окне заполнить соответствующие параметры и сохранить изменения кнопкой «ОК»;

8) удаление. При нажатии кнопки «Удалить» необходимо в открывшемся окне в дополнительных настройках определиться с гарантированным удалением диска, после чего подтвердить операцию, нажав кнопку «Удалить».

3.8.9.5. При отключении диска не происходит удаления диска с хранилища (из пула данных) и его можно будет использовать повторно. Удаление диска не только отключит его от ВМ, но и удалит файл диска.

3.8.9.6. Информация о диске содержит:

– название и описание диска (редактируемые параметры);

– ВМ, к которой подключен диск;

– пул данных;

– размер виртуального диска с возможностью его увеличения по кнопке  ;

– расположение;

– тип шины;

– SSD эмуляция;

– тип кэширования;

– тип драйвера;

– имя назначения;

– доступность только чтения ВМ (редактируемый параметр);

– дата и время создания;

– дата и время изменения;

– сообщения о работе дисков с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.8.10. «Виртуальные машины» – <имя ВМ> – «CD-ROM»

3.8.10.1. В окне «Виртуальные машины» – <имя ВМ> – «CD-ROM» содержится список приводов CD-ROM, включая их название, подключение, пул данных и статус. Также позволяет управлять подключенными в ВМ приводами CD-ROM и подключенными в них ISO-образами.

3.8.10.2. CD-ROM добавляется автоматически по кнопке «Добавить», после чего необходимо перейти к процедуре подключения. Процедура подключения CD/DVD-диска к виртуальному CD-ROM полностью повторяет аналогичные операции при создании ВМ (см. 3.8.1 данного руководства).

3.8.10.3. По кнопке «Монтировать образ utils» ведется автоматический поиск доступного образа с именем, начинающимся с «guest-utils», и после нахождения он монтируется к ВМ. Если образ есть в системе, но недоступен на узле, где находится ВМ, то образ скопируется на локальный пул этого узла, и уже после этого примонтируется к ВМ.

3.8.10.4. При нажатии на название CD-ROM в окне состояния CD-ROM доступны следующие операции:

– обновление информации по кнопке  ;

– монтирование образа (доступно, если образ не смонтирован).

При нажатии кнопки «Монтировать образ» в открывшемся окне необходимо выбрать из раскрывающегося списка тип хранилища, хранилище и ISO-образ. После этого подтвердить операцию, нажав кнопку «Монтировать»;

– извлечение образа (доступно, если образ смонтирован). При нажатии кнопки «Извлечь» в открывшемся окне необходимо подтвердить операцию, нажав на кнопку «Извлечь»;

– удаление. При нажатии кнопки «Удалить» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «Удалить».

3.8.10.5. Также в окне состояния CD-ROM содержится следующая информация:

– название;

– подключение (ISO-образ);

– пул данных;

– устройство dev;

– дата и время создания.

3.8.11. «Виртуальные машины» – <имя ВМ> – «USB-устройства»

3.8.11.1. В окне «Виртуальные машины» – <имя ВМ> – «USB-устройства» имеется возможность подключения к ВМ USB-устройств, подключенных к физическому серверу – Web-камеры, клавиатуры, манипуляторы, накопители и прочие устройства.

3.8.11.2. Для подключения USB-устройства необходимо в окне управления USB-устройствами нажать на кнопку «Подключить» и далее в открывшемся окне «Подключение usb-устройства» включить (отключить) режим SPICE USB, выбрать USB-устройство, раскрыв перечень по кнопке  , и USB-контроллер из раскрывающегося списка. Далее необходимо подтвердить операцию, нажав кнопку «ОК».

3.8.11.3. Для создания USB-канала для клиентов SPICE необходимо включить режим SPICE USB. Добавить SPICE USB-канал, выбрать контроллер и нажать «ОК».

3.8.12. «Виртуальные машины» – <имя ВМ> – «PCI-устройства»

3.8.12.1. В окне «Виртуальные машины» – <имя ВМ> – «PCI-устройства» имеется возможность подключения к ВМ некоторых физических устройств сервера, подключенных по шине PCI/PCI-express.

Необходимо учитывать, что подключение аппаратных средств сервера в ВМ может вызвать ошибку гипервизора, отказ в работе системных устройств или перехватить используемые другими частями системы устройства. Также некоторые устройства являются «составными» и не могут быть подключены к ВМ независимо.

3.8.12.2. Видеокарта может быть связана с аудио кодеком для HDMI. Некоторые сетевые карты могут быть 2/4/8-портовыми. «Составные» устройства необходимо подключать к ВМ целиком. При подключении к ВМ сетевых карт необходимо учитывать, что физическое устройство может быть занято для «mgmt» сети или для другого виртуального коммутатора.

3.8.12.3. Для подключения устройства PCI необходимо в окне управления PCI-устройствами нажать на кнопку «Подключить» и далее в открывшемся окне «Подключение PCI-устройства» выбрать PCI-устройство, раскрыв перечень по кнопке  , и PCI-контроллер из раскрывающегося списка. Далее необходимо подтвердить операцию, нажав кнопку «OK».

Примечание. Кнопка «Подключить» доступна только для выключенной ВМ.

3.8.12.4. Для добавления PCI-устройства в CLI узла необходимо:

– выполнить команду *system pci set on*;

– перезагрузить узел;

– ВМ должна быть выключена;

– подключить PCI-устройство.

3.8.12.5. При подключении видеокарты необходимо учитывать следующее:

– обычная видеокарта состоит из двух устройств – видеокарты и аудиоустройства. Для стабильной работы необходимо подключать оба;

– тип машины должен быть «q35», тип загрузки – «efi». Это связано с некоторыми особенностями работы BIOS видеокарты;

– подключать видеокарту необходимо строго на свободную шину. Для определения свободного номера можно воспользоваться командой *vm xml*, посмотреть, какой номер «bus» в устройствах свободен и выбрать его при подключении устройства в pcie-root-port (в обычной ситуации, если не было подключений дополнительных контроллеров, то номер «5» свободен);

– аудиоустройство также требует отдельной шины.

3.8.12.6. Чтобы включить функцию предоставления доступа ВМ к части устройства SR-IOV, необходимо указать параметр «intel_iommu=on» или «amd_iommu=on» в зависимости от конфигурации вашего сервера в конфигурационном файле загрузчика «grub».

Чтобы добиться максимальной производительности при использовании SR-IOV, необходимо задать параметр «iommu=pt» в файле конфигурации загрузчика «grub». В случае доступа ВМ к адаптеру напрямую не требуется использования преобразования DMA, за счет чего и улучшается производительность системы. Параметр «iommu=pt» нужен в основном для гипервизора и не влияет на работу ВМ. Если «intel_iommu=on» или «amd_iommu=on» работает, то можно попробовать заменить их на «iommu=pt» или «amd_iommu=pt» в зависимости от конфигурации узла. Параметр «pt» включает IOMMU только для тех устройств, доступ к которым предоставлен ВМ, и обеспечивает лучшую производительность узла.

3.8.12.7. В чем разница между «PCI pass-through» устройств к ВМ и IOMMU? «PCI pass-through» не требует вмешательств гипервизора для работы гостевой ОС с физическим устройством.

IOMMU при работе не использует DMA трансляции гипервизора. Таким образом, гипервизору не нужно обрабатывать запросы DMA, когда включен режим IOMMU. «PCI pass-through» и IOMMU работают совместно для обеспечения доступа гостевой ОС напрямую к физическому устройству.

3.8.13. «Виртуальные машины» – <имя ВМ> – «Mediated-устройства»

3.8.13.1. В окне «Виртуальные машины» – <имя ВМ> – «Mediated-устройства» имеется возможность управлять mediated-устройствами.

3.8.13.2. Для подключения mediated-устройства необходимо в окне управления mediated-устройствами нажать на кнопку «Подключить» и далее в открывшемся окне «Подключение mediated-устройства» выбрать mediated-устройство, PCI-контроллер, дисплей (вкл/выкл) и Ramfb (вкл/выкл). Далее необходимо подтвердить операцию, нажав кнопку «ОК».

3.8.13.3. При выборе mediated-устройство, которое уже подключено к ВМ, разворачивается окно с его характеристиками:

– название;

– PCI;

– Display (вкл/выкл);

– Ramfb (вкл/выкл);

– тип устройства (имя шаблона);

– фреймбуфер (размер видеопамяти);

– Frl config;

– max Instance;

– max разрешение;

– Num heads.

3.8.14. «Виртуальные машины» – <имя ВМ> – «Снимки»

3.8.14.1. В окне «Виртуальные машины» – <имя ВМ> – «Снимки» имеется возможность управлять снимками состояний ВМ.

3.8.14.2. В окне «Управление снимками состояний» можно создавать резервные копии ВМ с помощью кнопки «Сохранить состояние ВМ». В открывшемся окне необходимо заполнить:

– название и описание состояния;

– выбрать из раскрывающегося списка виртуальные диски и хранилище для снимков памяти;

– определить необходимость сохранения состояния памяти.

После этого необходимо подтвердить операцию, нажав кнопку «Сохранить».

Снимок ВМ по сути является слепком состояния системы ВМ на конкретный момент времени.

3.8.14.3. Для работающей ВМ также делается слепок памяти ВМ.

3.8.14.4. В окне «Управление снимками состояний» снимки отображаются в виде вершин графа. Текущее состояние машины отображается в виде анимированной вершины графа.

Между снимками может проводиться навигация.

Ветвление снимков формируется по принципу «дерева».

3.8.14.5. Перед операциями над снимками (кроме создания) необходимо выключить ВМ, так как могут потребоваться операции по слиянию данных с нескольких копий дисков ВМ.

3.8.14.6. Нажав на изображении снимка, открывается информационное окно «Состояние снимка», содержащее информацию о сохраненном состоянии ВМ:

– название (редактируемый параметр);

– описание (редактируемый параметр);

– статус;

– дата и время создания;

– дата и время изменения;

– состояние ВМ на момент создания.

3.8.14.7. Кроме редактирования параметров снимка в окне «Состояние снимка» возможны действия:

– переход в состояние снимка. При нажатии на кнопку «Перейти в состояние снимка» открывается окно, в котором можно определить настройки – ВМ будет восстановлена во включенном состоянии и ВМ будет восстановлена в приостановленном состоянии. После этого подтвердить операцию, нажав кнопку «Перейти»;

– удаление состояния снимка.

При нажатии на кнопку «Удалить состояние снимка» открывается окно, в котором можно включить опцию «Удалить вместе с потомками», после чего подтвердить операцию, нажав кнопку «Удалить» или отменить действие, нажав кнопку «Отмена».

3.8.14.8. В некоторых случаях при создании снимка включенная ВМ будет переходить в состояние «Приостановлено».

3.8.14.9. При переходе на сохраненное состояние текущее состояние безвозвратно теряется.

3.8.14.10. На неактивной ветке можно удалить все снимки от выбранного до последнего, что позволяет без трудностей удалить всю ненужную ветку.

3.8.14.11. Нажатие на кнопку «Удалить все состояния» приводит к тому, что цепочка снэпшотов от текущего состояния вливается в базовый образ диска, и все файлы снимков удаляются, включая снимки неактивных состояний.

3.8.14.12. Нажатие на кнопку «Разбить дерево состояний» приводит к тому, что удаляются сохраненные состояния ВМ, но при этом остаются снимки дисков, делая их неконсолидированными.

Эта операция требуется для возможности исключить проблемный диск из ВМ, но затем потребуется провести операцию «Консолидировать» для каждого диска в отдельности.

3.8.14.13. Делая копию диска, имеющего снимки, делается копия от первого сохраненного состояния.

3.8.14.14. При удалении ВМ происходит вызов «Удалить все состояния», то есть все текущие состояния вливаются в диски, а неактивные ветки состояний удаляются.

3.8.14.15. При клонировании ВМ клонируются также сохраненные состояния, кроме наличия дисков с сохраненными состояниями на thin-LVM хранилище. В этом случае клонирование невозможно, требуется операция «Удалить все состояния».

3.8.14.16. Если ВМ включена, то доступен ее гостевой агент и создается снимок без памяти. Перед созданием снимка через гостевого агента запускается команда сброса кэша и заморозки ФС всех дисков на госте.

3.8.15. «Виртуальные машины» – <имя ВМ> – «Интерфейсы»

3.8.15.1. В окне «Виртуальные машины» – <имя ВМ> – «Интерфейсы» имеется возможность управлять виртуальными сетевыми картами ВМ.

В данном окне отображается список интерфейсов, включая для каждого из них его виртуальную сеть, MAC-адрес, NIC-драйвер и статус.

3.8.15.2. Процесс добавления интерфейса аналогичен процессу создания ВМ. Для этого в окне управления интерфейсами ВМ необходимо нажать на кнопку «Добавить виртуальный интерфейс». В открывшемся окне необходимо заполнить:

– виртуальную сеть (выбор из раскрывающегося списка);

– MAC-адрес (необязательный параметр);

– NIC_драйвер (выбор из раскрывающегося списка). Может принимать значение «virtio», «e1000», «rtl8139» или «vmxnet3»;

– описание (при необходимости);

– состояние линка (вкл «по умолчанию»);

– QoS (вкл/выкл).

Примечание. Для ОС Windows драйвер «e1000» нативный (родной) и не требует доустановки драйверов, но не может на ходу применять изменения MTU. Рекомендуется после установки «virtio» драйверов в ВМ сменить на «virtio».

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

3.8.15.3. В окне «Управление интерфейсами виртуальных машин» имеется возможность удалить интерфейсы, нажав кнопку «Удалить все виртуальные интерфейсы». В открывшемся окне необходимо подтвердить операцию, нажав на кнопку «Да».

3.8.15.4. При нажатии на существующий интерфейс в окне состояния интерфейса доступны следующие операции:

– обновление информации по кнопке  ;

– изменение параметров. Для этого необходимо нажать кнопку «Изменение параметров» и в открывшемся окне выбрать из раскрывающегося списка виртуальную сеть и заполнить MAC-адрес. Далее необходимо подтвердить операцию, нажав «ОК»;

– удаление. Для этого необходимо нажать кнопку «Удалить» и в открывшемся окне необходимо подтвердить операцию, нажав на кнопку «Удалить».

3.8.15.5. Также в окне состояния интерфейса содержатся следующие сведения:

– название;

– описание (редактируемый параметр);

– виртуальная сеть;

– ВМ;

– MAC-адрес;

– NIC_драйвер;

– состояние линка;

– статус;

– время и дата создания;

– сообщения о работе виртуального диска с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.8.15.6. При необходимости использования VLAN для ВМ следует создать на коммутаторе группу интерфейсов и назначить ей требуемый VLAN-тег. При необходимости использовать несколько VLAN-тегов следует создать для каждого из них свою группу.

Внутренняя организация виртуальных интерфейсов не позволяет назначить несколько VLAN-тегов интерфейсу внутри ОС ВМ.

3.8.16. «Виртуальные машины» – <имя ВМ> – «Виртуальные функции»

3.8.16.1. Для подключения виртуальной функции необходимо в окне управления виртуальными функциями нажать на кнопку «Добавить функцию» и в открывшемся окне выбрать доступную виртуальную функцию. Далее необходимо подтвердить операцию, нажав кнопку «ОК».

3.8.16.2. При выборе виртуальной функции открывается окно, которое содержит следующие параметры:

– название;

– дата изменения;

– дата создания;

– MAC-адрес;

– PCI-домен;

– PCI-шина;

– PCI-слот;

– PCI-назначение;

– виртуальная машина;

– сообщения.

3.8.16.3. Для отключения виртуальной функций необходимо в окне управления виртуальными функциями нажать на «Отключение виртуальной функций» и в открывшемся окне подтвердить операцию, нажав на кнопку «Да».

3.8.16.4. Использование виртуальных функций смотрите в 3.6.11.6.

3.8.17. «Виртуальные машины» – <имя ВМ> – «Контроллеры»

3.8.17.1. В окне «Виртуальные машины» – <имя ВМ> – «Контроллеры» имеется возможность управлять подключенными к ВМ контроллерами.

3.8.17.2. В окне управления контроллерами содержится информация о контроллерах по группам:

1) тип контроллера:

– тип;

– количество;

– свободные слоты;

2) все контроллеры:

– тип;

– модель;

– действие – возможность удаления контроллера по кнопке «Удалить».

3.8.17.3. Также в окне управления контроллерами имеется возможность обновления информации и добавления контроллера.

При нажатии кнопки «Добавить контроллер» в открывшемся окне необходимо выбрать из раскрывающегося списка тип контроллера – «pci», «sata», «scsi» или «usb» и подтвердить операцию, нажав кнопку «Создать». Это необходимо в случаях, если виртуальные контроллеры, предоставляемые ВМ гипервизором, не работают в ОС, установленной на ВМ.

3.8.17.4. Шины, к которым возможно подключение (HotPlug) устройств:

– PCI;

– SCSI.

Примечания:

1. Если добавляются устройства и для них не хватает свободных слотов, то гипервизор сам добавляет узел (хаб) в соответствующий контроллер, и новые устройства добавляются в него.

SpaceVM автоматически добавляет контроллеры в базу ВМ, и после перезагрузки ВМ ее фактическая конфигурация будет соответствовать базе.

2. При изменении контроллеров USB и PCI все примонтированные USB- и PCI-устройства убираются и выставляется порядок контроллеров.

3.8.17.5. Ниже приведены характеристики слотов и контроллеров чипсета PC:

1) IDE – всегда один контроллер, добавить/удалить нельзя, четыре слота на контроллер.

Занимают слоты:

– CD-ROM;

– виртуальные диски и LUN, подключенные по IDE;

2) PCI – «по умолчанию» два контроллера – «pci-root» и «pci-bridge», 31 слот на каждом (в сумме 62).

Занимают слоты:

– каждый контроллер ЛЮБОГО типа, кроме «pci-root»;

– виртуальные диски и LUN, подключенные по «virtio»;

– сетевые интерфейсы и функции;

– PCI и mediated-устройства;

– звуковая карта при наличии («по умолчанию» есть);

– видеокарта при наличии («по умолчанию» есть);

– «balloon» устройство при выключенном безопасном режиме («по умолчанию»);

– «virtio-serial» контроллер (всегда есть);

3) USB – «по умолчанию» один контроллер – «nec-xhci» (USB3.0), четыре слота на контроллер.

Занимают слоты:

– USB-устройства;

– USB TCP-каналы;

– SPICE USB-каналы;

4) SATA – «по умолчанию» один контроллер, шесть слотов на контроллер.

Занимают слоты – виртуальные диски и LUN, подключенные по SATA;

5) SCSI – «по умолчанию» ноль контроллеров. При наличии контроллера – шесть слотов на контроллер.

Занимают слоты – виртуальные диски и LUN, подключенные по SCSI.

Итого:

– на шине IDE максимум четыре диска (если удалить CD-ROM);

– на шине PCI проверено подключение 256 дисков;

– на шине SATA проверено подключение 256 дисков;

– на шине SCSI проверено подключение 256 дисков.

3.8.17.6. Ниже приведены характеристики слотов и контроллеров чипсета Q35:

1) IDE – всегда ноль контроллеров, добавить нельзя;

2) PCI – «по умолчанию» два контроллера – «pci-root» и «pci-bridge», 31 слот на каждом (в сумме 62).

Занимают слоты:

– каждый контроллер ЛЮБОГО типа, кроме «pci-root»;

– виртуальные диски и LUN, подключенные по «virtio»;

– сетевые интерфейсы и функции;

– PCI и mediated-устройства;

– звуковая карта при наличии («по умолчанию» есть);

– видеокарта при наличии («по умолчанию» есть);

– «balloon» устройство при выключенном безопасном режиме («по умолчанию»);

– «virtio-serial» контроллер (всегда есть);

3) USB – «по умолчанию» один контроллер – «nec-xhci» (USB3.0), четыре слота на контроллер.

Занимают слоты:

– USB-устройства;

– USB TCP-каналы;

– SPICE USB-каналы;

4) SATA – «по умолчанию» один контроллер, шесть слотов на контроллер.

Занимают слоты:

– CD-ROM;

– виртуальные диски и LUN, подключенные по SATA;

5) SCSI – «по умолчанию» ноль контроллеров. При наличии контроллера – шесть слотов на контроллер.

Занимают слоты – виртуальные диски и LUN, подключенные по SCSI.

Итого:

– на шине IDE нет дисков;

– на шине PCI проверено подключение 210 дисков;

– на шине SATA проверено подключение 256 дисков;

– на шине SCSI проверено подключение 256 дисков.

3.8.17.7. Отличие между чипсетом PC и Q35 заключается в том, что в Q35 нет IDE, поэтому CD-ROM в PC монтируются по IDE, в Q35 монтируются по SATA.

3.8.18. «Виртуальные машины» – <имя ВМ> – «LUNs»

3.8.18.1. В окне «Виртуальные машины» – <имя ВМ> – «LUNs» имеется возможность подключить блочное устройство (LUN) с iSCSI target или оптическую сеть блочного доступа (FC) напрямую к ВМ в качестве диска ВМ (НЖМД). Необходимо учитывать, что при потере связи ОС ВМ будет реагировать аналогично аварийному извлечению НЖМД.

3.8.18.2. Для подключения LUN необходимо в окне управления LUN нажать кнопку «Присоединить» и в открывшемся окне выбрать из раскрывающегося списка iscsi-хранилище, LUN, тип шины («virtio», «ide», «scsi» или «sata») и тип кэширования («default», «none», «writethrough», «writeback», «directsync» или «unsafe»). В расширенных опциях можно включить настройку «Режим мульти использования LUN несколькими ВМ». Далее подтвердить операцию, нажав кнопку «ОК».

3.8.18.3. Также в окне управления LUN имеется возможность обновления информации по кнопке  и выбора устройства с применением фильтра по кнопке «Фильтр».

3.8.19. «Виртуальные машины» – <имя ВМ> – «Высокая доступность»

3.8.19.1. В окне «Виртуальные машины» – <имя ВМ> – «Высокая доступность» имеется возможность назначить индивидуальные настройки высокой доступности ВМ. Централизованная настройка ВД для кластера производится в настройках кластера. Индивидуальные настройки для ВМ идентичны настройке ВД для кластера.

3.8.19.2. В окне управления системой высокой доступности предусмотрены следующие операции:

– синхронизация всех настроек с настройками системы ВД кластера. Происходит автоматически при нажатии кнопки «Синхронизировать с кластером» и загрузит для данной ВМ настройки ВД от кластера, в состав которого входит данная ВМ;

– сохранение. Происходит автоматически при нажатии на кнопку «Сохранить»;

– просмотр информации о порядке загрузки ВМ. При нажатии соответствующей кнопки открывается информационное окно с очередностью загрузки существующих ВМ. Окно закрывается с помощью кнопки «Закрыть» или  ;

– просмотр информации о порядке серверов для восстановления. При нажатии соответствующей кнопки открывается информационное окно с очередностью серверов для восстановления. Окно закрывается с помощью кнопки «Закрыть» или  .

3.8.19.3. Также в окне управления системой ВД существует возможность редактировать следующие параметры:

– количество попыток восстановления ВМ;

– интервал между попытками восстановления ВМ (в секундах);

– номер в очереди на восстановление (может повторяться – ВМ с одинаковым номером будут восстановлены одновременно);

– признак полной загрузки ВМ – истечение заданного времени (в секундах);

– признак полной загрузки ВМ – запуск гостевого агента ВМ. Задается максимальное время ожидания (в секундах);

– включение или выключение ВД;

– включение или выключение автоматического выбора сервера для восстановления ВМ.

Для сохранения всех изменений необходимо нажать на кнопку «Сохранить».

Примечание. Если все попытки восстановления ВМ завершились неудачей, то высокая доступность выключается для этой ВМ, что можно проследить по журналу событий.

3.8.20. «Виртуальные машины» – <имя ВМ> – «Опции загрузки»

3.8.20.1. В окне «Виртуальные машины» – <имя ВМ> – «Опции загрузки» имеется возможность настройки типа загрузчика ВМ (LegacyMBR/UEFI) и выбора порядка опроса загрузочных устройств.

3.8.20.2. В окне управления загрузчиком имеется возможность:

– включить (выключить) автозапуск ВМ при активации узла;

– включить (выключить) загрузочное меню;

– задать время ожидания до начала загрузки (в секундах);

– выбрать тип загрузки – «LegacyMBR» или «UEFI»;

– перераспределить устройства между нераспределенными и устройствами, используемыми в загрузке устройства. Порядок используемых устройств сверху вниз соответствует порядку опроса при загрузке ВМ. В случае, если первым в очереди стоит CD-ROM, но нет образа, который в него установлен, то загрузка произойдет со следующего устройства.

Для сохранения всех изменений необходимо нажать на кнопку «Сохранить».

3.8.20.3. При переходе узла в активный режим (неважно, по какой причине, ручной ли это вывод узла из сервисного режима или автоматический после сбоев), проверяются все ВМ этого узла с включенной опцией автозапуска и включаются.

3.8.21. «Виртуальные машины» – <имя ВМ> – «Резервное копирование»

3.8.21.1. В окне «Виртуальные машины» – <имя ВМ> – «Резервное копирование» имеется возможность создавать и управлять резервными копиями ВМ.

3.8.21.2. Также в окне отображается список файлов копий данной ВМ и их параметры:

– название файла с архивом ВМ;

– пул данных;

– название ВМ;

– размер;

– статус.

3.8.21.3. Для создания резервной копии необходимо нажать кнопку «Создать резервную копию» и в открывшемся окне «Создание архива ВМ» включить (выключить) следующие опции:

– «Исключить ISO из резервной копии» – эта опция позволяет не включать в резервную копию образ ISO, так как этот образ неизменяемый, и может быть нерациональным сохранение его таким способом;

– «Создать резервную копию с возможностью инкремента» – эта опция позволяет создать резервную копию с возможностью дополнять ее последними изменениями;

– «Выбрать резервную копию для инкремента» – эта опция позволяет дополнить одну из имеющихся резервных копий. При включении появится раскрывающийся список резервных копий из доступных для дополнения;

– «Инкрементировать последнюю резервную копию». При включении выбирается новейшая из доступных инкрементальных резервных копий или создается новая с возможностью инкремента;

– «Выбрать пул данных». При включении опции появляется раскрывающийся список пулов, в котором перечислены доступные для этой операции пулы данных. Если не включать опцию, то резервная копия будет создана на базовом пуле данных узла;

– «Сжать» – эта опция позволяет создать или инкрементировать резервную копию со сжатием.

Далее необходимо подтвердить операции, нажав кнопку «ОК».

3.8.22. «Виртуальные машины» – <имя ВМ> – «Удаленный доступ»

3.8.22.1. В окне «Виртуальные машины» – <имя ВМ> – «Удаленный доступ» имеется возможность управлять удаленным доступом в консоль ВМ.

3.8.22.2. Для возможности удаленного доступа к ВМ необходимо в данной вкладке включить опцию «Удаленный доступ». Опция «Удаленный доступ» предоставляет доступ к консоли ВМ по протоколу SPICE, осуществляемый с помощью стороннего приложения-клиента и (или) из-за периметра кластера. Пароль для доступа генерируется автоматически и его можно посмотреть и изменить.

При включении удаленного доступа отобразится IP-адрес и порт для подключения. В качестве IP-адреса подключения используется адрес контроллера.

Если требуется использовать адрес, отличный от основного адреса контроллера, то необходимо на сервере, выполняющем роль контроллера, создать дополнительный внутренний интерфейс. После этого необходимо в разделе «Настройки» – «Контроллер» – «Настройки ограждения» указать IP-адрес, присвоенный дополнительному внутреннему интерфейсу контроллера для перенаправления соединений к консолям ВМ.

Также за счет использования дополнительного интерфейса, его можно подключить в отдельный коммутатор «для доступа к ВМ пользователей» и ограничить VLAN и другими средствами изоляции от сети управления кластера.

3.8.22.3. В окне управления удаленным доступом при включенной опции «Удаленный доступ» имеется возможность настройки следующих параметров:

1) SPICE. Для настройки SPICE необходимо нажать кнопку «Настройки SPICE» и в открывшемся окне задать следующие параметры:

– сжатие JPEG (выбор из раскрывающего списка);

– потоковый режим (выбор из раскрывающего списка);

– буфер обмена (выбор из раскрывающего списка);

– режим «мыши» (выбор из раскрывающего списка);

– сжатие zlib (выбор из раскрывающего списка);

– сжатие воспроизведения (выбор из раскрывающего списка);

– передача файлов (выбор из раскрывающего списка);

– сжатие изображения (выбор из раскрывающего списка);

– множественные подключения.

2) в настройках SPICE ВМ режим поддержки аппаратного сжатия видео spice (редактируемый параметр) – вкл/выкл;

3) включение (отключение) удаленного доступа;

4) задание пароля. При нажатии кнопки  необходимо ввести пароль, после чего подтвердить операцию, нажав кнопку «Сохранить»;

5) просмотр IP-адреса и порта подключения;

6) определение возможности доступа со всех адресов. Если доступ разрешен только с конкретного адреса, то необходимо заполнить поля в группе «Доступ разрешен с:»:

– IP-адрес;

– маска подсети;

– комментарий;

– возможность добавления дополнительных адресов по кнопке «Добавить адрес».

Для сохранения изменений необходимо нажать кнопку «Сохранить», для удаления адресов нажать кнопку «Очистить список».

3.8.22.4. Изменение настроек SPICE возможно только, если ВМ не запущена.

3.8.23. «Виртуальные машины» – <имя ВМ> – «Настройка безопасности»

3.8.23.1. В окне «Виртуальные машины» – <имя ВМ> – «Настройка безопасности» имеется возможность управлять гарантированной очисткой памяти ВМ («Настройка безопасности» – «Очистка памяти») и разграничением доступа для пользователей («Настройка безопасности» – «Разграничение доступа для операторов»).

3.8.23.2. Настройка осуществляется с помощью:

– опция «Очистка памяти» – это механизм дополнительной очистки страниц физической памяти сервера после того, как они перестали использоваться ВМ. Эта опция предотвращает доступ к остаточной информации в страницах памяти средствами слежения уровня гипервизора.

Дополнительно эта опция включает очистку дискового пространства ВМ при удалении диска, а также выбор из раскрывающегося списка количества циклов перезагрузки памяти и типа очистки памяти. Для сохранения изменений необходимо нажать на кнопку «Сохранить»;

– опция «Разграничение доступа для операторов» – это возможность указать список операторов кластера, которым будет доступна эта ВМ, а также сменить владельца данной ВМ. При этом эти ограничения не относятся к пользователям, чья роль соответствует «администратору» кластера. Они имеют полный доступ ко всем ВМ кластера. Для того чтобы изменить пользователей ВМ, необходимо нажать кнопку «Изменить пользователей ВМ» и в открывшемся окне выбрать из раскрывающегося списка операторов, после чего подтвердить операцию, нажав «Изменить».

3.8.24. «Виртуальные машины» – <имя ВМ> – «События»

3.8.24.1. В окне «Виртуальные машины» – <имя ВМ> – «События» отображается список последних событий для данной ВМ по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.8.25. «Виртуальные машины» – <имя ВМ> – «Теги»

3.8.25.1. В окне «Виртуальные машины» – <имя ВМ> – «Теги» отображается список присвоенных меток для ВМ.

3.8.25.2. Также в данном окне «Теги и метки» имеется возможность следующих операций:

1) обновление информации по кнопке  ;

2) применение тега. При нажатии кнопки «Применить» в открывшемся окне необходимо выбрать тег, после чего подтвердить операцию, нажав кнопку «ОК»;

3) создание тега. При нажатии кнопки «Создать» в открывшемся окне необходимо заполнить:

– название тега;

– идентификатор тега (Slug);

– выбрать цвет тега из палитры, после чего подтвердить операцию, нажав кнопку «ОК».

После заполнения полей необходимо подтвердить операцию, нажав «Добавить».

3.8.25.3. Для удаления тега (метки) от ВМ необходимо выбрать его в списке тегов и в открывшемся окне выбрать одну из следующих операций:

1) удалить тег. При нажатии на соответствующую кнопку в открывшемся окне подтвердить операцию, нажав «Да»;

2) удалить метку. Можно сделать двумя способами:

– нажать кнопку «Открепить тег от ВМ» и открывшемся окне «Удаление метки» подтвердить операцию, нажав «Да»;

– раскрыть список «Сущности» и нажать на кнопку  . В открывшемся окне «Удаление метки» подтвердить операцию, нажав «Да».

3.8.26. «Виртуальные машины» – <имя ВМ> – «Задачи по расписанию»

3.8.26.1. В окне «Виртуальные машины» – <имя ВМ> – «Задачи по расписанию» отображается список задач, запланированных на данной ВМ, включая для каждой из них ее название, действие, статус, дату и время последнего и следующего запуска. Также в данном окне имеется возможность обновления и добавления.

3.8.26.2. Для создания задачи по расписанию необходимо нажать кнопку «Добавить». В открывшемся окне заполнить следующие поля:

– название задачи;

– действие (выбор из раскрывающегося списка). Может принимать значения «start», «shutdown», «destroy», «suspend», «reboot», «reset», «migrate», «clone», «snapshot», «backup» или «remove»;

– периодичность (выбор из раскрывающегося списка);

– дата и время запуска;

– описание;

– указать при необходимости дополнительные параметры для запуска задач миграции «migrate», клонирования «clone», создания снимка памяти «snapshot», создания резервной копии «backup», удаления «remove».

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

3.8.26.3. При нажатии на название задачи открывается окно состояния задачи, в котором предусмотрены следующие операции с выбранной задачей:

– обновление информации;

– запуск. При нажатии кнопки «Запуск» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «Да»;

– удаление. При нажатии кнопки «Удалить» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «Да».

Также в окне состояния задачи содержится следующая информация:

– название (редактируемый параметр);

– описание (редактируемый параметр);

– периодичность (редактируемый параметр);

– дата и время первого запуска задачи (редактируемый параметр);

– дата и время следующего запуска задачи;

– дата и время последнего запуска задачи;

– статус последнего запуска задачи;

– дата и время создания задачи;

– дата и время изменения задачи;

– сообщения о работе планировщика задач с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений.

3.8.27. Катастрофоустойчивая ВМ

3.8.27.1. Катастрофоустойчивой считается ВМ, работоспособность которой можно восстановить после потери связи (выхода из строя) всей локации, где она размещалась в кратчайшие сроки. Для обеспечения данного функционала предусмотрено использование реплицируемого между локациями iSCSI LUN.

При использовании в качестве СХД «Raidix» предусмотрено управление ролями репликации из интерфейса SpaceVM по Application Programming Interface (API) «Raidix».

3.8.27.2. Для обеспечения данной возможности необходимо настроить реплицируемый между локациями LUN и подключить его в качестве НЖМД ВМ.

При использовании СХД «Raidix» SpaceVM определит автоматически, какой LUN является «дополнительным». Для настройки СХД «Raidix» необходимо обратиться к документации производителя СХД.

3.8.27.3. Настройка и проверка статуса катострофоустойчивости производится во вкладке «Информация» окна состояния ВМ.

В пункте «Катастрофоустойчивость» присутствуют две кнопки  и  :

3) первая кнопка  открывает окно «Ручное восстановление ВМ».

В этом окне можно проверить соблюдение всех требований для переноса ВМ на другой сервер:

– наличие на целевом сервере коммутатора и группы портов, совпадающих с текущими параметрами ВМ;

– наличие на целевом сервере подключенного LUN, являющегося репликой основного LUN ВМ;

– наличие на целевом сервере достаточного количества ресурсов для запуска ВМ;

– совпадение параметров тегирования на целевом сервере с текущими параметрами ВМ.

Для проверки состояния необходимо нажать кнопку «Проверить состояние». В открывшемся окне отобразятся следующие сведения:

– сервер (выбор из раскрывающегося списка);

– общее состояние;

– состояние сети;

– состояние хранилищ;

– состояние ресурсов;

– состояние тегирования.

Для выполнения ручного переноса ВМ в другую локацию необходимо нажать кнопку «ОК»;

4) вторая кнопка  открывает окно «Настройка катастрофоустойчивости ВМ», в котором можно включить данную опцию и указать, в какую локацию будет переключена ВМ (выбор из раскрывающегося списка). Данная опция включится только, если в предыдущем окне для выбранного в нем сервера все проверки завершились успешно. Для подтверждения операции необходимо нажать кнопку «ОК».

3.8.28. Файл конфигурации ВМ

3.8.28.1. Посмотреть действующую конфигурацию XML запущенной ВМ можно в CLI сервера командой

vm xml [имя или id ВМ]

3.8.28.2. Посмотреть действующую конфигурацию XML ВМ можно через REST API запрос командой

GET /api/domains/{id}/xml/

3.8.28.3. Модифицировать конфигурацию XML ВМ вручную не рекомендуется из-за сложности обработки всех случаев при создании и импорте резервных копий ВМ, а также при работе с ними. Если все же есть такая необходимость, то можно добавить свою часть XML через REST API.

3.8.28.4. Ниже приведен пример изменения пользовательского XML:

PUT http(s):///<адрес контроллера>/api/domains/94450c3e-b452-46b0-af4a-f688c726f054/

{

"user_xml": "<features>\n<acpi/>\n<apic/>\n</features>"

}

3.8.29. Гостевой агент, драйверы и утилиты для SPICE

3.8.29.1. Загрузка образа

3.8.29.1.1. Образ содержит пакеты для ОС Linux и Windows. Включает «qemu_guest_agent», «virtio» драйверы и утилиты для SPICE.

3.8.29.1.2. Получить образ с драйверами можно по запросу у предприятия-разработчика.

3.8.29.2. Состав образа

3.8.29.2.1. В состав образа входят:

1) «Spice guest tools» – этот установщик содержит некоторые дополнительные драйверы и службы, которые можно установить в гостевой системе Windows для повышения производительности и интеграции SPICE.

Он включает видеодрайвер «qxl» и гостевой агент SPICE (для копирования и вставки, автоматического переключения разрешения и прочее). Все драйверы, которые будут доступны при установке, указаны далее в «Virtio guest tools»;

2) «Spice vdagent» – необязательный компонент, улучшающий интеграцию окна гостевой системы с графическим интерфейсом удаленного пользователя. SPICE-протокол поддерживает канал связи между клиентом и агентом на стороне сервера. Агент работает внутри гостевой системы. Для связи с агентом в гостевой системе также используется специальное устройство, так называемый VDI-порт;

3) «Spice webdavd» – служба, которая использует протокол WebDAV для предоставления общего доступа к файлам ВМ;

4) «Virtio guest tools» – этот установщик содержит некоторые дополнительные драйверы и службы, которые можно установить в гостевой системе:

– NetKVM – Virtio сетевой драйвер;

– viostor – Virtio блочный драйвер;

– vioscsi – Virtio драйвер интерфейса SCSI;

– viorng – Virtio RNG (генератор случайных чисел) драйвер;

– vioser – Virtio serial driver (предоставляет несколько портов гостю в виде простых символьных устройств для простого ввода-вывода между гостевым и хостовым пользовательскими пространствами. Это также позволяет открывать несколько таких устройств, снимая ограничения на одно устройство);

– Balloon – Virtio memory balloon driver («Баллонное устройство» virtio позволяет гостям KVM уменьшить объем своей памяти (тем самым освободив память для хоста) и увеличить ее обратно (тем самым забрав память у хоста));

– qxl – QXL графический драйвер для Windows 7 и ниже;

– qxldod – QXL графический драйвер для Windows 8 и выше;

– pvpanic – драйвер устройства QEMU pvpanic (устройство «pvpanic» – это смоделированное устройство ISA);

– guest-agent – Qemu Guest Agent 32bit and 64 bit MSI installers;

– qemupciserial – драйвер QEMU PCI.

3.8.29.3. Другие варианты скачивания Virtio Drivers

3.8.29.3.1. Обычно драйверы довольно стабильны, поэтому сначала следует попробовать самый последний выпуск.

Последние драйверы «virtio» можно скачать по ссылке *https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/latest-virtio/virtio-win.iso.*

Стабильные драйверы «virtio» можно скачать по ссылке *https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/stable-virtio/virtio-win.iso.*

3.8.29.4. Монтирование образа

3.8.29.4.1. После загрузки образа в SpaceVM необходимо примонтировать образ к ВМ и используя стандартные установщики поставить требуемое ПО в ВМ.

3.8.29.5. Установка «qemu-guest-agent» на Linux ВМ

3.8.29.5.1. В Linux ВМ нужно просто установить утилиту «qemu-guest-agent» из стандартных репозиториев. За дополнительной информацией следует обратиться к документации вашей ОС.

3.8.29.5.2. Для систем на базе Debian/Ubuntu с «apt-get» запустите команду

apt-get install qemu-guest-agent

3.8.29.5.3. Для систем на базе RedHat с «yum» запустите команду

yum install qemu-guest-agent

3.8.29.5.4. При отсутствии доступа к репозиториям можно установить агент с образа. Для этого следует перейти в образы по пути «/linux/qemu-guest-agent/» и установить нужную версию, например,
«dpkg -i qemu-guest-agent_5.2+dfsg-9_amd64.deb».

3.8.29.5.5. В зависимости от дистрибутива гостевой агент может не запуститься автоматически после установки. Тогда запустите его командой *systemctl start qemu-guest-agent* (для дистрибутивов, использующих «systemd») или перезагрузите ВМ.

3.8.29.6. Взаимодействие гипервизора с «qemu-guest-agent»

3.8.29.6.1. «qemu-guest-agent» – это небольшая утилита, которая принимает команды от хоста через «virtio» канал с именем «org.qemu.guest_agent.0» и исполняет их в контексте гостя. На стороне гипервизора канал заканчивается unix-сокетом, в который можно писать текстовые команды.

Для каждой ВМ создается отдельный канал взаимодействия гипервизора с гостевым агентом (не зависящий от наличия сети у ВМ).

Ниже показан пример канала взаимодействия

<channel type='unix'>

<source mode='bind' path='/var/lib/libvirt/qemu/channel/target/domain-89-d1134f72-2b4e-41c4-a/org.qemu.guest_agent.0'/>

<target type='virtio' name='org.qemu.guest_agent.0' state='disconnected'/>

<alias name='channel3'/>

<address type='virtio-serial' controller='0' bus='0' port='4'/>

</channel>

3.8.29.6.2. В SpaceVM «qemu-guest-agent» используется для:

– получения сетевых адресов, hostname;

– корректного выключения ВМ вместо посылания ACPI команд;

– «замораживания» файловой системы перед созданием снимка (то есть и при создании резервных копий ВМ);

– ввода/вывода из AD;

– установки hostname;

– добавления SSH ключей;

– любых пользовательских команд и скриптов при необходимости.

Подробности работы «qemu-guest-agent» смотрите в по ссылке *http://wiki.qemu.org/Features/GuestAgent.*

3.8.29.7. Настройка «qemu-guest-agent»

3.8.29.7.1. После установки «qemu» агента создайте административную локальную учетную запись, откройте службы Windows и настройте запуск службы «qemu» агента не от «local system», а от ранее созданной учетной записи. Следует помнить, что при блокировании пароля данной учетной записи, служба гостевого агента не будет работать.

Примечание. Необходимо для автоматического ввода ВМ в AD.

3.8.29.8. Проверка связи SpaceVM с гостевым агентом

3.8.29.8.1. Удостоверьтесь, что связь с «qemu_guest_agent» есть во вкладке «Информация ВМ».

3.8.29.8.2. Также в CLI сервера есть команды работы с гостевым агентом

vm guest_info

3.8.29.9. Установка hostname

3.8.29.9.1. В ВМ во вкладке «ВМ/Шаблон» при активном гостевом агенте можно установить hostname ВМ.

Примечание. Для разных ОС установка hostname происходит по-разному. Для Windows через «powershell» командой *Rename-Computer* с последующей перезагрузкой для принятия изменений. Для Linux командой */usr/bin/hostnamectl* при включенной ВМ. Для Linux утилитой «virtsysprep» с сервера при выключенной ВМ.

3.8.29.10. Windows Sysprep

3.8.29.10.1. Для подготовки шаблона с ОС Windows можно использовать утилиту «Sysprep». Для этого необходимо:

– в ВМ во вкладке «ВМ/Шаблон» при включенной ВМ и активном гостевом агенте нажать кнопку «SysPrep»;

– в открывшемся окне выбрать стандартные опции утилиты «SysPrep» из раскрывающегося списка;

– после настройки нажать кнопку «ОК».

3.8.29.11. Linux Virt-sysprep

3.8.29.11.1. Для подготовки шаблона с ОС Linux можно использовать утилиту «virt-sysprep». Для этого необходимо:

– в ВМ во вкладке «ВМ/Шаблон» при выключенной ВМ нажать кнопку «VirtSysPrep»;

– в открывшемся окне выбрать загрузочный диск и стандартные опции утилиты «virt-sysprep» из раскрывающегося списка;

– после настройки нажать кнопку «ОК».

3.8.29.12. Добавление в AD

3.8.29.12.1. В ВМ во вкладке «ВМ/Шаблон» при активном гостевом агенте можно добавить ВМ в AD, указав:

– hostname (необязательный параметр);

– имя домена;

– логин;

– пароль;

– опция рестарта после применения параметров («по умолчанию» – включено).

Примечание. Не забудьте прописать DNS домена или настройте DHCP.

3.8.29.13. Удаление из AD

3.8.29.13.1. Во вкладке ВМ/Шаблон ВМ при активном гостевом агенте можно убрать ВМ из AD, указав:

– логин;

– пароль.

3.8.29.14. Добавление SSH-ключей

3.8.29.14.1. В SpaceVM реализовано добавление SSH-ключей.

3.8.29.14.2. Условия корректного добавления SSH-ключей в ВМ:

– ОС Linux;

– ВМ выключена или ВМ включена и активен гостевой агент.

3.8.29.14.3. В ВМ во вкладке «ВМ/Шаблон» при активном гостевом можно добавить SSH ключи, указав:

– SSH-пользователя. «По умолчанию» – «root»;

– SSH-ключ.

3.8.29.15. Запуск пользовательских скриптов через гостевой агент

3.8.29.15.1. Условия для запуска пользовательских скриптов через гостевой агент:

– ОС Linux;

– ВМ включена и активен гостевой агент.

3.8.29.16. Изменение шаблона

3.8.29.16.1. Способ изменить шаблон без ручного пересоздания всех клонов – это воспользоваться операцией вливания снимка тонкого клона в шаблон.

Для этого требуется подготовить тонкие клоны с панели SpaceVM, выполнив:

– на всех тонких клонах не должно быть сохраненных состояний. Требуется при необходимости зайти во вкладку «Снимки» и «Удалить все состояния»;

– внести нужные изменение в имеющийся тонкий клон или создать новый тонкий клон и произвести там изменения;

– отключить все включенные тонкие клоны от родительского шаблона;

– для ОС Windows рекомендуется перед вливанием подготовить тонкий клон через Sysprep, если это использовали для шаблона;

– произвести операцию в тонком клоне, который подготовили для вливания в шаблон, нажав во вкладке «ВМ/Шаблон» кнопку «Изменить шаблон» и подтвердив свои намерения в открывшемся окне.

Эти действия внесут изменения из подготовленного тонкого клона в диски шаблона, и от них пересоздадутся диски во всех остальных тонких клонах.

ВНИМАНИЕ! Изменение шаблона напрямую при наличии тонких клонов запрещено, так как это приведет в нерабочее состояние все тонкие клоны.

3.8.29.17. Оптимизатор работы Windows 10/Windows Server 2019 в виртуальной среде

3.8.29.17.1. Для оптимизации работы Windows в виртуальной среде необходимо:

– запустить файл «install-menu» в образе диска «guest-utils»;

– запустить пункт «optimize guest tools»;

– дождаться сообщения «Оптимизация завершена, требуется перезагрузка».

Во время работы могут выдаваться сообщения типа «Отказ в доступе» или ошибки определения экрана. Это штатная ситуация, вызванная архитектурными различиями дистрибутивов.

Некоторые модификации применяются исключительно для новых пользователей, и окружение, созданных ранее до модификации пользователей, не изменяется, чтобы не возникало проблем с изменением окружения.

3.8.30. Cloud-init

3.8.30.1. Общая информация

3.8.30.1.1. Cloud-init – это программа, запускающаяся на ВМ при загрузке, которая ищет данные конфигурации для применения к ВМ во время инициализации.

3.8.30.1.2. Идея состоит в том, чтобы иметь определенный независимый от операционной системы формат конфигурации для параметров, общих для многих систем (таких, как имя хоста и конфигурация сети).

3.8.30.1.3. Подробные примеры командной строки смотрите в документации Cloud-init по ссылке *https://cloudinit.readthedocs.io/en/latest/index.html.*

3.8.30.1.4. Рекомендуется использовать источник NoCloud. Подробное описание смотрите в документации Cloud-init по ссылкам *https://cloudinit.readthedocs.io/en/latest/topics/datasources/nocloud.html* и *https://cloudinit.readthedocs.io/en/latest/topics/datasources.html#datasource-documentation.*

3.8.30.2. Использование в SpaceVM

3.8.30.2.1. При включении Cloud-init для ВМ создается ISO-образ, содержащий два YAML-файла – «user-data» и «meta-data» и монтирующийся через виртуальный CD-ROM (через первый свободный имеющийся или создаваемый новый).

3.8.30.2.2. user-data – строка (может быть закодированной в base64), содержащая в формате «yaml» конфигурацию «user_data».

3.8.30.2.3. meta-data – строка (может быть закодированной в base64), содержащая в формате «yaml» конфигурацию «meta_data».

Примечание. Если «meta_data» не задана пользователем, то «instance-id» и «local-hostname» будут заданы, как ID ВМ.

Пример «meta_data»:

instance-id: 898a905c-e9b8-4ea1-87a3-452497e467b6
local-hostname: ubuntu-guacamole

Пример «meta_data» с настройкой интерфейса «eth0»:

instance-id: 898a905c-e9b8-4ea1-87a3-452497e467b6
local-hostname: ubuntu-guacamole
network-interfaces: |
iface eth0 inet static
address 192.168.1.10
network 192.168.1.0
netmask 255.255.255.0
broadcast 192.168.1.255
gateway 192.168.1.254

3.8.30.2.4. Пример генерации хешированного пароля в Python3:

```
import crypt, getpass
print(crypt.crypt(getpass.getpass()))
```

3.8.30.2.5. Пример кодирования в base64 «meta-data» и «user-data» в Python:

```
 import base64

 user_data  = '''#cloud-config

 groups:
 - ubuntu: [root,sys]
 - cloud-users


 package_update: True
 package_upgrade: False

 packages:
  - docker.io
  - curl
  - openssh-server
  - qemu-guest-agent

 write_files:
  - path: /etc/rancher/rancherd/config.yaml
    permissions: "0444"
    content: |
      role: cluster-init
      token: bazalt

 runcmd:
  - curl -fL https://raw.githubusercontent.com/rancher/rancherd/master/install.sh | sh -

 final_message: "The system is finally up, after $UPTIME seconds"
 '''
 user_data_bytes = user_data.encode('ascii')
```

base64_bytes = base64.b64encode(user_data_bytes)
base64_user_data = base64_bytes.decode('ascii')
print(base64_user_data)

meta_data = '''
instance-id: b73e86d6-6b77-4d14-bcef-a1df736ce87e
local-hostname: somedomain
'''

meta_data_bytes = meta_data.encode('ascii')
base64_bytes = base64.b64encode(meta_data_bytes)
base64_meta_data = base64_bytes.decode('ascii')
print(base64_meta_data)

3.8.30.2.6. Пример «json» параметров запроса создания тонкого клона с cloud_init:

POST http(s)://<адрес контроллера>/api/domains/multi-create-domain/?async=1

{"parent": "bfd282a4-3b1f-4f68-98cb-16deee43a3b8", # id шаблона ВМ
"start_on": true, # Включить тонкий клон после создания
"thin": true, # Параметр, что создается тонкий клон
"cloud_init": true, # Включение подготовки образа с cloud_init
"cloud_init_config": {
"user_data": "I2Nsb3VkLWNvbmZpZwoKZ3JvdXBzOgotIHVidW50dTogW3Jvb3Qsc3lzXQotIGNsb3VkLXVzZXJzCgpwYWNrYWdlX3VwZGF0ZTogVHJ1ZQpwYWNrYWdlX3VwZ3JhZGU6IEZhbHNlCgpwYWNrYWdlczoKICAtIGRvY2tlci5pbwogIC0gY3VybAogIC0gb3BlbnNzaC1zZXJ2ZXIKICAtIHFlbXUtZ3Vlc3QtYWdlbnQKCndyaXRlX2ZpbGVzOgogIC0gcGF0aDogL2V0Yy9yYW5jaGVyL3JhbmNoZXJkL2NvbmZpZy55YW1sCiAgICBwZXJtaXNzaW9uczogJzA0NDQiCiAgICBjb250ZW50OiB8CiAgICAgIHJvbGU6IGNsdXN0ZXIta2V5pdAogICAgICB0b2tlbjogYmF6YWx0CgpydW5jbWQ6CiAtIGN1cmwgLWZMIGh0dHBzOi8vcmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbS9yYW5jaGVyL3JhbmNoZXJkL21hc3RlciI9pbnN0YWxsLnNoIHwgc2ggLQoKZmluYWxfbWVzc2FnZTogIlRoZSBzeXN0ZW0gaXMgZmluYWxseSB1cCwgYWZ0ZXIgJFVQVElNRSBzZWNvbmRzIiAgIAo",
"meta_data": "Cmluc3RhbmNlLWlkOiBiNzNlODZkNi02Yjc3LTRkMTQtYmNlZi1hMWRmNzM2Y2U4N2UKbG9jYWwtaG9zdG5hbWU6IHNvbWVkb21haW4KCg=="

}

}

3.8.30.2.7. Пример создания SSH-ключей через «ssh-keygen»:

[user@host ~]$ ssh-keygen -t rsa -b 4096

Generating public/private rsa key pair.

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in .ssh/key-with-password.

Your public key has been saved in .ssh/key-with-password.pub.

The key fingerprint is:

SHA256:s7GGB7EyHUry4aOcNPKmhNKS7dl1YsMVLvFZJ77VxAo user@host.lab.example.com

The key's randomart image is:

```
+---[RSA 2048]----+
|    . + =.o ...  |
|     = B XEo o.  |
|  . o O X =....  |
| = = = B = o.    |
|= + * * S .      |
|.+ = o + .       |
|  + .            |
|                 |
|                 |
+----[SHA256]-----+
```

«По умолчанию» ключи будут сохранены в «~/.ssh/id_rsa» и «~/.ssh/id_rsa.pub» соответственно.

3.8.30.2.8. Для создания «cloud» образа необходимо выполнить команду

genisoimage -output seed.iso -volid cidata -joliet -rock user-data meta-data

3.8.30.3. Подготовка ВМ

3.8.30.3.1. Для подготовки ВМ необходимо выполнить следующие действия:

1) установить нужную ОС. Это может быть любая ОС, на которую можно поставить пакет Cloud-init. Желательно ставить наиболее свежую версию Cloud-init;

2) загрузить в пул данных нужный «cloud» образ;

3) импортировать этот файл в виртуальный диск;

4) расширить размер виртуального диска до нужной величины;

5) создать ВМ, добавить к ней этот диск, сетевой интерфейс, две консоли (необходимы для Cloud_init);

6) перевести ВМ в шаблон;

7) создать первый тонкий клон, который будет мастером кластера, используя приведенный ниже конфигурационный файл «cloud»:

```
#cloud-config
groups:
- cloud-users

package_update: False
package_upgrade: False

users:
  - default
  - name: user
    groups: sudo
    sudo: ALL=(ALL) NOPASSWD:ALL
    shell: /bin/bash
    lock_passwd: false
    # пароль user для пользователя user
    passwd:
$6$rounds=4096$9cYh.jYsend9bOZ$VBqFtH6Jc6cgpYga.sWD.G5l/h.Fedn.CRO7ouw7S7
JiMbwXvf5cuENpOk9W4pqAAmF7vxKJy62QCHZ9xVvAd0
    # сгенерируйте свой ключ
    ssh_authorized_keys:
```

```
      - ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCWRyWsZAFDAiUuCPAz0cN1jFREnnBdLkpI
oQygLJqkrzh85l47Omib+IlryIaa7QsjaKhI2dYUfviTiOeUM0yLH17YD7IR+8n2uADy3kNHbj
wDn3+9OOfCGExLXH6Az1imenWJj6ErLmeITJi66xLWcGQhBNtr37XwOlL8eguP4TwZ1L
moUqWseKXEerUoOKqP2abYu5zgWNtkWJ5604V8lvQt5JgMJMqr7oGCIT/DgD/ndqOOu
0G6698deEk/ooADVB1CUglrPni+ZPBHhwwMrovpkKgwbOTUXrmE5I9OrmsjLGiaLkjsSyQ
rfx5xfrXhogbCE174PWJaCy8zD7HLGArmhsBnMz8FKEbX/We547llCKGPGmc4H6IMhbryi
Zky3XuGK3nBKvmOiwwKUNoamt7yXUIRfFcoOqhC63DZfHT/4OvfvKnv3HtnY2VoDgZCa
YCcT6ZZwntk2p6LY2zoDwqThXLtvZwouPkhtdOs2ATvW04CMnXCKBsu2W76c60=
user@user-To-be-filled-by-O-E-M

    manage_resolv_conf: false
    manage_etc_hosts: false

    # qemu-guest-agent нужен для интеграции ВМ с гипервизором
    # curl, openssl нужен для загрузки и установки rancherd
    # openssh-server нужен для подключения по ssh
    packages:
      - qemu-guest-agent
      - openssl
      - curl
      - openssh-server

    # Конфигурация rancherd
    write_files:
      - path: /etc/rancher/rancherd/config.yaml
        permissions: "0444"
        content: |
          kubernetesVersion: v1.21
          rancherVersion: stable
          rancherValues:
            # сгенерируйте свой пароль
            bootstrapPassword: veil
          role: cluster-init
```

token: random
 # Disable Selinux
- path: /etc/sysconfig/selinux
encoding: b64
permissions: "0644"
owner: root:root
content:
ClNFTElOVVg9ZGlzYWJsZWQKU0VMSU5VWFRZUEU9dGFyZ2V0ZWQK

runcmd:
 # Принудительное отключение Selinux сразу
- setenforce 0
 # Старт гостевого агента
- systemctl start qemu-guest-agent
 # Скачивание и запуск rancherd
- curl -fL https://raw.githubusercontent.com/rancher/rancherd/master/install.sh | sh -

8) дождаться завершения активации мастера кластера. Проверить, что «Rancher» доступен для управления по адресу *https://{адрес ВМ}:8443* и там появился первый узел;

9) создать необходимое количество тонких клонов, которые будут нодами кластера, используя приведенный ниже конфигурационный файл «cloud»:

#cloud-config

groups:
- cloud-users

package_update: False
package_upgrade: False

users:
- default
- name: user
groups: sudo

```
    sudo: ALL=(ALL) NOPASSWD:ALL
    shell: /bin/bash
    lock_passwd: false
    passwd:
$6$rounds=4096$9cYh.jYsend9bOZ$VBqFtH6Jc6cgpYga.sWD.G5l/h.Fedn.CRO7ouw7S7
JiMbwXvf5cuENpOk9W4pqAAmF7vxKJy62QCHZ9xVvAd0
    ssh_authorized_keys:
      - ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCWRyWsZAFDAiUuCPAz0cN1jFREnnBdLkpI
oQygLJqkrzh85l47Omib+IlryIaa7QsjaKhI2dYUfviTiOeUM0yLH17YD7IR+8n2uADy3kNHbj
wDn3+9OOfCGExLXH6Az1imenWJj6ErLmeITJi66xLWcGQhBNtr37XwOlL8eguP4TwZ1L
moUqWseKXEerUoOKqP2abYu5zgWNtkWJ5604V8lvQt5JgMJMqr7oGCIT/DgD/ndqOOu
0G6698deEk/ooADVB1CUglrPni+ZPBHhwwMrovpkKgwbOTUXrmE5I9OrmsjLGiaLkjsSyQ
rfx5xfrXhogbCE174PWJaCy8zD7HLGArmhsBnMz8FKEbX/We547llCKGPGmc4H6IMhbryi
Zky3XuGK3nBKvmOiwwKUNoamt7yXUIRfFcoOqhC63DZfHT/4OvfvKnv3HtnY2VoDgZCa
YCcT6ZZwntk2p6LY2zoDwqThXLtvZwouPkhtdOs2ATvW04CMnXCKBsu2W76c60=
user@user-To-be-filled-by-O-E-M

  manage_resolv_conf: false
  manage_etc_hosts: false

  packages:
    - qemu-guest-agent
    - curl
    - openssh-server

  write_files:
    - path: /etc/rancher/rancherd/config.yaml
      permissions: "0444"
      content: |
        kubernetesVersion: v1.21
        rancherVersion: stable
        role: server
        server: https://{адрес мастера}:8443
```

token: random

runcmd:
 # Принудительное отключение Selinux сразу
- setenforce 0
 # Старт гостевого агента
- systemctl start qemu-guest-agent

 # запуск rancherd
- curl -fL https://raw.githubusercontent.com/rancher/rancherd/master/install.sh | sh -

Примечание. Не забудьте указать адрес мастера (первой ВМ) в конфигурации «Rancherd»;

10) дождаться завершения активации узлов кластера. Проверить, что они доступны в интерфейсе управления «Rancher».

3.8.31. Анализ крахов ВМ

3.8.31.1. Для анализа крахов ВМ необходимо выполнить следующие действия:

– установить «gdb» с помощью команды CLI

install gdb

– установить «qemu-system-x86-dbgsym» с помощью команды CLI

install qemu-system-x86-dbgsym

– в файле «/etc/libvirt/qemu.conf» раскомментировать строку «max_core = "unlimited"». Она перезаписывается при обновлении;

– рестартовать сервис «libvirtd».

3.8.31.2. Файлы дампов крахов ВМ будут складироваться в «/var/log/crash/», автоматически ротироваться и сжиматься.

Анализировать дампы крахов ВМ можно через «gdb», например,

gdb /usr/bin/qemu-system-x86_64 /var/log/crash/qemu-system-x86_1640520577.dmp

Полученную информацию рекомендуется выслать вендору.

Пример команд CLI:

node nodes_cli 'install gdb'

node nodes_cli 'install qemu-system-x86-dbgsym'

node nodes_cli 'system libvirt_set_unlimited'

3.9. Хранилища

3.9.1. Общая информация

3.9.1.1. Хранилища предназначены для размещения виртуальных дисков ВМ, их резервных копий и шаблонов, выделение разделов дисков для подключения в виртуальные машины (с помощью LVM), загрузку образов CD/DVD и других файлов. Управление хранением файлов и разделами дисков производится в интерфейсе управления SpaceVM в разделе «Хранилища» – «Пулы данных» основного меню.

3.9.1.2. В SpaceVM предусмотрено 10 типов объектов управления хранилищами:

– пулы данных;

– диски;

– образы ISO;

– файлы;

– блочные устройства LUNs;

– ZFS-пулы;

– сетевые хранилища (файловые и блочные);

– кластерные хранилища (кластерные транспорты и тома);

– ISCSI-сервер (ISCSI-storage и ISCSI-target).

3.9.1.3. Для управления хранилищами необходимо перейти в раздел «Хранилища» основного меню и выбрать тот тип хранилища, которым собираетесь управлять.

3.9.2. Типы пулов данных

3.9.2.1. Пулы данных – это объекты уровня подключения хранилища к физическому серверу.

3.9.2.2. В таблице 1 приведены типы пулов данных.

Таблица 1

Название	Тип	Документация	Поддержка тонких клонов	Особенности	Ограничения
local	файловый, локальный	Локальные пулы (см. примечание)	+	размер блока 512 байт	доступность на 1 узле
zfs	файловый, локальный/сетевой	ZFS-пулы (3.9.8)	+	снимки памяти zfs, размер блока 8192 байт	доступность на 1 узле
nfs	файловый, сетевой	Файловые хранилища (3.9.9.1)	+	-	-
gluster	файловый, распределенный (гиперконвергентный)	Кластер-ные транспорты (3.9.11.1)	+	-	минимум 2 сервера
gfs2	файловый, сетевой	Кластер-ные транспорты (3.9.11.1)	+	-	минимум 2 сервера, крайне желательно наличие IPMI у каждого сервера перед созданием
glusterfs	файловый, сетевой	Файловые хранилища (3.9.9.1)	+	-	-
cifs	файловый, сетевой	Файловые хранилища (3.9.9.1)	+	-	-
ocfs2 (deprecated)	файловый, сетевой	Кластерные транспорты (3.9.11.1)	+	-	минимум 2 сервера

Название	Тип	Документация	Поддержка тонких клонов	Особенности	Ограничения
lvm	блочный, локальный	LVM-пулы данных (3.9.3.2)	-	-	нельзя хранить образы и файлы, а также делать снимки ВМ (то есть создавать тонкие клоны)
thinlvm	блочный, локальный	LVM-пулы данных (3.9.3.2)	-	-	нельзя хранить образы и файлы, а также делать снимки ВМ (то есть создавать тонкие клоны)
lvm_shared	блочный, сетевой	LVM-пулы данных (3.9.3.2)	-	-	нельзя хранить образы и файлы, а также делать снимки ВМ (то есть создавать тонкие клоны)

Название	Тип	Документация	Поддержка тонких клонов	Особенности	Ограничения
outside	файловый, сетевой	Внешние пулы данных (3.9.4)	-	только на чтение, создается поверх nfs, cifs, glusterfs сетевого хранилища	нельзя ничего создавать
Примечание. Локальные хранилища с типом пула «local» привязаны к конкретному серверу и размещаются на его ресурсах. При подключении сервера в кластер на нем создается файловое хранилище, размещаемое в корневой файловой системе «/storages/local».					

3.9.2.3. Ниже приведены примеры выбора типа пулов данных под инфраструктуру:

– один и более серверов, локальные диски/iSCSI(FC) LUNs, общий пул не нужен – ZFS;

– один и более серверов, сетевые файловые хранилища – NFS;

– два и более серверов, локальные диски/iSCSI(FC) LUNs, нужен общий пул – Gluster;

– два и более серверов, iSCSI(FC) LUNs, нужен общий пул – gfs2;

– один и более серверов, много iSCSI(FC) LUNs, общий пул не нужен, но нужна живая миграция – выдать LUN напрямую ВМ;

– VDI, только файловые пулы.

3.9.2.4. Структура пулов данных типа «файловый» следующая:

– метафайл с информацией о пуле

[Абсолютный путь к пулу]/datapool-[id пула].meta

– каталог для «heartbeat» файлов, создаваемых каждым узлом, на котором есть этот пул

[Абсолютный путь к пулу]/_HEARTBEAT/

– каталог для образов

[Абсолютный путь к пулу]/_LIBRARY/

– каталог для образов

[Абсолютный путь к пулу]/_ISO/

– виртуальные диски и снимки лежат в корне абсолютного пути пула. Для виртуальных дисков рядом с ними создаются метафайлы с информацией о дисках.

Примечание. У пула данных типа ZFS виртуальные диски лежат в подкаталогах, являющихся одновременно ZFS dataset.

3.9.3. Пулы данных

3.9.3.1. Локальные файловые хранилища

3.9.3.1.1. В разделе «Хранилища» – «Пулы данных» основного меню доступны следующие операции с пулами:

1) обновление информации о пулах по кнопке  ;

2) создание пула. Для этого необходимо нажать кнопку «Создать» и в открывшемся окне заполнить следующие поля:

– название пула данных;

– тип регистрируемого локального хранилища (выбор из раскрывающегося списка). Может принимать значения «local», «lvm», «thinlvm» или «zfs». Остальные типы из списка являются пулами сетевого размещения;

– параметры в зависимости от выбранного типа хранилища;

– описание данного хранилища, если требуется.

Для подтверждения операции необходимо нажать кнопку «ОК».

После регистрации хранилище появится в списке;

3) поиск пула с применением фильтра. Для этого необходимо нажать кнопку «Фильтр» и в открывшемся окне заполнить поля для фильтрации:

– «Имя пула» – название искомого пула;

– «Серверы» – выбор из раскрывающегося списка;

– «Кластеры» – выбор из раскрывающегося списка;

– «Локации» – выбор из раскрывающегося списка;

– «Пулы ресурсов» – выбор из раскрывающегося списка;

– «Файловые хранилища» – выбор из раскрывающегося списка;

– «Кластерные хранилища» – выбор из раскрывающегося списка;

– «Разделы (ZFS пулы)» – выбор из раскрывающегося списка;

– «Статус» – выбор из раскрывающегося списка («Без фильтра», «Исправно», «Нет соединения» или «Произошла ошибка»);

– «Тип пула» – выбор из раскрывающегося списка;

– «Теги» – выбор из раскрывающегося списка.

После настройки фильтра необходимо нажать «Применить» или «Сбросить все».

3.9.3.1.2. В пуле можно размещать виртуальные диски, образы ISO и другие файлы, если это возможно.

Примечание. Для блочных пулов (LVM) действует ограничение на размещение образов ISO и файлов, так как преобразование их в логический диск неэффективно.

3.9.3.1.3. Переход в окно состояния хранилища происходит с помощью нажатия на его названии. В окне параметров пула доступны следующие операции:

– обновление информации по кнопке  ;

– извлечение пула. При нажатии кнопки «Извлечь» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «ОК»;

– очистка пула. При нажатии кнопки «Очистить» в открывшемся окне следует определить необходимость принудительной очистки, после чего подтвердить операцию, нажав кнопку «ОК»;

– удаление пула (допускается, если пул не является базовым). При нажатии кнопки «Удалить» необходимо подтвердить операцию, нажав на кнопку «Удалить»;

– сканирование пула. При нажатии кнопки «Сканировать» произойдет сканирование дисков, файлов и образов.

ВНИМАНИЕ! Если пул данных перешел в статус FAILED, то удаление будет произведено форсировано, то есть из базы.

3.9.3.1.4. Информация о пуле данных разделена на группы:

– «Информация»;

– «Диски»;

– «Образы»;

– «Файлы»;

– «События»;

– «Теги».

3.9.3.1.5. В окне «Хранилища» – «Пулы данных» – <имя пула данных> – «Информация» содержатся следующие сведения о пуле данных:

– название (редактируемый параметр);

– описание (редактируемый параметр);

– тип хранилища;

– абсолютный путь расположения в файловой системе сервера;

– объем дискового пространства (всего, занято, свободно);

– приоритет;

– серверы размещения пула данных (раскрывающийся список). Список для локальных хранилищ содержит только одну запись. Для пула данных, зарегистрированного на сетевом хранилище, данный пункт будет содержать список серверов, к которым подключено сетевое хранилище;

– статус;

– дата и время создания;

– дата и время обновления данных.

3.9.3.1.6. В окне «Хранилища» – «Пулы данных» – <имя пула данных> –«Диски» отображены все виртуальные диски, расположенные в данном пуле данных, включая для каждого из них его название, подключение к ВМ, размер и статус. Также в окне управления дисками доступны следующие операции:

1) обновление информации;

2) создание нового диска. При нажатии кнопки «Создать» в открывшемся окне необходимо заполнить название, описание и размер виртуального диска, включить (выключить) предварительное выделение места, после чего подтвердить операцию, нажав кнопку «ОК»;

3) сканирование пула. Выполняется нажатием кнопки «Сканировать». Система сканирования регистрирует новые диски только в том случае, если структура их наименования совпадает с принятой в системе управления SpaceVM. Если виртуальный диск, загружаемый в пул данных имеет имя, отличное от принятого формата, то рекомендуется перейти во вкладку «Файлы» окна управления пулом данных.

Для получения информации о диске необходимо нажать на название диска. Подробное описание приведено в 3.9.5 данного руководства.

3.9.3.1.7. В окне «Хранилища» – «Пулы данных» – <имя пула данных> – «Образы» отображены все образы ISO, расположенные в данном пуле данных. Также в окне управления образами доступны следующие операции:

1) обновление информации;

2) загрузка образа из файловой системы. При нажатии кнопки «Загрузить образ из файловой системы» открывается стандартное окно загрузки файлов, где необходимо открыть папку (директорию) хранения образов CD/DVD-дисков, выбрать нужный образ и нажать кнопку «Открыть»;

3) загрузка образа по url. При нажатии кнопки «Загрузить по url» в открывшемся окне необходимо заполнить URL-адрес (ввести местонахождение образа диска по ссылке), после чего подтвердить операцию, нажав кнопку «Отправить»;

4) сканирование списка образов ISO. Сканирование пула данных на наличие неуказанных в списке образов выполняется нажатием кнопки «Сканировать»;

5) поиск образа с применением фильтра. При нажатии на «Фильтр» в открывшемся окне необходимо заполнить следующие поля для фильтрации:

– «Имя образа» – название искомого образа;

– «Пул данных» – выбор из раскрывающегося списка;

– «ВМ» – выбор из раскрывающегося списка.

После настройки фильтра необходимо нажать «Применить» или «Сбросить все».

Для получения информации об образе необходимо нажать на название диска. Подробное описание приведено в 3.9.6 данного руководства.

3.9.3.1.8. В окне «Хранилища» – «Пулы данных» – <имя пула данных> – «Файлы» отображены все файлы, расположенные в данном хранилище. Также в окне управления файлами доступны следующие операции:

1) обновление информации;

2) загрузка файла из файловой системы.

При нажатии кнопки «Загрузить из файловой системы» открывается стандартное окно загрузки файлов, где необходимо открыть папку (директорию) хранения файлов, выбрать нужный файл и нажать кнопку «Открыть». Допустимые форматы файлов приведены в приложении 2 данного руководства;

3) загрузка файла по URL. При нажатии кнопки «Загрузить по url» в открывшемся окне необходимо заполнить URL-адрес (ввести местонахождение образа диска по ссылке), после чего подтвердить операцию, нажав кнопку «ОК»;

4) сканирование. Выполняется нажатием кнопки «Сканировать».

Все операции с файлами аналогичны операциям с образами ISO – скопировать, скачать, удалить или перенести в другой пул данных. Для файлов формата «vmdk», «qcow2», «qcow», «raw», «img», «bin» (форматы дисков) будет доступна кнопка импорта или конвертации.

Для получения информации о файле необходимо нажать на название файла. Подробное описание приведено в 3.9.7 данного руководства.

3.9.3.1.9. В окне «Хранилища» – «Пулы данных» – <имя пула данных> – «События» отображаются зарегистрированные в системе события, связанные с работой выбранного хранилища, с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.9.3.1.10. В окне «Хранилища» – «Пулы данных» – <имя пула данных> –«Теги» имеется возможность добавления к хранилищу отличительной метки (тега), применения и обновления тега.

Для применения нового тега необходимо нажать кнопку «Применить» и в открывшемся окне выбрать тег. Для сохранения изменений необходимо нажать кнопку «ОК».

3.9.3.2. LVM-пулы данных

3.9.3.2.1. Для локальных пулов данных типа LVM, thin-LVM и LVM-shared не предусмотрена возможность размещения ISO-образов и монтирование в файловую систему сервера. В этом случае физический накопитель сервера (раздел, диск или RAID-массив) используется как блочное устройство, и создаваемые в нем логические диски подключаются к ВМ напрямую. Это позволяет предоставить ВМ диски с высокой производительностью, но уменьшает ее гибкость и мобильность. Для такой ВМ перенос на другой сервер кластера возможен только после конвертации ее дисков в файл формата «qcow2» с последующим копированием в целевое хранилище.

3.9.3.2.2. Отличие типа thin-LVM от обычного типа LVM в том, что обычный размещает логические разделы классическим способом, а thin-LVM (тонкий) заполняет пространство диска по факту записи информации. Такая методика позволяет «выделить» дискового пространства больше, чем есть, но опасна возможностью переполнения дискового пространства.

3.9.3.2.3. LVM-shared предназначен для использования блочного устройства LUN, представленного серверу по протоколу iSCSI или FC. В этом случае LUN размечается как локальное LVM-хранилище и переходит в монопольное использование одним из серверов. Предоставление монопольного доступа осуществляется по первому обращению к хранилищу. Остальные серверы сохраняют доступ к хранилищу, но при попытке обращения будут ждать своей очереди. Не рекомендуется подключать LVM-shared на нескольких серверах одновременно, так как при опросе состояния хранилища другим сервером все ВМ на основном сервере «замрут». В соответствии с этим ограничением для LVM-shared является невозможным живая миграция ВМ. При этом выключенная ВМ мигрирует без проблем. Таким образом, LVM-shared можно использовать как локальное хранилище сетевого размещения.

3.9.3.2.4. Для восстановления группы томов после сбоев используются следующие команды:

– список копий метаданных до выполнения команд можно увидеть с помощью просмотра содержимого каталога «/etc/lvm/archive»;

– список копий метаданных после выполнения команд можно увидеть с помощью просмотра содержимого каталога «/etc/lvm/backup» командой

vgcfgrestore --list [VG_name]

– восстановление метаданных возможно также через команду

vgcfgrestore -f /etc/lvm/archive/appvg_00_00000-123456.vg appvg

Примечание. Восстанавливаются только метаданные групп томов. Если данные уже были удалены с диска, то необходимо использовать другие методы.

3.9.3.3. Регистрация пулов данных для сетевых хранилищ

3.9.3.3.1. Для регистрации пула данных, размещаемых на сетевых хранилищах (NFS, блочные хранилища), необходимо предварительно зарегистрировать общее (сетевое) хранилище в разделе «Хранилища»–«Сетевые хранилища» основного меню. После регистрации сетевого хранилища необходимо указать серверы кластера SpaceVM, к которым оно будет подключено. Для NFS-пула регистрируется NFS-хранилище в разделе «Хранилища»–«Сетевые хранилища»–«Файловые» основного меню, а для iSCSI и FC в «Хранилища»–«Сетевые хранилища»–«Блочные».

Подробное описание сетевых хранилищ приведено в 3.9.9 данного руководства.

3.9.4. Внешние пулы данных

3.9.4.1. Внешние пулы данных («outside») не создают новые данные и не изменяют файловые системы. Их предназначение – просмотр и копирование данных со сторонних ресурсов. Для этого используются сетевые файловые хранилища, желательно их подключать в режиме «только на чтение», чтобы не иметь возможности повлиять на целостность внешних данных.

3.9.4.2. При создании пула данных на сетевом файловом хранилище не создаются дополнительные директории и файлы, даже если сетевая файловая система подключена в режиме «записи», так как пул не подразумевает каких-либо изменений на ней. По этой причине в основном окне такого пула нет кнопок «Очистить» и «Удалить» и на боковой панели нет вкладок «Диски», «Образы» и «Файлы». Но здесь присутствуют в основном окне кнопка «Сканировать», а на боковой панели вкладка «Структура». После нажатия кнопки «Сканировать» во вкладке «Структура» отображается древовидная файловая структура с директориями и файлами, включая ISO-образы.

3.9.4.3. У файлов во вкладке «Структура» при открытии отсутствует кнопка «Удалить» и при нажатии «Копировать» отсутствует выбор пула данных этого типа. У образов дисков при операции «Импортировать», а также у файлов из которых можно восстановить ВМ и где предлагается выбор пула данных, также отсутствует возможность выбрать этот тип пула данных.

3.9.4.4. Путь до внешнего пула данных совпадает с путем до подключенного файлового сетевого хранилища. По этой причине у хранилища, используемого внешний пул данных «outside», не может быть других пулов данных.

3.9.5. Диски

3.9.5.1. Диски – основные средства хранения данных ВМ. Но при этом – это самостоятельный объект кластера.

Примечание. Серийный номер диска, который увидит ВМ, является первыми 20 символами ID диска из базы данных контроллера.

3.9.5.2. Создание нового, несвязанного виртуального диска, описано в 3.8.1.2 (шаг 2) данного руководства. Создание связанного с ВМ диска происходит на этапе создания самой ВМ и полностью повторяет ранее описанный процесс.

3.9.5.3. Привязка диска к ВМ производится в интерфейсе управления ВМ и описана в 3.8.1.2 данного руководства.

3.9.5.4. В разделе «Хранилища» – «Диски» содержится общий список виртуальных дисков, подключенных к пулам данных, включая для каждого из них его название, пул данных, подключение к ВМ, размер и статус. В данном окне имеется возможность обновления информации о дисках по кнопке  .

3.9.5.5. Для перехода в окно состояния диска необходимо нажать на его название, и в открывшемся окне будут отображаться кнопки управления и информация о диске.

3.9.5.6. Управление диском допускает следующие операции:

1) обновление информации по кнопке  ;

2) копирование.

При нажатии кнопки «Копировать» в открывшемся окне «Копирование диска» необходимо выбрать из раскрывающегося списка пул данных, заполнить название и описание нового диска, после чего подтвердить операцию, нажав кнопку «Копировать»;

3) перенос диска. При нажатии кнопки «Перенос диска» в открывшемся окне необходимо выбрать из раскрывающегося списка пул данных или LUNs для переноса, после чего подтвердить операцию, нажав кнопку «Перенести»;

4) отключение диска (для подключенных к ВМ). При нажатии кнопки «Отключить» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «Да». При отключении диска не происходит удаления диска с хранилища (из пула данных), и его можно будет использовать повторно;

5) скачивание. Выполняется автоматически при нажатии кнопки «Скачать»;

6) проверка. Проверить диск (с возможностью починки) можно с помощью кнопки «Проверка диска». Операция доступна только для дисков, находящихся на файловых пулах данных;

7) разрежение. Разрежение (уменьшение размера диска) возможно с помощью кнопки «Разрежение». Операция доступна только для дисков, находящихся на файловых пулах данных. Если диск примонтирован к ВМ, то она должна быть выключена.

Разрежение может сделать диск виртуальной машины (или любой образ диска) разреженным, то есть тонким. Это означает, что свободное пространство в диске может быть преобразовано обратно в свободное пространство на узле.

Операция «Разрежение» может находить и разрежать свободное пространство в большинстве файловых систем (например, ext2/3/4, btrfs, NTFS и прочее), а также в физических томах LVM.

8) настройки параметров ввода (вывода). При нажатии кнопки «Настройка I/O» в открывшемся окне необходимо заполнить параметры, приведенные в таблице 2.

Таблица 2

Параметр	Описание
total_bytes_sec	Общий предел пропускной способности в байтах в секунду. Не может использоваться с read_bytes_sec или write_bytes_sec
read_bytes_sec	Предел пропускной способности чтения в байтах в секунду
write_bytes_sec	Предел пропускной способности записи в байтах в секунду
total_iops_sec	Общее количество операций ввода-вывода в секунду. Не может использоваться с read_iops_sec или write_iops_sec
read_iops_sec	Количество операций чтения в секунду

Параметр	Описание
write_iops_sec	Количество операций записи в секунду
total_bytes_sec_max	Общий предел пропускной способности в период высокой загрузки в байтах в секунду. Не может использоваться с read_bytes_sec_max или write_bytes_sec_max
read_bytes_sec_max	Предел пропускной способности чтения в период высокой загрузки в байтах в секунду
write_bytes_sec_max	Предел пропускной способности записи в период высокой загрузки в байтах в секунду
total_iops_sec_max	Общее количество операций ввода-вывода в период высокой загрузки в секунду. Не может использоваться с read_iops_sec_max или write_iops_sec_max
read_iops_sec_max	Количество операций чтения в период высокой загрузки в секунду
write_iops_sec_max	Количество операций записи в период высокой загрузки в секунду
size_iops_sec	Размер операций ввода-вывода в секунду
total_bytes_sec_max_length	Продолжительность в секундах для периода высокой загрузки total_bytes_sec_max. Действителен только при установленном параметре total_bytes_sec_max
read_bytes_sec_max_length	Продолжительность в секундах для периода высокой загрузки read_bytes_sec_max. Действителен только при установленном параметре read_bytes_sec_max
write_bytes_sec_max	Продолжительность в секундах для периода высокой загрузки write_bytes_sec_max. Действителен только при установленном параметре write_bytes_sec_max
total_iops_sec_max_length	Продолжительность в секундах для периода высокой загрузки total_iops_sec_max. Действителен только при установленном параметре total_iops_sec_max
read_iops_sec_max_length	Продолжительность в секундах для периода высокой загрузки read_iops_sec_max. Действителен только при установленном параметре read_iops_sec_max

Параметр	Описание
write_iops_sec_max	Продолжительность в секундах для периода высокой загрузки write_iops_sec_max. Действителен только при установленном параметре write_iops_sec_max.

Для сохранения изменений необходимо в нижней строчке окна нажать кнопку «ОК»;

9) конвертирование. Конвертирование виртуального диска в форматы «vmdk» (ESXI), «vhd» (HyperV), «vdi» (VirtualBox) можно в окне информации с помощью кнопки «Конвертировать» в верхней части этого окна;

10) удаление. При нажатии кнопки «Удалить» необходимо в открывшемся окне в дополнительных настройках определиться с гарантированным удалением диска, после чего подтвердить операцию, нажав кнопку «Удалить». Удаление диска по кнопке «Удалить» не только отключит его от ВМ, но и удалит файл диска. Удалить диск можно также во время удаления ВМ.

3.9.5.7. Информация о диске содержит:

– виджет используемого места с возможностью обновления;

– название (редактируемый параметр);

– описание диска (редактируемый параметр);

– привязка к ВМ, к которой подключен диск;

– пул данных;

– объем диска (редактируемый параметр) с возможностью его увеличения по кнопке  ;

– расположение;

– тип шины;

– SSD эмуляция;

– тип кэширования;

– опции I/O;

– тип драйвера;

– устройство dev;

– доступность только чтения ВМ (вкл/выкл) (редактируемый параметр);

– режим мульти использования диска несколькими ВМ;

– дата и время создания;

– дата и время изменения;

– сообщения о работе виртуального диска с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.9.5.8. Размер виртуального диска можно увеличить по кнопке  . Если диск уже привязан к ВМ, и она включена, то после расширения надо использовать средства управления дисками внутри ВМ для использования нового места на устройстве.

Примечание. Рекомендуется использовать шину диска «virtio» совместно с установленными драйверами в ВМ.

3.9.5.9. Для использования диска несколькими ВМ необходимо, чтобы диск находился в блочных пулах данных (LVM, thin-LVM, LVM_shared). При добавлении диска необходимо в окне состояния диска включить опцию «Режим мульти использования диска несколькими ВМ». Кластерная файловая система с блокировками обеспечивается ПО внутри ВМ (например, в Windows Server 2019).

3.9.6. Образы ISO

3.9.6.1. ISO-образы CD/DVD предназначены для установки ОС и ПО на виртуальные машины. Подключение образов к ВМ осуществляется в окне управления ВМ.

3.9.6.2. Создание (загрузка) нового ISO-образа CD/DVD-диска описано в 3.9.3 «Пулы данных».

3.9.6.3. Привязка ISO-образа к ВМ производится в интерфейсе управления ВМ и описана в 3.8.1 «Создание ВМ».

3.9.6.4. В разделе «Хранилища» – «Образы ISO» содержится общий список образов, подключенных к пулам данных, включая для каждого из них его название, пул данных, подключения к ВМ (к какому количеству ВМ подключен образ ISO), размер и статус. В данном окне имеется возможность обновления информации об образах по кнопке  .

3.9.6.5. Для перехода в окно состояния образа необходимо нажать на его название, и в открывшемся окне будут отображаться кнопки управления и информация об образе.

3.9.6.6. В окне состояния образа доступны следующие операции:

– обновление информации по кнопке  ;

– копирование в другой пул данных. При нажатии кнопки «Копировать» в открывшемся окне необходимо выбрать из раскрывающегося списка пул данных и нажать кнопку «Копировать»;

– перенос образа в другой пул данных. При нажатии кнопки «Перенести» в открывшемся окне необходимо выбрать из раскрывающегося списка пул данных и нажать кнопку «Перенести»;

– скачивание. Выполняется автоматически при нажатии кнопки «Скачать»;

– удаление. При нажатии кнопки «Удалить» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «Удалить».

3.9.6.7. Также в окне состояния образа содержится следующая информация:

– название образа;

– его описание;

– список ВМ, к которым подключен образ, с возможностью его отключения от всех ВМ по кнопке  ;

– пул данных;

– размер;

– дата и время создания;

– дата и время изменения;

– сообщения о работе образа с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.9.7. Файлы

3.9.7.1. В разделе «Хранилища» – «Файлы» содержится общий список файлов, включая для каждого из них его название, пул данных, тип, размер и статус. В данном окне имеется возможность обновления информации о файлах по кнопке  , загрузки файла из файловой системы и поиска файла с применением фильтра.

3.9.7.2. Для загрузки файла из файловой системы необходимо нажать кнопку «Загрузить из файловой системы» и в открывшемся окне (стандартное окно загрузки файлов) выбрать файл и пул для размещения из раскрывающегося списка.

3.9.7.3. Для загрузки файла по URL необходимо нажать кнопку «Загрузить по url» и в открывшемся окне выбрать место нахождения файла и пул для размещения из раскрывающегося списка.

3.9.7.4. Для группы файлов (в случае выделения некоторых файлов в списке) становятся доступны следующие групповые операции:

– копирование;

– перенос;

– удаление.

3.9.7.5. Для перехода в окно состояния файла необходимо нажать на его название, и в открывшемся окне будут отображаться кнопки управления и информация о файле.

3.9.7.6. В окне состояния файла содержится следующая информация:

– название (редактируемый параметр);

– расположение;

– пул данных;

– размер файла;

– описание (редактируемый параметр);

– хеш-сумма файла;

– дата и время создания;

– дата и время изменения;

– сообщения об операциях с файлом с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.9.7.7. Также в окне состояния файла доступны следующие операции:

– обновление информации по кнопке  ;

– копирование. При нажатии кнопки «Копировать» в открывшемся окне необходимо выбрать из раскрывающегося списка пул данных, после чего нажать кнопку «ОК»;

– перенос. При нажатии кнопки «Перенести» в открывшемся окне необходимо выбрать из раскрывающегося списка пул данных, после чего нажать кнопку «ОК»;

– скачивание. Выполняется автоматически при нажатии кнопки «Скачать»;

– удаление. При нажатии кнопки «Удалить» в открывшемся окне необходимо подтвердить операцию, нажав на кнопку «Удалить»;

– генерация или проверка хеш-суммы файла. Если хеш-сумма не отображается в окне информации, то для отображения хеш-суммы следует нажать кнопку «Генерация хеш-суммы файла» и в открывшемся окне подтвердить операцию. Процесс подсчета суммы отображается индикатором «Чтение». После генерации хеш-суммы появится возможность проверить ее по кнопке «Проверка хеш-суммы файла». Если хеш-сумма сразу отображается в окне информации, то сразу же имеется и возможность ее проверки. При нажатии кнопки «Проверка хеш-суммы файла» в открывшемся окне необходимо подтвердить операцию, нажав на кнопку «Да».

3.9.7.8. Для разных типов файлов операции различаются, расширяя базовые операции.

3.9.7.9. Для образов дисков доступна операция импорта. При нажатии кнопки «Импортировать» в открывшемся окне необходимо включить/выключить опции «Добавить пул данных», «Предварительно выделить место», «Удалить файл по завершению» и указать название диска, куда импортировать. После заполнения подтвердить операцию, нажав кнопку «ОК». При включенной опции «Добавить пул данных» необходимо выбрать из раскрывающегося списка сервер и пул данных.

Переключатель удаления оригинального файла после завершения операции «по умолчанию» находится в положении «выключено», и по завершении операции оригинальный файл сохраняется в списке файлов текущего хранилища.

3.9.7.10. Для образов профиля узла доступны следующие операции:

– отвязка профиля. При нажатии кнопки «Отвязать» в открывшемся окне необходимо выбрать из раскрывающегося списка сервер, к которому он сейчас привязан, после чего нажать кнопку «ОК»;

– применение профиля. При нажатии кнопки «Привязать» в открывшемся окне необходимо выбрать из раскрывающегося списка сервер, после чего нажать кнопку «ОК»;

– открытие конфигурации файла профиля. При нажатии кнопки «Конфигурация файла профиля» в открывшемся окне отображается сохраненная в профиле информация с узла.

3.9.7.11. Для резервных копий ВМ доступны следующие операции:

– обновление информации о резервной копии ВМ. Выполняется автоматически при нажатии кнопки «Обновить информацию о резервной копии». Эта операция доступна для вновь загруженной резервной копии. После ее выполнения дальнейшее повторение этой операции не требуется, и соответствующая кнопка пропадает. Но для файлов «ovf» эта операция доступна всегда, так как конфигурация зависит от наличия образов дисков в текущей директории;

– открытие конфигурации резервной копии ВМ. При нажатии кнопки «Конфигурация копии ВМ» в открывшемся окне отображается информация о ВМ в резервной копии, а также возможные операции восстановления и конвертации, в зависимости от типа резервной копии.

Дополнительную информацию о файлах резервных копий ВМ смотрите в 3.8.21.

3.9.7.12. Допустимые форматы файлов приведены в приложении 2 данного руководства.

3.9.8. ZFS-пулы

3.9.8.1. Общая информация

3.9.8.1.1. В разделе «Хранилища» – «ZFS» основного меню содержится информация обо всех хранилищах ZFS, сконфигурированных в системе. ZFS-хранилища являются локальными, но возможности данных хранилищ значительно шире, чем у локальных файловых хранилищ. Создавая хранилище ZFS, необходимо подготовить сервер к созданию на нем пула данных типа «zfs».

3.9.8.1.2. Для создания ZFS-хранилища необходимо в разделе «Хранилища» – «ZFS» основного меню нажать кнопку «Создать». В открывшемся окне необходимо выбрать и заполнить следующие поля:

1) сервер размещения ZFS-пула (выбор из раскрывающегося списка);

2) тип пула (выбор из раскрывающегося списка). В типе пула необходимо выбрать режим RAID-массива (способ хранения данных), который будет применятся к входящим в состав ZFS-хранилища дискам.

Доступны следующие режимы:

– stripe;

– mirror;

– raidz1;

– raidz2.

Режимы «raidz1» и «raidz2» соответствуют RAID5 и RAID6 соответственно (RAID5 и RAID6 – уровни RAID-массивов);

3) локальные устройства (выбор из раскрывающегося списка);

4) LUN-устройства (выбор из раскрывающегося списка);

5) название и описание пула.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

Примечание. В списке доступных блочных устройств показываются только устройства без разметки (разделов). Чтобы очистить требуемое устройство от ранее созданной разметки, следует воспользоваться командой CLI *wipefs [-h] [drive ...]*, после этого устройство появится в списке. В случае устройств LUN, возможно, потребуется отключить и заново присоединить устройство.

3.9.8.1.3. Управление работой ZFS-хранилища происходит в окне состояния ZFS-пула, которое открывается при нажатии на название хранилища. Логика управления ZFS соответствует управлению работой RAID-контроллера. В окне состояния ZFS-хранилища доступны следующие операции:

– обновление информации по кнопке  ;

– расширение (добавление блочных устройств верхнего уровня). Операция «Расширить» доступна для ZFS с типом пула «stripe». Операция «приклеивает» дополнительные устройства к имеющемуся хранилищу. При нажатии кнопки «Расширить» в открывшемся окне необходимо выбрать из раскрывающегося списка локальные устройства (local_devices) или подключенные к серверу сетевые блочные устройства LUN (lun_devices), после чего подтвердить операцию, нажав кнопку «ОК».

Примечание. Добавлять можно только по одному устройству. Один из списков или оба могут быть пустыми, если нет доступных устройств;

– монтирование блочного устройства. Операция «Примонтировать» доступна для ZFS с типами пула «stripe» и «mirror», в составе которого только один диск. Операция преобразует хранилище в тип «mirror».

При нажатии кнопки «Примонтировать» в открывшемся окне необходимо выбрать из раскрывающегося списка тип блочного устройства и присоединяемое устройство (НЖМД или LUN), после чего подтвердить операцию, нажав кнопку «ОК»;

– добавление реплики. Операция «Добавить реплику» позволяет создать задание репликации. При нажатии кнопки «Добавить реплику» в открывшемся окне необходимо выбрать из раскрывающегося списка тип хранилища и выбрать локальное устройство, после чего подтвердить операцию, нажав кнопку «ОК»;

– добавление устройства горячей замены. Операция «Добавить устройство горячей замены» позволяет отметить неиспользуемое системой устройство как hot-swap для данного хранилища. При нажатии кнопки «Добавить устройство горячей замены» в открывшемся окне необходимо выбрать из раскрывающегося списка локальные устройства (local_devices) или подключенные к серверу сетевые блочные устройства LUN (lun_devices), после чего подтвердить операцию, нажав кнопку «ОК»;

– добавление устройства кэширования. Операция «Добавить устройства кэширования» позволяет добавить кэш для ZFS RAID-массива. При нажатии кнопки «Добавить устройство кэширования» в открывшемся окне необходимо выбрать из раскрывающегося списка локальные устройства (local_devices) или подключенные к серверу сетевые блочные устройства LUN (lun_devices), после чего подтвердить операцию, нажав кнопку «ОК»;

– сброс ошибок в пуле. При нажатии кнопки «Сброс ошибок» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «Да»;

– проверка целостности данных (scrub). При нажатии кнопки «Проверка целостности (scrub)» в открывшемся окне необходимо подтвердить операцию, нажав на кнопку «Да»;

– получение расширенных сведений о ZFS;

– удаление пула. Операция «Удалить» позволяет расформировать ZFS-хранилище. При нажатии кнопки «Удалить» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «Удалить».

3.9.8.1.4. В окне состояния хранилища содержатся сведения, разделенные на следующие группы:

– «Информация»;

– «Пулы данных»;

– «События»;

– «Теги».

3.9.8.1.5. В окне «Хранилища» – «ZFS» – <имя ZFS-пула> – «Информация» отображаются следующие сведения о ZFS-хранилище:

1) название;

2) описание (редактируемый параметр);

3) сервер;

4) состояние;

5) общий размер;

6) свободное пространство;

7) дата и время создания;

8) дата и время изменения;

9) локальные устройства (раскрывающийся список). Каждое устройство содержит следующие сведения:

– название;

– размер;

– состояние;

– кэширование;

– устройство горячей замены.

Для каждого устройства доступны операции:

– включение (выключение). При нажатии кнопки вкл/выкл устройство» открывается окно, в котором необходимо подтвердить операцию, нажав кнопку «Да»;

– замена устройства. При нажатии кнопки «Замена устройства» открывается окно, в котором необходимо выбрать local_device, после чего подтвердить операцию, нажав кнопку «ОК»;

– демонтирование устройства. При нажатии кнопки «Демонтирование устройства» открывается окно, в котором необходимо подтвердить операцию, нажав кнопку «Да». Удаление диска из состава ZFS возможно только для хранилища, в составе которого два или более дисков. Если в составе ZFS с типом «mirror» останется только один диск, то он преобразуется в тип «stripe».

10) устройства LUN (раскрывающийся список);

11) дополнительные характеристики (раскрывающийся список):

– автозамена (вкл/выкл);

– точка монтирования;

– сдвиг (ashift).

3.9.8.1.6. В окне «Хранилища» – «ZFS» – <имя ZFS-пула> – «Пулы данных» отображаются созданные в хранилище пулы данных, включая для каждого из них его название, тип, количество серверов, виртуальных дисков, образов и файлов, использованный объем, приоритет и статус.

При нажатии на название пула открывается окно состояния пула, в котором доступны следующие операции:

– обновление информации по кнопке  ;

– извлечение пула. При нажатии кнопки «Извлечь» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «ОК»;

– очистка пула. При нажатии кнопки «Очистить» в открывшемся окне следует определить необходимость принудительной очистки, после чего подтвердить операцию, нажав кнопку «ОК»;

– удаление диска (если допускается). При нажатии кнопки «Удалить» необходимо подтвердить операцию, нажав на кнопку «Удалить»;

– сканирование пула. Выполняется нажатием кнопки «Сканировать».

3.9.8.1.7. Информация о хранилище разделена на группы:

– «Информация»;

– «Диски»;

– «Образы»;

– «Файлы»;

– «События»;

– «Теги».

3.9.8.2. Информация о выбранном пуле данных

3.9.8.2.1. В окне «Хранилища» – «ZFS» – <имя ZFS-пула> – «Пулы данных» – <имя пула данных> – «Информация» содержатся следующие сведения о пуле данных:

– название (редактируемый параметр);

– описание (редактируемый параметр);

– тип;

– абсолютный путь расположения в файловой системе сервера;

– объем дискового пространства (всего, занято, свободно);

– приоритет;

– серверы размещения пула данных (раскрывающийся список). Список для локальных хранилищ содержит только одну запись. Для пула данных, зарегистрированного на сетевом хранилище, данный пункт будет содержать список серверов, к которым подключено сетевое хранилище;

– статус;

– даты и время создания;

– дата и время обновления данных.

3.9.8.3. Диски

3.9.8.3.1. В окне «Хранилища» – «ZFS» – <имя ZFS-пула> – «Пулы данных» – <имя пула данных> – «Диски» отображены все виртуальные диски, расположенные в данном пуле данных, включая для каждого из них его название, подключение к ВМ, размер и статус.

3.9.8.3.2. Также в окне управления дисками доступны следующие операции:

1) обновление информации по кнопке  ;

2) создание нового диска. При нажатии кнопки «Создать» в открывшемся окне необходимо заполнить название, описание и размер виртуального диска, предварительное выделение места, после чего подтвердить операцию, нажав кнопку «ОК»;

3) сканирование. Выполняется нажатием кнопки «Сканировать». Система сканирования регистрирует новые диски только в том случае, если структура их наименования совпадает с принятой в системе управления SpaceVM. Если виртуальный диск, загружаемый в пул данных имеет имя, отличное от принятого формата, то рекомендуется перейти во вкладку «Файлы» окна управления пулом данных.

Для получения подробной информации о диске необходимо нажать на название диска. Подробное описание приведено в 3.9.5 данного руководства.

3.9.8.4. Образы

3.9.8.4.1. В окне «Хранилища» – «ZFS» – <имя ZFS-пула> – «Пулы данных» – <имя пула данных> – «Образы» отображены все образы ISO, расположенные в данном пуле данных.

Также в окне управления образами доступны следующие операции:

– обновление информации;

– загрузка образа из файловой системы. При нажатии кнопки «Загрузить образ из файловой системы» открывается стандартное окно загрузки файлов, где необходимо открыть папку (директорию) хранения образов CD/DVD-дисков, выбрать нужный образ и нажать кнопку «Открыть»;

– загрузка образа по URL. При нажатии кнопки «Загрузить по url» в открывшемся окне необходимо заполнить URL-адрес (ввести местонахождение образа диска по ссылке), после чего подтвердить операцию, нажав кнопку «ОК»;

– сканирование списка образов ISO. Сканирование пула данных на наличие неуказанных в списке образов выполняется нажатием кнопки «Сканировать»;

При переходе в окно состояния образа CD/DVD-дисков становятся доступны следующие операции:

– обновление информации по кнопке  ;

– копирование в другой пул данных. При нажатии кнопки «Копировать» в открывшемся окне необходимо выбрать из раскрывающегося списка пул данных и нажать кнопку «Копировать»;

– скачивание. Выполняется автоматически при нажатии кнопки «Скачать»;

– удаление. При нажатии кнопки «Удалить» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «Удалить».

В окне состояния образа содержится следующая информация:

– название образа (редактируемый параметр);

– его описание (редактируемый параметр);

– список ВМ, к которым подключен образ, с возможностью его отключения от всех ВМ по кнопке  ;

– пул данных;

– размер;

– дата и время создания;

– дата и время изменения;

– сообщения о работе образа с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором в интервале дат.

3.9.8.5. Файлы

3.9.8.5.1. В окне «Хранилища» – «ZFS» – <имя ZFS-пула> – «Пулы данных» – <имя пула данных> – «Файлы» отображены все файлы, расположенные в данном хранилище.

3.9.8.5.2. Также в окне управления файлами доступны следующие операции:

– обновление информации;

– загрузка файла из файловой системы. При нажатии кнопки «Загрузить из файловой системы» открывается стандартное окно загрузки файлов, где необходимо открыть папку (директорию) хранения файлов, выбрать нужный файл и нажать кнопку «Открыть». Допустимые форматы файлов приведены в приложении 2 данного руководства;

– загрузка файла по URL. При нажатии кнопки «Загрузить по url» в открывшемся окне необходимо заполнить URL-адрес (ввести местонахождение образа диска по ссылке), после чего подтвердить операцию, нажав кнопку «ОК»;

– сканирование. Выполняется нажатием кнопки «Сканировать».

Все операции с файлами аналогичны операциям с образами ISO – скопировать, скачать, удалить или перенести в другой пул данных.

Для файлов формата «vmdk», «qcow2», «qcow», «raw», «img», «bin» (форматы дисков) будет доступна кнопка импорта или конвертации.

Для получения информации о файле необходимо нажать на название файла. Подробное описание приведено в 3.9.7 данного руководства.

3.9.8.6. События

3.9.8.6.1. В окне «Хранилища» – «ZFS» – <имя ZFS-пула> – «Пулы данных» – <имя пула данных> – «События» отображаются зарегистрированные в системе события, связанные с работой выбранного хранилища, с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.9.8.7. Теги

3.9.8.7.1. В окне «Хранилища» – «ZFS» – <имя ZFS-пула> – «Пулы данных» – <имя пула данных> – «Теги» можно установить дополнительные цветные маркеры ZFS-пулу с целью визуального выделения его в общем списке.

3.9.8.8. ARC-кэш

3.9.8.8.1. При создании ZFS-пулов необходимо учитывать адаптивное использование памяти сервера под ARC-кэш.

3.9.8.8.2. Одним из основных моментов, о котором необходимо помнить при использовании ZFS на гипервизоре является факт того, что baloon ВМ, использующийся для оптимизации выделения и возвращения неиспользуемой памяти, некорректно работает вместе с динамическим ARC. Поэтому хорошим тоном будет выделение фиксированной памяти для ВМ – baloon=0, и указания максимального размера ARC, таким образом, чтобы суммарная утилизация памяти для машин и кэша была меньше общего количества RAM на 2 Гбайт.

3.9.8.8.3. Минимальный размер ARC для более-менее комфортной работы ФС без активного режима записи/перезаписи в файлы ВМ (например, этим грешат базы данных) примерно равен 1 Гбайт на хост + 1 Гбайт на 1 Тбайт, но фактически при кэше меньше 3 Гбайт могут возникнуть проблемы с «отвалом» хранилища, и для работы с активной перезаписью лучше использовать формулу 1 Гбайт + 4-5 Гбайт на 1 Тбайт без дедупликации, 5-6 Гбайт – с дедупликацией.

Разово задать максимальный размер кэша до перезагрузки можно командой

*echo $[N*1048576*1024] > /sys/module/zfs/parameters/zfs_arc_max*

где *N* – требуемый объем в Гбайтах.

Параметр «zfs_arc_max» не может быть ниже текущего минимального размера кэша («zfs_arc_min»), который можно посмотреть при выводе команды *arc_summary* в строке «Min size (hard limit)». Чтобы указать «zfs_arc_max» ниже данного значения, следует сначала таким же образом задать параметр «zfs_arc_min». Важно помнить, что эти параметры не могут быть менее 64 Мбайт, а также больше объема ОЗУ на узле. В противном случае эаданные значения параметров будут проигнорированы.

3.9.8.8.4. Для постоянного определения размера переопределить zfs_arc_max можно добавив в конфигурацию параметр «zfs_arc_max»

echo options zfs zfs_arc_max=16106127360>> /etc/modprobe.d/zfs.conf и пересобрав *initramfs* командой *update-initramfs -u.*

3.9.8.8.5. Также в ZFS есть возможность перенаправить чтение и запись на устройстве хранения, подключив отдельные «буферные» разделы на быстрых устройствах хранения (SSD):

– l2arc – на чтение. Он собирает используемые в данный момент обращения и выдает их через себя, что ускоряет запросы чтения к файловой системе хранилища. Минимальный размер l2arc примерно рассчитывается по формуле 2000 байт ARC на 1 блок l2arc, размер которого зависит от ashift ZFS-пула, то есть чем больше ashift, тем больше должен быть l2arc, но раздувать его за пределы 500 байт на 1 блок данных пула смысла нет – нельзя отдавать весь ARC под нужды l2arc, так как при максимальной загрузке вместо оперативной памяти пользователь будет работать с устройством кэширования;

– zil (slog) – кэширование записи. Каждая операция записи на пул будет считаться совершенной при попадании в zil, а на устройства хранения будет попадать уже так называемая «дельта» всех операций с минимальным количеством «грязных данных». Минимальный размер zil устройства рассчитывается примерно из скорости работы вашего устройства, где будет размещен лог, и «времени задержки записи «грязных данных» х 2». Максимальный размер для конкретной системы нужно определять индивидуально, но на практике размер больше, чем «скорость устройства х 10 с», имеет смысл только в узкоспециализированных, направленных на постоянное краткосрочное изменение данных с минимальной задержкой.

3.9.8.9. Импорт ZFS-пулов

3.9.8.9.1. Получить имена и параметры импортируемых ZFS-пулов можно командой CLI

zpool import

3.9.8.9.2. Импорт из файла кэша, если пул там прописан, выполняется командой

zpool import -C <pool_name>

3.9.8.9.3. При проблемах с файлом кэша или если запись о ZFS-пуле из кэша пропала (например, если ZFS-пул не импортировался ввиду отсутствия дисков на этапе загрузки, а потом с исправными пулами проводились какие-либо манипуляции, неимпортированные ZFS-пулы «забываются» кэшем) используется команда

zpool import -d /dev/disk/by-id <pool_name>

ВНИМАНИЕ! Важно указать каталог «/dev/disk/by-id», так как в противном случае возможен импорт ZFS-пула с «короткими» именами устройств, например, «/dev/sdc». Это может привести при последующей перезагрузке к пропаданию устройства из ZFS-пула, так как такие короткие имена назначаются устройствам лишь на основе порядка их определения, что может меняться от загрузки к загрузке, и одно и то же устройство может получать различные короткие имена.

3.9.8.9.4. Для проверки появления в системе используется команда

zpool list

3.9.8.9.5. Чтобы ZFS-пул сохранился после перезагрузки, нужно пересоздать кэш с указанием этого пула

zpool set cachefile=/etc/zfs/zpool.cache <pool_name>

3.9.8.10. Случай загрузки с неполным набором устройств, входящих в ZFS-пулы

3.9.8.10.1. Если ZFS-пул, в котором недостает устройств, обладает достаточной избыточностью, чтобы компенсировать их отсутствие (для типа «mirror» должно остаться хотя бы одно устройство, для типа «raidz1» возможно остаться без одного, для «raidz2» – без двух устройств; устройства горячего резерва и кэша чтения на работоспособность не влияют), то такой ZFS-пул импортируется при старте системы обычным образом. В противном случае этот ZFS пул не импортируется.

Если есть техническая возможность вернуть в систему недостающие устройства под теми же именами, то после их возврата пострадавший ZFS-пул будет импортирован автоматически при перезагрузке узла, либо «на лету» через CLI после проверки возможности импорта ZFS-пула командой (см. 3.9.8.9) *zpool import* или *zpool import -d /dev/disk/by-id*. Для проверки состояния кэша используют команду CLI *zdb*. Она отображает сохраненные в кэше ZFS-пулы, входящие в них устройства, их типы, а также некоторую дополнительную информацию.

ВНИМАНИЕ! Чтобы ZFS-пул был автоматически импортирован при старте системы, он должен быть прописан в кэше «/etc/zfs/zpool.cache». Записи о ZFS-пулах там появляются при их создании, также они модифицируются при манипуляциях с ZFS-пулами. Если какой-то ZFS-пул не импортирован из-за повреждений, то есть не виден в системе, то в момент модификации кэша (изменения имеющихся или создания новых ZFS-пулов) записи о нем УДАЛЯЮТСЯ из кэша, и при следующей перезагрузке данный ZFS-пул не будет импортирован автоматически. Это следует учитывать, и если есть необходимость и возможность вернуть данный ZFS-пул в работу, и в то же время проводить какие-то действия над имеющимися ZFS-пулами узла, то нужно обеспечить работоспособность поврежденного ZFS-пула и импортировать его вручную до перезагрузки системы, либо импортировать его вручную после перезагрузки. Первый вариант предпочтительней, особенно, если ZFS-пул участвует, например, в кластерном хранилище.

Также может быть полезна информация из меток устройств, входивших в ZFS-пул, получить которую можно командой

zdb -l <device>

Будет показано, принадлежит ли устройство ZFS-пулу, какому именно, какой GUID у этого устройства и на каком хосте создан данный ZFS-пул.

3.9.9. Сетевые хранилища

Раздел «Хранилища» – «Сетевые хранилища» основного меню содержит два подраздела – «Файловые» и «Блочные». Информация о сетевых хранилищах распространяется на весь кластер.

3.9.9.1. Файловые хранилища

3.9.9.1.1. К файловым хранилищам относятся хранилища, предоставляемые по протоколам NFS, CIFS и GlusterFS. Сетевое хранилище подразумевает доступ к ресурсам (файлам), хранящимся на нем по схеме «много к одному».

Такое хранилище может быть рекомендовано для хранения образов CD/DVD, шаблонов ВМ или ВМ, которые не требуют высокой производительности дисковой подсистемы ВМ.

Основным недостатком данного типа хранилищ является то, что в случае обрыва связи с ним, подключение не обрывается, а переходит в режим «read only» и все изменения в период недоступности будут потеряны. Это обусловлено принципами работы NFS.

В данный момент поддерживается NFS v4. Версия NFS v3 поддерживается в рамках обратной совместимости с v4. Более ранние версии имеют слишком низкую производительность.

3.9.9.1.2. При подключении файлового сетевого хранилища (NFS) необходимо внести все параметры подключения в соответствии с выбранным типом хранилища.

3.9.9.1.3. Для протокола NFS необходимо знать версию протокола, IP-адрес или доменное имя сервера хранения, какая из общедоступных папок данного сервера будет использоваться и настройки ограничений прав доступа. Ограничения прав доступа для NFS предусмотрены трех типов:

– «no_root_squash» – разрешено подключение с пользователем «root»;

– «root_squash» – доступ под именем «root» запрещен, используется «по умолчанию»;

– «all_squash» – все пользователи подключаются как анонимные.

3.9.9.1.4. Для NFS v4 режимы задаются через сопоставление пользователей «root» и «nobody/anonuid». При этом результирующая политика ограничений не изменяется.

Примечания:

1. При подключении к хранилищу NFS используются два режима – с включенной опцией «no_root_squash» и без нее. Без данной опции подключение к NFS производится пользователем, идентификаторы которого UID и GID (идентификатор основной группы) соответствуют номеру «931». Соответственно подключаемая к кластеру общая папка должна иметь владельца с этим UID/GID для отсутствия ограничений по чтению (записи) на уровне файловой системы сервера хранения.

2. Для CIFS (SMB) поддерживаются версии default (2.1), 2.0, 2.1, 3 (3.0 и выше).

3.9.9.1.5. Для подключения NFS-хранилища необходимо перейти в раздел «Хранилища» – «Сетевые хранилища» – «Файловые» основного меню и нажать кнопку «Добавить». В открывшемся окне необходимо заполнить следующие поля:

1) название сетевого хранилища;

2) тип подключения (выбор из раскрывающегося списка);

3) локация, в которой расположено хранилище (выбор из раскрывающегося списка);

4) сервер для монтирования сразу после создания (выбор из раскрывающегося списка);

5) IP-адрес или доменное имя сервера хранения;

6) проверить доступность сервера и получить список доступных папок хранения (томов) по кнопке «Проверить соединение и получить доступные тома (volumes)»;

7) каталог на сетевом хранилище – папка на сервере, которую подключаем;

8) каталог монтирования в SpaceVM – имя папки для монтирования;

9) включить (выключить) опцию «Только чтение»;

10) включить опцию «ID mapping», если на сервере включена опция «no_root_squash» (для NFS);

11) раскрыть опции монтирования и заполнить следующие поля (для NFS):

– sec (выбор из раскрывающегося списка);

– lookupcache (выбор из раскрывающегося списка);

– proto (выбор из раскрывающегося списка);

– версия nfs;

– clientaddr;

– определить включение или отключение параметров «noac», «bg», «nordirplus», «nosharecache», «noresvport», «fsc», «nointr», «nocto», «soft»;

– timeo;

– retrans;

– rsize;

– wsize;

– acregmin;

– acregmax;

– acdirmin;

– acdirmax;

– actimeo;

– retry;

– port;

12) раскрыть опции монтирования и заполнить следующие поля (для CIFS):

– username (необязательный, при отсутствии монтирование будет происходить в режиме гостя);

– password (необязательный);

– vers (выбор из раскрывающегося списка);

13) заполнить описание.

После внесения изменений необходимо подтвердить операцию, нажав кнопку «ОК».

3.9.9.1.6. Для подключения серверов к созданному хранилищу необходимо:

– нажать на название хранилища в списке;

– в открывшемся окне во вкладке «Информация» рядом с надписью «Серверы» нажать кнопку добавления сервера  . При добавлении сервера в открывшемся окне необходимо проверить соединение с сервером, нажав кнопку «Проверить», выбрать из раскрывающегося списка сервер, после чего подтвердить операцию, нажав кнопку «Добавить».

После добавления серверов рядом с надписью «Серверы» появится количество серверов и кнопка раскрытия списка серверов.

3.9.9.1.7. Далее необходимо создать пул данных, размещаемый на сетевом хранилище, для использования его как локального. Данная процедура предусмотрена для возможности регистрации нескольких пулов на одном сетевом хранилище. Регистрация пула описана в 3.9.3 данного руководства.

3.9.9.1.8. В окне состояния хранилища отображаются сведения о нем, разделенные на группы:

– информация;

– пулы данных;

– события;

– теги.

3.9.9.1.9. В окне «Хранилища» – «Сетевые хранилища» – «Файловые» – <имя хранилища> – «Информация» содержатся следующие сведения о сетевом хранилище:

– название (редактируемый параметр);

– описание (редактируемый параметр);

– тип подключения;

– точка монтирования (путь подключения);

– root_squash (для NFS);

– том;

– опция «Только чтение» (вкл/выкл) (редактируемый параметр);

– адрес хранилища (IP-адрес/доменное имя) (редактируемый параметр);

– опции монтирования (nfsvers);

– объем дискового пространства хранилища (всего, занято, свободно);

– локация;

– дата и время создания;

– дата и время обновления;

– серверы размещения (раскрывающийся список с возможностью подключения нового сервера по кнопке  , отключения сервера от хранилища по кнопке  и обновления по кнопке ).

3.9.9.1.10. В окне «Хранилища» – «Сетевые хранилища» – «Файловые» – <имя хранилища> – «Пулы данных» содержится информация о пуле данных, включая для каждого из них его название пула данных, тип, количество серверов, дисков, образов и файлов, используемый объем и статус.

Также в этом окне существует возможность создать новый пул с помощью кнопки «Создать» и найти пул с применением фильтра.

При нажатии на название пула данных открывается окно, в котором информация распределена на следующие группы:

– информация;

– виртуальные диски;

– образы;

– файлы;

– события;

– теги.

Подробная информация о виртуальных дисках, образах и файлах приведена в 3.9.5, 3.9.6, 3.9.7 данного руководства.

Также существует возможность извлечения с помощью кнопки «Извлечь», очистки пула данных с помощью кнопки «Очистить» и удаления с помощью кнопки «Удалить».

3.9.9.1.11. В окне «Хранилища» – «Сетевые хранилища» – «Файловые» – <имя хранилища> – «События» содержатся события, зарегистрированные в системе, возникающие при работе с файловыми хранилищами с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.9.9.1.12. В окне «Хранилища» – «Сетевые хранилища» – «Файловые» – <имя хранилища> – «Теги» имеется возможность добавления к хранилищу отличительной метки (тега), применения и обновления тега.

3.9.9.2. Блочные хранилища

3.9.9.2.1. К блочным хранилищам относят хранилища, предоставляемые по протоколам iSCSI и FC.

3.9.9.2.2. Сетевые хранилища типов iSCSI и FC основаны на принципе предоставления блочных устройств, которые после подключения воспринимаются системой как локальные диски. Основное отличие данных хранилищ – это метод подключения к ним серверов.

3.9.9.2.3. Технология iSCSI работает поверх протокола TCP/IP. На стороне СХД настраиваются точки подключения, именуемые «цели» (iSCSI target), в которых презентуются блочные устройства (LUN). Подключение к ним со стороны сервера осуществляется «инициатором» (iSCSI initiator). В качестве «инициатора» может выступать клиентское ПО или физический сетевой адаптер, настроенный в режим iSCSI-инициатора. Возможность настройки адаптера как «инициатора» следует уточнять у производителя. Блочные устройства становятся доступными на сервере после запуска «инициатора» и, в случае работы программного клиента, доступны только после загрузки ОС гипервизора.

3.9.9.2.4. Блочный доступ FC основывается на собственной технологии передачи данных, требует установки специализированных адаптеров (карт расширения), специализированных коммутаторов и систем хранения с поддержкой данной технологии. За счет собственных адаптеров использование «инициатора» не требуется и блочные устройства презентуются серверу на аппаратном уровне и воспринимаются как локальные диски. При использовании FC необходимо учитывать данный момент, так как добавление LUN может изменить порядок подключенных физических носителей в ОС гипервизора.

3.9.9.2.5. Правила предоставления блочных устройств от СХД к серверам для FC настраиваются в коммутаторе и в ПО управления самой СХД, так как основными идентификаторами «клиентов» и портов на СХД являются WWN – аналог MAC-адреса для обычного сетевого адаптера. Другие идентификаторы для данной технологии не предусмотрены.

3.9.9.2.6. На сервере или в ВМ работа с подключенным блочным устройством LUN происходит также, как и с НЖМД – его можно отдать под управление LVM, отформатировать в файловую систему. При использовании коллективного доступа к LUN необходимо форматировать его в кластерную файловую систему, которая будет следить за конкурентным доступом к ресурсам устройства.

3.9.9.2.7. Существенным плюсом использования доступа к блочным устройствам является то, что многие системы хранения имеют механизмы повышения отказоустойчивости. Некоторые СХД также предоставляют возможность объединения их в кластер и настройки репликации одного блочного устройства LUN таким образом, что при выходе из строя одного сервера, подключенная система автоматически переключится на резервную копию.

3.9.9.2.8. При подключении блочного сетевого хранилища необходимо внести все параметры подключения в соответствии с выбранным типом хранилища.

3.9.9.2.9. При подключении к хранилищу iSCSI необходимо знать IP-адрес или доменное имя хранилища (sources), порты подключения, имена целей (iSCSI target), логин и пароль подключения (если требуется). Имена целей должны соответствовать формату, установленному стандартом, и иметь вид «iqn.2018-11.com.raidix:target0». В рамках одной цели может предоставляться несколько блочных устройств.

3.9.9.2.10. Для подключения блочного хранилища iSCSI необходимо перейти в раздел «Хранилища» – «Сетевые хранилища» – «Блочные» основного меню и нажать кнопку «Добавить». В открывшемся окне необходимо заполнить следующие поля:

– название сетевого хранилища;

– определить возможность подключения узлов сети хранения данных с использованием нескольких маршрутов (состояние Multipath I/O);

– тип подключения (выбор из раскрывающегося списка);

– локация, в которой расположено хранилище (выбор из раскрывающегося списка);

– имя сервера для монтирования сразу после создания (выбор из раскрывающегося списка);

– IP-адрес или доменное имя сервера хранения и порт;

– проверить доступность сервера и получить список доступных таргетов по кнопке «Получить доступные таргеты (target)»;

– имя iSCSI target;

– логин и пароль для подключения (если требуется);

– производитель (выбор из раскрывающегося списка);

– раскрыть опции и заполнить поля «Таргет» и «Адреса (ip-адрес/доменное имя)»;

– описание хранилища.

Для подтверждения операции необходимо нажать кнопку «ОК».

3.9.9.2.11. Для подключения серверов к созданному хранилищу необходимо:

– нажать на название хранилища в списке;

– в открывшемся окне во вкладке «Информация» рядом с надписью «Серверы» нажать кнопку добавления сервера  . При этом открывается окно с возможностью выбора серверов, к которым будет подключено данное хранилище. После заполнения окна необходимо подтвердить операцию, нажав кнопку «Добавить».

После добавления серверов рядом с надписью «Серверы» появится количество серверов и кнопка раскрытия списка серверов.

3.9.9.2.12. При использовании хранилища, подключаемого по FC, СХД предоставляет блочные устройства LUN на аппаратном уровне в соответствии с правилами, настроенными на FC коммутаторе и на стороне СХД. Для настройки правил подключения (презентации) LUN с СХД к серверам необходимо обратиться к документации производителя СХД и FC коммутатора. При использовании схемы прямого подключения СХД к серверам SpaceVM (схема DAS – Direct Attached Storage) настройка производится на самом СХД.

3.9.9.2.13. Для регистрации в системе управления подключенных LUN необходимо знать адрес WWN порта СХД, с которого происходит обслуживание подключений от серверов SpaceVM. Это необходимо для того, чтобы система управления SpaceVM собрала в группу только те LUN, которые подключены от этого WWN. Это сделано для возможности группировки LUN по WWN СХД, если по FC доступно более одного СХД.

При регистрации система опрашивает все блочные устройства, подключенные к серверу, находит имеющие пометку о подключенных по шине FC и презентованные от указанного WWN.

3.9.9.2.14. После подключения блочных хранилищ к серверам SpaceVM видимые активные LUN можно использовать как LVM-shared хранилища, как часть ZFS-пула, форматировать их в кластерную файловую систему (OCFS2/GFS2) и подключать их напрямую к ВМ. Не рекомендуется подключать напрямую в ВМ LUN, презентованный по FC. Это связано с тем, что ВМ создаст на этом LUN загрузочную область, которая будет доступна аппаратному серверу, так как FC LUN подключается на уровне основной системы ввода-вывода (BIOS/UEFI).

3.9.9.2.15. При установке SpaceVM на сервер с уже подключенным по FC СХД следует обратить внимание на то, что при установке FC LUN могут отображаться в конце списка доступных к установке накопителей, но при загрузке гипервизора могут переместиться в начало списка (занять место диска */dev/sda*). Для предотвращения такого поведения необходимо корректно настроить FC карту сервера (FC HBA) и параметры презентуемых LUN на стороне СХД.

3.9.9.2.16. При использовании хранилища производства «Raidix» можно указать логин и пароль для доступа к API управления. При реализации катастрофоустойчивой ВМ переключение между основным и дополнительным LUN, а также проверка их статуса репликации происходит с помощью обращения к API «Raidix».

3.9.9.2.17. При использовании хранилища производства «Yadro» на данный момент учитывается, что оно не поддерживает метод «discovery», то есть статично, поэтому сопоставление всех таргетов к путям необходимо выполнить вручную путем записи словаря в поле «vendor_options» блочного хранилища, где ключами являются таргеты, а значениями-списки их путей.

3.9.9.2.18. В окне состояния блочного хранилища содержится информация, разделенная на группы:

– информация;

– LUNs;

– события;

– теги.

3.9.9.2.19. В окне «Хранилища» – «Сетевые хранилища» – «Блочные» – <имя блочного хранилища> – «Информация» содержатся следующие сведения:

– название (редактируемый параметр);

– описание (редактируемый параметр);

– тип подключения;

– локация;

– дата и время создания;

– дата и время обновления;

– target;

– состояние Multipath I/O (редактируемый параметр);

– производитель;

– опции iSCSI;

– sources (редактируемый параметр). Путь доступа к хранилищу;

– серверы (раскрывающийся список) с возможностью добавления сервера по кнопке  и удаления по кнопке  . При добавлении сервера в открывшемся окне необходимо для проверки соединения с сервером нажать кнопку «Проверить», после чего выбрать сервер из доступных и нажать кнопку «Добавить».

3.9.9.2.20. В окне «Хранилища» – «Сетевые хранилища» – «Блочные» – <имя блочного хранилища> – «LUNs» содержится информация о LUNs на хранилище (путь, подключение, серийный номер, ВМ, хранилище, размер и статус). Имеется возможность обновления, сканирования хранилища, а также поиск дискового устройства в сетях хранения по адресу.

При нажатии на существующий LUN в открывшемся окне доступны следующие операции:

– обновление информации по кнопке  ;

– копирование данных на LUN. При нажатии на кнопку «Перенос данных LUN» в открывшемся окне необходимо выбрать из раскрывающегося списка Lun, после чего подтвердить операцию, нажав кнопку «Перенести»;

– форматирование в файловую систему. При нажатии на кнопку «Форматировать в ФС» в открывшемся окне необходимо выбрать из раскрывающегося списка тип файловой системы, после чего подтвердить операцию, нажав кнопку «Отправить»;

– монтирование. При нажатии на кнопку «Монтировать» необходимо подтвердить операцию, нажав кнопку «Да»;

– размонтирование. При нажатии на кнопку «Размонтировать» необходимо подтвердить операцию, нажав кнопку «Да»;

– настройка I/O. Настроить I/O LUN можно с помощью кнопки «Настройки I/O». В открывшемся окне заполнить необходимые поля и нажать «ОК»;

– статистика I/O. Для сбора статистики необходимо нажать кнопку «Статистика I/O».

В открывшемся окне выбрать из раскрывающегося списка тип теста, указать период проведения и количество одновременных потоков для тестирования. Далее нажать кнопку «Собрать статистику»;

– очистка. При нажатии кнопки «Очистить» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «Да». Данная операция очистит все данные на LUN;

– удаление. При нажатии кнопки «Удалить» запускается мастер, где необходимо нажать на кнопку «Да», чтобы удалить данный LUN, или нажать на кнопку «Отмена» для отказа от операции.

Если LUN используется в GFS2, то сначала надо очистить и удалить пул данных GFS2, созданный на нём, отмонтировать LUN на всех узлах, и только потом его удалять.

Если LUN используется в ZFS-пуле, то сначала надо удалить LUN из состава ZFS-пула, и только потом его удалять.

Если LUN напрямую подключен к ВМ, то сначала надо отключить его от ВМ, и только потом удалять.

Под названием хранилища имеется его ID (UUID).

Также в данном окне содержится следующая информация:

– путь;

– устройство dev (при присоединении к ВМ);

– тип шины (при присоединении к ВМ);

– размер;

– тип файловой системы;

– тип кэширования (с возможностью изменения);

– опции I/O (с возможностью изменения);

– статус;

– хранилище;

– серийный номер;

– присоединенная ВМ;

– репликация LUN;

– количество серверов (раскрывающийся список). Для каждого сервера указаны IP-адрес, статус «примонтирован» или «не примонтирован» и путь к LUN;

– дата и время создания;

– дата и время изменения.

3.9.9.2.21. В окне «Хранилища» – «Сетевые хранилища» – «Блочные» – <имя блочного хранилища> – «События» содержатся события, зарегистрированные в системе, возникающие при работе с блочными сетевыми хранилищами с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.9.9.2.22. В окне «Хранилища» – «Сетевые хранилища» – «Блочные» – <имя блочного хранилища> – «Теги» содержится список присвоенных хранилищу меток. Также имеется возможность обновления, создания и применения тега.

3.9.9.2.23. Для просмотра настроек Multipath в CLI есть команда

storage multipath_conf

Для сканирования доступных путей в CLI есть команда

storage scsi_host_discovery

Для изменения политики группировки путей LUN в CLI есть команда

storage modify_multipath_path_grouping_policy [path_grouping_policy]

«По умолчанию» «path_grouping_policy» = *failover*.

Варианты «path_grouping_policy»:

– *failover* – One path per priority group;

– *multibus* – All paths in one priority group;

– *group_by_serial* – One priority group per serial number;

– *group_by_prio* – One priority group per priority value. Priorities are determined by callout programs specified as a global, per-controller or per-multipath option in the configuration file;

– *group_by_node_name* – One priority group per target node name. Target node names are fetched in /sys/class/fc_transport/target*/node_name.

Для изменения политики выбора путей LUN в CLI есть команда

storage modify_multipath_path_selector [path_selector]

«По умолчанию» «path_selector» = *service-time 0*.

Варианты «path_selector»:

– *service-time 0* – Send the next bunch of I/O down the path with the shortest estimated service time, which is determined by dividing the total size of the outstanding I/O to each path by its relative throughput;

– r*ound-robin 0* – Loop through every path in the path group, sending the same amount of I/O to each;

– *queue-length 0* – Choose the path for the next bunch of I/O based on the amount of outstanding I/O to the path.

3.9.9.2.24. При физическом подключении блочного хранилища по FC к серверу контроллер выдаст подсказку у сервера о том, что есть неизвестные блочные хранилища.

Если есть подсказка, то стоит перейти в окно «Сервер» – <имя сервера> – «Хранилища» – «Блочные хранилища» и нажать кнопку «Сканировать». Если на сервере найдутся незарегистрированные в базе контроллера хранилища, то они создадутся в базе или обновится связь с теми, что есть в базе.

Если хранилище подключено к разным узлам по разным WWN (путям), то стоит включить в настройках Multipath I/O режим использования «failover». Тогда при подключении узлов будет проверяться наличие хотя бы одного активного пути из всех.

Команда CLI *storage hba_npiv* позволяет увидеть имеющиеся FC-карточки, включая состояние их портов (port_state и speed).

Команда CLI *storage fc_luns* позволяет увидеть FC LUNs.

Команда CLI *storage multipath* позволяет увидеть LUN и пути, по которым они доступны.

Просмотр WWNS подключенных хранилищ возможен в окне «Сервер» – <имя сервера> – «Хранилища» – «Блочные хранилища» по кнопке «WWNS» или в CLI командой *storage fc_wwns.*

Просмотр локальных WWNS сервера возможен в окне «Сервер» – <имя сервера> – «Хранилища» – «Блочные хранилища» по кнопке «Локальные WWNS» или в CLI командой *storage local_wwns*.

Пересканировать SCSI шину узла можно в CLI командой *storage rescan_scsi_bus*.

3.9.9.2.25. Далее описаны действия после изменения размера LUN на хранилище или его удаления.

В том случае, если LUN был сначала виден на серверах SpaceVM, а потом его удалили в хранилище или изменили его размер, то автоматически обновление информации об этом действии не произойдет.

Стоит попробовать:

1) пересканировать SCSI шину узла можно в CLI командой *storage rescan_scsi_bus*

Так как размер LUN проверяется на всех узлах, где он виден, то стоит пересканировать шину на всех узлах. Для удобства можно это делать из CLI контроллера с помощью команды

node nodes_cli 'storage rescan_scsi_bus'

2) рестартовать сервис «multipathd» в CLI командой

services restart multipathd

Так как размер LUN проверяется на всех узлах, где он виден, то стоит рестартовать сервис на всех узлах. Для удобства можно это делать из CLI контроллера с помощью команды

node nodes_cli 'services restart multipathd'

Проверить изменение размера LUN можно, используя в CLI команду *storage luns (storage fc_luns, storage iscsi_luns)*. Необходимо учитывать, что размер в CLI выводится в Гибибайтах (Тебибайтах…).

В Web-интерфейсе контроллера размер LUN выводится в Гигабайтах (для удобства, так как в других местах выводится в таких же единицах) и изменяется автоматически после того, как узел увидел новый размер LUN.

3.9.10. Блочные устройства LUN

3.9.10.1. LUN – это блочные устройства, предоставляемые хранилищами по протоколу iSCSI или FC.

3.9.10.2. В разделе «Хранилища» – «LUN» основного меню содержится информация обо всех блочных устройствах в системе.

В окне LUNs доступно обновление информации о LUN по кнопке  .

3.9.10.3. При выборе блочного устройства из списка открывается окно состояния, содержащие информацию о нем. В окне состояния LUN доступны следующие операции:

– обновление информации;

– перенос (копирование) данных на другой LUN. При нажатии на кнопку «Перенос данных LUN» в открывшемся окне необходимо выбрать из раскрывающегося списка LUN, после чего подтвердить операцию, нажав кнопку «ОК». Пример использования – перенос данных с одного блочного хранилища на другое. Размер LUN назначения должен быть больше либо равен исходному LUN.

– форматирование в ФС. При нажатии на кнопку «Форматировать в ФС» запускается мастер «Форматирование в ФС», где необходимо выбрать из раскрывающегося списка тип файловой системы («ocfs2» или «gfs2») и указать максимальное количество узлов в кластере, после чего подтвердить операцию, нажав кнопку «ОК».

Примечание. Под каждый узел на LUN создается журнал блокировок, поэтому желательно выбирать реальное количество узлов, а не максимальное;

– монтирование. Данная операция необходима при использовании LUN в качестве общего хранилища OCFS/GFS2.

При нажатии на кнопку «Монтировать» запускается мастер «Монтирование LUN», где необходимо нажать на кнопку «Да», чтобы примонтировать данный LUN, или нажать на кнопку «Отмена» для отказа от операции;

– размонтирование. При нажатии на кнопку «Размонтировать» запускается мастер «Размонтирование LUN», где необходимо нажать на кнопку «Да», чтобы размонтировать данный LUN, или нажать на кнопку «Отмена» для отказа от операции;

– настройка I/O. При нажатии на кнопку «Настройка I/O» откроется окно настроек I/O. В таблице 3 приведены параметры и их описание.

Таблица 3

Параметр	Описание
total_bytes_sec	Общий предел пропускной способности в байтах в секунду. Не может использоваться с read_bytes_sec или write_bytes_sec
read_bytes_sec	Предел пропускной способности чтения в байтах в секунду
write_bytes_sec	Предел пропускной способности записи в байтах в секунду
total_iops_sec	Общее количество операций ввода-вывода в секунду. Не может использоваться с read_iops_sec или write_iops_sec
read_iops_sec	Количество операций чтения в секунду
write_iops_sec	Количество операций записи в секунду
total_bytes_sec_max	Общий предел пропускной способности в период высокой загрузки в байтах в секунду. Не может использоваться с read_bytes_sec_max или write_bytes_sec_max
read_bytes_sec_max	Предел пропускной способности чтения в период высокой загрузки в байтах в секунду
write_bytes_sec_max	Предел пропускной способности записи в период высокой загрузки в байтах в секунду
total_iops_sec_max	Общее количество операций ввода-вывода в период высокой загрузки в секунду. Не может использоваться с read_iops_sec_max или write_iops_sec_max
read_iops_sec_max	Количество операций чтения в период высокой загрузки в секунду
write_iops_sec_max	Количество операций записи в период высокой загрузки в секунду
size_iops_sec	Размер операций ввода-вывода в секунду

Параметр	Описание
total_bytes_sec_max_length	Продолжительность в секундах для периода высокой загрузки total_bytes_sec_max. Действителен только при установленном параметре total_bytes_sec_max
read_bytes_sec_max_length	Продолжительность в секундах для периода высокой загрузки read_bytes_sec_max. Действителен только при установленном параметре read_bytes_sec_max
write_bytes_sec_max	Продолжительность в секундах для периода высокой загрузки write_bytes_sec_max. Действителен только при установленном параметре write_bytes_sec_max
total_iops_sec_max_length	Продолжительность в секундах для периода высокой загрузки total_iops_sec_max. Действителен только при установленном параметре total_iops_sec_max
read_iops_sec_max_length	Продолжительность в секундах для периода высокой загрузки read_iops_sec_max. Действителен только при установленном параметре read_iops_sec_max
write_iops_sec_max	Продолжительность в секундах для периода высокой загрузки write_iops_sec_max. Действителен только при установленном параметре write_iops_sec_max.

Для сохранения изменений необходимо в нижней строчке окна нажать кнопку «ОК»;

– статистика I/O. Для сбора статистики необходимо нажать кнопку «Статистика I/O». В открывшемся окне выбрать из раскрывающегося списка тип теста, указать период проведения и количество одновременных потоков для тестирования. Далее нажать кнопку «Собрать статистику»;

– очистка. При нажатии кнопки «Очистить» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «Да»;

– удаление. При нажатии на кнопку «Удалить» запускается мастер «Удаление LUNs», где необходимо нажать на кнопку «Да», чтобы удалить данный LUN, или нажать на кнопку «Отмена» для отказа от операции.

Если LUN используется в GFS2, то сначала надо очистить и удалить пул данных GFS2, созданный на нем, отмонтировать LUN со всех узлов, и лишь потом его удалять.

Если LUN используется в ZFS-пуле, то сначала надо удалить LUN из состава ZFS-пула, и лишь потом его удалять.

Если LUN напрямую подключен к ВМ, то сначала надо отключить его от ВМ, и лишь потом удалять.

3.9.10.4. Во вкладке «Информация» содержатся параметры блочного устройства:

– путь;

– устройство dev (при присоединении к ВМ);

– тип шины (при присоединении к ВМ);

– размер (в Гбайтах);

– тип ФС;

– тип кэширования;

– статус;

– хранилище;

– серийный номер;

– присоединенная ВМ;

– репликация LUN;

– количество серверов (раскрывающийся список). Для каждого сервера указаны IP-адрес, статус «примонтирован» или «не примонтирован» и путь к LUN.

Примечание. LUN может быть доступен по нескольким путям (source). Например, на одном сервере может быть доступен по одному пути, на другом – по шести путям;

– дата и время создания;

– дата и время изменения.

3.9.10.5. Во вкладке «События» отображаются зарегистрированные в системе события, связанные с работой выбранного хранилища, с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.9.10.6. Во вкладке «Теги» имеется возможность добавления к хранилищу отличительной метки (тега), применения и обновления тега.

3.9.10.7. Ниже приведены варианты использования LUN:

1) присоединение LUN напрямую к ВМ. Необходимо перейти в окно «Виртуальные машины» – <имя ВМ> – «LUN» и подключить блочное устройство (LUN) с iSCSI target или оптическую сеть блочного доступа (FC) напрямую к ВМ в качестве диска ВМ (НЖМД). Надо учитывать, что при потере связи ОС ВМ будет реагировать аналогично аварийному извлечению НЖМД.

Для подключения LUN необходимо в окне управления LUN нажать кнопку «Присоединить» и в открывшемся окне выбрать из раскрывающегося списка iscsi-хранилище, LUN, тип шины («virtio», «ide», «scsi» или «sata») и тип кэширования («default», «none», «writethrough», «writeback», «directsync» или «unsafe»). Далее подтвердить операцию, нажав кнопку «ОК».

Примечание. При этом нужно учитывать, что файловую систему присоединенного LUN надо контролировать средствами ОС вашей ВМ;

2) создание LVM_shared на LUN. Необходимо выполнить следующее:

– создать пул данных типа «lvm_shared» на LUN в соответствии с 3.9.3 данного руководства.

Примечание. LVM_shared пул доступен только на узле, на котором его создали, то есть ВМ не могут быть перемещены «наживую»;

– создать диски на пуле данных в соответствии с 3.9.5 данного руководства;

3) создание ZFS-пула на LUN. Необходимо выполнить следующее:

– создать ZFS-пул на LUN в соответствии с 3.9.8 данного руководства.

Примечание. ZFS-пул доступен только на узле, на котором его создали, то есть ВМ не могут быть перемещены «наживую». Рекомендуется использовать несколько LUN или локальных дисков для отказоустойчивости ZFS-пула. Также рекомендуется использовать отдельные диски или LUN для кеша ZFS-пула для большей производительности;

– создать пул данных типа ZFS на ZFS-пуле в соответствии с 3.9.3 данного руководства;

– создать диски на пуле данных в соответствии с 3.9.5 данного руководства;

4) создание GFS2 на LUN.

Необходимо выполнить следующее:

– создать кластерный транспорт GFS2 в соответствии с 3.9.10 данного руководства.

Примечание. В кластере должно быть не менее двух узлов (рекомендуется минимум три);

– отформатировать LUN в нужную файловую систему GFS2 в соответствии с 3.9.9 данного руководства;

– примонтировать LUN в соответствии с 3.9.9 данного руководства;

– создать пул данных типа GFS2 на этом LUN в соответствии с 3.9.3 данного руководства;

– создать диски на пуле данных в соответствии с 3.9.5 данного руководства.

3.9.11. Кластерные хранилища

3.9.11.1. Кластерные транспорты

3.9.11.1.1. Кластерные транспорты – это общее название для кластерных (OCFS2, GFS2) и распределенных (Gluster) транспортов.

3.9.11.1.2. Для создания кластерного транспорта необходимо перейти в раздел «Хранилища» – «Кластерные хранилища» – «Кластерные транспорты» основного меню и в рабочем окне нажать кнопку «Создать». В открывшемся окне необходимо заполнить следующие поля:

– название;

– описание;

– кластер, на узлах которого будет развернут кворум (выбор из раскрывающегося списка);

– тип транспорта (выбор из раскрывающегося списка);

– LUN (выбор из раскрывающегося списка);

– внешняя сеть, физическая сеть которой будет использована для обмена данными между участниками кворума. Если опция включена, то выбрать внешнюю сеть из раскрывающегося списка.

После внесения изменений необходимо подтвердить операцию, нажав кнопку «Создать».

3.9.11.1.3. Для создания общего(их) для кластера пула(ов) данных GFS2 на LUN(s) необходимо выполнить:

– создать сетевое блочное iSCSI или FC хранилище. Проверить, что оно доступно на всех узлах кластера. Проверить, что его LUN(s) видны на всех узлах кластера. Подробности смотрите в блочных хранилищах 3.9.9.2;

– настроить IPMI. Перед созданием GFS2 транспорта необходимо убедиться в наличии IPMI-настроек ВСЕХ серверов кластера (см. 3.6.7.2). Через IPMI будет вестись ограждение узлов кворумом. При отсутствии IPMI-настроек хотя бы одного сервера кворум будет вести ограждение только через контроллер, и нельзя будет на 100 % быть уверенным в отсутствии «Split Brain» при всех возможных ситуациях потери связи с узлами;

– создать внешнюю сеть (необязательный шаг). Трафик между узлами для типа GFS2 крайне мал, так как они в рамках кворума обмениваются лишь «heartbeat», то есть использование внешней сети рекомендуется, но не является критическим условиям устойчивой работы;

– создать кластерный транспорт GFS2. Для удобства можно выбрать LUN, который будет сразу отформатирован, примонтирован, и на нем будет создан пул данных. В дальнейшем можно отформатировать, примонтировать и создать пул данных на других LUN.

3.9.11.1.4. Для создания общего(их) для кластера пула(ов) данных GFS2 на LUN(s), если уже есть кластерный транспорт GFS2, необходимо выполнить:

– отформатировать LUN в файловую систему GFS2;

– примонтировать LUN (он должен примонтироваться на всех узлах кластера с транспортом);

– создать пул данных GFS2 на этом LUN.

3.9.11.1.5. При наличии платы «watchdog» в BMC сервер будет следить за своим состоянием через него.

При отсутствии платы при включении сервера будет активирован программный «watchdog» («softdog»). Просмотр и управление «watchdog» происходит в CLI командой

*system watchdog **

В работе GFS2 участвует большое количество сервисов на каждом узле:

1) «watchdog» (описание в 3.9.11.1.13);

2) «corosync». Зависит от «watchdog». Отвечает за общение серверов друг с другом по сети. При создании или реконфигурировании кластерного транспорта обновляется конфигурационный файл «corosync» по пути «/etc/corosync/corosync.conf» и рестартуется этот сервис. Для узлов типа «Node» назначается одна квота, для узлов типа «Controller+Node» две квоты. То есть, например, если кластер состоит из 20 узлов без контроллеров, то будет всего 20 квот. Если, например, кластер состоит из двух узлов, один из которых контроллер, а другой узел, то всего будет три квоты. Для кворума необходимо минимальное значение, равное «общее количество квот / 2 + 1». Если будет меньше, то кворум прекратит работу и будет ожидать, когда количество квот достигнет минимально нужного значения;

3) «dlm». Занимается блокировками файловой системы и запуском ограждения узлов. Зависит от «corosync». Ограждение узлов ведется двумя способами:

– ограждение через API контроллера;

– ограждение через IPMI узла.

То есть сервис «dlm», если видит, что узел выпал из кворума, пытается его оградить. Для этого он делает API запросы попыток ограждения на SpaceVM контроллер, а при наличии IPMI пытается перезагрузить узел.

3.9.11.1.6. В кластере для создания транспорта типа Gluster должно быть не менее двух узлов, в остальных случаях не менее трех узлов. При создании транспорта типа Gluster на двух узлах надо осознавать, что такая конфигурация влечет за собой теоретическую возможность ситуации, когда узлы не могут определить мастера при потере сетевой связности (split-brain), а значит могут писать данные в одно место.

При создании транспорта типа OCFS2 и GFS2 на двух узлах надо осознавать, что такая конфигурация влечет за собой теоретическую возможность ситуации, когда оба узла будут ограждены.

Рекомендуется использовать отдельную от сети управления внешнюю сеть. После создания транспорта без использования внешней сети необходимо убедиться с помощью кнопки «Получение расширенных сведений о транспорте», что связь узлов идет через UUID узлов, а с использованием внешней сети через UUID узлов плюс имя внутреннего интерфейса. С помощью команды «hosts» на любом узле можно удостовериться, что UUID узла плюс имя внутреннего интерфейса соответствует IPv4-адресу интерфейса.

3.9.11.1.7. Трафик между узлами для типа OCFS2 крайне мал, так как они в рамках кворума обмениваются лишь «heartbeat», то есть использование внешней сети рекомендуется, но не является критическим условиям устойчивой работы.

Дополнительную информацию про работу OCFS2 можно получить по ссылкам *https://community.oracle.com/tech/apps-infra/discussion/4417713/ocfs2-best-practices-guide* и *https://raw.githubusercontent.com/markfasheh/ocfs2-tools/master/documentation/ocfs2_faq.txt.*

Серверы транспорта OCFS2 постоянно опрашивают друг друга по сети для поддержки кворума и через хранилища (LUN). Когда кворум теряет сервер из вида по причине недоступности его по сети или через хранилища, сервер автоматически перезагружается во избежание проблем с сетевой связностью (split-brain).

3.9.11.1.8. Для получения информации о транспорте необходимо нажать на его название. В окне состояния транспорта отображаются сведения о нем, разделенные на группы:

– информация;

– события;

– теги.

3.9.11.1.9. Управление работой транспорта происходит в окне состояния, где доступны следующие операции:

– удаление;

– переконфигурирование (добавление новых серверов кластера);

– получение расширенных сведений о транспорте;

– получение расширенных сведений о транспорте со всех узлов.

3.9.11.1.10. Вкладка «Информация» содержит следующие сведения о транспорте:

– название (редактируемый параметр);

– описание (редактируемый параметр);

– кластер;

– тип;

– статус;

– даты создания;

– дата обновления;

– серверы со статусами (раскрывающийся список).

3.9.11.1.11. Вкладка «События» содержит сообщения о работе транспорта с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений.

3.9.11.1.12. Вкладка «Теги» содержит список присвоенных транспорту меток. Также имеется возможность обновления, создания и применения тега.

3.9.11.1.13. Для работы кластерных транспортов OCFS и GFS2 требуется наличие устройства «/dev/watchdog». Появление этого устройства в системе зависит от того, загружен ли один правильный из множества вариантов модуль ядра для разных возможных плат BMC. SpaceVM автоматически при загрузке, раз в сутки или по требованию администратора, проверяет наличие устройства и, при его отсутствии, пытается последовательно загрузить модули «ipmi-watchdog», «iTCO_wdt», «softdog». После каждой попытки проверяется наличие устройства, если оно есть, дальше попытки не ведутся.

Указанный порядок, с нашей точки зрения, является наиболее универсальным для тех серверов, которые подвергались тестированию. При необходимости стоит выбирать подходящий для своего сервера модуль.

Управлять «watchdog» можно в CLI командой

*system watchdog *.*

3.9.11.1.14. Для добавления (удаления) узлов от кластерного транспорта GFS2 необходимо:

– если узел, который нужно удалить, активен, то перевести его в сервисный режим;

– нажать кнопку «Переконфигурирование» у кластерного транспорта.

Что произойдет:

– возьмутся все активные узлы кластера;

– на всех активных узлах пропишется новая конфигурация «corosync» и «dlm»;

– на всех активных узлах сервисы «corosync» перепрочитают конфигурацию.

3.9.11.2. Тома

3.9.11.2.1. Для создания тома необходимо перейти в раздел «Хранилища» – «Кластерные хранилища» – «Тома» основного меню и в рабочем окне нажать кнопку «Создать». В открывшемся окне необходимо заполнить следующие поля:

– название;

– описание;

– тип тома («Распределенный» или «Дисперсный»);

– кластерный транспорт, на узлах которого будет развернут том (выбор из раскрывающегося списка);

– ZFS-пулы (выбор из раскрывающегося списка);

– размер записи (выбор из раскрывающегося списка);

– значение репликации тома;

– включить (выключить) опцию «Наличие раздела арбитра в реплицированном томе»;

– включить (выключить) опцию «Создать пул данных».

После внесения изменений необходимо подтвердить операцию, нажав кнопку «ОК».

Примечание. После создания том будет сразу примонтирован на всех узлах кластерного транспорта. После примонтирования будет создан пул данных с тем же именем, что и том.

3.9.11.2.2. Пошаговое описание создания пула данных типа Gluster заключается в следующем:

– создаем внешнюю сеть на узлах кластера на отдельных физических интерфейсах или бондах, создавая внутренние интерфейсы на каждом узле;

– создаем кластерный транспорт с указанием внешней сети;

– создаем ZFS-пулы на узлах кластера;

– создаем том, выбирая кластерный транспорт и ZFS-пулы;

– создаем пул данных типа Gluster, указывая том.

ВНИМАНИЕ! При создании тома или замене разделов тома рекомендуется использовать заново созданные ZFS-пулы, а не использовать имеющиеся повторно. Это связано с особенностями очистки ZFS-пулов перед созданием тома или заменой разделов. То есть, если в системе имеются ZFS-пулы, использовавшиеся ранее под ZFS-датапул или том Gluster, лучше удалить их и собрать заново перед использованием.

Рекомендации:

1. Подробную информацию по томам можно прочитать на официальном сайте Gluster *https://docs.gluster.org/en/latest/.*

2. Подробно описанные рекомендации по томам можно прочитать по ссылке *https://rajeshjoseph.gitbooks.io/test-guide/content/appendices/chap-Recommended_Configuration_Dispersed_Volumes.html*.

3. Не рекомендуется использовать «management» сеть для томов.

4. Рекомендуется иметь пропускную способность не менее 10 GbE для сети хранилищ.

5. Рекомендуется сразу поднять MTU физических интерфейсов до значения «9100».

6. Рекомендуется создавать ZFS-пулы типа «mirror» с учетом ARC кэша, L2ARC, ZIL (см. описание в 3.9.8).

3.9.11.2.3. Управление работой тома происходит в окне состояния, которое открывается при нажатии на название тома. В окне состояния тома доступны следующие операции:

– удаление;

– монтирование;

– размонтирование;

– статус подорожника. Более подробную информацию можно прочитать по ссылке *https://docs.gluster.org/en/latest/Administrator-Guide/Managing-Volumes/#triggering-self-heal-on-replicate;*

– действия подорожника («enable», «disable » или «full »);

– статус ребалансировки;

– действия ребалансировки («старт» или «стоп»);

– действия («старт» или «стоп»);

– получение расширенных сведений о томе.

3.9.11.2.4. В окне состояния тома отображаются сведения о нем, разделенные на группы:

– информация;

– разделы (ZFS-пулы);

– события.

3.9.11.2.5. Вкладка «Информация» содержит следующие сведения о томе:

1) название;

2) описание (редактируемый параметр);

3) кластерный транспорт;

4) тип;

5) объем дискового пространства (всего, занято, свободно);

6) статус;

7) Gluster-статус;

8) дата и время создания;

9) дата и время обновления;

10) опции тома:

– наличие раздела арбитра в реплицированном томе;

– число разделов (ZFS-пулов) в томе, тип тома «dispersed»;

– число разделов данных (ZFS-пулов) в «dispersed» томе;

– путь монтирования тома;

– число разделов избыточности (ZFS-пулов) в «dispersed» томе;

– значение репликации тома;

11) серверы кластера со статусами связи и монтирования (раскрывающийся список).

3.9.11.2.6. Вкладка «Разделы (ZFS пулы)» позволяет управлять разделами:

– добавить раздел;

– заменить раздел;

– остановить раздел;

– удалить раздел.

3.9.11.2.7. Вкладка «События» содержит сообщения о работе тома с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений.

3.9.11.2.8. Том состоит из одного или более подтомов (subvolumes), их число указано в параметре «distribute» готового тома. Каждый подтом в данном томе имеет одну и ту же структуру, может быть реплицированным либо дисперсным. Простейшая структура тома Gluster – это один подтом из одного раздела.

3.9.11.2.9. Типы Gluster-томов и их основные отличия приведены ниже:

1) распределенный (distributed) том – примерный аналог JBOD или RAID-0 массива. Не обладает избыточностью и какой-либо защитой от сбоев на уровне Gluster.

При отказе хотя бы одного из разделов данные могут стать недоступны на всем томе. Может быть составлен из разделов (bricks) различающегося объема, при этом объем разделов используется полностью.

Это самый «легкий» тип тома в плане требуемой вычислительной мощности и сетевого трафика. В свойствах распределенного тома отображается значение репликации «1». При этом том создается с указанием значения репликации «0».

Это самый быстрый том. Если отдельные подтома (subvolumes, составляющие том разделы) располагаются на разных узлах, то случайный обмен данными с томом делится между дисковыми подсистемами узлов, хранящих разделы, что положительно влияет на производительность.

Добавлять разделы к распределенному тому можно двумя способами:

– с увеличением размера, в этом случае нет требований к размерам и числу добавляемых разделов;

– с повышением реплики, в этом случае следует указывать новое значение реплики и учитывать распределение разделов в подтомах данного тома по размерам, а число разделов должно быть равно <*числу разделов в исходном томе*> *x* <*изменение реплики*>. В результате образуется распределенный реплицированный том.

Примечание. Если при добавлении разделов к тому параметр реплики не указан (равен «0»), то «по умолчанию» производится увеличение размера тома (увеличивается параметр «distribute»).

2) реплицированный (replicated) том – аналог MIRROR (RAID-1) массива. Обладает N-кратной избыточностью, где N – параметр репликации. Технически сохраняет работоспособность при отказе N-1 реплик. Фактически поведение тома зависит от настроек кворума. Подробнее о кворуме можно прочитать по ссылке *https://rajeshjoseph.gitbooks.io/test-guide/content/features/arbiter-volume-and-quorum.html.*

При составлении реплик из разделов разного объема эффективный объем тома равен объему наименьшего раздела в реплике. При записи на том генерируется N-кратный трафик в сети, объединяющей разделы.

Добавлять разделы к реплицированному тому можно двумя способами:

– с увеличением размера и сохранением параметра репликации, в этом случае число разделов должно быть кратно параметру репликации. Этот режим выбирается «по умолчанию», если не указывать новый параметр репликации;

– с сохранением размера и увеличением параметра репликации. При этом не следует добавлять разделы размером меньше уже составляющих том;

3) реплицированный том с арбитром – является компромиссным решением между вариантом с репликой «2», подверженной проблеме «split-brain» в случае потери связи между разделами, и репликой «3», требующей трехкратного объема хранилища по отношению к полезному объему тома. В этом случае реплика равна «3», но на последнем томе реплики хранится только метаинформация о файлах и каталогах, а не их содержимое. Такой том называется арбитром. Это позволяет в случае нарушения связности между узлами избежать проблемы «split-brain» и сэкономить дисковый объем. Для создания реплицированного тома с арбитром следует указать при создании тома значение реплики «2», а значение арбитра в реплицированном томе равным «1». Порядок следования разделов при создании тома описан в 3.9.11.2.10 данного руководства.

Добавление разделов к реплицированному тому с арбитром возможно только в режиме увеличения размера. При этом можно оставить значения «по умолчанию». Увеличивать значение реплики в таком томе нельзя.

Примечание. Возможно создать реплицированный том с арбитром из реплицированного тома с параметром реплики «2». При этом следует указать реплику «3», наличие арбитра «1», а число разделов должно быть равно параметру «distribute» исходного тома;

4) распределенный реплицированный (distributed replicate) том – является по сути репликой распределенных томов (примерный аналог RAID10). Обладает так же, как и реплицированный, N-кратной избыточностью. Сохраняет работоспособность, пока исправна минимум одна реплика.

При создании томов такого типа из разделов разного размера следует учесть, что общий объем тома будет определяться суммой минимальных объемов разделов в репликах каждого из подтомов (см. 3.9.11.2.10). При записи генерирует так же, как и реплицированный том, N-кратный трафик в сети, связывающей разделы.

Для создания тома такого типа следует указать значение реплики и выбрать число разделов, кратное этому значению. К примеру, при указании реплики «2» и всего шести разделов будет создан том со значениями «replica = 2», «distribute = 3». Если нужно создать распределенный реплицированный том с арбитром, то значение реплики нужно указать «2», значение арбитра «1», а число томов кратным «3». При этом каждый третий раздел будет являться арбитром, следовательно, это может быть раздел существенно меньшего размера.

Ниже приведен пример создания распределенного реплицированного тома из шести разделов с арбитром.

Пусть у пользователя есть четыре ZFS-пула размером 1 Тбайт (zp_1T_0 ... zp_1T_3) и два ZFS-пула размером 40 Гбайт (zp_40G_0, zp_40G_1). Тогда для создания нужного тома можно выбрать ZFS-пулы в такой последовательности (условно, важно, чтобы разделы 40 Гбайт попали в последнюю реплику) – zp_1T_0 zp_1T_1 zp_40G_0 zp_1T_2 zp_1T_3 zp_40G_0. Значение реплики выберем равным «2», а значение арбитра равным «1». Тогда после создания тома в закладке «Расширенные сведения о томе» пользователь увидит роль разделов zp_1T_0, 1, 2, 3 – 'Brick', а zp_40G_0, 1 – 'Arbiter'. Суммарная емкость тома будет равна 2 Тбайт;

5) дисперсный (dispersed) том – является примерным аналогом RAID-5, 6, raidz1, 2 или выше в зависимости от числа разделов избыточности. Сохраняет работоспособность при отказе до R разделов, где R – значение избыточности (disperse redundancy), заданная при создании тома.

Объем тома в случае одинаковых размеров разделов равен «D x Vрзд», где D – число разделов с данными (disperse data).

Имеет преимущество перед реплицированным томом в более эффективном расходе дискового пространства, но более активно использует мощность CPU-узлов и сравнимо генерирует трафик, так как для записи некоторого объема данных на этот том требуется считывание D-1 объемов данных, вычисление и запись R-объемов данных коррекции ошибок (избыточности). В сочетании с нагрузкой на CPU-узлов при использовании raidz для защиты от отказов отдельных накопителей, составляющих разделы, может создаваться видимая загрузка CPU-узлов.

При создании дисперсного тома из разделов разного размера общий объем тома равен «D x Vmin», где Vmin – минимальный размер из всех разделов тома. При создании распределенного дисперсного тома это справедливо для каждого подтома в отдельности.

Для создания дисперсного раздела нужно задать список разделов и любые из параметров:

– N – общее число указанных для создания тома разделов, «по умолчанию» – «0»;

– Nt – число разделов на дисперсный том, «по умолчанию» – «0»;

– D – число разделов данных в дисперсном томе, «по умолчанию» – «0»;

– R – число разделов избыточности, «по умолчанию» – «1».

Число разделов на дисперсный том Nt берется равным N. Указывается в случае создания дисперсного распределенного тома. В этом случае задается кратно меньшим N, при этом степень кратности будет равняться параметру «distribute» в полученном томе.

Число разделов данных в дисперсном томе D берется равным Nt-1.

Если какие-то параметры заданы явно, то остальные вычисляются автоматически.

Ниже приведены примеры создания дисперсных томов.

Пусть имеется восемь разделов объемом по 1 Тбайт:

а) зададим параметры «по умолчанию», кроме числа разделов данных на дисперсный том равное «8». Тогда получим том объемом 7 Тбайт, переносящий потерю любого одного раздела;

б) из этих восьми разделов создадим том с параметром «Nt = 4», прочие параметры «по умолчанию».

Тогда получим том 6 Тбайт, состоящий из двух подтомов (первая и вторая группа по четыре раздела в списке разделов при создании тома) и переносящий потерю любого раздела в каждом из подтомов;

в) из этих разделов создадим том с параметром «D = 5», прочие параметры «по умолчанию». Получаем том объемом 5 Тбайт, переносящий отказ до трех любых разделов в томе.

Примечания:

1. При добавлении разделов к дисперсному тому их число должно быть кратно сумме параметров D + R, при этом образуется дисперсный распределенный том.

2. Существует понятие оптимальности конфигурации дисперсного тома. Дело в зависимости размера блоков обмена данными при обращениях к тому от конфигурации тома. Она равна «S = D x 512 байт», где D – число разделов с данными в дисперсном томе. Оптимальной считается конфигурация тома, при которой размер блока данных является степенью двойки (то есть 512, 1024, 2048, 4096, 8192, ... байт). Следовательно, оптимальным числом разделов с данными в томе будет 2, 4, 8, … разделов. К этому числу нужно прибавить число разделов для обеспечения требуемой избыточности. Например, для стойкости к потере 1 раздела и оптимальности конфигурации нужно иметь в томе 3 (2+1), 5 (4+1), 9 (8+1), … разделов. Если конфигурация будет неоптимальной, производительность тома будет понижена из-за того, что в основном обмен идет блоками размером, кратным степени двойки (например, кратными 4096 байт). Если требуемые или отдаваемые клиентом блоки не будут кратны блокам, отдаваемым хранилищем, то на каждую операцию будет приходиться фактически две или более операции обмена с томом, в случае записи это приводит к множеству дополнительных, так называемых, «read-modify-write» операций. Поэтому при создании дисперсного тома следует стремиться к оптимальной конфигурации;

6) распределенный дисперсный (distributed disperse) том – примерный аналог RAID60. Состоит из нескольких дисперсных томов, объединенных наподобие разделов в распределенном томе. Получается при добавлении разделов к дисперсному тому либо при создании дисперсного тома, когда значение <число разделов данных в дисперсном томе> кратно меньше заданного числа разделов.

3.9.11.2.10. Важно учитывать выбор последовательности разделов при создании и модификации тома.

Разделы, составляющие распределенный том, называются подтомами (subvolumes). Это, по большей части, неявный параметр, но он имеет большое значение для реплицированных томов с арбитром и распределенных реплицированных томов. Какой раздел отнесется к какой реплике и в каком подтоме он будет находиться, однозначно определяется порядком указания разделов при создании. В распределенном реплицированном томе с k-подтомов (*distribution* = *k*) и n-реплик (*replica* = *n*) это задается так:

S1R1 S1R2 … S1Rn S2R1 S2R2 … S2Rn … SkR1 … SkRn,

где S1…Sk – subvolumes тома;

R1...Rn – номер реплики.

То есть, как видим, друг за другом указываются реплики одного подтома. Соответственно, если создается распределенный реплицированный том из разделов различной емкости или том с арбитром, нужно учитывать это. В одном подтоме желательно располагать разделы одинаковой емкости, чтобы избежать неиспользуемого объема, а в одной реплике – разделы из одного узла, если такие имеются, что обеспечит отказ только одной реплики при отказе какого-либо из узлов.

ВАЖНО помнить, что добавление разделов к томам нужно производить с установленным движком «Принудительное добавление», иначе задача завершится с ошибкой.

3.9.11.2.11. Краткое резюме:

– простейший ненадежный тип тома – аналог JBOD – распределенный (distributed);

– простейший тип тома с избыточностью, неэффективный по объему – аналог MIRROR – реплицированный (replicated);

– более эффективный по объему – реплицированный с арбитром;

– самый продвинутый – аналог RAID5,6 – дисперсный (dispersed).

3.9.11.2.12. При профилировании томов используются следующие команды:

– *gluster volume profile {volume_name} start* – для запуска профилирования;

– *gluster volume profile {volume_name} info* – для получения информации о томе (перед запуском этой команды надо подождать после команды старта);

– *gluster volume profile {volume_name} stop* – для окончания профилирования.

3.9.11.2.13. При создании к тому автоматически применяются дополнительные оптимизирующие опции.

Операция производится в несколько этапов:

1) сначала к тому применяется одна из стандартных (поставляемых разработчиками «Gluster») групп опций в зависимости от типа тома:

– распределенный том – группа «distributed-virt»;

– реплицированный том – группа «virt»;

– дисперсный том – группа «dispersed-virt» (модифицированная группа «virt» без параметра «cluster.shd-max-threads»);

2) далее к тому применяется группа параметров SpaceVM (см. ниже);

3) также отключается опция тома «sharding», так как она может в данной версии «Gluster» приводить к повреждению данных;

4) вручную группы можно применить к уже созданным томам, зайдя в CLI любого сервера, на котором развернут «gluster»-том, и выполнить команды (к примеру, для распределенного тома):

gluster volume set {volume_name} group distributed-virt

gluster volume set {volume_name} group virt

gluster volume set {volume_name} features. shard o

Примечание. Важно отключить «sharding» после установки групп, так как предустановленные группы («virt», «distributed-virt», «dispersed-virt») могут его включить.

В случае создания реплицированного тома с арбитром устанавливается параметр

gluster volume set {volume_name} server-quorum-type server

Подробнее о параметрах и группах параметров томов можно посмотреть по ссылке

https://rajeshjoseph.gitbooks.io/test-guide/content/cluster/chap-Managing_Gluster_Volumes.html.

Опции группы SpaceVM:

– *performance. quick-read=o;*

– *performance. read-ahead=o;*

– *performance.io-cache=o;*

– *performance.low-prio-threads=32;*

– *network. remote-dio=disable;*

– *performance.strict-o-direct=on;*

– *cluster.eager-lock=enable;*

– *cluster.quorum-type=none;*

– *cluster.server-quorum-type=none;*

– *cluster.data-self-heal-algorithm=full;*

– *cluster.locking-scheme=granular;*

– *user.cifs=off;*

– *cluster.choose-local=off;*

– *client.event-threads=4;*

– *server.event-threads=4;*

– *performance.client-io-threads=on;*

– *network.ping-timeout=20;*

– *server.tcp-user-timeout=20;*

– *server.keepalive-time=10;*

– *server.keepalive-interval=2;*

– *server.keepalive-count=5;*

– *cluster.lookup-optimize=off*

3.9.11.2.14. В некоторых случаях возможно сократить размер тома или его избыточность путем удаления части разделов из тома.

Сокращение размера тома возможно при наличии более чем одного подтома (distribute > 1), следовательно, применяется на томах типа «distributed», «distributed_replicate», «distributed_disperse». Перед удалением следует убедиться, что свободного места на оставшихся подтомах достаточно, чтобы вместить данные с удаляемого подтома. Также важно понимать, что так как каждый файл, хранящийся на томе Gluster в текущей конфигурации, хранится целиком на каком-либо подтоме, то при конфигурации, например, когда на удаляемом подтоме лежит файл размером 40 Гбайт, а на двух оставшихся есть 20 и 20 Гбайт свободного места, операция удаления завершится с ошибкой. Следует обеспечить свободное место, достаточное для копирования файлов с удаляемого подтома целиком.

При удалении разделов с уменьшением объема раздела значение репликации нужно оставить равным «0» или текущему значению репликации тома (в случае дисперсного тома значение репликации смысла не имеет, поэтому его следует оставить равным «0»), а при удалении разделов с уменьшением числа реплик (уменьшением избыточности) у реплицированных томов значение репликации нужно установить равным результирующему значению репликации тома.

Для правильного выбора разделов, подлежащих удалению, см. 3.9.11.2.10. Фактический порядок разделов в томе и, следовательно, их отношение к различным подтомам и расположение в них, можно увидеть по нажатию кнопки «Расширенная информация о томе».

Ниже приведены примеры томов:

1) том типа «distributed_replicate», параметры *replica=3, distribute=2*. Следовательно, имеется два подтома, каждый из них имеет значение реплики «3». Всего в томе шесть разделов.

Расположение разделов (из информации «Расширенных сведений о томе» – z1, z2, z3, z4, z5, z6.

Первый подтом состоит из разделов (z1, z2, z3), второй из (z4, z5, z6). Первая реплика подтомов состоит из разделов (z1, z4), вторая – из (z2, z4), третья (она же при наличии арбитра в томе содержит разделы арбитров) – (z3, z6).

Чтобы уменьшить размер тома, следует удалить какой-либо из подтомов целиком. Следовательно, возможно выбрать к удалению тройки разделов (z1, z2, z3) или (z4, z5, z6). При этом тип тома изменится на «replicated», так как в нем останется только один подтом.

Чтобы уменьшить степень избыточности тома, следует выбрать пары разделов из разных подтомов. В зависимости от наличия или отсутствия арбитра в томе возможны два варианта:

– если нет арбитра, разделы в пределах подтома равноправны. То есть, если нет арбитра, то для уменьшения реплики можно выбрать по одному любому разделу из разных подтомов, например, пары (z1, z5), или (z2, z4), или (z3, z4);

– в случае тома с арбитром ситуация меняется. Разделы типа «arbiter», являющиеся третьими репликами в каждом подтоме (в нашем случае это будут разделы z3 и z6), при удалении нужно выбирать только синхронно.

То есть, если в этом случае нужно удалить разделы с данными, то они по-прежнему равноправны между собой в пределах подтома, и можно выбрать пары (z1, z4), или (z2, z4), или (z1, z5). А разделы (z3 и z6), являющиеся арбитрами, следует удалять только синхронно. Комбинации (z1, z6), или (z4, z3), или подобные недопустимы в данном случае;

2) том типа «distributed_disperse» с параметрами «disperse = 3», «distribute = 2». Содержит 2 подтома дисперсного типа «2+1». Всего в томе 6 разделов.

Расположение разделов (из информации «Расширенных сведений о томе») – z1, z2, z3, z4, z5, z6.

Дисперсные тома не поддерживают изменение избыточности, поэтому здесь возможно только удаление разделов с уменьшением размера, то есть удаление подтома целиком. Следовательно, при удалении нужно выбирать только тройки разделов (z1, z2, z3) или (z4, z5, z6). При этом том превратится в тип «dispersed», так как в нем останется только один подтом.

ВНИМАНИЕ! После уменьшения размера тома путем удаления разделов, если результирующий том имеет более 1 подтома, желательно запустить ребалансировку тома.

3.9.11.2.15. В случае проблем с каким-либо ZFS-пулом, используемым под раздел тома Gluster, возможно временно «вывести из эксплуатации» данный раздел (при наличии избыточности у тома), провести необходимые работы, включая удаление неисправного ZFS-пула, а затем заменить остановленный раздел на исправный.

Если нужно произвести замену раздела, и заменяющий раздел уже доступен, тогда во вкладке «Разделы (ZFS пулы)» выбрать действие «Замена раздела», где указать заменяемый и заменяющий разделы.

Если раздела для замены заранее нет, то заменяемый раздел можно остановить путем выбора действия «Остановка раздела» во вкладке «Разделы (ZFS пулы)», после чего при необходимости можно удалить ZFS-пул, составляющий данный раздел, пересобрать его с другим именем, а затем выполнить «Замену раздела», где заменяемый раздел будет уже остановленный и может быть удаленный, а заменяющий – вновь полученный исправный раздел.

Остановленный раздел можно привести обратно в состояние «Online» либо перезапуском тома по кнопке «Действия тома», далее «стоп» – «старт», либо если остановка тома недопустима, заменой раздела на другой.

ВНИМАНИЕ! После замены разделов следует проверить исправность данных на томе по кнопке «Статус подорожника» тома. Значение NR_ENTRIES для всех разделов должно быть равным «0», а все разделы должны быть в состоянии «Connected». В случае, если значения NR_ENTRIES для какого-либо раздела через несколько минут после замены не становятся равным «0», следует провести лечение тома по кнопке «Действия подорожника», далее «full», а в случае неудачи перезапустить том.

Примечания:

1. При отсутствии избыточности у тома замена раздела может в некоторых случаях пройти успешно, однако в связи с непредсказуемостью результата данное действие производить не рекомендуется, а сохранность данных даже в случае успешного завершения не гарантируется.

2. В некоторых случаях задача прямой замены раздела может сопровождаться ошибкой с сообщением «another transaction is in progress». В результате желаемое действие все равно завершается успешно, если же нет, то следует произвести замену с предварительной остановкой заменяемого раздела.

3. Попытка удалить ZFS-пул, содержащий раздел тома Gluster в состоянии «Online», завершится с ошибкой. Сначала раздел необходимо остановить.

4. Таблица разделов (ZFS-пулов) тома содержит два схожих поля – «Online» и «Статус». Первое поле указывает на состояние раздела с точки зрения тома Gluster, а второе – на исправность самого ZFS-пула.

3.9.12. NPIV

3.9.12.1. NPIV (N_Port ID Virtualization) – это технология Fibre Channel, позволяющая разбить физический адаптер (HBA) на виртуальные (VHBA). Каждый виртуальный адаптер идентифицируется своим уникальным именем порта (WWPN) и именем узла (WWNN), что позволяет со стороны хранилища идентифицировать их и привязать отдельный LUN на каждый VHBA.

3.9.12.2. Порядок действия для создания VHBA следующий:

– перейти в CLI сервера;

– командой *storage hba_npiv* просмотреть имеющиеся SCSI NPIV устройства. Удостовериться в поддержке устройством NPIV можно, посмотрев на наличие поля «max_vports» и его значение, отличное от «0»;

– создать VHBA командой *storage pool_create*, указав «name», «parent_fabric_wwn» и, при желании, «wwnn» и «wwpn»;

– на хранилище создать маппинг (соотвествие данных) LUNs к WWPN;

– пересканировать SCSI корзины узла командой *storage rescan_vhba*;

– увидеть появившиеся LUNs можно командой *storage fc_luns*;

– при необходимости перезагрузить сервер для обнаружения им новых LUNs;

– далее необходимо зайти в Web-интерфейс контроллера и просканировать блочные устройства сервера, и у найденного блочного хранилища просканировать LUNs;

– найденные LUNs можно присоединить к ВМ.

Удалить VHBA можно командой *storage pool_destroy*, указав «name».

Посмотреть VHBA можно командой *storage pools*.

3.9.13. ISCSI-сервер

ISCSI-сервер предназначен для предоставления доступа к хранилищам по TC/IP в виде блочных устройств LUN.

В разделе «Хранилища» – «ISCSI сервер» основного меню содержится интерфейс управления ISCSI storage и ISCSI target.

3.9.13.1. ISCSI storage

3.9.13.1.1. В ISCSI storage создаются хранилища на основе блочных устройств, доступных на узле, чтобы они были доступны в ISCSI target.

3.9.13.1.2. В окне ISCSI storage доступны следующие операции:

– обновление информации о всех ISCSI-хранилищах по кнопке  ;

– создать новое ISCSI-хранилище по кнопке «Создать»;

– открыть ISCSI-хранилище в списке.

При нажатии ISCSI-хранилища в списке открывается окно с информацией о нем, где доступны следующие операции:

– обновление информации о всех LUN, с которыми связано выбранное ISCSI-хранилище;

– удаление ISCSI-хранилища по кнопке «Удалить».

3.9.13.1.3. При нажатии кнопки «Создать» открывается окно с полями и чекбоксами, где необходимо указать:

– сервер, выбрать из раскрывающегося списка доступных узлов;

– локальные устройства, выбрать из раскрывающегося списка доступных блочных устройств на узле;

– readonly – флаг запрещающий запись, «по умолчанию» – выключен;

– write_back – кэш обратной записи, «по умолчанию» – включен.

После заполнения полей необходимо нажать кнопку «ОК», чтобы создать объект.

3.9.13.1.4. При нажатии кнопки «Удалить» открывается окно, где необходимо нажать «Да», чтобы удалить данный ISCSI storage, или нажать «Отмена» для отказа от операции.

Если ISCSI storage используется LUN, который в свою очередь используется Mapped LUN, то они тоже будут удалены.

3.9.13.1.5. Во вкладке «Информация» в окне объекта ISCSI storage содержатся параметры блочного устройства:

– локальное устройство (путь до устройства);

– plugin (так как сейчас поддерживаются только блочные устройства, то всегда «block»);

– status;

– устройства LUN (при присоединении к LUN).

3.9.13.2. ISCSI target

3.9.13.2.1. В ISCSI target непосредственно создается целевой ISCSI на основе доступных ISCSI-хранилищ, созданных во вкладке «ISCSI storage».

3.9.13.2.2. В окне ISCSI target доступны следующие операции:

– обновление информации о всех целях ISCSI по кнопке  ;

– создание новой цели ISCSI по кнопке «Создать»;

– сканировать информацию о ISCSI и его хранилищах с узла по кнопке «Сканировать»;

– открыть целевой ISCSI в списке.

При выборе целевого ISCSI открывается окно с информацией о нем, где доступны следующие операции:

– обновление информации о всех порт-группах, с которыми связан целевой ISCSI;

– удаление целевого ISCSI по кнопке «Удалить».

3.9.13.2.3. При нажатии кнопки «Создать» открывается окно, где необходимо заполнить следующие поля:

– сервер, выбрать из раскрывающегося списка доступных узлов;

– название;

– описание;

– WWN – уникальный идентификатор типа IQN.

После заполнения полей необходимо нажать кнопку «ОК», чтобы создать объект.

3.9.13.2.4. При нажатии кнопки «Удалить» запускается мастер, где необходимо нажать «Да», чтобы удалить данный ISCSI target, или нажать «Отмена» для отказа от операции.

При удалении целевого ISCSI удаляются все его порт-группы и другие объекты, связанные с ним, кроме ISCSI-хранилищ.

3.9.13.2.5. Во вкладке «Информация» в окне объекта ISCSI target содержатся параметры блочного устройства:

– название;

– wwn;

– tpgs_count (количество порт-групп);

– status.

3.9.13.2.6. Во вкладке «Порт-группы» доступны следующие операции:

– добавить новую порт-группу, нажав на кнопку «Добавить»;

– открыть порт-группу в списке порт-групп.

При нажатии кнопки «Добавить» открывается окно с полями и чекбоксами, где необходимо указать:

– tag – фактически является индексом объекта, уникальный номер для порт-группы в текущем целевом ISCSI в диапазоне от «1» до «255»;

– chap_userid – идентификатор пользователя;

– chap_password – пароль;

– chap_mutual_userid – идентификатор пользователя для двунаправленной аутентификации;

– chap_mutual_password – пароль для двунаправленной аутентификации;

– enable – флаг включения использования порт-группы, «по умолчанию» – включен;

– authentication – флаг включения аутентификации;

– generate_node_acls – добавляет автоматически узлы без необходимости добавления Node ACL.

После заполнения полей необходимо нажать кнопку «ОК», чтобы создать объект.

При нажатии кнопки «Удалить» запускается мастер, где необходимо нажать «Да», чтобы удалить данную порт-группу, или нажать «Отмена» для отказа от операции.

При удалении порт-группы удаляются дочерние объекты, связанные с ней – LUN, Node ACL, Portal, Mapped LUN.

Во вкладке «Информация» в окне объекта порт-группы содержатся следующие параметры:

– tag;

– chap_userid;

– chap_password;

– chap_mutual_userid;

– chap_mutual_password;

– enable;

– authentication;

– generate_node_acls.

3.9.13.2.7. Во вкладке «LUNs» доступны следующие операции:

– добавить новый LUN, нажав на кнопку «Добавить»;

– открыть объект LUN в списке.

При нажатии кнопки «Добавить» открывается окно, где необходимо выбрать storage из раскрывающегося списка доступных хранилищ ISCSI storage. После этого необходимо нажать кнопку «ОК», чтобы создать объект.

При нажатии кнопки «Удалить» запускается мастер, где необходимо нажать «Да», чтобы удалить данный LUN, или нажать «Отмена» для отказа от операции.

При удалении LUN удаляются связанные с ним Mapped LUN.

Во вкладке «Информация» в окне объекта LUN содержатся следующие параметры:

– index;

– storage_object (с полем «dev» содержит путь до блочного устройства);

– статус.

3.9.13.2.8. Во вкладке «Node ACLs» доступны следующие операции:

– добавить новый Node ACL, нажав на кнопку «Добавить»;

– открыть объект Node ACL в списке.

При нажатии кнопки «Добавить» открывается окно, где необходимо указать:

– node_wwn – имя инициатора ISCSI с узла клиента типа IQN;

– chap_userid – идентификатор пользователя;

– chap_password – пароль;

– chap_mutual_userid – идентификатор пользователя для двунаправленной аутентификации;

– chap_mutual_password – пароль для двунаправленной аутентификации.

После заполнения полей необходимо нажать кнопку «ОК», чтобы создать объект.

При нажатии кнопки «Удалить» запускается мастер, где необходимо нажать «Да», чтобы удалить данный Node ACL, или нажать «Отмена» для отказа от операции.

При удалении Node ACL удаляются связанные с ним Mapped LUN.

В окне объекта Node ACL содержатся следующие параметры:

– node_wwn;

– chap_userid;

– chap_password;

– chap_mutual_userid;

– chap_mutual_password;

– mapped_luns_count;

– tpg;

– статус.

В поле «mappend lun» находится кнопка добавления объекта «Mapped LUN add mapped lun».

Ниже находится список объектов Mapped LUN. В строке объекта присутствует кнопка «Удалить», запускающая мастер удаления.

При нажатии кнопки «add mapped lun» открывается окно с полями и чекбоксами, где необходимо указать:

– tpg_lun – имя инициатора ISCSI с узла клиента типа IQN;

– write_protect – запрет на запись с данного узла.

После заполнения полей необходимо нажать кнопку «ОК», чтобы создать объект.

При нажатии кнопки «Удалить» запускается мастер, где необходимо нажать «Да», чтобы удалить данный Mapped LUN, или нажать «Отмена» для отказа от операции.

3.9.13.2.9. Во вкладке «Portals» доступны следующие операции:

– добавить новый LUN, нажав на кнопку «Добавить»;

– открыть объект LUN в списке.

При нажатии кнопки «Добавить» открывается окно, где необходимо указать:

– ip_address – текстовое поле, в котором можно указать IP-адреса и сети;

– port – номер порта.

После заполнения полей необходимо нажать кнопку «ОК», чтобы создать объект.

При нажатии кнопки «Удалить» запускается мастер, где необходимо нажать «Да», чтобы удалить данный Portal, или нажать «Отмена» для отказа от операции.

Во вкладке «Информация» в окне объекта Portal содержатся следующие параметры:

– ip_address;

– port;

– tpg;

– iser (ISCSI Extensions for RDMA);

– offload;

– статус.

3.9.14. S3 объектное хранилище

3.9.14.1. Общая информация

3.9.14.1.1. От облачных решений для резервного копирования данных до обеспечивающих бесперебойную работу сетей доставки контента (CDN), возможность хранения неструктурированных больших бинарных объектов (blob) с возможностью доступа к этим объектам через HTTP API, известное как хранилище объектов, является неотъемлемой частью современной технологической среды.

3.9.14.1.2. MinIO – это популярный сервер хранения объектов с открытым исходным кодом, совместимый с облачным хранилищем Amazon S3 (подробности см. по ссылке *https://aws.amazon.com/ru/free/storage/?sc_channel=PS&sc_campaign=acquisition_US&sc_publisher=google&sc_medium=ACQ-P%7CPS-GO%7CBrand%7CDesktop%7CSU%7CStorage%7CS3%7CUS%7CEN%7CText&sc_content=s3_e&sc_detail=amazon%20s3&sc_category=Storage&sc_segment=293617570044&sc_matchtype=e&sc_country=US&s_kwcid=AL!4422!3!293617570044!e!!g!!amazon%20s3&ef_id=EAIaIQobChMI0JiSkYys5gIVRZyzCh3Y8wcFEAAYASAAEgLqg_D_BwE:G:s*).

Приложения, которые были настроены для связи с Amazon S3, могут также быть настроены для связи с MinIO, что позволяет MinIO служить жизнеспособной альтернативой S3, если пользователю потребуется более эффективный контроль сервера хранилища объектов.

Служба может хранить неструктурированные данные, такие как фото, видео, файлы журнала, резервные копии и образы контейнеров или виртуальных машин, и даже может предоставить один сервер хранения объектов, объединяющий в пул множество дисков, размещенных на разных серверах.

3.9.14.1.3. MinIO написана на языке Go, имеет клиент командной строки и интерфейс браузера и поддерживает простую службу очереди для расширенного протокола организации очереди сообщений (AMQP), Elasticsearch, Redis, NATS и PostgreSQL. По всем этим причинам знакомство с настройкой сервера хранения объектов MinIO может обеспечить большую гибкость и практическую пользу для пользвательского проекта.

3.9.14.2. MinIO Gateway NAS

3.9.14.2.1. Реализация MinIO Gateway NAS в SpaceVM заключается в удобном запуске сервиса MinIO поверх любого созданного в SpaceVM файлового пула данных (то есть всех типов, кроме LVM и thin-LVM). На пуле данных создается отдельный каталог «_MinIO» (например, «/storages/local/default/_MINIO»), где и будут лежать все объекты MinIO вместе с его служебной информацией. MinIO Gateway NAS будет развернут на всех активных узлах этого пула данных. То есть, если это локальный пул или ZFS-пул, то MinIO Gateway NAS будет развернут на одном узле, а если это NFS или Glusterfs, то он будет развернут на всех его активных узлах, обычно на всех узлах кластера.

3.9.14.2.2. После активации MinIO API будет доступно на порту «9400», а MinIO console – на порту «9401». Для удобства можно использовать MinIO console через URL *https://{server_address}/minio.*

Ограничения:

– только файловые пулы данных;

– максимум один пул данных на сервер.

3.9.14.3. Управление MinIO для пула данных SpaceVM

3.9.14.3.1. Ниже приведен пример включения (реконфигурации) MinIO для пула данных:

POST http(s)://<адрес контроллера>/api/data-pools/31129cca-f7de-4cc4-a89f-d79997ef15ec/minio-gateway/

{

"enabled": true,

"root_password": "ChangeMe",

"root_user": "admin"

}

3.9.14.3.2. Ниже приведен пример выключения MinIO для пула данных:

POST http(s)://<адрес контроллера>/api/data-pools/31129cca-f7de-4cc4-a89f-d79997ef15ec/minio-gateway/

{

"enabled": false

}

3.9.14.4. MinIO SSL

3.9.14.4.1. «По умолчанию» на каждом сервере SpaceVM при включении MinIO генерируются самоподписанные сертификаты в каталог «/etc/minio» (управлять этим можно через параметр «certgen» REST запроса). Пользователь может сам заменить эти сертификаты на свои.

Подробности смотрите по ссылке *https://docs.min.io/docs/how-to-secure-access-to-minio-server-with-tls.html.*

3.9.14.5. MinIO CLI

3.9.14.5.1. С MinIO идет утилита «mc», но так как SpaceVM также использует «mc» для Midnight Commander, то в SpaceVM «mc» переименована в «mcli» и доступна из CLI.

3.10. Сети

3.10.1. Краткое описание сетевой подсистемы SpaceVM

3.10.1.1. Данный раздел содержит описание построения и функционирования сетевой подсистемы SpaceVM, основных объектов, составляющих сетевую подсистему, их взаимодействия и доступные пользователю настройки. Сетевая подсистема построена на основе виртуальных коммутаторов, представляющих собой изолированные сетевые устройства на уровне ОС вычислительного узла.

ВК являются связующим звеном для других объектов сетевой подсистемы:

1) сетевых интерфейсов всех типов:

– физических интерфейсов вычислительного узла;

– агрегированных интерфейсов;

– внутренних (сервисных) интерфейсов;

– сетевых интерфейсов ВМ;

2) L2-туннелей.

Описание типов сетевых интерфейсов приведено ниже в данном разделе. Описание сетевых интерфейсов ВМ приведено в разделе «Виртуальные машины» (см. 3.8.15).

3.10.2. Основные объекты сетевой подсистемы

3.10.2.1. Виртуальные коммутаторы

3.10.2.1.1. ВК представляют собой виртуальные изолированные сетевые устройства на уровне ОС вычислительного узла. Используются для подключения к ним интерфейсов всех типов для построения сетевой инфраструктуры SpaceVM.

3.10.2.1.2. Виртуальные коммутаторы могут быть трех типов:

– «uplink» – к ВК этого типа можно подключать только физические или агрегированные интерфейсы;

– «mixed» – к ВК этого типа можно подключать любые интерфейсы, кроме интерфейсов ВМ;

– «virtual» – к ВК этого типа можно подключать только сетевые интерфейсы ВМ.

Примечания:

1. ВК типа «virtual» создаются автоматически и только при создании и в составе виртуальной сети.

2. На ВК типов «uplink» и «mixed» протоколы семейства STP (Spanning Tree Protocol) выключены, а также происходит фильтрация транзита пакетов BPDU (Bridge Protocol Data Units). Для проверки необходимо из CLI-интерфейса вычислительного узла выполнить команду:

tcpdump -i “интерфейс” stp –direction=’out’

где <интерфейс> – это имя физического интерфейса узла в состоянии «UP».

В выводе на экран не должно быть уведомлений о пакетах STP. Это означает отсутствие исходящих BPDU с портов ВК.

3.10.2.1.3. Создать виртуальный коммутатор можно двумя способами в разделах «Сети» и «Серверы» основного меню:

1) перейти в раздел «Сети» – «Сетевые настройки» основного меню и далее выполнить:

– выбрать нужную подсеть управления;

– выбрать пункт меню «Виртуальные коммутаторы»;

– выбрать целевой вычислительный узел и нажать кнопку «Добавить виртуальный коммутатор»;

– в открывшемся окне заполнить необходимые поля и нажать кнопку «ОК»;

2) перейти в раздел «Серверы» основного меню и далее выполнить:

– выбрать целевой сервер;

– выбрать пункт меню «Сети» – «Виртуальные коммутаторы» и нажать на кнопку «Добавить виртуальный коммутатор»;

– в открывшемся окне заполнить необходимые поля и нажать кнопку «ОК».

3.10.2.2. Группы портов

3.10.2.2.1. Группы портов представляют собой объекты для группировки интерфейсов по совокупности параметров VLAN и MTU (для внутренних интерфейсов и интерфейсов ВМ) и привязываются к ВК.

3.10.2.2.2. Порт-группы могут быть четырех типов:

– «internal» – предназначены для внутренних интерфейсов;

– «uplink» – предназначены для физических и агрегированных интерфейсов;

– «kernel» – предназначены для внутренних интерфейсов;

– «virtual» – предназначены для интерфейсов ВМ.

Примечания:

1. Порт-группы типа «kernel» создаются автоматически. Их нельзя создать или удалить. Помимо этого, в порт-группы типа «kernel» нельзя подключить интерфейсы, созданные пользователем.

2. Порт-группы типа «virtual» создаются автоматически при создании виртуальных сетей.

3.10.2.2.3. При создании или изменении параметров порт-группы доступны следующие режимы VLAN:

– none;

– access;

– trunk;

– native-tagged;

– native-untagged.

3.10.2.2.4. Также предоставлена возможность привязки порт-группы к нескольким ВК. Создание порт-групп производится из окна информации ВК с помощью кнопки «Добавить порт-группу».

3.10.2.3. Физические интерфейсы

3.10.2.3.1. Физические интерфейсы в SpaceVM являются представлением физических сетевых интерфейсов сервера. Объекты этого типа нельзя создать или удалить, используя Web-интерфейс или интерфейс командной строки. Информация о существующих физических интерфейсах собирается автоматически на этапе добавления вычислительного узла и хранится на протяжении всего времени существования объекта вычислительного узла. Собираемая информация включает в себя сведения о производителе сетевой карты, используемом драйвере, максимальной поддерживаемой величине MTU, скорости соединения (при условии, что сетевой интерфейс подключен) и другие сведения.

3.10.2.3.2. Однако, пользователю предоставляется возможность настройки некоторых параметров и состояния физических интерфейсов:

– изменение величины MTU интерфейса;

– включение/выключение «promiscuous» (неразборчивого) режима интерфейса;

– включение/выключение интерфейса (перевод в состояние «UP»/«DOWN»);

– включение/выключение SR-IOV интерфейса (при условии, что сетевой адаптер поддерживает эту функцию).

3.10.2.3.3. Подключение физических интерфейсов может быть осуществлено двумя способами в разделах «Сети» и «Серверы» основного меню:

1) перейти в раздел «Сети» – «Сетевые настройки» основного меню и далее:

– выбрать нужную подсеть управления;

– выбрать пункт меню «Виртуальные коммутаторы»;

– выбрать нужные вычислительный узел и виртуальный коммутатор;

– в открывшемся окне нажать кнопку «Подключить интерфейс», выбрать тип интерфейса «physical» и следовать шагам мастера добавления интерфейса;

2) перейти в раздел «Серверы» основного меню и далее выполнить:

– выбрать целевой сервер;

– выбрать пункт меню «Сети» – «Физические интерфейсы» и нажать кнопку «Подключить»;

– в открывшемся окне заполнить необходимые поля и нажать кнопку «ОК».

3.10.2.4. Агрегированные интерфейсы

3.10.2.4.1. Агрегированные интерфейсы в SpaceVM является представлением объединенных интерфейсов с целью:

– объединения пропускной способности;

– резервирования физических интерфейсов.

Объекты этого типа можно создать, удалить или модифицировать, используя Web-интерфейс.

3.10.2.4.2. Создание агрегированного интерфейса может быть осуществлено двумя способами в разделах «Сети» и «Серверы» основного меню:

1) перейти в раздел «Сети» – «Сетевые настройки» основного меню и далее выполнить:

– выбрать нужную подсеть управления;

– выбрать пункт меню «Виртуальные коммутаторы»;

– выбрать нужные вычислительный узел и виртуальный коммутатор;

– нажать кнопку «Подключить интерфейс», выбрать тип интерфейса «aggregated» и следовать шагам мастера добавления интерфейса;

2) перейти в раздел «Серверы» основного меню и далее выполнить:

– выбрать целевой сервер;

– выбрать пункт меню «Сети» – «Агрегированные интерфейсы» и нажать кнопку «Добавить»;

– в открывшемся окне заполнить необходимые поля и нажать кнопку «ОК».

3.10.2.4.3. При создании или модификации параметров агрегированного интерфейса предоставляется выбор следующих режимов агрегации:

– «active-backup» – используется для резервирования подключения. В этом режиме работает один из физических интерфейсов, включенных в агрегацию, а остальные будут задействованы в случае отказа активного;

– «balance-slb» – используется для объединения пропускной способности нескольких физических интерфейсов и балансировки нагрузки на них;

– «balance-tcp» – используется для объединения пропускной способности нескольких физических интерфейсов и балансировки нагрузки на них, однако, в отличие от «balance-slb», использует протокол LACP для отслеживания состояния подключения.

ВНИМАНИЕ! Для работы агрегации в режиме «balance-tcp» необходима настройка порт-групп со стороны физического коммутатора. Для работы агрегации в режимах «active-backup» и «balance-slb» порты физического коммутатора НЕ ДОЛЖНЫ быть объединены в порт-группу.

3.10.2.5. Внутренние (сервисные) интерфейсы

3.10.2.5.1. Внутренние (сервисные) интерфейсы в SpaceVM представляют собой виртуальное сетевое устройство, которое используется для обеспечения доступности вычислительных узлов на сетевом уровне. Этим интерфейсам назначаются IP-адреса. При создании внутреннего интерфейса выбирается ВК, в который интерфейс будет подключен и параметры интерфейса:

– режим получения адреса – динамический или статический;

– IP-адрес;

– маска подсети;

– MAC-адрес;

– порт-группа, которой будет принадлежать интерфейс.

ВНИМАНИЕ! При выборе динамического режима получения адреса интерфейсом, необходимо убедиться, что к выбранному для подключения ВК также подключен физический или агрегированный интерфейс. В противном случае, созданный внутренний интерфейс не будет иметь доступ к сети и, как следствие, не сможет получить IP-адрес от DHCP-сервера.

ВНИМАНИЕ! Также необходимо убедиться, что настройки VLAN выбранной порт-группы и настройки VLAN порт-группы, к которой относится физический или агрегированный интерфейс, указанный выше, не будут препятствовать прохождению сетевого трафика, порождаемого создаваемым внутренним интерфейсом.

3.10.2.5.2. Создание внутреннего интерфейса может быть осуществлено двумя способами в разделах «Сети» и «Серверы» основного меню:

1) перейти в раздел «Сети» – «Сетевые настройки» основного меню и далее выполнить:

– выбрать нужную подсеть управления;

– выбрать пункт меню «Виртуальные коммутаторы»;

– выбрать нужные вычислительный узел и виртуальный коммутатор;

– нажать кнопку «Подключить интерфейс», выбрать тип интерфейса «internal» и следовать шагам мастера добавления интерфейса;

2) перейти в раздел «Серверы» основного меню и далее выполнить:

– выбрать целевой сервер;

– выбрать пункт меню «Сети» – «Внутренние интерфейсы» и нажать кнопку «Добавить»;

– в открывшемся окне заполнить необходимые поля и нажать кнопку «ОК».

3.10.2.6. MAC-адреса

3.10.2.6.1. Первые три октета генерируемых MAC-адресов (Organizational Unique Identifier (OUI)) контроллером SpaceVM для виртуальных и внутренних интерфейсов везде одни и те же – «02:ff:f0».

Четвертый октет в десятичной системе счисления генерируется случайно от «0» до «127» при установке контроллера и доступен для изменения пользователем.

При генерации он переводится в шестнадцатеричную систему счисления.

Далее приведены примеры для различных значений четвертого октета:

– четвертый октет – «0». Генерируемый MAC-адрес – «02:ff:f0:00:68:33»;

– четвертый октет – «22». Генерируемый MAC-адрес – «02:ff:f0:16:b4:82»;

– четвертый октет – «99». Генерируемый MAC-адрес – «02:ff:f0:63:6a:b0».

3.10.2.6.2. С помощью команды *controller macs* в CLI можно увидеть все имена и MAC-адреса внутренних интерфейсов, физических интерфейсов, виртуальных интерфейсов, виртуальных функций.

3.10.2.7. Описание параметров вывода команды «net show bonds»

3.10.2.7.1. Ниже приведено описание параметров вывода команды *net show bonds*:

1) Name – имя интерфейса;

2) Bond mode – режим работы бонда. Возможные режимы:

– balance-tcp;

– balance-slb;

– active-backup;

Дополнительную информацию про режимы смотрите в 3.6.11.4;

3) Lacp – отображает поведение протокола управления агрегацией каналов (LACP). Только некоторые коммутаторы поддерживают LACP. Если ваш коммутатор не поддерживает LACP, используйте bond_mode=balance-slb или bond_mode=active-backup. Возможные варианты:

– active;

– passive;

– off;

4) Lacp time – устанавливает период проверки работоспособности (heartbeat) к 1 секунде (fast) или 30 секундам (slow). Возможные варианты:

– fast;

– slow.

«По умолчанию» – slow;

5) Fallback – определяет поведение бонда «openvswitch» в режиме LACP. Если коммутатор не поддерживает LACP, установка этого параметра в значение «true» позволяет вернуться к «active-backup» режиму работы. Если для параметра установлено значение «false», бонд будет отключен.

В обоих случаях, когда коммутатор настроен на использование режима LACP, бонд будет использовать LACP-протокол. Возможные варианты:

– true;

– false;

6) Members – имена интерфейсов, входящих в бонд;

7) Connected to – виртуальный коммутатор, которому принадлежит бонд;

8) Updelay – количество миллисекунд, в течение которых соединение должно быть активным, перед тем как будет принято решение, что интерфейс поднят;

9) Downdelay – количество миллисекунд, в течении которых соединение находится в выключенном состоянии, перед тем как будет принято решение, что интерфейс выключен. Значение «0» отключает интерфейс немедленно;

10) Lacp_status – отображает состояние протокола LACP. Сконфигурирован или нет;

11) Active member mac – MAC-адрес и имя активного интерфейса в бонде;

12) Bond member – имя интерфейса, участвующего в бонде;

13) State – состояние интерфейса (включен/выключен);

14) Status – статус интерфейса (активный/неактивный член бонда);

15) May_enable – статус возможности включения интерфейса.

3.10.3. Сетевые настройки

Управление сетевыми настройками вычислительных узлов осуществляется в разделе «Сети» – «Сетевые настройки» основного меню. В нем перечислены сети управления, включая для каждой из них ее название, количество серверов, IP-адрес подсети управления и IP-адрес контроллера.

Объект подсети управления представляет собой общие сведения о сетевых настройках, сгруппированных по адресу подсети управления, вычислительных узлах.

Также в окне «Сетевые настройки» имеется возможность обновить информацию по кнопке  и выбора сети по названию с помощью поля «Найти  » и кнопки  .

При выборе существующей подсети управления, открывается окно с информацией об общих для группы и индивидуальных сетевых настройках вычислительных узлов. Управление сетевыми настройками осуществляется в этом же окне с помощью соответствующей вкладки. Для управления доступны следующие вкладки:

– «Информация»;

– «Настройки серверов»;

– «Пограничный брандмауэр»;

– «Виртуальные коммутаторы»;

– «LLDP»;

– «L2-туннели»;

– «События»;

– «Теги».

В окне состояния сети имеется возможность обновить информацию по кнопке  и удалить сетевые настройки по кнопке «Удалить». При нажатии на кнопку «Удалить» необходимо в открывшемся окне подтвердить операцию, нажав кнопку «Удалить».

3.10.3.1. Информация о сети

3.10.3.1.1. В окне «Сети» – «Сетевые настройки» – <имя сети> –«Информация» содержатся следующие сведения:

– название сети (редактируемый параметр);

– описание сети (редактируемый параметр);

– IP-адрес подсети управления и ее маска;

– IP-адрес контроллера;

– дата и время создания;

– дата и время обновления информации;

– раскрывающийся список серверов, подключенный к этой сети управления, с возможностью переноса сервера по кнопке  и синхронизации информации о сетевых настройках сервера по кнопке  для всех и для каждого.

3.10.3.2. Настройки серверов

3.10.3.2.1. В окне «Сети» – «Сетевые настройки» – <имя сети> –«Настройки серверов» содержится следующая информация о сервере с возможностью выбора из раскрывающегося списка (при смене сервера будет меняться информация о нем):

1) название;

2) DHCP-статус интерфейса управления;

3) IP-адрес сервера (редактируемый параметр);

4) маска подсети управления;

5) состояние соединения интерфейса управления;

6) параметры основного шлюза сервера (редактируемый параметр), содержащий информацию:

– об интерфейсе;

– о состоянии DHCP;

– о возможном шлюзе;

7) настройки DNS-сервера (редактируемый параметр), содержащий информацию:

– об интерфейсе;

– состоянии DHCP;

– DNS-сервере и DNS-суффиксе;

– поддомене;

8) статические маршруты, настроенные для сервера, с возможностью их добавления по кнопке  .

При нажатии кнопки  в открывшемся окне необходимо заполнить информацию о назначении, шлюзе и метрике, а также включить/выключить интерфейс. После этого необходимо подтвердить операцию, нажав кнопку «ОК».

3.10.3.2.2. При выборе опции «Общие» имеется возможность настроить DNS, шлюз «по умолчанию» и статические маршруты сразу для нескольких серверов. Для этого необходимо открыть нужную вкладку («DNS», «Статические маршруты» или «Основные шлюзы»), выбрать соответствующие «…настройки» справа и добавить список серверов через меню «Добавление сервера».

3.10.3.2.3. Для смены адреса управления узла (контроллера) необходимо выполнить следующие действия:

– выбрать узел на контроллере;

– убедиться, что узел не задействован в виртуальных сетях. При необходимости отключить узел из виртуальной сети;

– убедиться, что узел не задействован в кластерных хранилищах. При необходимости отключить узел из кластерного хранилища;

– выключить все ВМ узла;

– перевести узел в сервисный режим;

– сменить IP-адрес узла в окне «Сети» – «Сетевые настройки» – <имя сети> – «Настройки серверов» – выбрать нужный узел;

– после смены адреса узел автоматически станет активным. Потребуется некоторое время для активации всех сущностей узла. При появлении предупреждений необходимо предпринять действия по их устранению. Возможны ситуации, когда узел некоторое время не сможет отсылать статусы о своих сущностях контроллеру, пока не выйдет тайм-аут соединения. В таких ситуациях можно подождать около 10 минут или перезапустить супервизор узла через Web-интерфейс контроллера или CLI узла;

– после смены адреса узла на контроллере возможны ситуации, когда узлы некоторое время не смогут отсылать статусы о своих сущностях контроллеру, пока не выйдет тайм-аут соединения. В таких ситуациях можно подождать около 10 минут или перезапустить супервизор контроллера в CLI узла.

3.10.3.3. Пограничный брандмауэр

3.10.3.3.1. В окне «Сети» – «Сетевые настройки» – <имя сети> –«Пограничный брандмауэр» содержится раскрывающийся список серверов, для каждого из которых можно просмотреть перечень имеющихся правил и добавить собственные правила. Перечисленные в данной вкладке правила влияют только на сеть управления и внутренний интерфейс «loopback». Они не затрагивают сети ВМ. Настройки брандмауэра для сети ВМ выполняются в разделе «Сети» – «Виртуальные сети» основного меню, описанные в 3.10.5 данного руководства.

3.10.3.3.2. Для каждого сервера имеются следующая информация и операции брандмауэра:

1) текущее состояние службы брандмауэра;

2) состояние политики безопасности;

3) запуск. При нажатии кнопки «Запуск брандмауэра на узле» в открывшемся окне необходимо подтвердить операцию, нажав на кнопку «Да»;

4) остановка. При нажатии кнопки «Остановка брандмауэра на узле» в открывшемся окне необходимо подтвердить операцию, нажав на кнопку «Да»;

5) перезапуск. При нажатии кнопки «Перезапуск брандмауэра на узле» в открывшемся окне необходимо подтвердить операцию, нажав на кнопку «Да»;

6) логирование. При нажатии кнопки «Включить логирование» в открывшемся окне необходимо подтвердить операцию, нажав на кнопку «Да»;

7) создание правила. Для создания правила необходимо нажать на кнопку «Добавить правила» и в открывшемся окне заполнить следующие поля:

– действие – выбор из раскрывающегося списка («accept» – пропускать пакеты или «drop» – блокировать пакеты);

– протокол, на котором будет применено правило – выбор из раскрывающегося списка («icmp», «tcp», «udp» или «none»);

– направление правила – выбор из раскрывающегося списка («in» или «out»);

– тип ICMP – выбор из раскрывающегося списка;

– код ICMP – выбор из раскрывающегося списка;

– состояние соединения – выбор из раскрывающегося списка («Выбрать все», «invalid» – недействительное, «new» – новое, «established» – действительное или «related» – связанное);

– адрес источника;

– адрес назначения (получатель пакетов);

– входящий интерфейс – выбор из раскрывающегося списка;

– включение (выключение) правила после его создания.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК»;

8) обновление правил. Для обновления правил необходимо нажать на кнопку «Обновить базовые правила» и в открывшемся окне включить (выключить) сброс пользовательских правил, после чего подтвердить операцию, нажав на кнопку «ОК»;

9) применение правил. Для применения правил необходимо нажать на кнопку «Применить правила» и в открывшемся окне подтвердить операцию, нажав кнопку «Да».

3.10.3.3.3. Правила брандмауэра подразделяются на четыре типа, для каждого из которых можно создавать правила и каждому соответствует собственная вкладка:

– фильтрация входящего трафика;

– фильтрация исходящего трафика;

– шейпинг входящего трафика;

– шейпинг исходящего трафика.

Шейпинг – это ограничение пропускной способности для определенного типа трафика.

3.10.3.3.4. При нажатии «Фильтр. вх. трафик» в окне параметров правила содержится следующая информация:

– индекс;

– интерфейс;

– протокол;

– адрес источника;

– адрес назначения;

– порт источника;

– порт назначения;

– состояние соединения;

– тип ICMP;

– код ICMP;

– действие для правила;

– состояние (включено или выключено правило).

3.10.3.3.5. Для добавления правила фильтрации трафика необходимо выбрать одну из двух вкладок «Фильтр. вх. трафик» или «Фильтр. исх. трафик» и нажать кнопку «Добавить правила». При добавлении правила необходимо в открывшемся окне заполнить следующие поля:

– действие («accept» или «drop»);

– протокол, на котором будет применено правило («icmp», «tcp», «udp» или «none»);

– направление трафика, обрабатываемого правилом («in» или «out»);

– параметры, соответствующие выбранному протоколу;

– критерии отбора источника пакетов (адрес, порт);

– критерии отбора получателей пакета (адрес, порт);

– входящий интерфейс, на котором будет действовать правило;

– включение правила после создания.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

3.10.3.3.6. При нажатии на выбранное правило в открывшемся окне «Параметры правила» можно обновить, изменить параметры или удалить правило. Для каждого правила доступны следующие параметры для изменения:

– действие для правила («accept» – пропускать пакеты, «drop» – блокировать пакеты);

– протокол, на котором будет применено правило («icmp», «tcp», «udp» или «none»);

– состояние соединения («Выбрать все», «invalid» – недействительное, «new» – новое, «established» – действительное, «related» – связанное);

– порт источника (раскрывающийся список имеющихся портов. Также можно ввести название интересующего порта и нажать кнопку «Добавить»);

– порт назначения (раскрывающийся список имеющихся портов. Также можно ввести название интересующего порта и нажать кнопку «Добавить»);

– адрес источника (раскрывающийся список имеющихся адресов. Также можно ввести адрес источника и нажать кнопку «Добавить»);

– адрес назначения (раскрывающийся список имеющихся адресов. Также можно ввести адрес назначения и нажать кнопку «Добавить»);

– включение или выключение правила.

После заполнения полей необходимо сохранить изменения, нажав кнопку «ОК».

Для удаления правила необходимо в окне параметров правила нажать кнопку «Удалить» и в открывшемся окне подтвердить операцию, нажав кнопку «Удалить».

3.10.3.3.7. Для добавления шейпинга трафика необходимо выбрать одну из двух вкладок «Шейп. вх. трафик» или «Шейп. исх. трафик» и нажать кнопку «Добавить правила».

При добавлении правила необходимо в открывшемся окне заполнить следующие поля:

– протокол, на котором будет применено правило («icmp», «tcp», «udp» или «none»);

– направление трафика, обрабатываемого правилом («in» или «out»);

– лимит, сверх которого трафик будет отбрасываться, если не разрешено превышение лимита;

– единицы измерения лимита («bytes», «kbytes», «mbytes» или «packets»);

– разрешение превышения лимита;

– размер буфера, на который разрешено превышение установленного лимита и единицы измерения буфера («bytes», «kbytes», «mbytes» или «packets»), если разрешено превышение лимита;

– параметры, соответствующие выбранному протоколу;

– критерии отбора источника пакетов (адрес);

– критерии отбора получателей пакета (адрес);

– включение правила после создания.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

3.10.3.3.8. При нажатии на правило открывается окно, в котором можно обновить, изменить параметры или удалить правило.

Для каждого правила доступны следующие параметры для изменения:

– лимит, сверх которого трафик будет отбрасываться, если не разрешено превышение лимита;

– единицы измерения лимита («bytes», «kbytes», «mbytes» или «packets»);

– разрешение превышения лимита;

– размер буфера, на который разрешено превышение установленного лимита и единицы измерения буфера («bytes», «kbytes», «mbytes» или «packets»), если разрешено превышение лимита;

– параметры, соответствующие выбранному протоколу;

– адрес источника (раскрывающийся список имеющихся адресов). Также можно ввести адрес источника и нажать кнопку «Добавить»;

– адрес назначения (раскрывающийся список имеющихся адресов). Также можно ввести адрес назначения и нажать кнопку «Добавить»;

– включение или выключение правила.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

3.10.3.4. Виртуальные коммутаторы

3.10.3.4.1. В окне «Сети» – «Сетевые настройки» – <имя сети> – «Виртуальные коммутаторы» содержится раскрывающийся список серверов, для каждого из которых можно просмотреть список созданных на нем ВК. Интерфейс управления позволяет создавать, изменять и удалять ВК.

3.10.3.4.2. Для каждого коммутатора можно добавлять, изменять и удалять порт-группы. Порт-группы для физических интерфейсов и агрегированных физических портов должны иметь тип «uplink», а для внутренних интерфейсов сервера – «internal». Для каждого коммутатора можно создать несколько порт-групп. Для каждой порт-группы можно назначить разные параметры VLAN и MTU.

3.10.3.4.3. Для того чтобы добавить ВК, необходимо нажать на кнопку «Добавить виртуальный коммутатор» и в открывшемся окне заполнить следующие поля:

– название ВК;

– описание ВК;

– тип ВК («mixed» или «uplink»).

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

3.10.3.4.4. Для просмотра информации о существующем ВК необходимо нажать на его название, после чего в открывшемся окне отобразится информация, разграниченная по следующим группам:

– информация;

– подключенные интерфейсы;

– таблица MAC-адресов;

– топология виртуального коммутатора;

– события.

В окне состояния ВК существует возможность обновления данных по кнопке  и удаление коммутатора по кнопке «Удалить». При нажатии на кнопку «Удалить» необходимо в открывшемся окне подтвердить операцию, нажав кнопку «Удалить».

3.10.3.4.5. В окне «Сети» – «Сетевые настройки» – <имя сети> – «Виртуальные коммутаторы» – <имя ВК> – «Информация» содержатся следующие сведения о ВК:

– название ВК;

– описание ВК (редактируемый параметр);

– тип ВК («mixed» или «uplink»);

– коммутатор ядра – является ли ВК коммутатором ядра («true» – да, «false» – нет);

– статус ВК;

– список существующих порт-групп, включая для каждой из них название, тип, режим VLAN, тег VLAN, транки и количество интерфейсов.

3.10.3.4.6. В окне «Сети» – «Сетевые настройки» – <имя сети> – «Виртуальные коммутаторы» – <имя ВК> – «Подключенные интерфейсы» содержится информация об интерфейсах, разделенная на группы:

– внутренние интерфейсы – содержит список внутренних интерфейсов, подключенных к ВК;

– агрегированные интерфейсы – содержит список агрегированных интерфейсов, подключенных к ВК;

– физические интерфейсы – содержит список физических интерфейсов сервера, подключенных к ВК.

3.10.3.4.7. В окне «Сети» – «Сетевые настройки» – <имя сети> – «Виртуальные коммутаторы» – <имя ВК> – «Таблица MAC-адресов» – «Адреса» содержится информация, которая включает следующие параметры:

– порт;

– тип интерфейса;

– название подключенного физического интерфейса;

– VLAN;

– MAC-адрес;

– время устаревания.

В окне управления адресами имеется возможность обновления и очистки информации, а также поиск адреса с применением фильтра по кнопке «Фильтр».

Для его настройки необходимо в открывшемся окне заполнить следующие поля:

– порт;

– VLAN;

– MAC-адрес.

В окне «Сети» – «Сетевые настройки» – <имя сети> – «Виртуальные коммутаторы» – <имя ВК> – «Таблица MAC-адресов» – «Статистика» содержится статистика по выбранному ВК.

3.10.3.4.8. В окне «Сети» – «Сетевые настройки» – <имя сети> –«Виртуальные коммутаторы» – <имя ВК> – «Топология виртуального коммутатора» содержит информацию о подключенных к выбранному ВК внутренних и физических интерфейсах, включающую:

– название интерфейса;

– состояние;

– порт;

– драйвер;

– тип.

3.10.3.4.9. В окне «Сети» – «Сетевые настройки» – <имя сети> –«Виртуальные коммутаторы» – <имя ВК> – «События» содержатся сообщения о работе ВК с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные».

Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.10.3.4.10. Для создания новой порт-группы на ВК, необходимо нажать на кнопку «Добавить порт-группу» и в открывшемся окне заполнить следующие поля:

– название порт-группы;

– ее описание;

– режим VLAN (выбор из раскрывающегося списка). Может принимать значения «none», «access», «trunk», «native-tagged» или «native-untagged». При выборе «access» станет доступно для заполнения поле «Тег VLAN», при выборе «trunk» станет доступно для заполнения поле «Транки», при выборе «native-tagged» или «native-untagged» станут доступны для заполнения оба перечисленные поля;

– тип (выбор из раскрывающегося списка);

– значение MTU.

После заполнения всех полей необходимо подтвердить операцию, нажав кнопку «ОК».

3.10.3.4.11. Для изменения существующей порт-группы необходимо нажать на ее название в списке порт-групп (во вкладке «Информация»), после чего в открывшемся окне отобразится информация, разграниченная по следующим группам:

– информация;

– внутренние интерфейсы (для «kernel» или «internal» порт-группы);

– физические интерфейсы (для «uplink» порт-группы);

– агрегированные интерфейсы (для «uplink» порт-группы).

Примечание. В разных порт-группах могут быть разные вкладки. Это зависит от конфигурации сети и типа порт-группы.

3.10.3.4.12. Во вкладке «Информация» содержатся следующие сведения о порт-группе:

– название порт-группы (редактируемый параметр);

– описание порт-группы (редактируемый параметр);

– настройки VLAN и MTU (редактируемый параметр), в котором задается режим VLAN (выбор из раскрывающегося списка «none», «access», «trunk», «native-tagged» или «native-untagged»), тег VLAN и транки;

– возможность связать (переключить) порт-группу с другим ВК (доступно для «uplink» порт-группы). При нажатии на соответствующую кнопку в открывшемся окне необходимо выбрать из раскрывающегося списка ВК, после чего подтвердить операцию, нажав кнопку «ОК»;

– сообщения о работе порт-группы с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения» и «Информационные». Также имеется возможность отображения только непрочитанных сообщений.

3.10.3.4.13. Для «kernel» порт-группы во вкладке «Внутренние интерфейсы» перечислены виртуальные интерфейсы гипервизора, собранные в эту группу. Посредством создания нескольких «kernel» порт-групп с разными настройками VLAN и MTU можно подключить один сервер к разным сетям предприятия.

Наиболее частое применение такого функционала – создание на сервере, выполняющем роль контроллера, нескольких интерфейсов, подключенных в разные VLAN предприятия для предоставления администраторам и пользователям системы доступа в интерфейс управления без объединения сетей и построения сложной маршрутизации. Также для серверов таким образом можно обеспечить подключения к выделенным сетям хранения данных NFS/CIFS/iSCSI.

В свойствах внутреннего интерфейса, использующего DHCP для получения адреса, принудительное обновление аренды осуществляется кнопкой «Обновление адреса экземпляра».

Добавление внутреннего интерфейса в «internal» порт-группу осуществляется нажатием кнопки «Добавить» во вкладке «Внутренние интерфейсы» окна свойств порт-группы. Для добавления интерфейса необходимо указать следующие параметры:

– название;

– описание;

– виртуальный коммутатор;

– «internal» порт-группа коммутатора;

– тип назначения адреса интерфейсу – автоматически (DHCP) или вручную;

– если адрес назначается вручную, то необходимо указать адрес и маску сети;

– MAC-адрес интерфейса генерируется автоматически, но можно указать его вручную.

Для изменения параметров необходимо в окне свойств внутреннего интерфейса нажать кнопку «Изменение параметров» и в открывшемся окне отредактировать требуемую информацию.

3.10.3.4.14. Перед назначением зеркалирования физических портов коммутатора необходимо создать дополнительную «uplink» порт-группу, в которую необходимо подключить физический порт, в который будет зеркалироваться трафик. После этого во вкладке «Зеркалирование портов» свойств виртуального коммутатора будет возможность создать правило зеркалирования, в котором можно указать источник и интерфейс назначения.

3.10.3.4.15. Во вкладке «Физические интерфейсы» «uplink» порт-группы содержится список подключенных к группе физических интерфейсов, включая их названия, MAC-адрес, включение в агрегацию, состояние, подключение и статус.

Также существует возможность подключения физических интерфейсов путем нажатия кнопки «Подключить» и заполнения поля «Физические интерфейсы» (выбор из раскрывающегося списка), а также включение или отключение физического интерфейса после подключения. После заполнения полей необходимо нажать кнопку «ОК».

При необходимости подключить больше одного физического интерфейса к физическому коммутатору или стеку коммутаторов следует воспользоваться операцией агрегации нескольких интерфейсов.

3.10.3.4.16. Во вкладке «Агрегированные интерфейсы» содержится информация об агрегированных интерфейсах. Также существует возможность добавления агрегированного интерфейса путем нажатия кнопки «Добавить» и заполнения в открывшемся окне следующих полей:

1) название;

2) описание;

3) виртуальный коммутатор (выбор из раскрывающегося списка);

4) порт-группа (выбор из раскрывающегося списка);

5) физические интерфейсы (выбор из раскрывающегося списка);

6) тип агрегации (выбор из раскрывающегося списка). Может принимать значения:

– «active-backup» – режим резервирования. Резервный канал не используется;

– «balance-tcp» – режим балансировки с использованием LACP;

– «balance-slb» – режим простой балансировки на основе MAC и VLAN;

7) связь протокола управления агрегацией каналов (выбор из раскрывающегося списка). Может принимать значения «выключено», «active» или «passive»;

8) включение или отключение агрегированного интерфейса после подключения. После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

Примечание. Режимы работы LACP должны быть согласованы с физическим коммутатором.

Для изоляции трафика ВМ от сети управления на логическом уровне рекомендуется использовать VLAN. Для этого достаточно назначить на порт-группы распределенного коммутатора, в которые подключаются ВМ, тег VLAN.

Для изоляции трафика ВМ от сети управления на физическом уровне рекомендуется использовать отдельные сетевые интерфейсы. Для этого необходимо создать в ВК отдельную порт-группу типа «uplink», включить в нее выделенные интерфейсы и подключить к ней распределенный коммутатор.

Объединение физических интерфейсов в агрегированные и подключение их в порт-группы коммутатора можно производить в настройках сервера в настройках порт-групп коммутатора.

ВНИМАНИЕ! При настройке агрегированных интерфейсов с использованием режима «balance-tcp» необходима поддержка LACP на стороне физического коммутатора. Группы агрегируемых портов каждого сервера должны объединяться на коммутаторе в свою группу портов. Перед началом настройки все агрегируемые порты должны быть включены в свою группу. Также необходимо помнить, что до момента идентификации на портах коммутатора наличия агрегации, коммутатор не будет пропускать трафик в группу интерфейсов. Если агрегация будет настроена для физических портов сервера, не подключенных в соответствующую группу портов коммутатора, это сформирует сетевую петлю.

Для работы агрегации в режимах «active-backup» и «balance-slb» порты физического коммутатора НЕ ДОЛЖНЫ быть объединены в порт-группу.

3.10.3.4.17. Существует возможность добавления сетевых интерфейсов из интерфейса ВК.

Для этого необходимо нажать на кнопку «Подключить интерфейс» и следовать шагам мастера подключения интерфейсов:

1) на шаге 1 необходимо выбрать тип подключаемого интерфейса – «physical», «internal» или «aggregated». После заполнения полей необходимо подтвердить операцию, нажав кнопку «Далее»;

2) на шаге 2 необходимо задать параметры подключаемого интерфейса.

Для «physical» типа интерфейса:

– физические интерфейсы – выбрать подключаемый интерфейс (раскрывающийся список);

– включить после подключения – определяет, будет ли интерфейс переведен в состояние «UP» после подключения к ВК.

Для «internal» типа интерфейса:

– название;

– описание;

– тип назначения адреса интерфейсу – автоматически (DHCP) или вручную;

– если адрес назначается вручную, то необходимо указать адрес и маску сети;

– MAC-адрес интерфейса генерируется автоматически, но можно указать его вручную.

Для «aggregated» типа интерфейса:

– название;

– описание;

– физические интерфейсы (выбор из раскрывающегося списка);

– тип агрегации (выбор из раскрывающегося списка). Может принимать значения:

а) «active-backup» – режим резервирования. Резервный канал не используется;

б) «balance-tcp» – режим балансировки с использованием LACP;

в) «balance-slb» – режим простой балансировки на основе MAC и VLAN;

– связь протокола управления агрегацией каналов (выбор из раскрывающегося списка). Может принимать значения «выключено», «active» или «passive»;

– включение или отключение агрегированного интерфейса после подключения.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «Далее»;

3) на шаге 3 необходимо выбрать порт-группу, в которую подключается интерфейс (раскрывающийся список).

Примечание. Режимы работы LACP должны быть согласованы с физическим коммутатором.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

3.10.3.5. LLDP

3.10.3.5.1. В окне «Сети» – «Сетевые настройки» – <имя сети> – «LLDP» можно настроить сервис LLDP на SpaceVM.

3.10.3.5.2. Сервис LLDP поддерживает следующие протоколы:

– LLDP;

– CDP (версии 1 и 2);

– SONMP;

– FDP.

3.10.3.5.3. «По умолчанию» сервис LLDP включен на сервере.

Примечание. LLDP (Link Layer Discovery Protocol) – протокол канального уровня, позволяющий сетевому оборудованию оповещать оборудование, работающее в локальной сети, о своем существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения. Описание протокола приводится в стандарте IEEE 802.1AB-2009, формально утвержденном в сентябре 2009 года. Протокол не зависит от производителей сетевого оборудования и является заменой аналогичных, но патентованных протоколов, таких как Cisco Discovery Protocol, Extreme Discovery Protocol, Foundry Discovery Protocol и Nortel Discovery Protocol (последний также известен как SONMP).

3.10.3.5.4. Сервис LLDP позволяет серверу получать информацию от «соседей» и передавать информацию для них.

В данном окне содержится список контроллеров, включая для каждого из них:

– его название;

– IP-адрес сервера, на котором запущен сервис;

– интервал передачи информации «соседу» (в секундах);

– множитель удержания информации о «соседе»;

– состояние соединения.

При нажатии на имя контроллера в открывшемся окне «Сети» – «Сетевые настройки» – <имя сети> – «LLDP» – <имя контроллера> содержится следующая информация:

1) название контроллера;

2) дата и время создания;

3) IP-адрес;

4) системное название;

5) порты, на которых работает сервис – раскрывающаяся информация включает список портов, каждый из которых содержит:

– имя порта;

– статус или режим работы;

– описание.

Есть возможность изменять режим работы и описание по каждому порту. Для этого необходимо нажать на название порта в списке портов. Доступны следующие режимы статуса:

– rx-and-tx – на данном порту будет приниматься и передаваться информация;

– rx-only – на данному порту будет только приниматься информация;

– tx-only – на данном порту будет только передаваться информация;

– disabled – на данном порту сервис будет выключен.

Для редактирования описания порта необходимо изменить поле «Описание»;

6) протокол сервиса, который работает на данном сервере (редактируемый параметр). Для изменения параметра необходимо нажать на кнопку редактирования и в открывшемся окне выбрать из раскрывающегося списка протокол. Доступны следующие типы протоколов и их режимы:

– lldp – обмен информацией с использованием протокола LLDP;

– cdpv2_forced(cdpv1_enadled) – обмен информацией с использованием протокола CDP версии 2. При этом также будет приниматься информация от «соседа», который использует протокол CDP версии 1;

– cdpv2_forced(cdpv1_disabled) – протокол CDP версии 2. Будет приниматься информация от «соседа», использующего только протокол CDP версии 2;

– fdp – обмен информацией с использованием протокола FDP;

– sonmp – обмен информацией с использованием протокола SONMP.

После редактирования подтвердить информацию, нажав на кнопку «ОК».

7) системное описание;

8) интервал передачи в секундах;

9) множитель удержания;

10) daemon run (вкл/выкл).

В окне состояния протокола есть возможность следующих операций:

1) обновление информации по кнопке  ;

2) изменение параметров. Для изменения параметра необходимо нажать на кнопку «Изменение параметров» и в открывшемся окне заполнить следующие поля:

– Chassis_ID. «По умолчанию» передается UUID узла;

– IP_адрес. В качестве «Managment Address» «по умолчанию» передается IP-адрес сервера;

– системное название. «По умолчанию» передается имя сервера;

– системное описание. «По умолчанию» передается версия ОК;

– интервал передачи в секундах. «По умолчанию» интервал равен 30 секунд;

– множитель удержания. «По умолчанию» множитель удержания равен «4».

После заполнения полей необходимо подтвердить информацию, нажав на кнопку «ОК»;

3) остановка службы LLDP. При нажатии на кнопку «Остановка службы LLDP» необходимо в открывшемся окне подтвердить операцию, нажав на кнопку «Да»;

4) перезапуск службы LLDP. При нажатии на кнопку «Перезапуск службы LLDP» необходимо в открывшемся окне подтвердить операцию, нажав на кнопку «Да»;

5) получение данных о соседях. Выполняется автоматически по кнопке «Получение данных о соседях». В открывшемся окне появится следующая информация:

– локальный порт;

– протокол;

– подтип шасси;

– шасси ID;

– подтип порта;

– порт ID;

– системное название;

– системное описание;

– порт MFS;

– VLAN ID;

– VLAN PVID;

– время жизни;

– способности системы;

– включение способности системы;

– IP-адрес управления.

Для возврата к предыдущему окну необходимо нажать на кнопку «Информация».

3.10.3.5.5. Управление конфигурацией сервиса LLDP можно выполнять двумя способами:

– используя Web-интерфейс;

– используя CLI.

Примечание. Далее все действия будем осуществлять через Web-интерфейс.

3.10.3.5.6. Выполним проверку того, что в SpaceVM существует возможность предоставления информации от подключенных активных сетевых устройствах с применением протокола LLDP.

Для этого необходимо сделать следующие действия:

1) проверить, что сервис LLDP работает на сервере SpaceVM. Настройки сервиса LLDP выполняются в разделе «Сети» – «Сетевые настройки» – <имя сети> – «LLDP».

Примечание. Для того чтобы SpaceVM получил информацию от «соседа» по протоколу LLDP, необходимо только включить протокол LLDP на оборудовании, которое подключено к физическим портам SpaceVM, в данном случае на активном сетевом устройстве. Таким образом, если соответствующие настройки на сетевом оборудовании уже выполнены, то можно выбрать нужный сервер и нажать кнопку «Получение данных о соседях».

В данном вкладке «LLDP» отображается следующая информация:

– название;

– IP-адрес сервера, на котором запущен сервис;

– интервал передачи информации «соседу» (в секундах);

– множитель удержания информации о «соседе»;

– состояние сервиса («Daemon run»).

Установленная метка в столбце «Daemon run» сообщает о том, что сервис LLDP работает на данном сервере. Детали элементов контроля и настройки сервиса LLDP, а также получения информации о «соседях» можно увидеть, выбрав необходимый сервер из списка;

2) в открывшемся окне нас интересуют следующие параметры:

– порты, на которых работает сервис. Для отображения настроек сервиса на порту необходимо нажать на его название.

В данном месте отображается следующая информация:

а) статус порта или другими словами режим работы порта;

б) описание порта.

Есть возможность изменять режим работы и описание по каждому порту. Для этого необходимо нажать на имя порта и в открывшемся окне «Изменение порта» изменить параметры.

Доступны разные режимы статуса, выберем «rx-and-tx». Этот режим означает, что на данном порту будет приниматься и передаваться информация по выбранному протоколу.

Для редактирования описания порта необходимо изменить поле «Описание».

После редактирования параметров необходимо нажать кнопку «ОК»;

– протоколы сервиса, который работает на данном сервере.

Для изменения типа протокола необходимо нажать на кнопку редактирования рядом с именем протокола.

Доступны разные протоколы. Согласно нашей задаче выберем протокол LLDP. Это означает обмен информацией с использованием протокола LLDP;

– Daemon run – убедимся, что значение этого поля «Включен». В противном случае нажмите кнопку «Запуск службы LLDP»;

– остальные параметры можно оставить «по умолчанию».

Необходимые предварительные требования завершены.

3) для того чтобы SpaceVM получил информацию от сетевого устройства по настроенному протоколу (в данном случае LLDP), необходимо нажать кнопку «Получение данных о соседях».

В открывшемся окне должна отобразиться информация:

– локальный порт – физический порт SpaceVM, к которому подключено активное сетевое устройство;

– протокол – протокол, по которому происходит обмен информацией с сетевым устройством;

– остальная информация – это информация, которую нам передало сетевое устройство.

Если пользователь не видит информацию от сетевого устройства или другого оборудования, подключенного к SpaceVM необходимо убедиться, что на этом оборудовании включен протокол LLDP. За подробностями настройки оборудования следует обратится к документации производителя оборудования.

3.10.3.6. L2-туннели

3.10.3.6.1. В окне «Сети» – «Сетевые настройки» – <имя сети> – «L2 туннели» содержится список созданных vxlan/geneve туннелей.

Туннели – это инструмент для формирования L2-связанности между локациями (дата-центрами), передача трафика между которыми происходит через явно заданные маршрутизаторы. Маршрутизаторы задаются в явном виде при настройке серверов, описанном в 3.10.3.2 данного руководства.

Туннели обеспечивают имитацию сетевой связанности на L2-уровне двух коммутаторов разных локаций. В таком случае виртуальным машинам разных локаций не требуются настройки маршрутизации между локациями.

Туннель строится между сервисными интерфейсами двух серверов, по одному из каждой локации. Перед настройкой необходимо убедиться, что маршрутизация между серверами осуществляется корректно.

3.10.3.6.2. При добавлении туннеля по кнопке «Добавить туннель» в открывшемся окне необходимо заполнить следующие поля:

– название туннеля;

– описание туннеля;

– выбрать сервер 1 и 2 из раскрывающегося списка;

– выбрать коммутатор 1 и 2 из раскрывающегося списка;

– выбрать сервисный интерфейс 1 и 2 из раскрывающегося списка;

– проверить соединение;

– значение идентификатора сети VNI;

– значение MTU;

– выбрать протокол из раскрывающегося списка («vxlan» или «geneve»);

– включить (выключить) перезапуск виртуальных машин.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

3.10.3.7. События

3.10.3.7.1. В окне «Сети» – «Сетевые настройки» – <имя сети> – «События» отображаются события, зарегистрированные в системе для этого коммутатора с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные».

Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.10.3.8. Теги

3.10.3.8.1. В окне «Сети» – «Сетевые настройки» – <имя сети> – «Теги» имеется возможность добавления к сети отличительной метки (тега), применения и обновления тега.

3.10.3.8.2. Для создания нового тега необходимо нажать кнопку «Создать» и в открывшемся окне заполнить следующие поля:

– название тега;

– идентификатор тега (Slug);

– цвет тега из открывающейся палитры. При выборе цвета необходимо подтвердить изменения, нажав кнопку «ОК», либо выйти без сохранения изменений, нажав кнопку «Отмена».

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

3.10.3.8.3. Для применения нового тега необходимо нажать кнопку «Применить» и в открывшемся окне выбрать тег. Для сохранения изменений необходимо нажать кнопку «ОК».

3.10.4. Обработка трафика

3.10.4.1. Контроль трафика

3.10.4.1.1. В окне «Сети» – «Контроль трафика» основного меню собрана информация о политиках безопасности, применяемых к виртуальным сетям. В данном окне отображаются созданные автоматически и создаваемые пользователем наборы политики безопасности для виртуальных сетей. Здесь отображается список политик безопасности, доступных в системе.

3.10.4.1.2. В окне «Сети» – «Контроль трафика» основного меню существует возможности:

– обновления информации по кнопке  ;

– добавления политик безопасности. При нажатии кнопки «Добавить» необходимо заполнить названия и описания политики, после чего подтвердить операцию, нажав кнопку «ОК»;

– выбора по названию политики. В поле «Найти» после ввода названия политики необходимо нажать кнопку поиска  или отказаться, нажав кнопку  . Если в результате поиска были найдены подходящие варианты, то они отобразятся в открывшемся окне.

3.10.4.1.3. При нажатии на набор политики безопасности открывается окно, в котором можно обновить информацию о наборе правил или удалить правило. Каждый набор правил имеет вкладки «Информация», «События» и «Теги».

Кроме этого, имеются вкладки для управления набором правил:

– «Политики фильтрации виртуальных сетей»;

– «Политики QoS виртуальных сетей»;

– «Зеркалирование портов».

3.10.4.1.4. В окне «Сети» – «Контроль трафика» – <имя политики безопасности> – «Информация» содержатся следующие сведения о правилах:

– название (редактируемый параметр);

– описание (редактируемый параметр);

– дата и время создания;

– дата и время изменения.

3.10.4.2. Политика фильтрации виртуальных сетей

3.10.4.2.1. В окне «Сети» – «Контроль трафика» – <имя политики безопасности> – «Политика фильтрации виртуальных сетей» содержится список имеющихся наборов правил, входящих в состав этой политики безопасности, а также имеется возможность добавления нового набора правил. При нажатии кнопки «Добавить» необходимо заполнить названия и описания наборов правил, после чего подтвердить операцию, нажав кнопку «ОК».

3.10.4.2.2. При нажатии на набор правил открывается окно, в котором отображается информация о правилах фильтрации трафика, входящих в данный набор, разделенная на группы:

– фильтрация входящего трафика – это набор правил, применяемый при взаимодействии виртуальной сети с сетью предприятия. Применяется на внешнем интерфейсе контейнера сетевых служб виртуальной сети;

– фильтрация исходящего трафика – это набор правил, применяемый при взаимодействии виртуальной сети с сетью предприятия. Применяется на внутреннем интерфейсе контейнера сетевых служб виртуальной сети;

– перенаправление входящего трафика (SNAT) – это перенаправление трафика по источнику, в том числе включение транслятора сетевых адресов (NAT) из виртуальной сети в сеть предприятия (masquerade);

– перенаправление исходящего трафика (DNAT) – это перенаправление трафика по получателю.

3.10.4.2.3. В данном окне имеется возможность настройки логирования. Для этого необходимо нажать кнопку «Включить логирование», после чего в открывшемся окне нажать «Да» для подтверждения операции.

3.10.4.2.4. Для каждой группы имеются следующие операции:

1) добавление правила. Для добавления правила необходимо сначала выбрать группу правил и потом нажать кнопку «Добавить правила». При добавлении правила в открывшемся окне необходимо заполнить следующие поля:

– для группы фильтрации входящего (исходящего) трафика:

а) основное действие для правила (выбор из раскрывающегося списка). Может принимать значения «accept» – разрешить, «drop» – запретить;

б) протокол (выбор из раскрывающегося списка). Может принимать значения «icmp», «tcp», «udp» или «none»;

в) направление трафика (выбор из раскрывающегося списка). Может принимать значения «in» или «out»;

г) параметры правила, зависящие от типа протокола;

д) состояние соединения (выбор из раскрывающегося списка). Может принимать значения «invalid», «new», «established» или «related»;

е) адрес источника (выбор из раскрывающегося списка с возможностью добавления путем ввода IP-адреса и нажатия кнопки «Добавить»);

ж) адрес назначения (выбор из раскрывающегося списка с возможностью добавления путем ввода IP-адреса и нажатия кнопки «Добавить»);

з) включение правила после создания;

и) счетчик пакетов;

– для SNAT:

а) основное действие для правила (выбор из раскрывающегося списка). Может принимать значения «src_nat», «masquerade»;

б) протокол (выбор из раскрывающегося списка). Может принимать значения «icmp», «tcp», «udp» или «none»;

в) адрес источника (выбор из раскрывающегося списка с возможностью добавления путем ввода IP-адреса и нажатия кнопки «Добавить»);

г) SNAT-адрес;

д) включение правила после создания;

е) счетчик пакетов;

– для DNAT:

а) основное действие для правила. Может принимать значение «dst»;

б) адрес назначения;

в) порт назначения;

г) DNAT-адрес;

д) DNAT-порт;

е) адрес источника (выбор из раскрывающегося списка с возможностью добавления путем ввода IP-адреса и нажатия кнопки «Добавить»);

ж) включение правила после создания;

з) счетчик пакетов;

После заполнения полей подтвердить операцию, нажав кнопку «ОК»;

2) применение всех правил. При нажатии кнопки «Применить правила» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «Да»;

3) удаление одного правила. Для удаления правила необходимо нажать на правило в списке. В открывшемся окне можно изменить параметры правила и удалить его. После удаления правила необходимо в окне управления набором правил заново применить все правила с помощью соответствующей кнопки;

4) удаление набора правил. Происходит в окне управления набором правил. При нажатии кнопки «Удалить» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «Удалить».

3.10.4.3. Политики QoS виртуальных сетей

3.10.4.3.1. В окне «Сети» – «Контроль трафика» – <имя политики безопасности> – «Политики QoS виртуальных сетей» содержится информация по работе с сетевым трафиком.

3.10.4.3.2. Пункт «Политики QoS виртуальных сетей» позволяет добавить политику. Для создания Политики QoS необходимо нажать кнопку «Добавить», ввести имя и, если необходимо, описание политики в соответствующих полях формы.

3.10.4.3.3. Для управления политикой необходимо нажать на ее название и перейти в окно состояния, в котором содержатся следующие сведения:

1) название политики (редактируемый параметр);

2) описание (редактируемый параметр);

3) возможные действия:

– создание правила. Политика QoS состоит из набора правил, которые необходимо предварительно создать;

– применение Политики QoS;

– отмена Политики QoS;

– удаление Политики QoS.

3.10.4.3.4. Для создания правила необходимо:

– выбрать направление «Маркировка входящего трафика» или «Маркировка исходящего трафика»;

– нажать кнопку «Добавить правило»;

– выбрать тип и указать значение dscp. Dscp – значение поля «dscp» в IPv4-заголовке (обязательное поле). Значение следует задать в диапазоне от «0» до «63» включительно;

– выбрать Ethertype – значение поля «ethertype» в ethernet-фрейме (обязательное поле);

– заполнить IP-протокол – значение поля «ip protocol» в IPv4-заголовке;

– заполнить IP-адрес источника – значение поля «source ip address» в IPv4-заголовке;

– заполнить IP-адрес назначения – значение поля «destination ip address» в IPv4-заголовке;

– заполнить порт источника – значение поля «source port» в заголовке транспортного уровня;

– заполнить порт назначения – значение поля «destination port» в заголовке транспортного уровня;

– заполнить MAC-адрес источника – значение поля «source mac-address» в ethernet-фрейме;

– заполнить MAC-адрес назначения – значение поля «destination mac-address» в ethernet-фрейме;

– включить (выключить) правило. Опция «Включить» означает, будет ли применяться правило или нет;

– нажать на кнопку «ОК».

3.10.4.3.5. Чтобы применить политику, необходимо нажать кнопку «Применить правила». В открывшемся окне необходимо выбрать название виртуальной сети, к которой будут применены текущие правила Политики QoS и нажать кнопку «ОК». В поле «Виртуальные сети» отображается информация о статусе применения Политики QoS для определенной виртуальной сети. Таким образом, сетевой трафик, попадающий под условия параметров, будет маркироваться заданным значением «dscp».

3.10.4.3.6. Чтобы редактировать правило, необходимо выбрать нужное правило. В открывшемся окне отображаются текущие параметры. Необходимо нажать кнопку «Изменение параметров» и изменить значения. Для того чтобы сохранить новые значения, необходимо нажать кнопку «Сохранить».

Примечание. После изменения или добавления нового правила изменится статус применения политики на виртуальную сеть. Чтобы изменения вступили в силу, необходимо вновь применить Политику QoS на виртуальную сеть.

3.10.4.3.7. Чтобы отменить политику QoS, необходимо нажать кнопку «Отменить правила». В открывшемся окне необходимо выбрать название виртуальной сети, для которой будет выполнена отмена текущей Политики QoS, и нажать кнопку «ОК».

3.10.4.3.8. Чтобы удалить Политику QoS, необходимо нажать кнопку «Удалить». Удаление Политики QoS невозможно в случае, если политика применена к виртуальной сети. В этом случае необходимо отменить применение политики на все виртуальную сеть и после этого выполнить удаление.

3.10.4.4. Зеркалирование портов

3.10.4.4.1. В окне «Сети» – «Контроль трафика» – <имя политики безопасности> – «зеркалирование портов» содержится информация по настройке сервиса Port-Mirroring. Сервис позволяет выполнять зеркалирование трафика данных между портами компонентов системы SpaceVM. Сервис поддерживает создание множества конфигураций зеркалирования.

3.10.4.4.2. Также в данном окне имеется возможность добавления зеркалирования для портов. Для того чтобы добавить конфигурацию зеркалирования необходимо нажать кнопку «Добавить зеркалирование портов». В открывшемся окне необходимо задать следующие параметры:

– название конфигурации;

– описание конфигурации (необязательный параметр);

– сервер, на котором будет работать конфигурация (выбор из раскрывающегося списка);

– порты источника трафика (выбор из раскрывающегося списка). Допускается выбрать несколько портов;

– порт назначения трафика (выбор из раскрывающегося списка). Допускается выбрать только один порт;

Примечание. Конфигурация не будет выполнена, если в качестве порта источника и порта назначения будет выбран один и тот же порт.

ВНИМАНИЕ! Будьте осторожны при выборе в качестве порта назначения физического интерфейса, так как в этом случае существует вероятность образования петли и потери доступа к интерфейсу управления системы SpaceVM. Это зависит от настройки подключения SpaceVM к транспортной сети предприятия;

– направление трафика (выбор из раскрывающегося списка). Может принимать значения «ingress» (входящий трафик), «egress» (исходящий трафик) или «ingress-and-egress» (входящий и исходящий трафик).

ВНИМАНИЕ! Направление трафика – это направление трафика в портах источника. Направление трафика выбирается относительно коммутатора сервера SpaceVM. Другими словами, если выбрали направление трафика – «ingress», это означает «зеркалирование» трафика, который идет в направлении «входящем» в порт коммутатора сервера SpaceVM (но в направлении «исходящем» от виртуальной машины).

После заполнения всех полей необходимо подтвердить операцию, нажав кнопку «ОК».

В окне списка конфигураций появится созданная конфигурация зеркалирования. Таким образом создаются конфигурации Port-Mirroring. Поле «Статус» описывает текущее состояние конфигурации.

3.10.4.4.3. Для изменения параметров конфигурации необходимо выбрать соответствующую конфигурацию. В открывшемся окне необходимо нажать кнопку «Изменение параметров».

Для изменения доступны следующие параметры:

– порты источника;

– порт назначения;

– направление трафика.

3.10.4.4.4. Для удаления конфигурации необходимо выбрать соответствующую конфигурацию и в открывшемся окне подтвердить действие, нажав кнопку «Удалить».

3.10.4.4.5. В данном абзаце описывается совместимость SpaceVM с технологией «Зеркалирования трафика» Cisco RSPAN.

Примечание. Коммутаторы Cisco должны поддерживать технологию Cisco RSPAN. За описанием технологии Cisco RSPAN и настройкой следует обратиться к документации производителя оборудования.

Рассмотрим два варианта работы:

1) зеркалированный трафик «приходит» на SpaceVM со стороны коммутатора Cisco.

Схема выглядит так: зеркалированный трафик –> коммутатор Cisco (RSPAN) –> ... –> коммутатор Cisco (RSPAN) –> SpaceVM.

Пример. Необходимо проанализировать трафик с помощью специализированного ПО (анализатора трафика).

Для этого необходимо зеркалировать трафик источника и передать на ВМ, размещенную на SpaceVM. На ВМ необходимо установить специализированное ПО. В сетевой инфраструктуре назначается номер VLAN, в котором будет передаваться зеркалируемый трафик между коммутаторами. Сетевая подсистема SpaceVM также настраивается на прохождение трафика выбранного VLAN согласно документации SpaceVM.

Также необходимо создать ВМ для анализа трафика и добавить ее сетевой интерфейс в виртуальную сеть. Настройки ВМ и сети описаны в разделах 3.8 и 3.10 данного руководства;

2) зеркалированный трафик «уходит» с SpaceVM в сторону коммутатора Cisco.

Схема выглядит так: ПК <– коммутатор Cisco(RSPAN) <– ... <– коммутатор Cisco(RSPAN) <– SpaceVM («Зеркалирование трафика»).

При настройке «Зеркалирования трафика» на SpaceVM есть возможность выбрать физический порт в качестве порта назначения. Данный физический порт необходимо подключить к порту коммутатора и настроить этот порт на обработку зеркалированного трафика согласно документации производителя.

3.10.4.4.6. Проверка возможности зеркалирования трафика, приходящего с сетевых интерфейсов ВМ на сетевые интерфейсы других ВМ осуществляется следующим образом:

1) предварительно необходимо подготовить инфраструктуру SpaceVM:

– для простоты проверки необходимо, чтобы в инфраструктуре был развернут DHCP-сервис и настроена маршрутизация таким образом, чтобы ВМ получали IP-адресацию автоматически и имели доступ в Интернет;

– создать «Виртуальную сеть» через оснастку «Управление виртуальными сетями» Web-интерфейса SpaceVM. В процессе создания «Виртуальной сети» задать подключение к физической сети;

– создать три ВМ на одном и том же сервере. В процессе создания ВМ необходимо добавить хотя бы один сетевой интерфейс для каждой ВМ. Сетевые интерфейсы ВМ должны быть добавлены к одной и той же «Виртуальной сети»;

– установить ОС на созданные ВМ.

Примечания:

1. Если установленная ОС будет без GUI (Graphical user interface), то необходимо обладать практическими навыками работы в консольном режиме ОС.

2. В данном примере в качестве ОС ВМ используется ОС Debian 10.3.0. Все команды на ОС ВМ будут выполняться в консольном режиме от имени пользователя «root»;

– через оснастку «Терминал» SpaceVM необходимо выполнить проверку настройки IP-адресации сетевого интерфейса на каждой ОС ВМ.

Для примера предположим, что DHCP-сервер назначил следующие IP-адреса для каждой ВМ:

а) сетевому интерфейсу ВМ-1 назначен IP-адрес «192.168.20.87» с маской «/24»;

б) сетевому интерфейсу ВМ-2 назначить IP-адрес «192.168.20.222» с маской «/24»;

в) сетевому интерфейсу ВМ-3 назначен IP-адрес «192.168.20.209» с маской «/24»;

– проверить IP доступность между ВМ можно утилитой «ping». Выполним эту проверку с ВМ-1. Для этого в консоле ОС выполним команды:

ping 192.168.20.222 -c 4

ping 192.168.20.209 -c 4

Доступность по IP между ВМ будет выполнена успешно, если в результате выполнения каждой команды на экране будет строка вида

4 packets transmitted, 4 received, 0% packet loss

Необходимые предварительные требования завершены;

2) выполним настройку «Зеркалирования трафика» (входящего и исходящго) порта ВМ-3 на порт ВМ-2.

Примечание. Настройка сервиса «Port-Mirroring» происходит в разделе «Сети», далее перейти в раздел «Контроль трафика», выбрать «Политики Виртуальных сетей», далее выбрать «Зеркалирование портов».

Для того чтобы добавить конфигурацию зеркалирования, необходимо нажать кнопку «Добавить зеркалирование портов».

В открывшемся окне необходимо задать следующие параметры:

– название – название конфигурации;

– описание – описание конфигурации (необязательный параметр);

– сервер – выбрать сервер, на котором были установлены ВМ-2 и ВМ-3;

– порты источника – выбрать из раскрывающегося списка интерфейс ВМ-3;

– порт назначения – выбрать из раскрывающегося списка интерфейс ВМ-2;

– направление трафика – выбрать из раскрывающего списка направление трафика «ingress-and-egress».

ВНИМАНИЕ! «Направление трафика» – это направление трафика в портах источника. Оно выбирается относительно коммутатора сервера SpaceVM. Другими словами, если выбрали «Направление трафика: ingress», это означает «зеркалирование» трафика, который идет в направлении «входящем» в порт коммутатора сервера SpaceVM (но в направлении «исходящем» от виртуальной машины).

После заполнения полей формы необходимо нажать кнопку «ОК».

В окне списка конфигураций появится созданная конфигурация зеркалирования;

3) выполним процедуру проверки «Зеркалирования трафика» с порта ВМ-3 на порт ВМ-2:

– для этого необходимо перейти в «Терминал» SpaceVM ВМ-1, затем выполнить команду

ping 192.168.20.209

– затем необходимо произвести «захват» интересующего нас трафика. Для этого выполним команду

tcpdump -i ens4 icmp

ВНИМАНИЕ! Ens4 – это имя интерфейса, на котором работает утилита «tcpdump». В вашем случае имя интерфейса может быть другим. Для того чтобы узнать имя интерфейса, необходимо выполнить команду *ip addr show* и найти на каком интерфейсе настроен IP-адрес «192.168.20.222».

В результате выполнения команды вывод на экран должен содержать следующее:

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on ens4, link-type EN10MB (Ethernet), capture size 262144 bytes

08:51:52.728457 IP 192.168.20.87 > 192.168.20.209: ICMP echo request, id 577, seq 309, length 64

08:51:52.729384 IP 192.168.20.209 > 192.168.20.87: ICMP echo reply, id 577, seq 309, length 64

08:51:53.730499 IP 192.168.20.87 > 192.168.20.209: ICMP echo request, id 577, seq 310, length 64

08:51:53.731185 IP 192.168.20.209 > 192.168.20.87: ICMP echo reply, id 577, seq 310, length 64

08:51:54.732128 IP 192.168.20.87 > 192.168.20.209: ICMP echo request, id 577, seq 311, length 64

08:51:54.734222 IP 192.168.20.209 > 192.168.20.87: ICMP echo reply, id 577, seq 311, length 64

Примечание. Приведена только часть вывода.

Таким образом, была произведена настройка «Зеркалирования трафика» с порта ВМ-3 на порт ВМ-2. Согласно выводу утилиты «tcpdump», запущенной на ВМ-2, видим «входящий» и «исходящий» трафик интерфейса ВМ-3.

Примечание. Для простоты в данном примере использовали ICMP-трафик и утилиту «tcpdump», чтобы увидеть сам факт работы сервиса «Зеркалирования трафика».

3.10.4.4.7. Проверка возможности «Зеркалирования трафика», приходящего с сетевых интерфейсов ВМ на сетевые интерфейсы физических серверов, осуществляется подобным образом.

Примечание. Настройка сервиса «Port-Mirroring» происходит в разделе «Сети», далее перейти в раздел «Контроль трафика», выбрать «Политики Виртуальных сетей», далее выбрать «Зеркалирование портов».

Единственное отличие заключается в том, что при настройке сервиса «Зеркалирования трафика» в качестве «Порта назначения» небходимо выбирать физический интерфейс SpaceVM, к которому подключен физический сервер.

ВНИМАНИЕ! Будьте осторожны при выборе в качестве «Порт назначения» физического интерфейса, через который выполняется управление SpaceVM, так как в этом случае существует вероятность образования петли и потери доступа к интерфейсу управления системы SpaceVM. Это зависит от настройки подключения SpaceVM к транспортной сети предприятия.

3.10.4.5. События и теги

3.10.4.5.1. В окне «Сети» – «Контроль трафика» – <имя политики безопасности> – «События» отображаются события, зарегистрированные в системе, возникающие при выполнении правил, с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.10.4.5.2. В окне «Сети» – «Контроль трафика» – <имя политики безопасности> – «Теги» можно добавить правилу отличительную метку (тег), применить тег, а также обновить теги.

3.10.5. Виртуальные сети

3.10.5.1. Общие сведения

3.10.5.1.1. Объединение виртуальной сети между серверами осуществляется на основе технологии VxLAN, что накладывает ограничение на значение MTU внутри виртуальной сети.

Оно должно быть меньше на 54 байта, чем минимальное значение MTU внутренних интерфейсов серверов, которые объединяются VxLAN-туннелями.

Таким образом, если виртуальная сеть строится с использованием интерфейсов управления, при стандартном размере MTU для «mgmt» интерфейса в «1500» для виртуальной сети и распределенного коммутатора размер MTU не может превышать 1446 байта. Если ПО на ВМ в силу технических особенностей требует штатного значения размера MTU, можно обойти данное ограничение увеличив значение MTU на физическом коммутаторе и порт-группе, используемой для виртуальной сети. Перед увеличением значения MTU для порт-группы «management» коммутатора «default» необходимо удостовериться, что физический коммутатор, к которому подключены серверы, поддерживает «jumbo frames» и данная опция включена. Максимальное значение размера пакета на коммутаторе указано в документации к нему.

Виртуальная сеть, не имеющая подключения к внешней сети, будет находиться в изоляции от внешней сети и сможет коммутировать только трафик между ВМ, которые имеют сетевой адаптер, подключенный к данной сети, а связность между ВМ, расположенными на разных узлах, будет обеспечиваться при помощи VxLAN.

3.10.5.1.2. Управление виртуальными сетями осуществляется в разделе «Сети» – «Виртуальные сети» основного меню. В нем перечислены все созданные в кластерах виртуальные сети со следующей информацией:

– название виртуальной сети;

– связность;

– адрес подсети;

– VLAN ID;

– использование брандмауэра;

– статус подключения.

В окне управления виртуальными сетями имеется возможность:

– обновить информацию по кнопке  ;

– создать виртуальную сеть.

При выборе существующей виртуальной сети открывается окно с информацией о ней. Управление параметрами виртуальной сети осуществляется в этом же окне с помощью соответствующей вкладки.

Для управления доступны следующие вкладки:

– «Информация»;

– «Структура»;

– «Подключенные виртуальные машины»;

– «Настройки DHCP» (доступно только в том случае, если создан контейнер сетевых служб);

– «Настройки брандмауэра» (доступно только в том случае, если создан контейнер сетевых служб);

– «Разграничение доступа для операторов»;

– «События»;

– «Теги».

Если службы брандмауэра или DHCP не были активированы, то соответствующие вкладки могут не отображаться.

3.10.5.1.3. Виртуальная сеть представляет собой комплекс из виртуальных коммутаторов, созданных на каждом вычислительном узле кластера. Виртуальные коммутаторы для каждой виртуальной сети создаются автоматически на этапе создания виртуальной сети. Виртуальные коммутаторы объединяются в одну логическую сеть с помощью L2-туннелей по протоколу VxLAN. При необходимости доступа к физической (внешней) сети коммутатор виртуальной сети и виртуальный коммутатор, через который осуществляется доступ к физической сети, соединены «патч-интерфейсом». Если для виртуальной сети будут настроены несколько подключений к физической сети, то только одно из них будет активно, а остальные будут резервными. Прохождение трафика через резервные соединения блокируется на уровне виртуальных коммутаторов.

Состояние подключений к физической сети отслеживается автоматически и, в случае необходимости, происходит переключение. Также пользователю предоставлена возможность вручную изменять состояние подключения к физической сети с резервного на активное.

Примечание. Патч-интерфейс – это виртуальная сущность, которая служит для соединения двух виртуальных коммутаторов между собой и обеспечивает прохождение между ними траффика.

Также предоставлена возможность, в рамках одной виртуальной сети, создать сетевые службы – DHCP, NAT и брандмауэр.

Сетевые службы запускаются в контейнере и, в случае использования брандмауэра или NAT, подключаются между коммутатором виртуальной сети и ВК, используемым для подключения к физической сети на вычислительном узле, на котором расположено активное подключение к физической сети данной виртуальной сети.

Примечание. Для балансировки нагрузки на вычислительные узлы и сетевого трафика рекомендуется для разных виртуальных сетей настраивать активные подключения к физической сети на разных вычислительных узлах.

При создании виртуальной сети с сетевыми службами параметр «Подсеть» является определением сети и ее маски, которую будут обслуживать DHCP, SNAT, DNAT и брандмауэр.

При создании контейнера сетевых служб задаются два виртуальных сетевых интерфейса – «internal» (внутренний) и «external» (внешний). При создании внешнего сетевого интерфейса его настройка должна соответствовать той физической сети, к которой он будет подключен. Также внутренний сетевой интерфейс должен соответствовать параметру «Подсеть» виртуальной сети и, желательно, быть для нее шлюзом «по умолчанию» в соответствии с RFC.

3.10.5.1.4. Существует возможность создать виртуальную сеть без связности. В этом случае вычислительные узлы, входящие в виртуальную сеть, не будут объединены L2-туннелями.

Если необходимо, чтобы ВМ имели IP-связность через другие виртуальные коммутаторы узла и другие физические интерфейсы, нужно создать физическое подключение от коммутатора виртуальной сети к заранее созданному виртуальному коммутатору типа «mixed» или «uplink». Этот коммутатор должен иметь подключение к физическому интерфейсу узла.

3.10.5.2. Создание виртуальной сети

3.10.5.2.1. Для создания виртуальной сети необходимо в разделе «Сети» – «Виртуальные сети» основного меню нажать кнопку «Создать».

Далее следовать шагам мастера создания виртуальной сети:

1) на шаге 1 «Общие настройки» необходимо заполнить следующие поля:

– название;

– описание (при необходимости);

– переключатель связности («по умолчанию» – без связности);

– VNI (идентификатор сети, заполняется автоматически);

– VLAN (заполняется автоматически, для создания виртуальной сети без VLAN необходимо указать «0»);

– MTU.

После заполнения полей необходимо нажать кнопку «Далее» и перейти к шагу 2;

2) на шаге 2 «Добавление серверов» необходимо выбрать серверы, подключаемые к виртуальной сети:

– включить (выключить) опцию «Использовать интерфейсы управления». Опция определяет, будут ли в качестве точек подключения L2-туннелей, посредством которых серверы объединяются в единое L2-пространство, использоваться интерфейсы управления «mgmt»;

– нажать «Добавить сервер» и в открывшемся окне, если переключатель в положении «вкл», будет раскрывающийся список, в котором необходимо выбрать подключаемые серверы (возможно выбрать несколько значений единовременно), если переключатель в положении «выкл», будет два раскрывающихся списка. В первом списке необходимо выбрать подключаемый сервер, а во втором –внутренний интерфейс, который будет использоваться в качестве точки подключения.

После заполнения полей необходимо подтвердить операцию, нажав «Добавить».

Нажать на кнопку «Далее» и перейти к шагу 3;

3) на шаге 3 «Создание сетевых служб» (только для сетей с L2-связностью) в открывшемся окне необходимо включить (выключить) использование сетевых служб виртуальной сети.

Если опция «Создать сетевые службы» включена, то необходимо заполнить следующую информацию:

– адрес подсети – задает подсеть, которую будет обслуживать DHCP-сервер;

– выбрать ограничение по памяти (Мбайт) – максимальный размер оперативной памяти, доступный сетевым службам;

– интерфейсы сетевых служб виртуальной сети – можно создать сетевые интерфейсы для контейнера сетевых служб, нажав кнопку «Добавить интерфейс» и в открывшемся окне заполнить поля:

а) направление (выбор из раскрывающегося списка) – «Internal» или «external». Интерфейс типа «internal» будет внутренним интерфейсом, доступным со стороны виртуальной сети и ВМ, подключенным к ней. Интерфейс типа «external» будет внешним интерфейсом, доступным для внешних сетей;

б) DHCP – только для интерфейса типа «external»;

в) IP-адрес и маска подсети;

г) MAC-адрес – если не указан, то будет сгенерирован автоматически.

Примечание. Если интерфейсы не были добавлены пользователем, они будут созданы автоматически.

После заполнения полей необходимо нажать на кнопку «Добавить»;

– включить (выключить) настройки DHCP – позволяет задать настройки DHCP-сервера виртуальной сети.

Если опция включена, то необходимо ввести:

а) пулы адресов – позволяет добавить пул адресов, из которого будут назначаться адреса ВМ, нажав кнопку «Добавить пул». В открывшемся окне заполнить начальный и конечный адреса пула, после чего нажать кнопку «Добавить»;

б) резервирование адресов – позволяет добавить резервирование IP-адреса для указанного MAC-адреса, нажав кнопку «Добавить адрес». В открывшемся окне заполнить поля «hw-adress» и «ip-adress», после чего нажать кнопку «Добавить»;

в) опции DHCP – позволяет добавить опциональные параметры, отдаваемые DHCP-сервером, нажав кнопку «Добавить опцию». В открывшемся окне заполнить название опции (выбор из раскрывающегося списка), код опции (выбор из раскрывающегося списка) и данные опции, после чего нажать кнопку «Добавить»;

г) включение (выключение) автозапуска DHCP – указывает, будет ли служба DHCP запускаться автоматически при запуске сетевых служб;

– включить (выключить) опцию «Использование брандмауэра» для этой сети – определяет будет ли в виртуальной сети использоваться брандмауэр.

Если опция включена, то необходимо задать его параметры:

а) политика фильтрации виртуальной сети – используемый службой брандмауэра набор правил фильтрации трафика, а также правил NAT;

б) автозапуск брандмауэра – указывает, будет ли служба брандмауэра запускаться автоматически при запуске сетевых служб.

После заполнения полей необходимо нажать на кнопку «Далее» и перейти к шагу 4;

4) на шаге 4 «Задание физического подключения» можно добавить физическое подключение виртуальной сети. В открывшемся окне необходимо включить (выключить) опцию «Задать подключение к физической сети».

Если опция включена, то необходимо выбрать из раскрывающегося списка ВК, который будет использоваться виртуальной сетью в качестве физического подключения.

Подключение виртуальной сети к физической сети описано в 3.10.5.4. Подсеть должна соответствовать формату Ipv4.

Если опция использования брандмауэра или создания сетевых служб отключена, то их можно включить и настроить позже в свойствах виртуальной сети.

После заполнения полей необходимо нажать на кнопку «Далее» и перейти к шагу 5;

5) на шаге 5 «Сводка всех настроек» проверяются введенные данные. После проверки необходимо подтвердить операцию, нажав на кнопку «ОК».

3.10.5.3. Свойства виртуальной сети

3.10.5.3.1. При выборе виртуальной сети из уже созданных сетей в группе, открывается окно состояния сети. В окне «Сети» – «Виртуальные сети» – <имя сети> доступны следующие операции:

– обновление информации о сети по кнопке  ;

– удаление виртуальной сети;

– сброс ошибки.

3.10.5.3.2. При нажатии кнопки «Удалить виртуальную сеть» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «Да».

3.10.5.3.3. При нажатии кнопки «Сброс ошибки» в открывшемся окне необходимо подтвердить операцию, нажав кнопку «Да».

3.10.5.3.4. В окне «Сети» – «Виртуальные сети» – <имя сети> – «Информация» содержатся следующие сведения о виртуальной сети:

1) название (редактируемый параметр);

2) описание (редактируемый параметр);

3) подсеть и маска;

4) настройка VLAN;

5) идентификатор сети VNI;

6) MTU сети;

7) состояние брандмауэра сети (редактируемый параметр). Включение и отключение брандмауэра производится нажатием кнопки  . Если контейнер сетевых служб не запущен, то и брандмауэр не функционирует, а виртуальная сеть находится в изоляции от физической сети. При этом связанность данной сети между серверами кластера сохраняется;

8) параметры Netflow (редактируемый параметр). Раскрывающийся список содержит следующую информацию:

– IP коллектора;

– порт коллектора;

– тайм-аут активного потока;

– добавление ID к названию интерфейса (вкл/выкл);

9) статус;

10) физический интерфейс, через который сеть подключена (раскрывающийся список с возможностью добавления по кнопке ).

При нажатии  открывается окно подключения ВК с выбором из раскрывающегося списка. Для подтверждения операции необходимо нажать кнопку «ОК».

В раскрывшейся информации о ВК имеются следующие параметры:

– название ВК;

– сервер, к которому подключен ВК;

– состояние;

– возможность удаления по кнопке «Удалить».

О подключении виртуальной сети к физической смотрите в 3.10.5.4;

11) серверы, на которых развернута сеть (раскрывающийся список с возможностью добавления по кнопке ). При нажатии  открывается окно добавления сервера с опцией «Использовать интерфейсы подключения», с выбором из раскрывающегося списка сервера и интерфейса управления при выключенной опции. Для подтверждения операции необходимо нажать кнопку «ОК».

В раскрывшейся информации о сервере имеются следующие параметры:

– название сервера (его IP-адрес);

– интерфейс управления (название и IP-адрес);

– статус;

– возможность удаления по кнопке «Удалить»;

12) информация о порт-группе:

– название;

– тип;

– режим VLAN;

– тег VLAN;

– транки;

– количество интерфейсов.

3.10.5.3.5. В окне «Сети» – «Виртуальные сети» – <имя сети> – «Структура» содержится схематичное представление выбранной виртуальной сети, которое включает следующие объекты виртуальной инфраструктуры:

– распределенный коммутатор;

– серверы;

– порт-группа;

– виртуальные машины;

– физическое подключение.

При наведении на объект высвечивается его краткая характеристика.

3.10.5.4. Подключение виртуальной сети к физической сети

3.10.5.4.1. Подключение виртуальной сети к физической сети может быть осуществлено при создании виртуальной сети или путем изменения настроек виртуальной сети после ее создания.

3.10.5.4.2. Для подключения виртуальной сети к физической сети во время ее создания, необходимо на шаге 4 мастера создания виртуальной сети включить опцию «Задать подключение к физической сети» и выбрать из предлагаемого списка виртуальный коммутатор, через который будет осуществлено подключение к физической сети.

3.10.5.4.3. Для подключения виртуальной сети к физической сети после ее создания необходимо перейти в окно «Сети» – «Виртуальные сети» – <имя сети> – «Информация» и в поле «Физическое подключение» нажать кнопку  , в результате чего откроется окно для выбора виртуального коммутатора, через который будет осуществляться подключение к физической сети.

3.10.5.4.4. Если был выбран виртуальный коммутатор, входящий в состав внешней сети («Сети» – «Внешние сети»), то виртуальная сеть будет подключена к виртуальным коммутаторам этой внешней сети на всех подключенных к ней узлах. Активным будет подключение через выбранный виртуальный коммутатор.

Предположим, что виртуальная сеть «vnet1» создана на узлах «node1», «node2», «node3» и «node4», при этом «node2» – «node4» подключены к внешней сети «external».

При подключении виртуальной сети «vnet1» к физической сети через виртуальный коммутатор, входящий в состав внешней сети «external» на узле «node3», автоматически будут созданы резервные подключения на узлах «node2» и «node4». Подключение на узле «node3» будет активным.

3.10.5.4.5. Если у виртуальной сети есть подключение к физической сети через виртуальный коммутатор, не входящий в состав какой-либо внешней сети, то невозможно добавить физическое подключение через виртуальный коммутатор, входящий в состав внешней сети.

И наоборот, если виртуальная сеть подключена к физической сети через виртуальные коммутаторы, входящие в состав внешней сети, невозможно добавить физическое подключение через отдельный виртуальный коммутатор.

3.10.5.4.6. При удалении физического подключения виртуальной сети, которое использовало виртуальный коммутатор, входящий в состав внешней сети, будут удалены все подключения к физической сети данной виртуальной сети.

3.10.5.4.7. Если виртуальная сеть подключена к физической сети с помощью виртуальных коммутаторов, входящих в состав внешней сети, то при добавлении узла к виртуальной сети, если данный узел также подключен к этой внешней сети, на нем автоматически будет создано резервное подключение виртуальной сети к физической сети.

3.10.5.5. Настройка DHCP-сервера для виртуальной сети

3.10.5.5.1. Для настройки сервиса DHCP-сервера для виртуальной сети необходимо перейти во вкладку «Настройки DHCP» окна состояния виртуальной сети.

3.10.5.5.2. В данной вкладке отображается следующая информация:

– состояние службы DHCP;

– необходимость автозапуска службы с запуском контейнера сетевых служб (редактируемый параметр);

– время аренды IP-адреса;

– диапазон адресов, выдаваемых ВМ (редактируемый параметр);

– список привязок IP-адресов к MAC-адресам (резервирование, редактируемый параметр);

– опции DHCP (редактируемый параметр). Содержит поля – название, код и адрес.

Новые параметры применяются после перезапуска службы DHCP.

3.10.5.5.3. Возможные опции DHCP-сервера для виртуальной сети следующие:

– *code=3, name=’routers’*;

– *code=4, name=’time-servers’*;

– *code=5, name=’name-servers’;*

– *code=6, name=’domain-name-servers’;*

– *code=15, name=’domain-name’;*

– *code=23, name=’default-ip-ttl’;*

– *code=24, name=’path-mtu-aging-timeout’;*

– *code=25, name=’path-mtu-plateau-table’;*

– *code=26, name=’interface-mtu’;*

– *code=28, name=’broadcast-address’;*

– *code=35, name=’arp-cache-timeout’;*

– *code=37, name=’default-tcp-ttl’;*

– *code=38, name=’tcp-keepalive-interval’;*

– *code=39, name=’tcp-keepalive-garbage’;*

– *code=42, name=’ntp-servers’;*

– *code=44, name=’netbios-name-servers’;*

– *code=66, name=’tftp-server-name’;*

– *code=67, name=’boot-file-name’.*

– *code=119, name=’domain-search’.*

Опция *«code=119, name='domain-search'»* выполняет поиск доменов DNS. Список доменов будет использоваться для выполнения DNS-запросов на основе короткого имени с использованием суффиксов, представленных в этом списке.

3.10.5.6. Настройки брандмауэра для виртуальной сети

3.10.5.6.1. Для настройки брандмауэра и функционирующего на его основе NAT-сервиса необходимо в разделе «Контроль трафика» основного меню выбрать целевую политику безопасности и настроить в ней набор правил для данной виртуальной сети. Создание и настройка политики безопасности и набора правил описаны в 3.10.4 данного руководства.

3.10.5.6.2. В данной вкладке отображается следующая информация:

1) состояние службы брандмауэра;

2) необходимость старта службы с запуском контейнера сетевых служб (редактируемый параметр);

3) политика фильтрации трафика (редактируемый параметр). Политика фильтрации трафика выбирается из созданных ранее наборов правил, управление которыми выполняется в разделе «Сети» – «Контроль трафика» основного меню;

4) состояние политики безопасности;

5) логирование;

6) список правил для входящего трафика;

7) список правил для исходящего трафика;

8) правила source NAT (по источнику);

9) правила destination NAT (по получателю);

10) действия с правилами:

– добавление;

– применение;

– удаление.

3.10.5.7. Добавление резервных физических подключений в виртуальную сеть с L2-связностью

3.10.5.7.1. Для проведения проверок необходимо иметь несколько серверов, подключенных к физической сети как минимум двумя физическими сетевыми интерфейсами.

3.10.5.7.2. Необходимо как минимум на одном сервере создать виртуальный коммутатор с группой портов типа «uplink» и подключить к нему физический сетевой интерфейс, подключенный к физической сети.

Для этого необходимо перейти в раздел «Серверы» основного меню, выбрать целевой сервер, перейти во вкладку «Сети» – «Виртуальные коммутаторы» и нажать кнопку «Добавить виртуальный коммутатор». Далее в открывшемся окне ввести следующие параметры:

– название – «uplink-sw»;

– тип – «uplink».

После чего нажать кнопку «ОК».

В списке виртуальных коммутаторов выбрать созданный виртуальный коммутатор «uplink-sw» и в окне состояния нажать кнопку «Добавить порт-группу». Далее в открывшемся окне ввести следующие параметры:

– название – «uplink group»;

– режим VLAN – «none»;

– тип – «uplink»;

– значение MTU.

После чего нажать кнопку «ОК».

Далее нажать кнопку «Подключить интерфейс» и в открывшемся окне ввести следующие параметры:

1) на шаге 1 ввести тип «physical» и нажать кнопку «Далее»;

2) на шаге 2 выбрать из раскрывающегося списка физический сетевой интерфейс, подключенный к физической сети. Включить опцию «Включить после подключения» и нажать кнопку «Далее»;

3) на шаге 3 выбрать из раскрывающегося списка порт-группу «uplink group» и нажать кнопку «ОК».

3.10.5.7.3. Далее необходимо создать виртуальную сеть с активным и резервным физическими подключениями. Для этого перейти в раздел «Сети» – «Виртуальные сети» основного меню и нажать кнопку «Создать». В открывшемся окне ввести следующие параметры:

1) на шаге 1 ввести название «virtual network» и нажать кнопку «Далее»;

2) на шаге 2 включить опцию «Использовать интерфейсы управления» и нажать кнопку «Добавить сервер».

В открывшемся окне выбрать из раскрывающегося списка серверы, включая сервер, на котором создан виртуальный коммутатор «uplink-sw», подключаемые к виртуальной сети (в раскрывающемся списке допускается выбор нескольких серверов одновременно). Нажать кнопку «Добавить» и потом «Далее»;

3) на шаге 3 нажать кнопку «Далее»;

4) на шаге 4 включить опцию «Задать подключение к физической сети», при этом станет доступно поле «Подключение к физической сети», где в раскрывающемся списке выбрать виртуальный коммутатор «uplink-sw» и нажать кнопку «ОК».

В списке виртуальных сетей выбрать виртуальную сеть «virtual network», во вкладке «Информация», нажать рядом с полем «Физическое подключение» кнопку  . В открывшемся окне необходимо выбрать из раскрывающегося списка виртуальный коммутатор «default», расположенный на сервере, отличном от сервера, на котором расположен виртуальный коммутатор «uplink-sw» и нажать кнопку «ОК».

3.10.5.7.4. Далее необходимо создать ВМ на сервере, отличном от того, на котором расположен виртуальный коммутатор «uplink-sw».

Проверка возможна при загрузке с live-cd, поэтому создание диска и последующая установка операционной системы необязательны. После создания ВМ перейти в раздел «Виртуальные машины» основного меню, выбрать созданную ВМ, перейти во вкладку «Интерфейсы» и нажать кнопку «Добавить виртуальный интерфейс».

Далее в открывшемся окне ввести следующие параметры:

– выбрать из раскрывающегося списка виртуальную сеть «virtual network»;

– выбрать из раскрывающегося списка nic_driver «virtio» и нажать кнопку «ОК».

3.10.5.7.5. Включить созданную ВМ после завершения загрузки. Если физические сетевые интерфейсы серверов подключены к физической сети с доступным DHCP-сервером убедиться, что ВМ получила IP-адрес от DHCP сервера. В противном случае назначить сетевому интерфейсу ВМ IP-адрес, маску подсети, а также настроить основной шлюз, соответствующие конфигурации физической сети, к которой подключены серверы. В терминале ВМ выполнить команду *ping 77.88.8.1*, убедиться, что приходят ответы на echo-запросы. Не прерывая выполнения команды «ping», перейти в раздел «Серверы» основного меню и выбрать сервер, на котором расположен виртуальный коммутатор «uplink-sw».

Нажать кнопку «Сервисный режим» и в открывшемся окне нажать кнопку «Перейти». После завершения перехода узла в сервисный режим убедиться, что в терминале ВМ продолжается выполнение команды «ping» и приходят ответы на echo-запросы.

3.10.5.8. Выбор внутренних интерфейсов распределенного коммутатора при создании виртуальной сети

3.10.5.8.1. Проверка осуществляется следующим образом:

1) необходимо на всех серверах, подключаемых к виртуальной сети, создать виртуальный коммутатор типа «mixed» с группами портов типа «uplink» и «internal» и подключить к нему физический сетевой интерфейс, подключенный к физической сети, а также создать на нем внутренний интерфейс. Для этого необходимо перейти в раздел «Серверы» основного меню, выбрать целевой сервер, перейти во вкладку «Сети» – «Виртуальные коммутаторы» и нажать кнопку «Добавить виртуальный коммутатор».

В открывшемся окне ввести следующие параметры:

– название – «tunnel-sw»;

– тип – «mixed».

Далее нажать кнопку «ОК».

В списке виртуальных коммутаторов выбрать созданный виртуальный коммутатор «tunnel-sw» и в окне состояния создать две порт-группы. Нажать кнопку «Добавить порт-группу» и в открывшемся окне ввести следующие параметры:

– название – «uplink group»;

– режим VLAN – «none»;

– тип – «uplink».

Далее нажать кнопку «ОК».

Еще раз нажать кнопку «Добавить порт-группу» и в открывшемся окне ввести следующие параметры:

– название – «internal group»;

– режим VLAN – «none»;

– тип – «internal»;

– MTU – «1500».

Далее нажать кнопку «Подключить интерфейс». В открывшемся окне ввести следующие параметры:

а) на шаге 1 выбрать тип из раскрывающегося списка «physical» и нажать кнопку «Далее»;

б) на шаге 2 выбрать физический сетевой интерфейс из раскрывающегося списка, подключенный к физической сети. Включить опцию «Включить после подключения» и нажать кнопку «Далее»;

в) на шаге 3 выбрать порт-группу из раскрывающегося списка «uplink group» и нажать кнопку «ОК».

Еще раз нажать кнопку «Подключить интерфейс» и в открывшемся окне ввести следующие параметры:

а) на шаге 1 выбрать тип из раскрывающегося списка «internal» и нажать кнопку «Далее»;

б) на шаге 2 заполнить:

– название – «tep»;

– переключатель «Протокол DHCP» перевести в состояние «выкл»;

– IP-адрес и маска подсети – заполнить для каждого сервера таким образом, чтобы выделенные адреса были доступны для каждого сервера.

Проверку доступности можно провести, выполнив команду

ping {ip-address} -I tep,

где {ip-address} – адрес, назначенный интерфейсу «tep» сервера, отличного от того, на котором запускается команда;

– MAC-адрес генерируется автоматически, менять не нужно.

Нажать кнопку «Далее»;

в) на шаге 3 выбрать порт-группу из раскрывающегося списка «internal group» и нажать кнопку «ОК»;

2) после выполнения вышеуказанных шагов на каждом из серверов, которые планируется подключить к виртуальной сети, необходимо создать виртуальную сеть. Для этого перейти в раздел «Сети» – «Виртуальные сети» основного меню и нажать кнопку «Создать». В открывшемся окне ввести следующие параметры:

– на шаге 1 ввести название «virtual network» и нажать кнопку «Далее»;

– на шаге 2 выключить опцию «Использовать интерфейсы управления» и нажать кнопку «Добавить сервер».

В открывшемся окне выбрать сервер, подключаемый к виртуальной сети, в раскрывающемся списке «Интерфейс управления» выбрать интерфейс «tep». Нажать кнопку «Добавить». Повторить для каждого сервера, который планируется подключить к виртуальной сети. Нажать кнопку «Далее»;

– на шаге 3 нажать кнопку «Далее»;

– на шаге 4 выключить опцию «Задать физическое подключение и нажать кнопку «ОК».

3) подключиться к любому из серверов, включенных в виртуальную сеть по SSH. Выполнить команду *tcpdump -i tep udp*, убедиться, что в выводе команды присутствуют строки, содержащие

IP {server-addr}.52045 > {peer-addr}.4789: VXLAN, flags [I] (0x08), vni {vnet-vni}

где {server-addr} – адрес интерфейса «tep» сервера, на котором запущена команда;

{peer-addr} – адреса интерфейсов «tep» серверов, также подключенных к виртуальной сети;

{vnet-vni} – VNI виртуальной сети, присвоенный ей при создании.

3.10.5.9. Подключенные виртуальные машины

3.10.5.9.1. В окне «Сети» – «Виртуальные сети» – <имя сети> –«Подключенные виртуальные машины» перечислены все ВМ, подключенные к данной сети. Также существует возможность обновления информации о ВМ и добавления ВМ.

3.10.5.9.2. При нажатии кнопки «Подключить ВМ» в открывшемся окне необходимо заполнить следующие поля:

– виртуальную машину (выбор из раскрывающегося списка);

– NIC-драйвер (выбор из раскрывающегося списка). Может принимать значения «virtio», «e1000», «rtl8139» или «vmxnet3»;

– описание;

– состояние линка, «по умолчанию» – включено;

– переключатель QoS.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

3.10.5.10. Разграничение доступа для операторов

3.10.5.10.1. В окне «Сети» – «Виртуальные сети» – <имя сети> – «Разграничение доступа для операторов» можно управлять доступом пользователей.

3.10.5.10.2. Для изменения списка пользователей виртуальных сетей необходимо нажать на кнопку «Изменить пользователей», далее в открывшемся окне выбрать из раскрывающегося списка пользователей для управления сетью и нажать «ОК».

3.10.5.11. События

3.10.5.11.1. В окне «Сети» – «Виртуальные сети» – <имя сети> – «События» отображаются события, зарегистрированные в системе для этой сети с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.10.5.12. Теги

3.10.5.12.1. В окне «Сети» – «Виртуальные сети» – <имя сети> – «Теги» имеется возможность добавления к сети отличительной метки (тега), применения и обновления тега.

3.10.5.12.2. Для создания нового тега необходимо нажать кнопку «Создать» и в открывшемся окне заполнить следующие поля:

– название тега;

– идентификатор тега (Slug);

– цвет тега из открывающейся палитры. При выборе цвета необходимо подтвердить изменения, нажав кнопку «ОК», либо выйти без сохранения изменений, нажав кнопку «Отмена».

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

3.10.5.12.3. Для применения нового тега необходимо нажать кнопку «Применить» и в открывшемся окне выбрать тег. Для сохранения изменений необходимо нажать кнопку «ОК».

3.10.6. Внешние сети

3.10.6.1. Общие сведения

3.10.6.1.1. Управление подключениями к внешним сетям осуществляется в разделе «Сети» – «Внешние сети» основного меню. В нем перечислены все созданные подключения к внешним сетям с указанием следующей информации:

– название внешней сети;

– адрес подсети;

– тег VLAN;

– значение MTU;

– серверы – количество подключенных вычислительных узлов;

– статуса подключения.

3.10.6.1.2. Каждое подключение к внешней сети представляет собой комплекс из внутреннего ВК, внешнего ВК, патч-соединения между ними, а также физического или агрегированного интерфейса, подключенного к внешнему ВК и, опционально, внутреннего интерфейса, подключенного к внутреннему ВК. Создается на каждом вычислительном узле, подключаемом к внешней сети.

3.10.6.1.3. При создании подключения к внешней сети, опциональный параметр «Подсеть» является определением адреса и маски сети, к которой производится подключение серверов. При указании этого параметра предоставляется возможность создания внутреннего интерфейса вычислительного узла, адрес которого должен входить в диапазон адресов указанной подсети. Также предоставляется возможность создания пулов адресов для их дальнейшего использования в качестве адресов интерфейсов ВМ и сетевых служб подключенных виртуальных сетей.

3.10.6.1.4. В разделе «Сети» – «Внешние сети» перечислены внешние сети управления. Также в окне «Внешние сети» имеется возможность обновить информацию по кнопке  и создать сеть.

3.10.6.1.5. При выборе существующего подключения к внешней сети открывается окно с информацией о выбранной внешней сети. Управление параметрами подключения осуществляется в этом же окне с помощью соответствующей вкладки.

Для управления доступны следующие вкладки:

– «Информация»;

– «Подключенные серверы»;

– «Подключенные виртуальные сети»;

– «События»;

– «Теги».

3.10.6.1.6. В данном окне имеется возможность удаления выбранной сети по кнопке «Удалить сеть».

3.10.6.1.7. В окне свойств внешней сети имеются следующие опции:

– «Использовать для миграции»;

– «Использовать для копирования и переноса файлов».

Для использования данных опций у каждого сервера во внешней сети должен быть внутренний интерфейс с IP-адресом. Если активного интерфейса нет или у интерфейса нет IP-адреса, то будет использоваться следующая внешняя сеть. Если адрес не найден, то используется адрес «mgmt» интерфейса выбранного сервера. Сервер может выбираться автоматически при миграции или берется первый случайный активный у пула данных назначения.

Если есть две и более внешних сети с установленными на каждой опциями «…для копирования и переноса файлов» и «…для миграции», то во всех случаях (миграция, копирование, клонирование) будет использована первая из отсортированных по имени внешних сетей с имеющимся активным интерфейсом с IP-адресом.

При этом допускается включить обе опции (копирование и миграция) на одной и той же внешней сети, которая в один и тот же момент времени может быть использована и для кластерного транспорта.

Ниже приведено описание операций миграции, копирования и клонирования при наличии внешней сети:

– клонирование – при наличии внешней сети с установленной опцией «…для копирования» диски будут переноситься или копироваться через нее, а если сети нет или не включена опция, то через «mgmt» интерфейс;

– миграция без переноса дисков – при наличии внешней сети с установленной опцией «…для миграции» ВМ будут мигрировать через нее, а если сети нет или не включена опция, то через «mgmt» интерфейс;

– миграция включенных ВМ с переносом дисков – при наличии внешней сети с установленной опцией «…для миграции» включенные ВМ будут мигрировать через нее, а если сети нет или не включена опция, то через «mgmt» интерфейс;

– миграция выключенных ВМ с переносом дисков – при наличии внешней сети с установленной опцией «…для копирования» выключенные ВМ будут мигрировать через нее, а если сети нет или не включена опция, то через «mgmt» интерфейс;

– копирование файлов, образов, дисков – при наличии внешней сети с установленной опцией «…для копирования» все будет переноситься или копироваться через нее, а если сети нет или не включена опция, то через «mgmt» интерфейс.

3.10.6.2. Создание подключения к внешней сети

3.10.6.2.1. Для создания подключения к внешней сети необходимо в разделе «Сети» – «Внешние сети» нажать кнопку «Создать», расположенную над списком существующих подключений к внешним сетям.

Далее следовать шагам мастера создания подключения к внешним сетям:

1) на шаге 1 доступны следующие поля и элементы управления:

– название;

– описание (необязательное поле);

– переключатель «Указать адрес подсети»;

– адрес подсети (доступно, если переключатель «Указать адрес подсети» находится в положении «вкл»).

После заполнения полей, необходимо подтвердить операцию, нажав кнопку «Далее»;

2) на шаге 2 доступны серверы и элементы управления.

Для добавления сервера необходимо нажать кнопку «Добавить» и заполнить открывшуюся форму, на которой доступны следующие поля и элементы управления:

– сервер – раскрывающийся список, содержащий все зарегистрированные на контроллере вычислительные узлы;

– интерфейс подключения – раскрывающийся список, содержащий доступные на сервере физические и агрегированные интерфейсы. Из списка исключены физические интерфейсы с включенной функцией SR-IOV и физические интерфейсы, входящие в состав агрегированных интерфейсов;

– переключатель «Создать агрегированный интерфейс». При включении переключателя «Создать агрегированный интерфейс» становится активной кнопка «Создать», при нажатии на которую откроется форма с параметрами нового агрегированного интерфейса, содержащая следующие поля и элементы управления:

а) название;

б) физические интерфейсы – раскрывающийся список доступных для включения в агрегацию физических интерфейсов вычислительного узла с возможностью выбора нескольких элементов списка;

в) тип агрегации (режим связи) – раскрывающийся список возможных значений;

г) связь протокола управления агрегацией каналов – раскрывающийся список возможных значений.

Также при выборе режима связи «balance-tcp» становятся доступными поля:

а) резервный вариант протокола управления агрегацией каналов – раскрывающийся список возможных значений;

б) время протокола управления агрегацией каналов – раскрывающийся список возможных значений.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «Добавить».

Если на шаге 1 был указан адрес внешней подсети, становится доступен переключатель «Добавить внутренний интерфейс». При переводе переключателя в положение «вкл», становится доступен переключатель «dhcp», указывающий на режим получения адреса создаваемым интерфейсом.

Если переключатель «dhcp» в положении «выкл», доступны поля:

а) название;

б) IP-адрес;

в) маска подсети;

г) MAC-адрес.

После заполнения полей, необходимо подтвердить операцию, нажав кнопку «Добавить».

После добавления серверов, необходимо подтвердить операцию, нажав кнопку «Далее». Для возврата на предыдущие шаги необходимо нажать кнопку «Назад»;

3) на шаге 3 доступны следующие поля и элементы управления:

– тег VLAN;

– mtu;

– пулы адресов. Для добавления пулов адресов внешней сети необходимо нажать кнопку «Добавить» и заполнить открывшуюся форму, на которой доступны следующие поля:

а) название;

б) описание;

в) начальный адрес;

г) конечный адрес.

После заполнения полей, необходимо подтвердить операцию, нажав кнопку «Добавить».

После заполнения полей на всех шагах мастера создания подключения к внешней сети необходимо подтвердить операцию, нажав кнопку «ОК».

3.10.6.3. Свойства внешней сети

3.10.6.3.1. В окне «Сети» – «Внешние сети» – «Информация» находится следующая информация о состоянии подключения к внешней сети:

1) название (редактируемый параметр);

2) описание (редактируемый параметр);

3) подсеть (редактируемый параметр);

4) VLAN (редактируемый параметр);

5) MTU (редактируемый параметр);

6) признак использования для миграции («да» или «нет»);

7) признак использования для копирования и переноса файлов («да» или «нет»);

8) статус;

9) дата и время изменения;

10) дата и время создания;

11) серверы (раскрывающийся список) с возможностью добавления по кнопке  .

Серверы содержат следующую информацию в табличном виде:

– название и статус подключенного сервера;

– название и статус физического или агрегированного интерфейса, с помощью которого сервер подключен к внешней сети;

– название и статус внутреннего интерфейса сервера, относящегося к внешней сети;

12) виртуальные сети (раскрывающийся список) с возможностью добавления по кнопке  . При нажатии  открывается окно добавления виртуальной сети, где необходимо выбрать из списка виртуальную сеть, добавить адрес, после нажать кнопку «ОК».

В раскрывшейся информации о виртуальной сети имеются следующие параметры:

– название;

– статус подключенной виртуальной сети;

13) пулы адресов (раскрывающийся список) с возможностью добавления по кнопке  .

При нажатии  открывается окно добавления пулов адресов, где необходимо заполнить название, описание, начальный и конечный адрес пула, после нажать кнопку «ОК».

В раскрывшейся информации о пуле адресов имеются следующие параметры:

– название;

– начальный адрес;

– конечный адрес;

– использованные адреса.

3.10.6.3.2. Для настройки и изменения параметров подключения доступны следующие поля и элементы управления:

1) рядом с полями «Название», «Описание», «Подсеть», «VLAN», «MTU», «Использовать для миграции», «Использовать для копирования и переноса файлов» расположена кнопка редактирования для изменения значения соответствующего параметра;

2) рядом с полем «Серверы» расположена кнопка «Добавление сервера», с помощью которой можно подключить к внешней сети новые серверы.

При нажатии на нее в открывшемся окне необходимо нажать «Добавить сервер» и заполнить открывшуюся форму, в которой доступны следующие поля и элементы управления:

– сервер – раскрывающийся список, содержащий все зарегистрированные на контроллере вычислительные узлы;

– интерфейс подключения – раскрывающийся список, содержащий все доступные физические и агрегированные интерфейсы выбранного вычислительного узла. Из списка исключены физические интерфейсы с включенной функцией SR-IOV и физические интерфейсы, входящие в состав агрегированных интерфейсов;

– переключатель «Создать агрегированный интерфейс»;

При включении переключателя «Создать агрегированный интерфейс» становится активной кнопка «Создать», при нажатии на которую откроется форма с параметрами нового агрегированного интерфейса, содержащая следующие поля и элементы управления:

– название;

– физические интерфейсы – раскрывающийся список доступных для включения в агрегацию физических интерфейсов вычислительного узла с возможностью выбора нескольких элементов списка;

– тип агрегации – режим связи (раскрывающийся список);

– связь протокола управления агрегацией каналов (раскрывающийся список).

Также при выборе режима связи «balance-tcp» становятся доступными поля:

– резервный вариант протокола управления агрегацией каналов (раскрывающийся список);

– время протокола управления агрегацией каналов (раскрывающийся список).

После заполнения полей необходимо подтвердить операцию, нажав кнопку «Добавить».

Если на шаге 1 был указан адрес внешней подсети, то становится доступен элемент управления – переключатель «Добавить внутренний интерфейс». При переводе переключателя в положение «вкл», становится доступен переключатель «dhcp», указывающий на режим получения адреса создаваемым интерфейсом.

Если переключатель «dhcp» в положении «выкл», доступны поля:

– название;

– IP-адрес;

– маска подсети;

– MAC-адрес.

После заполнения полей, необходимо подтвердить операцию, нажав кнопку «Добавить».

После добавления серверов, необходимо подтвердить операцию, нажав кнопку «ОК».

В последнем столбце таблицы, содержащей данные о подключенных серверах, в каждой строке расположена кнопка «Удалить», нажав на которую, можно отключить сервер от внешней сети. При этом на выбранном сервере будут удалены внутренний коммутатор и внутренний интерфейс (при наличии), относящиеся к внешней сети, внешний коммутатор, в случае если этот коммутатор был создан при подключении сервера к внешней сети, и, в этом же случае, будет удален агрегированный или отключен физический интерфейс, используемый для подключения сервера к внешней сети;

3) рядом с полем «Виртуальные сети» расположена кнопка «Добавить», с помощью которой можно добавить новую виртуальную сеть, заполнив поля в открывшемся окне;

4) рядом с полем «Пулы адресов» расположена кнопка «Добавить», с помощью которой можно добавить новый пул адресов, заполнив поля в открывшемся окне.

3.10.6.3.3. При включении опции «Использовать для миграции» при запуске миграции будет осуществляться проверка, что узел назначения состоит в активных внешних сетях с включенной опцией, и далее миграции будет идти через IP-адрес внутреннего интерфейса узла назначения первой внешней сети.

3.10.6.4. Подключенные серверы

3.10.6.4.1. В этой вкладке находится раскрывающийся список серверов, подключенных к внешней сети, для каждого из которых выводится информация о параметрах:

1) внутреннего интерфейса, относящегося к внешней сети (при его наличии):

– название;

– DHCP;

– MAC-адрес;

– IP-адрес;

– маска подсети;

– статус;

2) физического или агрегированного интерфейса, с помощью которого сервер подключен к внешней сети:

– название;

– тип;

– статус.

Также предоставляется возможность:

– создать (при его отсутствии), изменить параметры или удалить внутренний интерфейс;

– изменить интерфейс, через который осуществляется физическое подключение сервера к внешней сети.

3.10.6.4.2. Для создания или изменения параметров внутреннего интерфейса необходимо нажать кнопку  справа от названия «Параметры внутреннего интерфейса» и заполнить соответствующие параметры формы. Для удаления внутреннего интерфейса необходимо нажать кнопку  .

3.10.6.4.3. Для изменения интерфейса, используемого для подключения к внешней сети, необходимо нажать кнопку  справа от названия «Параметры физического подключения» и выбрать существующий физический или агрегированный интерфейс или создать новый агрегированный интерфейс.

3.11. Журнал

3.11.1. Общие сведения

3.11.1.1. В разделе «Журнал» основного меню можно просмотреть все операции и предупреждения, регистрируемые системой управления SpaceVM. Операции, выполняемые пользователем, регистрируются в системе как «Задачи». Каждая задача порождает одно или несколько событий.

3.11.1.2. Система управления, реагируя на изменение состояние системы, может автоматически создавать задачи и регистрировать события без участия пользователя.

Задачи и события, создаваемые системой управления, могут относиться к состоянию системы, работе механизмов высокой доступности ВМ и динамического управления ресурсами.

3.11.1.3. Регистрируемые в системе «Предупреждения» – это сообщения системы контроля состояния кластера, не влияющие на работоспособность текущей конфигурации, но сообщающие о найденных в системе несоответствиях конфигурации, хранимой в БД системы управления и текущей конфигурации на серверах. К таким несоответствиям могут относится незарегистрированные в БД пулы данных, подключенные сетевые хранилища, ВМ. Также системой управления проверяется текущая и записанная в БД конфигурация «Сетевых стеков».

3.11.2. События

3.11.2.1. Системные события делятся на следующие категории:

– информационные;

– предупреждения;

– ошибки.

3.11.2.2. События являются регистрируемыми системой управления операциями. Несколько операций могут входить в состав одной задачи.

3.11.2.3. События категории «Информационные» (info) – это успешно выполненные операции.

3.11.2.4. События категории «Предупреждения» (warning) – это зарегистрированные системой изменения, которые могут негативно повлиять на работу системы.

Примером такого события является недоступность сервера из состава кластера (если сообщение о состоянии сервера не поступило в течение стандартного времени ожидания). В этом случае сервер переводится в состояние «ERROR» и система управления производит операции по проверке состояния сервера. Если сервер из состава кластера не сообщил о своем состоянии более трех периодов ожидания ответа, недоступен по каналам контроля его состояния, то он признается сбойным («HERMIT»), и система управления старается выключить такой сервер. Далее сервер переходит в состояние «авария» («FAILED»). Такое событие имеет категорию «Ошибки».

3.11.2.5. События категории «Ошибки» («error») – это операции и события, выполнение которых невозможно или они критично влияют на работу системы управления кластером. К таким относятся выходы из строя оборудования, невозможность запустить ВМ, невозможность создать объект в составе кластера или невозможность выполнить другую операцию. Если невозможно выполнить операцию в составе «Задачи», то вся задача становится в состояние «Не выполнена» и система управления пытается отменить сделанные в рамках задачи изменения.

3.11.2.6. При просмотре журнала предусмотрен вывод как всех событий с датой их возникновения, так и с применением фильтра по определенному типу события и сущности. Также можно просмотреть события, не связанные с задачами (автоматически зарегистрированные) и события, не отмеченные как прочтенные. Информацию о событиях можно обновить вручную. Дополнительная информация о событии открывается в новом окне при нажатии на сообщение, связанное с этим событием.

3.11.2.7. Существует возможность отображения событий определенных пользователей. Для этого необходимо в категории «Все пользователи» выбрать из раскрывающегося списка одного из пользователей.

3.11.2.8. Существует возможность отображения событий из определенных групп.

Для этого необходимо в категории «Все сущности» выбрать из раскрывающегося списка одну из следующих групп:

– все сущности;

– локации;

– контроллер;

– безопасность;

– кластеры;

– серверы;

– SSL-сертификаты;

– задачи;

– задачи по расписанию;

– виртуальные машины;

– снимки состояний;

– файловые хранилища;

– кластерные хранилища;

– Gluster тома;

– пулы данных;

– виртуальные диски;

– образы ISO;

– CD-ROM;

– файлы;

– события;

– события безопасности;

– подсказки;

– теги;

– блочные хранилища;

– внешние блочные разделы энергонезависимых запоминающих устройств LUN;

– службы каталогов;

– keytabs;

– соответствия;

– ZFS-пулы;

– логические коммутаторы;

– виртуальные коммутаторы;

– порт-группы;

– внутренние интерфейсы;

– физические интерфейсы;

– агрегированные интерфейсы;

– виртуальные интерфейсы;

– L2-туннели;

– виртуальные функции;

– LLDP;

– группы политик контроля трафика;

– политики фильтрации трафика узлов;

– правила фильтрации трафика узлов;

– правила шейпинга трафика узлов;

– политики фильтрации трафика ВМ;

– правила фильтрации трафика ВМ;

– правила NAT;

– зеркалирование портов;

– vmachines-qospolicies;

– vmachines-qosmarking-rules;

– виртуальные сети;

– сетевые службы виртуальной сети;

– интерфейсы сетевых служб;

– сетевые настройки узлов;

– внешние сети;

– организации;

– пулы ресурсов;

– безопасность;

– CLI;

– лицензии.

3.11.2.9. Для работы с событиями при нажатии кнопки «Действия» доступны следующие операции:

– выгрузить события;

– отметить все события прочитанными;

– выгрузить абсолютные пути к таблицам журнала.

3.11.2.10. При выборе «Выгрузить события» в открывшемся окне «Сбор событий для выгрузки» необходимо заполнить следующие поля:

– пул данных (выбор из раскрывающегося списка);

– начальную дату выгрузки. При нажатии на поле с датой появляется календарь с возможностью выбора даты, а также секция с выбором времени;

– конечную дату выгрузки. При нажатии на поле с датой появляется календарь с возможностью выбора даты, а также секция с выбором времени;

– включить или выключить опцию «Выгрузка журнала задач контроллера;

– включить или выключить опцию «Выгрузка базы данных контроллера»;

– включить или выключить опцию «Выгрузка системных журналов узлов»;

– включить или выключить опцию «Выгрузка журнала событий контроллера»;

– включить или выключить опцию «Выгрузка статистики подсистем узлов» (из Prometheus);

– выгрузка оборудования узлов;

– выгрузка состояния IPMI датчиков серверов;

– IP-адрес хоста (management адрес узла для фильтрации журналов по нему из Elasticsearch);

– Hostname (UUID узла для фильтрации журналов по нему из Elasticsearch).

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

3.11.2.11. Если в системе присутствуют ошибки и предупреждения, то в левом нижнем углу интерфейса управления присутствуют индикатор с указанием количества непрочитанных сообщений. Также при наличии в системе ошибок отображается индикатор рядом с типом ресурса кластера, к которому они относятся. Если требуется сбросить эти индикаторы, то необходимо все события отметить прочитанными. Отметить события прочитанными можно нажатием кнопки «Действия» – «Отметить все события прочитанными».

3.11.3. Задачи

3.11.3.1. Задачи – это операции, выполняемые пользователем системы управления, включающие сообщения, дату создания, прогресс и статус.

3.11.3.2. Для задач предусмотрено несколько состояний:

– все задачи;

– не выполнено;

– выполнено;

– в процессе;

– потерянные;

– частичные;

– отмененные.

3.11.3.3. Задачи формируются системой управления на основании действий пользователя. Каждая задача формирует одно или несколько событий. Некоторые могут создавать подчиненные задачи. Сложносоставные задачи на определенном этапе могут быть в состоянии «Частичные», так как не все подчиненные задачи выполнились.

3.11.3.4. Задачи в состоянии «Не выполнено» – это задачи, выполнение которых завершилось ошибкой.

3.11.3.5. Задачи в состоянии «Выполнено» – это задачи, выполнение которых завершилось успешно.

3.11.3.6. Задачи в состоянии «В процессе» – это задачи, находящиеся в процессе выполнения. Ошибок в процессе выполнения не произошло, время ожидания ответа о результате выполнения задачи еще не истекло.

3.11.3.7. Задачи в состоянии «Потерянные» – это задачи, от которых не поступил результат выполнения в течение заданного времени ожидания. Потеря задачи чаще всего связана с запуском другой задачи (тем же или другим пользователем), выполняющей это же действие или отменяющее выполнение текущей. Примером может быть попытка выполнить создание еще одного снимка состояния работающей ВМ до окончания создания предыдущего (двойное выполнение операции).

3.11.3.8. Задачи в состоянии «Частичные» – это задачи, выполнение которых завершилось частично, например, на части узлов выполнение завершилось успешно, а на других нет.

3.11.3.9. Задачи в состоянии «Отмененные» – это задачи, выполнение которых отменил пользователь путем нажатия кнопки «Отменить» в нижнем меню журнала.

3.11.3.10. Информацию о задаче и связанные с ней события можно посмотреть в окне информации, которое открывается при нажатии на сообщение о задаче. Окно информации содержит следующие сведения:

– информация о действии;

– ID задачи;

– дата и время создания задачи;

– время выполнения задачи в секундах;

– прогресс выполнения задачи в процентах;

– ответ от узлов во время выполнения задачи;

– логин пользователя, создавшего задачу;

– статус выполнения задачи;

– перезапуск задачи с теми же параметрами по кнопке «Перезапуск». Это достаточно удобно, когда, например, уже вводили параметры, но задача завершилась с ошибкой, а позже надо снова проверить.

Информационное окно закрывается по кнопке «Закрыть» или  .

3.11.3.11. Для задач существует возможность обновления статуса по кнопке «Действия» – «Обновить статус задач».

3.11.3.12. Задачи со статусом «В процессе» можно отменить. Для этого в строке у каждой такой задачи есть кнопка «Отменить». При нажатии на кнопку делается попытка завершения ее фактического выполнения. Вне зависимости от результата задача переходит в статус «Отмененные» и снимает блокировки с сущностей, которые были заблокированы на время ее выполнения.

Если задача подразумевала действия на узле или группе узлов, то тогда на узел (узлы) посылается команда попытки завершения задачи, и если поток задачи активен и из него можно на ходу выйти, то так и будет.

Если это была мультизадача, то буден произведен выход из всех ее дочерних задач со статусом «В процессе».

3.11.3.13. Для задач существует возможность отмены всех задач в процессе по кнопке «Действия» – «Отменить все задачи».

3.11.4. Задачи по расписанию

3.11.4.1. Раздел «Задачи по расписанию» предназначен для централизованного управления задачами, которые можно применять к вычислительным узлам и ВМ. Задачи, созданные в системе управления, будут отображены в данном разделе.

3.11.4.2. Существует возможность создать задачу по расписанию. Для этого необходимо в окне «Журнал» – «Задачи по расписанию» нажать кнопку «Добавить».

В открывшемся окне выбрать из раскрывающегося списка тип сущности и сущность из выбранного типа. После этого подтвердить операцию, нажав кнопку «Отправить».

3.11.4.3. На следующем шаге необходимо в диалоговом окне заполнить следующие поля:

– название задачи;

– действие (выбор из раскрывающегося списка);

– периодичность задачи (выбор из раскрывающегося списка);

– дата и время запуска задачи;

– описание (при необходимости);

– включить (выключить) опцию «Удалить задачу после запуска».

После этого подтвердить операцию, нажав кнопку «ОК».

3.11.4.4. В окне «Задачи по расписанию» содержится список задач, включая для каждой из них название, действие, дата и время запуска, статус, дата и время следующего запуска.

3.11.4.5. Система контроля повторяемости имен не позволяет создавать задачи с одинаковым названием.

3.11.4.6. В окне отдельной задачи можно видеть следующую информацию:

1) название (редактируемый параметр);

2) описание (редактируемый параметр);

3) сущность:

– тип сущности;

– имя;

– ID;

4) периодичность (редактируемый параметр – «once», «2min», «5min», «10min», «20min», «30min», «hourly», «4h», «6h», «8h», «12h», «daily», «d3», «weekly», «monthly»);

5) действие;

6) время первого запуска задачи (редактируемый параметр);

7) удалить задачу после запуска («Да» или «Нет») (редактируемый параметр);

8) время следующего запуска задачи;

9) время последнего запуска задачи;

10) статус последнего запуска задачи;

11) дата создания;

12) дата изменения;

13) сообщения об ошибках, связанные с этой задачей.

В этом же окне в верхней строчке можно обновить информацию, запустить задачу по кнопке «Запуск» или удалить задачу по кнопке «Удалить».

3.11.5. Предупреждения

3.11.5.1. При проверке системой управления и системой контроля конфигурации системы состояния кластера соответствия данных, записанных в БД кластера с текущим состоянием системы могут быть найдены несоответствия.

В этом случае система зарегистрирует предупреждение о необходимости синхронизировать состояние объекта кластера с БД. Проверяются следующие объекты:

– подключенные сетевые хранилища;

– пути расположения пулов данных;

– конфигурация сетевого стека;

– конфигурация сетевых адаптеров.

3.11.5.2. Список контролируемых метрик будет постоянно расширяться. Для некоторых метрик может быть применено принудительное приведение к состоянию, записанному в БД, так как они могут влиять на работоспособность кластера.

3.11.5.3. Предупреждения можно обновить, просмотреть по типам и сущностям.

3.11.5.4. В категории «По всем типам» доступна сортировка по следующим состояниям:

– по всем типам;

– ошибки;

– предупреждения;

– информационные.

3.11.5.5. Доступна сортировка по всем типам сущностей. В категории «Все сущности» доступны следующие группы:

– все сущности;

– локации;

– кластеры;

– серверы;

– пулы ресурсов;

– виртуальные машины;

– пулы данных;

– файловые хранилища;

– блочные хранилища;

– диски;

– внешние блочные разделы энергонезависимых запоминающих устройств LUN;

– ZFS;

– файлы формата ISO;

– файлы;

– кластерные хранилища;

– тома;

– снэпшоты ВМ;

– снэпшоты дисков;

– виртуальные коммутаторы;

– распределенные коммутаторы;

– виртуальные интерфейсы;

– внутренние интерфейсы;

– агрегированные интерфейсы;

– зеркалирование портов;

– физические интерфейсы;

– контроль трафика;

– виртуальные сети;

– внешние сети;

– сетевые настройки;

– снэпшоты памяти;

– приводы (cd-rom);

– теги;

– пользователи;

– сертификаты (ssl);

– задачи по расписанию;

– контроллер.

3.11.5.6. Информацию о предупреждении можно посмотреть в окне, которое открывается при нажатии на сообщение о нем.

Окно описания содержит следующие сведения:

– тип;

– сообщение;

– инициаторы (тип сущности вместе с именем и временем инициализации).

ВАЖНО! Крайне рекомендуется при наличии предупреждений принять соответствующие действия по их исправлению.

3.11.5.7. Список возможных предупреждений:

1) кластеры:

– «Высокая загрузка памяти»;

– «Критическая загрузка памяти»;

– «Высокая загрузка процессоров»;

– «Критическая загрузка процессоров»;

– «Не найден оптимальный узел в DRS кластере для миграции виртуальной машины»;

– «Предупреждение: в DRS кластере менее 2 узлов»;

– «Найдены несовместимые для всех возможных миграций типы процессоров на узлах кластера. Рекомендация: переместить несовместимый узел в другой кластер»;

– «Найдены несовместимая для всех возможных миграций конфигурация сетевых хранилищ на узлах кластера. Рекомендация: проверить подключение сетевых хранилищ ко всем узлам кластера»;

2) серверы:

– «Несоответствие ПО контроллера и сервера»;

– «Несоответствие времени контроллера и сервера»;

– «Высокая загрузка памяти»;

– «Критическая загрузка памяти»;

– «Высокая загрузка процессоров»;

– «Критическая загрузка процессоров»;

– «Найдены неизвестные супервизору контроллера виртуальные машины»;

– «Не приходят данные о сущностях хранилищ от супервизора узла. Состояния сущностей могут быть неактуальны. Рекомендация: проверка состояния супервизора узла через command line interface»;

– «Не приходят данные о сущностях виртуальных машин от супервизора узла. Состояния сущностей могут быть неактуальны. Рекомендация: проверка состояния супервизора узла через command line interface»;

– «Не приходят данные о сущностях сетевых устройств от супервизора узла. Состояния сущностей могут быть неактуальны. Рекомендация: проверка состояния супервизора узла через command line interface»;

– «Не приходят данные от агента узла»;

– «На узле найдены неизвестные супервизору контроллера файловые сетевые хранилища. Рекомендация: просканировать и добавить неопознанные сетевые хранилища»;

– «На узле найдены неизвестные супервизору контроллера кластерные хранилища. Рекомендация: просканировать и добавить неопознанные хранилища»;

– «На узле найдены неизвестные супервизору контроллера gluster тома. Рекомендация: просканировать и добавить неопознанные тома»;

– «На узле найдены неизвестные супервизору контроллера блочные сетевые хранилища. Рекомендация: просканировать и добавить неопознанные сетевые хранилища»;

– «На узле найдены неизвестные супервизору контроллера пулы данных. Рекомендация: просканировать и добавить неопознанные пулы данных»;

– «На узле найдены неизвестные супервизору контроллера ZFS-пулы. Рекомендация: просканировать узел и добавить неопознанные ZFS-пулы»;

– «Обнаружено расхождение с базой настроек распределенных коммутаторов. Рекомендация: синхронизировать сетевые настройки узла»;

– «Обнаружено расхождение с базой настроек виртуальных коммутаторов. Рекомендация: синхронизировать сетевые настройки узла»;

– «Обнаружено расхождение с базой настроек внутренних интерфейсов. Рекомендация: синхронизировать сетевые настройки узла»;

– «Обнаружено расхождение с базой настроек физических интерфейсов. Рекомендация: синхронизировать сетевые настройки узла»;

– «Обнаружено расхождение с базой настроек агрегированных интерфейсов. Рекомендация: синхронизировать сетевые настройки узла»;

– «Обнаружено расхождение базовых сетевых настроек узла с известными контроллеру. Рекомендация: синхронизировать сетевые настройки узла»;

– «Обнаружено несоответствие свободных физических интерфейсов на узле и базе данных. Рекомендация: синхронизировать сетевые настройки узла»;

– «Обнаружено несоответствие физических интерфейсов с включенной поддержкой SR-IOV на узле и базе данных. Рекомендация: синхронизировать сетевые настройки узла»;

– «Обнаружено несоответствие между ожидаемым и фактическим состоянием службы брандмауэра. Рекомендация: запустить или остановить службу брандмауэра в соответствии с вашими требованиями»;

– «Базовые правила брандмауэра были обновлены. Рекомендация: обновить базовые правила брандмауэра на узлах, используя функцию «Обновить правила», и применить их»;

– «Не обнаружены, ожидаемые согласно базе настроек, распределенные коммутаторы. Рекомендация: синхронизировать сетевые настройки узла»;

– «Не обнаружены, ожидаемые согласно базе настроек, виртуальные коммутаторы. Рекомендация: синхронизировать сетевые настройки узла»;

– «Не обнаружены, ожидаемые согласно базе настроек, внутренние интерфейсы. Рекомендация: синхронизировать сетевые настройки узла»;

– «Не обнаружены, ожидаемые согласно базе настроек, физические интерфейсы. Рекомендация: синхронизировать сетевые настройки узла»;

– «Не обнаружены, ожидаемые согласно базе настроек, агрегированные интерфейсы. Рекомендация: синхронизировать сетевые настройки узла»;

– «Обнаружены неизвестные распределенные коммутаторы. Рекомендация: синхронизировать сетевые настройки узла»;

– «Обнаружены неизвестные виртуальные коммутаторы. Рекомендация: синхронизировать сетевые настройки узла»;

– «Обнаружены неизвестные внутренние интерфейсы. Рекомендация: синхронизировать сетевые настройки узла»;

– «Обнаружены неизвестные физические интерфейсы. Рекомендация: синхронизировать сетевые настройки узла»;

– «Обнаружены неизвестные агрегированные интерфейсы. Рекомендация: синхронизировать сетевые настройки узла»;

– «Необходимо выполнить обновление виртуальной сети. Выполните сброс ошибок для обновления»;

– «В каталоге журналов и статистики узла осталось менее 5 процентов свободного места. Рекомендация: удалить ненужные журналы или уменьшить время хранения журналов или статистики через CLI»;

– «В каталоге корня узла осталось менее 5 процентов свободного места. Рекомендация: почистить место»;

3) виртуальные машины:

– «Нет доступных узлов для миграции или восстановления виртуальной машины. Рекомендация: проверить доступность сетевых интерфейсов в кластере»;

– «Нет доступных узлов для миграции или восстановления виртуальной машины. Рекомендация: проверить настройки тегирования кластера и конфигурацию тегов узлов и виртуальных машин в кластере»;

– «Нет доступных узлов для миграции или восстановления виртуальной машины. Рекомендация: проверить доступность пулов данных для кластера»;

– «Нет доступных узлов для миграции или восстановления виртуальной машины. Рекомендация: проверить доступность LUN сетевых хранилищ для серверов кластера»;

– «Нет доступных узлов для миграции или восстановления виртуальной машины. Рекомендация: проверить доступные ресурсы серверов кластера»;

– «Нет доступных узлов для миграции или восстановления виртуальной машины. Рекомендация: проверить настройку безопасного режима ВМ или подключенные серверные устройства»;

– «Нет доступных узлов для восстановления виртуальной машины с использованием механизма катастрофоустойчивости. Рекомендация: проверить настройку узлов локации, выбранной для восстановления виртуальной машины»;

– «Миграция виртуальной машины на менее загруженный узел»;

4) сетевые хранилища:

– «На сетевом хранилище найдены неизвестные супервизору контроллера LUN. Рекомендация: просканировать LUN на сетевом хранилище»;

5) пулы данных:

– «На пуле данных найдены неизвестные супервизору контроллера виртуальные диски. Рекомендация: просканировать пул данных»;

– «На пуле данных найдены неизвестные супервизору контроллера образы. Рекомендация: просканировать пул данных»;

– «На пуле данных найдены неизвестные супервизору контроллера файлы. Рекомендация: просканировать пул данных».

3.12. Безопасность

3.12.1. Пользователи

В разделе «Безопасность» – «Пользователи» основного меню содержится информация о ранее созданных пользователях системы (имя пользователя, его роли и статус). Также доступны следующие операции:

– обновление информации о пользователях по кнопке  ;

– возможность создания новых пользователей;

– управление политиками авторизации;

– выбор пользователя с применением фильтра.

3.12.1.1. Политика авторизации

3.12.1.1.1. Для настройки политики авторизации необходимо нажать на кнопку «Политика авторизации» и в открывшемся окне заполнить следующие поля:

– время ограничения в минутах;

– количество попыток авторизации до блокировки пользователя;

– время между попытками авторизации в секундах;

– включение (отключение) ограничения при превышении лимита попыток;

– включение (отключение) опции «Отображать ввод пароля во время аутентификации»;

– включение (отключение) опции «Авторизация с проверкой MAC-адресов»;

– при включенной опции «Авторизация с проверкой MAC-адресов» добавить разрешенные MAC-адреса;

– выбрать уровень безопасности пароля («low», «middle» или «high»);

– выбрать время действия кода двухфакторной аутентификации в секундах;

– дисклеймер (короткое текстовое сообщение).

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

Подробное описание уровней безопасности пароля приведено в 3.12.10 данного руководства.

3.12.1.2. Создание пользователя

3.12.1.2.1. Создание нового пользователя осуществляется с помощью нажатия кнопки «Добавить пользователей». В открывшемся окне необходимо заполнить следующие поля:

1) логин нового пользователя;

2) имя нового пользователя;

3) фамилия нового пользователя;

4) адрес электронной почты;

5) выбрать роли (из раскрывающегося списка). Выбор ролей зависит от прав пользователя, от имени которого происходит создание нового пользователя;

6) пароль для нового пользователя;

7) повторный ввод пароля для нового пользователя;

8) при включенной опции «Добавить организацию» выбрать организацию из списка;

9) при включенной опции «Дополнительные настройки» заполнить:

– выбрать часовой пояс (из раскрывающегося списка);

– дата окончания действия пользователя;

– дата окончания действия пароля;

– при включенной опции «Включить/выключить суточный период пользователя» ввести время начала и окончания работы;

– включить (выключить) опцию «Отправка сообщений об ошибках на электронную почту».

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

Доступ к данному разделу пользователям с ролью «оператор ВМ» ограничен.

3.12.1.2.2. Для корректировки данных о пользователе необходимо нажать на интересующего пользователя, после чего в открывшемся окне отобразится информация о пользователе.

3.12.1.3. Удаление пользователя

3.12.1.3.1. Удаление выбранного пользователя осуществляется по нажатию кнопки «Удалить пользователя» и подтверждением операции в диалоговом окне кнопкой «ОК».

«По умолчанию» удаление пользователей отключено. Для включения необходимо перейти в меню «Настройки» – «Системные» и включить «Возможность удаления пользователей».

ВНИМАНИЕ! Удаление пользователя приводит к потере всей истории его действий. При необходимости ограничения доступа конкретному пользователю можно сделать его неактивным, используя кнопку «Состояние» во вкладке «Информация».

3.12.1.3.2. Управление пользователями описано в разделе 3 руководства системного программиста ДСБР.30001-01 32 01.

3.12.1.4. Информация

3.12.1.4.1. Для перехода к конкретному пользователю необходимо нажать на его имя в списке пользователей.

В окне «Безопасность» – «Пользователи» – <имя пользователя> содержится следующая информация, разделенная на группы:

– информация о пользователе;

– настройки;

– роли и разрешения;

– доступ к ВМ;

– ресурсы пользователя;

– сессии;

– ключи интеграции;

– события;

– теги.

3.12.1.4.2. Для пользователя имеются следующие возможности:

– обновление информации;

– изменение пароля. При нажатии на кнопку «Изменить пароль» в открывшемся окне необходимо заполнить текущий пароль, новый пароль и повторить новый пароль, после чего подтвердить операцию, нажав кнопку «Изменить пароль».

3.12.1.4.3. Для корректировки данных о пользователе необходимо перейти в окно «Безопасность» – «Пользователи» – <имя пользователя> – «Информация», где отобразится следующая информация о нем:

– логин пользователя;

– имя пользователя (редактируемый параметр);

– фамилия пользователя (редактируемый параметр);

– электронная почта (редактируемый параметр);

– имя пользователя (редактируемый параметр);

– состояние пользователя (редактируемый параметр). Может принимать значения «Активный» и «Неактивный»). При нажатии на кнопку редактирования в открывшемся окне необходимо подтвердить операцию о смене статуса пользователя, нажав на кнопку «Изменить статус»;

– текущее количество неуспешных авторизаций;

– общее количество неуспешных авторизаций;

– время последней неуспешной авторизации;

– время последней успешной авторизации.

3.12.1.5. Настройки

3.12.1.5.1. Для изменения настроек пользователя необходимо перейти в окно «Безопасность» – «Пользователи» – <имя пользователя> – «Настройки», где доступны следующие поля:

– часовой пояс (редактируемый параметр);

– дата окончания действия пользователя (редактируемый параметр);

– дата окончания действия пароля (редактируемый параметр);

– суточный период пользователя (вкл/выкл) (редактируемый параметр);

– время начала суточного периода;

– время окончания суточного периода;

– отправка ошибок на электронную почту (вкл/выкл) (редактируемый параметр);

– двухфакторная аутентификация (вкл/выкл) (редактируемый параметр);

– максимальное количество одновременных сеансов (редактируемый параметр);

– время неактивности для деактивации пользователя в днях (редактируемый параметр).

3.12.1.6. Роли и разрешения

3.12.1.6.1. Для редактирования и просмотра ролей и разрешений пользователя необходимо перейти в окно «Безопасность» – «Пользователи» – <имя пользователя> – «Роли».

При нажатии на кнопку редактирования «Роли пользователя» в открывшемся окне необходимо внести изменения, выбрав роли из раскрывающегося списка, после чего подтвердить информацию, нажав «ОК».

3.12.1.6.2. Управление ролями пользователей описано в руководстве системного программиста ДСБР.30001-01 32 01.

3.12.1.7. Доступ к ВМ

3.12.1.7.1. Доступ пользователя к ВМ осуществляется в окне «Безопасность» – «Пользователи» – <имя пользователя> – «Доступ к ВМ». При нажатии на кнопку редактирования «Доступные ВМ» в открывшемся окне необходимо выбрать из раскрывающегося списка ВМ для доступа, после чего подтвердить операцию, нажав на кнопку «ОК».

3.12.1.8. Ресурсы пользователя

3.12.1.8.1. В окне «Безопасность» – «Пользователи» – <имя пользователя> – «Ресурсы пользователя» отображаются следующие ресурсы:

– пулы данных;

– диски;

– образы;

– файлы.

Примечание. Актуально только для роли «Оператор ВМ». Используется для контроля администратором сущностей владения оператора.

3.12.1.9. Сессии

3.12.1.9.1. В окне «Безопасность» – «Пользователи» – <имя пользователя> – «Сессии» содержится информация о текущих сессиях данного пользователя, включая для каждой из них IP-адрес клиента, агента клиента, статус, дата создания сессии, дата последнего использования, действие с возможность завершить любую сессию пользователя, кроме активной. Также есть кнопка завершения всех неактивных сессий.

3.12.1.10. Ключи интеграции

3.12.1.10.1. В окне «Безопасность» – «Пользователи» – <имя пользователя> – «Ключи интеграции» содержатся ключи для интеграции приложений с SpaceVM.

При нажатии кнопки «Создать ключ» в открывшемся окне необходимо указать в поле «Приложение для интеграции с контроллером» уникальное имя ключа и нажать кнопку «Сгенерировать ключ», после чего сгенерированный ключ появится в поле «Ключ интеграции». Далее для дальнейшего использования сторонним приложением необходимо скопировать ключ в буфер обмена с помощью кнопки  «Копировать».

Примечания:

1. Для создания ключа интеграции пользователь должен иметь роль «Администратора».

2. Просмотр и копирование ключа возможны только при его создании. При закрытии окна ключ будет недоступен для копирования.

3. Передача ключа сторонним приложениям осуществляется любым доступным способом обмена информацией (e-mail, USB-накопитель, CD-диск и другие).

4. Существует ограничение количества ключей – максимум 96 ключей на одного пользователя.

Для удаления ключа из списка необходимо нажать «Удалить ключ интеграции» и в открывшемся окне подтвердить операцию, нажав «Да».

3.12.1.11. События

3.12.1.11.1. В окне «Безопасность» – «Пользователи» – <имя пользователя> – «События» отображаются события, зарегистрированные в системе для данного пользователя с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.12.1.11.2. Любой пользователь может изменить свой пароль, указав текущий. Администратор безопасности может изменить пароль любого пользователя без указания текущего пароля.

3.12.1.11.3. В целях обеспечения информационной безопасности действует ограничение на использование старых паролей. Система запоминает до 10 использованных паролей.

3.12.2. Роли

В разделе «Безопасность» – «Роли» основного меню содержится информация о ранее созданных пользовательских ролях системы. Также доступны следующие операции:

– обновление информации о ролях;

– возможность создания новых ролей;

– возможность удаления ролей (кроме встроенных).

Доступ к данному разделу операторам ВМ ограничен.

3.12.2.1. Создание роли

3.12.2.1.1. Создание новой роли осуществляется с помощью нажатия кнопки «Добавить». В открывшемся окне необходимо заполнить следующие поля:

– название роли;

– приоритет;

– разрешения;

– тип.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

Примечание. Разрешения можно задать при создании роли, но удобнее это делать в таблице разрешений готовой роли.

3.12.2.1.2. Существует четыре типа ролей:

– «Администратор». Доступны все настройки, кроме тех, которые доступны только «Администратору безопасности»;

– «Администратор безопасности». Доступ к настройкам безопасности и авторизации;

– «Оператор ВМ». Доступ к ВМ и смежным ресурсам системы. Только операторы ВМ могут владеть ресурсами системы;

– «Только чтение». Доступ к объектам инфраструктуры как у администратора, но только на чтение.

3.12.2.2. Редактирование роли

3.12.2.2.1. Для корректировки данных о пользовательской роли необходимо нажать на интересующую роль, после чего в открывшемся окне отобразится информация о роли.

3.12.2.2.2. Во вкладке «Информация» содержатся:

– название (редактируемый параметр);

– приоритет (редактируемый параметр);

– тип (редактируемый параметр).

3.12.2.2.3. Удаление роли выполняется в окне состояния роли с помощью кнопки «Удалить»

Примечание. Удаление встроенных и используемых ролей недоступно.

3.12.2.2.4. Во вкладке «Разрешения» отображается таблица всех разрешений системы. Добавленные разрешения отмечены «галочками». Добавление (удаление) разрешений осуществляется с помощью выделения «галочками» нужных разрешений и нажатия появившейся кнопки «Сохранить.

В таблице пять столбцов:

– колонка с отметкой;

– название действия;

– метод;

– приложение (часть системы. Приложение может содержать несколько моделей);

– модель (часть приложения).

Для удобства работы с таблицей разрешений реализован поиск, вызываемый по кнопке «Фильтр».

Примечание. Редактирование встроенных ролей недоступно. Только вновь созданные роли могут быть изменены администратором безопасности.

3.12.2.2.5. Реализованы специальные разрешения для разграничения видимости тех или иных элементов пользовательского интерфейса для различных ролей пользователей. Такие разрешения имеют особые названия:

– «menu_», например, «menu_all_sessions» отвечает за отображение элементов главного меню;

– «button_», например, «button_dashboard» отвечает за отображение различных кнопок.

3.12.3. Разграничение доступа

3.12.3.1. В таблице 4 описано разграничение доступа ролей пользователей к моделям системы.

Таблица 4

Модель	Администратор	Администратор безопасности	Оператор ВМ	Только чтение
Пользователи (*user*)	Чтение: *access_tokens, list, permissions, retrieve, sessions, usernames*. Управление: *change_password, update*	Полный доступ	Чтение: *access_tokens, list, permissions, retrieve, sessions, usernames.* Управление: *change_password, update*	Чтение: *access_tokens, list, permissions, retrieve, sessions, usernames.* Управление: *change_password, update*
Кластеры (*cluster*)	Полный доступ	Нет доступа	Чтение: *list, optimal_node, retrieve*	Полный доступ на чтение
Кластерные хранилища (*clusterstorage*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение

Модель	Администратор	Администратор безопасности	Оператор ВМ	Только чтение
Gluster тома (*volume*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Группы политик контроля трафика (*controlplane*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Политики фильтрации трафика узлов (*internalaccess policy*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Правила фильтрации трафика узлов (*internalaccess rule*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Правила шейпинга трафика узлов (*internalshaping rule*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Зеркалирование портов (*portmirroring*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Политики фильтрации трафика ВМ (*vmachinesaccesspolicy*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Правила фильтрации трафика ВМ (*vmachines accessrule*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение

Модель	Администратор	Администратор безопасности	Оператор ВМ	Только чтение
Правила NAT (*vmachines natrule*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Правила маркировки политики QoS виртуальных сетей (*vmachinesqos markrule*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Политики QoS виртуальных сетей (*vmachinesqos policy*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Контроллер (*controller*)	Чтение всего, кроме: *security_ settings, ntp_servers.* Управление всем, кроме: *set_ntp_ servers, update_system _settings, update_security _settings*	Чтение: *base_version, list, ntp_servers, security_ settings, system_ settings, system_time.* Управление: *set_ntp_ servers, update, update_security _settings, update_system _settings*	Чтение: *base_version, system_time*	Чтение всего, кроме: *security_ settings, ntp_servers*
Области данных (*dataplane*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Виртуальные сети (*vnetwork*)	Полный доступ	Нет доступа	Чтение: *list*	Полный доступ на чтение
Интерфейсы сетевых служб (*vnservicesinf*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение

Модель	Администратор	Администратор безопасности	Оператор ВМ	Только чтение
Сетевые службы виртуальной сети (*vnservices instance*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Локации (*datacenter*)	Полный доступ	Нет доступа	Чтение: *list*	Полный доступ на чтение
Пулы данных (*datapool*)	Полный доступ	Нет доступа	Чтение: *available_types, list, retrieve.* Управление: *create, discover_files, discover_iso, discover_vdisks, free, check_verbose_ name*	Полный доступ на чтение
Виртуальные машины (*domain*)	Полный доступ	Нет доступа	Полный доступ на чтение. Управление всем, кроме: *set_owners*	Полный доступ на чтение
События (*event*)	Полный доступ	Полный доступ	Полный доступ	Полный доступ на чтение. Управление: *generate_event*
Пулы адресов (*addresspool*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Внешние сети (extnetwork)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Подсказки (*hint*)	Полный доступ	Полный доступ	Полный доступ	Полный доступ на чтение
CD-ROM (*cdrom*)	Полный доступ	Нет доступа	Полный доступ	Полный доступ на чтение
Образы ISO (*iso*)	Полный доступ	Нет доступа	Полный доступ	Полный доступ на чтение

Модель	Администратор	Администратор безопасности	Оператор ВМ	Только чтение
Сетевые настройки узлов (*management plane*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Файлы (*file*)	Полный доступ	Нет доступа	Полный доступ	Полный доступ на чтение
Лицензии (*license*)	Полный доступ	Чтение: check	Чтение: *check*	Полный доступ на чтение
Агрегированные интерфейсы (*aggregatedinf*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Внутренние интерфейсы (*internalinf*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
LLDP (*lldpdconfig*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Логические коммутаторы (*lswitch*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
L2-уннели (*overlaytunnel*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Физические интерфейсы (*physicalinf*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Порт-группы (*portgroup*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Виртуальные функции (*vfunction*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Виртуальные интерфейсы (*vmachineinf*)	Полный доступ	Нет доступа	Полный доступ	Полный доступ на чтение
Виртуальные коммутаторы (*vswitch*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение

Модель	Администратор	Администратор безопасности	Оператор ВМ	Только чтение
Серверы (*node*)	Полный доступ	Нет доступа	Чтение: *available_cpu_ models, list, retrieve.* Управление: *migrate_ domains, shutdown_ domains, start_domains*	Полный доступ на чтение
Пулы ресурсов (*resourcepool*)	Полный доступ	Нет доступа	Чтение: *list, retrieve*	Полный доступ на чтение
Файловые хранилища (*sharedstorage*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Снимки состояния ВМ (*domainsnap shot*)	Полный доступ	Нет доступа	Полный доступ	Полный доступ на чтение
LUN (*lun*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Блочные хранилища (*storage transport*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Теги (*tag*)	Полный доступ	Нет доступа	Полный доступ на чтение. Управление всем, кроме *remove*	Полный доступ на чтение
Задачи по расписанию (*scheduledtask*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Задачи (*task*)	Полный доступ	Нет доступа	Полный доступ	Полный доступ на чтение
Организации (*organization*)	Полный доступ	Нет доступа	Полный доступ на чтение	Полный доступ на чтение
Виртуальные диски (*vdisk*)	Полный доступ	Нет доступа	Полный доступ	Полный доступ на чтение

Модель	Администратор	Администратор безопасности	Оператор ВМ	Только чтение
ZFS-пулы (*zfspool*)	Полный доступ	Нет доступа	Нет доступа	Полный доступ на чтение
Службы каталогов (*authentication directory*)	Нет доступа	Полный доступ	Нет доступа	Нет доступа
Keytabs (*keytab*)	Нет доступа	Полный доступ	Нет доступа	Нет доступа
Соответствия (*rolemapping*)	Нет доступа	Полный доступ	Нет доступа	Нет доступа
События безопасности (*eventsecurity*)	Нет доступа	Полный доступ	Нет доступа	Нет доступа
SSL-сертификаты (*sslcertificate*)	Нет доступа	Полный доступ	Нет доступа	Нет доступа

3.12.4. Сессии

3.12.4.1. В разделе «Безопасность» – «Сессии» основного меню содержится информация о текущих сессиях всех пользователей, включая для каждой из них пользователя, IP-адрес клиента, агента клиента, статус, дата создания сессии, дата последнего использования.

3.12.5. NTP и время

3.12.5.1. В разделе «Безопасность» – «NTP и время» основного меню можно настроить список NTP-серверов, с которым будет синхронизироваться контроллер. При нажатии кнопки «Установка NTP» в открывшемся окне необходимо задать адреса NTP-серверов из раскрывающегося списка и нажать кнопку «Добавить». После этого сохранить изменения, нажав кнопку «ОК».

3.12.5.2. Также здесь отображается текущее системное время контроллера.

Примечания:

1. При использовании авторизации MS AD расхождение времени с контроллером AD не допускается.

2. При использовании кластерных хранилищ расхождение времени узлов друг с другом в кластере не допускается.

3.12.5.3. После установки время на сервере синхронизируется с указанными далее базовыми серверами времени с уменьшающимся приоритетом:

– 0.debian.pool.ntp.org;

– 1.debian.pool.ntp.org;

– 2.debian.pool.ntp.org;

– 3.debian.pool.ntp.org;

– 127.127.1.0 (в случае отсутствия интернета или недоступности серверов времени сервер синхронизируется со своими локальными часами).

3.12.5.4. При добавлении узла к контроллеру узел начинает использовать контроллер, как сервер времени. При использовании репликации контроллера сервером времени является активный мастер.

3.12.5.5. Время сервера можно посмотреть в Web-интерфейсе в окне «Сервер» – <имя сервера> – «Информация». Время на контроллере можно посмотреть в нижней строке Web-интерфейса слева.

3.12.5.6. Контроллер SpaceVM проверяет соответствие своего времени и каждого активного узла. При расхождении времени более чем на 60 секунд выдается предупреждение.

3.12.5.7. Для проверки статуса синхронизации в CLI используются команды:

– *ntp check;*

– *ntp test_connection;*

– *ntp conf.*

Примечание. Необходимо убедиться, что серверы времени доступны контроллеру.

3.12.6. Ключи шифрования SSH

3.12.6.1. Ключи шифрования SSH – это пара зашифрованных ключей (закрытый и открытый), которые используются для авторизации при подключении к серверу по протоколу SSH. При такой настройке SSH подключения не требуется ввод пароля.

Для подключения к серверу с помощью ключей шифрования SSH необходимо:

– создать пару ключей. После создания закрытый ключ сохраняется на компьютере, с которого осуществляется подключение, а открытый ключ размещается на сервере;

– разместить открытый ключ на сервере или ВМ с помощью Web-интерфейса SpaceVM.

Примечание. Каждый пользователь системы виртуализации SpaceVM (кроме администраторов) видит только свои ключи шифрования. У администраторов есть возможность просматривать и управлять всеми публичными ключами шифрования.

3.12.6.2. Для загрузки открытого (публичного) ключа шифрования необходимо нажать кнопку «Добавить ключ». В открывшемся окне необходимо заполнить следующие поля:

– название ключа;

– тип шифрования;

– выбрать файл публичного ключа или вставить ключ в форму из буфера обмена.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

Предполагается, что пользователь уже имеет приватный ключ.

3.12.6.3. Для генерации ключей шифрования необходимо нажать кнопку «Сгенерировать ключ». В открывшемся окне необходимо заполнить следующие поля:

– название ключа;

– тип шифрования (выбрать из раскрывающегося списка);

– длина ключа в битах (выбрать из раскрывающегося списка).

Примечание. Длина ключа – это количество битов, используемых для ключа алгоритма шифрования. Обычно, чем больше бит, тем более устойчив алгоритм к взлому.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК». Система сгенерирует приватный и публичные ключи и предложит сохранить приватный ключ на локальном диске компьютера.

Примечание. Путь к приватному ключу в Linux системе – «/home/USER_NAME/.ssh/id_rsa». В Windows расположение файла зависит от приложения SSH-доступа.

3.12.6.4. Для удаления ключей шифрования необходимо выделить нужные ключи с помощью отметки в чекбоксе и нажать на кнопку «Удалить».

Примечание. Удаление происходит только из базы данных – удаленные ключи все еще могут быть подключены к узлам. Чтобы отключить удаленные из базы ключи, необходимо выполнить «Удаление всех ключей» на узле для всех (если не известен конкретный) пользователей SSH.

3.12.6.5. Для удобства управления системой виртуализации SpaceVM реализована функция распространения публичного ключа на все узлы контроллера. Распространяемый публичный ключ выдается пользователю «root» на выбранных узлах.

По нажатию кнопки «Подключение SSH ключа», откроется диалоговое окно выбора узлов. После выбора узлов необходимо подтвердить операцию, нажав кнопку «ОК».

По нажатию кнопки «Отключение SSH ключа» откроется диалоговое окно выбора узлов. После выбора узлов необходимо подтвердить операцию, нажав кнопку «ОК».

ВНИМАНИЕ! «По умолчанию» данные функции доступны только администратору и администратору безопасности.

3.12.7. SSL-сертификаты

3.12.7.1. В разделе «Безопасность» – «SSL-сертификаты» основного меню содержится информация о действующих сертификатах и возможность загрузки нового комплекта SSL-сертификатов для доступа к системе управления по HTTPS.

3.12.7.2. Мастер загрузки сертификатов запускается по нажатию кнопки «Добавить». В открывшемся окне необходимо заполнить следующие поля:

– уникальное имя SSL-сертификата;

– описание сертификата;

– доменное имя, на которое сертификат выпущен;

– содержимое файлов сертификатов вместе со строками, содержащими признак начала и конца сертификата (со словами BEGIN и END) либо загрузить уже готовый SSL-сертификат. При нажатии кнопки «Загрузить файл» будет открыто стандартное окно загрузки файлов, в котором необходимо выбрать файл и нажать «Открыть»;

– содержимое ключа SSL-сертификата вместе со строками, содержащими признак начала и конца сертификата (со словами BEGIN и END) либо загрузить уже готовый SSL-сертификат. При нажатии кнопки «Загрузить файл» будет открыто стандартное окно загрузки файлов, в котором необходимо выбрать файл и нажать «Открыть»;

– цепочку SSL-сертификата вместе со строками, содержащими признак начала и конца сертификата (со словами BEGIN и END) либо загрузить уже готовый SSL-сертификат. При нажатии кнопки «Загрузить файл» будет открыто стандартное окно загрузки файлов, в котором необходимо выбрать файл и нажать «Открыть».

После заполнения полей необходимо подтвердить операцию, нажав кнопку «OK».

3.12.8. Службы каталогов

3.12.8.1. Окно службы каталогов

3.12.8.1.1. В разделе «Безопасность» – «Службы каталогов» основного меню производится настройка интеграции с сервером службы каталогов по Lightweight Directory Access Protocol (LDAP). Данная интеграция позволяет авторизовать в системе управления SpaceVM пользователей из Active Directory (далее MS AD), FreeIPA, OpenLdap, ALD. После успешной аутентификации пользователь в системе управления SpaceVM будет создан автоматически. Пароль пользователя хранится только на сервере службы каталогов, то есть такой пользователь и в дальнейшем проходит аутентификацию только через сервер LDAP.

3.12.8.1.2. Создание записи службы каталогов производится с помощью кнопки «Добавить». В открывшемся окне необходимо заполнить следующие поля:

– название службы каталогов;

– имя домена;

– адрес службы каталогов URL («LDAP» или «LDAPS»);

– тип службы каталогов (выбор из раскрывающегося списка). Может принимать значения «Active Directory», «FreeIPA», «OpenLDAP» или «ALD»;

– роль «по умолчанию»;

– пользователь (имя администратора);

– пароль администратора;

– проверка соединения;

– описание.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

3.12.8.1.3. В окне службы каталогов существует возможность обновления информации по кнопке  и поиска каталога по названию. Для этого в верхней строчке окна в поле «Найти  » необходимо ввести название искомого каталога и нажать кнопку  .

3.12.8.1.4. После первоначальной настройки службы AD, FreeIPA, OpenLDAP, ALD авторизуют пользователей как внешнее хранилище учетных записей LDAP. Предоставляется возможность сопоставлять группы пользователей AD, FreeIPA, OpenLDAP, ALD с уровнем доступа в систему управления (администратор или оператор).

3.12.8.1.5. Для авторизации пользователем домена Windows, Linux в окне ввода имени пользователя и пароля необходимо перевести переключатель авторизации в LDAP.

3.12.8.1.6. Интеграцию с MS AD можно расширить, применив настройки Kerberos (keytabs) и указав учетную запись пользователя, авторизованного для проверки учетных данных с контроллера системы управления. При правильном применении настроек появится возможность использования функционала SSO при авторизации пользователей домена MS AD.

3.12.8.1.7. Для MS AD также поддерживается работа со связными (доверенными) серверами.

3.12.8.1.8. В системе управления реализован автоматический повтор аутентификации при получении соответствующего ответа во время сильной загрузки сервера службы каталогов.

3.12.8.1.9. При нажатии на название службы каталогов в открывшемся окне содержатся сведения о ней, разделенные на следующие группы:

– информация;

– соответствия;

– keytabs;

– события.

Также существует возможность обновления информации, изменения конфигурации SSO и удаления службы.

3.12.8.1.10. При нажатии кнопки «Конфигурация SSO» в открывшемся окне необходимо заполнить следующие поля:

– включить или выключить режим SSO;

– субдомен SSO;

– URL сервера управления AD;

– список всех URL Key Distributed Centers.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

3.12.8.2. Информация

3.12.8.2.1. В окне «Безопасность» – «Службы каталогов» – <имя службы каталогов> – «Информация» содержатся следующие сведения:

– название службы (редактируемый параметр);

– описание службы (редактируемый параметр);

– имя домена (редактируемый параметр);

– тип службы (редактируемый параметр);

– URL службы (редактируемый параметр, записывается в формате *ldap://xxx.xxx.xxx.xxx*);

– пользователь (редактируемый параметр);

– пароль (редактируемый параметр);

– роль «по умолчанию» (редактируемый параметр);

– дата и время создания службы;

– дата изменения;

– проверка соединения.

3.12.8.3. Соответствия

3.12.8.3.1. В окне «Безопасность» – «Службы каталогов» – <имя службы каталогов> – «Соответствия» содержится возможность обновления и добавления соответствия.

Для добавления соответствия необходимо нажать кнопку «Добавить соответствие» и в открывшемся окне заполнить следующие поля:

– название соответствия;

– роли пользователей (выбор из раскрывающегося списка);

– добавить объекты LDAP;

– описание соответствия.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

В окне управления соответствиями групп пользователей при нажатии на название соответствия в списке открывается окно, в котором можно посмотреть текущую информацию о соответствии или изменить ее, внеся изменения в необходимые поля. После заполнения полей необходимо подтвердить операцию, нажав кнопку «Сохранить».

3.12.8.4. Keytabs

3.12.8.4.1. В окне «Безопасность» – «Службы каталогов» – <имя службы каталогов> – «Keytabs» существует возможность обновления, а также загрузки файлов. При нажатии кнопки «Загрузить» будет открыто стандартное окно загрузки файлов, в котором необходимо выбрать файл и нажать «Открыть».

3.12.8.5. События

3.12.8.5.1. В окне «Безопасность» – «Службы каталогов» – <имя службы каталогов> – «События» присутствуют все события, зарегистрированные в системе, возникающие при работе служб каталогов с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.12.9. События

3.12.9.1. В разделе «Безопасность» – «События» основного меню отображаются события, зарегистрированные в системе с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные». Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.12.9.2. В дополнение к обычному функционалу журнала событий, присутствуют следующие опции:

1) при нажатии кнопки «Действия» доступны следующие операции:

– архивы;

– очистить журналы.

2) при нажатии кнопки «Настройки архивации журнала» имеется возможность задать следующее:

– минимальное число событий для архивации журнала;

– размер хранилища архивов журналов;

– лимит заполненности журнала (в процентах);

– автоматическая очистка архивов журнала при превышении заданного времени (в днях).

3.12.9.3. При превышении определенного числа событий, происходит автоматическая архивация и очистка журнала. Если хранилище переполнено, происходит удаление самых старых архивов – пока не освободится достаточно места.

3.12.10. Web-sockets

3.12.10.1. В окне «Безопасность» – «Web-sockets» основного меню содержится таблица, отражающая обмен сообщениями между браузером и Web-сервером во время работы.

Примечание. «Web-sockets» используется для отладки SpaceVM.

3.12.11. Описание уровней стойкости паролей

3.12.11.1. Администратор безопасности устанавливает один из трех уровней качества паролей для пользователей в SpaceVM:

1) «low» – пароли с низкой степенью сложности – тестовые пароли, допускаются, когда для требований паролей стоит настройка, что ПО используется в тестовом режиме. Использование таких паролей в процессе штатной работы SpaceVM не допускается.

Пароль с низкой степенью сложности предусматривает следующее:

– минимальная длина – три символа;

– в пароле должны присутствовать символы как минимум одной из категорий – прописные буквы латинского алфавита от «A» до «Z», строчные буквы латинского алфавита от «a» до «z», десятичные цифры от «0» до «9»;

– могут присутствовать символы только одного регистра;

– допускается пароль, состоящий из одних и тех же символов (например, «zzz»);

2) «middle» – пароли со средней степенью сложности – пароли с ограниченным сроком действия, допускается, когда для требований паролей стоит настройка, что ПО используется в штатном режиме, но только для временных пользователей.

Пароль со средней степенью сложности предусматривает следующее:

– минимальная длина – пять символов;

– в пароле должны присутствовать символы как минимум двух категорий – прописные буквы латинского алфавита от «A» до «Z», строчные буквы латинского алфавита от «a» до «z», десятичные цифры от «0» до «9»;

– могут присутствовать символы только одного регистра;

– пароль, состоящий из одних и тех же символов (например, «zzzzz»), не допускается;

3) «high» – пароли с высокой степенью сложности – пароли для штатного режима работы.

Пароль с высокой степенью сложности предусматривает:

– минимальная длина – восемь символов;

– в пароле должны присутствовать символы как минимум трех категорий – прописные буквы латинского алфавита от «A» до «Z», строчные буквы латинского алфавита от «a» до «z», десятичные цифры от «0» до «9», символы, не принадлежащие алфавитно-цифровому набору (например, «~», «?», «:»);

– одновременно должны присутствовать символы двух регистров;

– пароль не может содержать имя этого пользователя (логин) или какую-либо его часть (частью считается и отдельный символ, присутствующий в логине).

3.12.12. Алгоритм хеширования паролей

3.12.12.1. При установке системы задается пароль пользователя «root». Инсталлятор системы хеширует его при помощи алгоритма «yescrypt». Все пароли, создаваемые или изменяемые после установки системы, хешируются уже с помощью алгоритма «gost-yescrypt», сочетающего расширенную устойчивость к перебору паролей благодаря «yescrypt» с криптографическими свойствами всей конструкции согласно ГОСТ Р 34.11–2012.

ВНИМАНИЕ! Для того чтобы пароль пользователя «root» хранился также с учетом ГОСТ Р 34.11–2012, достаточно сменить его (даже на тот же самый, что задан при установке) через Web-интерфейс либо при помощи команды CLI

ssh user change_password

3.12.12.2. Для хеширования паролей загрузчика применяется алгоритм PBKDF2 с хешем SHA512.

3.12.13. Парольная защита меню загрузки

3.12.13.1. Загрузчик SpaceVM обладает богатыми возможностями изменения параметров загрузки системы. Например, возможно запретить загрузку или задать параметры для каких-либо драйверов, параметры загрузки ядра, вручную задать образ ядра, начальный RAM-диск и прочее. Эти возможности реализуются через редактирование во время работы («на лету») пунктов меню загрузки SpaceVM или в режиме командной строки загрузчика.

«По умолчанию» данные возможности доступны для любого, кто имеет доступ:

1) к физической консоли узла SpaceVM;

2) к последовательному порту #2 системы (в том числе при возможности подключить к системе USB UART);

3) при наличии IPMI, логина и пароля IPMI:

– к удаленной консоли IPMI;

– к SOL.

С точки зрения безопасности бывает целесообразно ограничить доступ к подобным возможностям. SpaceVM позволяет задать имя пользователя и пароль, которые будут запрашиваться в любой ситуации при загрузке, кроме выбора пункта загрузочного меню «по умолчанию».

Для этой цели, а также для просмотра состояния и снятия парольной защиты, служит команда CLI *boot_protect*.

Стойкость пароля при его задании проверяется по уровню «middle» (см. 3.12.10).

3.12.13.2. Следует подчеркнуть, что при задании парольной защиты автоматическая загрузка узла остается полностью доступной.

3.12.14. Проверка целостности ПО SpaceVM

3.12.14.1. После установки или обновления ПО SpaceVM необходимо произвести фиксацию контрольных сумм.

3.12.14.2. Командой в CLI *aide init* создаем базу данных файлов с контрольными суммами.

3.12.14.3. Командой в CLI *aide log* можно просмотреть журнал последнего создания базы с контрольными суммами.

3.12.14.4. Командой в CLI *aide check* осуществляется сверка контрольных сумм файлов в файловой системе с базой контрольных сумм.

3.13. Настройки

В данном разделе содержатся:

– настройки ограждения;

– IP-адреса контроллера;

– информация о версии установленного ПО и возможность их обновления.

3.13.1. Организации

3.13.1.1. Раздел «Организации» предназначен для централизованного управления организациями и их пользователями.

3.13.1.2. В разделе «Настройки» – «Организации» основного меню содержится список организаций, включая для каждой из них название, количество пользователей и статус.

3.13.1.3. Для того чтобы добавить организацию, необходимо нажать на кнопку «Создать организацию» и в открывшемся окне заполнить следующие поля:

– название организации;

– описание организации.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

3.13.1.4. При нажатии на название организации в открывшемся окне имеется возможность обновить информацию и удалить организацию. При нажатии на кнопку «Удалить организацию» в открывшемся окне необходимо подтвердить операцию, нажав «Удалить».

3.13.1.5. Информация об организации разделена на следующие группы:

– информация;

– пользователи;

– пулы ресурсов;

– виртуальные сети;

– события;

– теги.

3.13.1.6. В окне «Настройки» – «Организации» – <имя организации> – «Информация» содержатся следующие сведения:

– название организации (редактируемый параметр);

– описание (редактируемый параметр);

– статус;

– дата и время создания;

– дата и время изменения.

3.13.1.7. В окне «Настройки» – «Организации» – <имя организации> – «Пользователи» содержится список пользователей, включая для каждого из них его имя, роли, статус, возможность отключения.

Имеется возможность добавить пользователей, нажав на кнопку «Добавить пользователей к организации». В открывшемся окне необходимо выбрать пользователей из раскрывающегося списка и после этого нажать кнопку «ОК».

3.13.1.8. Имеется возможность выбрать пользователя с применением фильтра. Для выбора определенного пользователя с применением фильтра необходимо в верхней строчке окна нажать на кнопку « Фильтр» и в открывшемся окне заполнить поля:

– «Имя» – имя искомого пользователя;

– «Роли» – выбор из раскрывающегося списка;

– «Организации» – выбор из раскрывающегося списка.

После настройки фильтра необходимо нажать «Применить» или «Сбросить все».

3.13.1.9. В окне «Настройки» – «Организации» – <имя организации> – «Пулы ресурсов» содержится список имеющихся пулов, включая для каждого из них название, количество ВМ, ограничение памяти и CPU.

Также в этом окне существует возможность создания нового пула по кнопке «Добавление пула ресурсов» и выбора определенного пула с применением фильтра по кнопке «Фильтр».

При нажатии на кнопку «Добавление пула ресурсов» открывается диалоговое окно для выбора пула из раскрывающегося списка, после чего необходимо подтвердить операцию, нажав «ОК».

При нажатии на кнопку «Фильтр» открывается диалоговое окно для настройки фильтра с соответствующими полями:

– «Имя пула ресурсов»;

– «Кластеры» – выбор из раскрывающегося списка;

– «Организации» – выбор из раскрывающегося списка;

– «Теги» – выбор из раскрывающегося списка.

После заполнения полей необходимо нажать «Применить» или «Сбросить все».

3.13.1.10. В окне «Настройки» – «Организации» – <имя организации> – «Виртуальные сети» содержится список виртуальных сетей, а также имеется возможность их добавления и отключения.

3.13.1.11. В окне «Настройки» – «Организации» – <имя организации> – «События» отображаются события, зарегистрированные в системе для этой организации с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные».

Также имеется возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.13.1.12. В окне «Настройки» – «Организации» – <имя организации> – «Теги» имеется возможность добавления к организации отличительной метки (тега), применения и обновления тега.

3.13.1.13. Для создания нового тега необходимо нажать кнопку «Создать» и в открывшемся окне заполнить следующие поля:

– название тега;

– идентификатор тега (Slug);

– цвет тега из открывающейся палитры. При выборе цвета необходимо подтвердить изменения, нажав кнопку «ОК», либо выйти без сохранения изменений, нажав кнопку «Отмена».

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

Для применения нового тега необходимо нажать кнопку «Применить» и в открывшемся окне выбрать тег. Для сохранения изменений необходимо нажать кнопку «ОК».

3.13.1.13.1. Пример выделения ресурсов для организации:

1) создаем организацию;

2) создаем пул ресурсов, добавляем к нему серверы, общие для этих серверов пулы данных, ВМ, ставим при необходимости ограничения на ресурсы. Более подробное описание пулов ресурсов приведено в 3.7 данного руководства;

3) добавляем пул ресурсов к организации;

4) создаем пользователей с ролью «Оператор ВМ» с указанием организации или добавляем нужных нам пользователей к организации.

После последнего шага все сущности пула ресурсов (пулы данных, образы на них, ВМ с их резервными копиями) станут доступными пользователю.

При изменении сущностей пула ресурсов для того, чтобы их увидел пользователь, необходимо переподключить пользователя к организации.

3.13.2. Контроллер

3.13.2.1. Информация

3.13.2.1.1. В разделе «Настройки» – «Контроллер» основного меню содержится следующая информация, разделенная на группы:

– «Информация» – информация о контроллере;

– «SNMP» – настройки Simple Network Management Protocol;

– «SMTP» – настройки SMTP-сервера;

– «ПО и Сервисы» – информация о версии ПО контроллера и сервисах;

– «Syslog» – управление получателями сообщений;

– «Контроллеры»;

– «Задачи по расписанию»;

– «Репликация».

3.13.2.1.2. Во вкладке «Информация» содержатся настройки контроллера:

– четвертый октет генерируемых MAC-адресов (редактируемый параметр);

– тайм-аут стартового ожидания переподключения к недоступным узлам (редактируемый параметр);

– начальный тайм-аут между попытками ограждения узлов (редактируемый параметр);

– максимальный тайм-аут между попытками ограждения узлов (редактируемый параметр);

– множитель увеличения тай-аута между попытками (редактируемый параметр);

– адрес интерфейса управления контроллера для протокола SPICE (редактируемый параметр);

– автоматическая синхронизация сети (при автотестировании, редактируемый параметр);

– автоматическое сканирование хранилищ (при автотестировании, редактируемый параметр);

– часовой пояс (редактируемый параметр);

– ID контроллера;

– опции (редактируемый параметр) – ключ, тип, значение;

– IP-адрес контроллера.

3.13.2.1.3. Кнопка «Сканировать хранилища контроллера» запускает сканирование и синхронизацию на всех серверах контроллера следующих хранилищ:

– сетевых хранилищ;

– блочных сетевых хранилищ;

– пулов zfs;

– кластерных транспортов;

– пулов данных.

Примечание. Поиск пулов данных будет осуществлен на всех (на уже известных и на найденных) хранилищах. Все пулы данных, включая найденные, будут просканированы на предмет содержащихся на них образов, дисков и файлов.

Также существует возможность обновления контроллера.

3.13.2.2. SNMP

3.13.2.2.1. В окне «Настройки» – «Контроллер» – «SNMP» перечислены настройки snmp-walk агента, необходимые для передачи по протоколу SNMP метрик системы с возможностью изменения, добавления или удаления параметров. При нажатии на кнопку добавления  в открывшемся окне необходимо ввести название объекта, после чего подтвердить операцию, нажав кнопку «Сохранить». При нажатии на кнопку редактирования  в открывшемся окне необходимо скорректировать название объекта, после чего подтвердить операцию, нажав кнопку «Сохранить». При нажатии на кнопку удаления  операция происходит автоматически.

В данном окне отображаются следующие параметры:

1) location;

2) contact;

3) community;

4) network;

5) agentaddress;

6) статус службы. «По умолчанию» статус сервера выключен. При нажатии на кнопку редактирования в открывшемся окне необходимо включить или выключить опцию «service ensure», после чего подтвердить операцию, нажав кнопку «Изменить». Статус сервиса дополнительно можно проверить для контроллера и узлов через вкладку «ПО и Сервисы»;

7) Snmpv3 user. При нажатии на кнопку редактирования в открывшемся окне необходимо заполнить следующие поля:

– username;

– auth password;

– private password.

После заполнения всех полей необходимо подтвердить операцию, нажав кнопку «Сохранить».

Если были внесены изменения в конфигурацию SNMP, то в нижней части окна становится доступна кнопка «Сохранить изменения», при нажатии на которую открывается диалоговое окно для подтверждения операции. Необходимо нажать «Да» для изменения конфигурации или «Отмена» для отказа от них.

Также в окне управления конфигурацией SNMP существует возможность обновления и отправки SNMP-запроса по кнопке «Отправить SNMP-запрос». При нажатии данной кнопки в открывшемся окне необходимо заполнить:

– IP-адрес сервера (выбор из раскрывающегося списка);

– версию (выбор из раскрывающегося списка). Может принимать значения «1», «2» или «3»;

– тип команд (выбор из раскрывающегося списка). Может принимать значения «snmpwalk» или «snmptable»;

– command.

После этого необходимо подтвердить операцию, нажав кнопку «Отправить».

3.13.2.2.2. Имеется зарегистрированная база управляющей информации в OID Repository – *http://www.oid-info.com/get/1.3.6.1.4.1.51290*.

Архив MIB доступен по запросу у предприятия-разработчика.

Список реализованных OID SNMP приведен в таблице 5.

Таблица 5

OID	Идентифи-катор	Значение	Тип	Описание
1.3.6.1.2.1.74.1.51290.1.1.1.0	veilVmCount.0	4	Gauge	Количество запущенных виртуальных машин

OID	Идентифи-катор	Значение	Тип	Описание
1.3.6.1.2.1.74.1.51290.1.1.2.1.2.36.x	veilVmUuid.	38754900-aaec-4480-8a41-9d1b1a3986a4	OctetString	ID виртуальной машины
1.3.6.1.2.1.74.1.51290.1.1.2.1.3.36.x	veilVmStatus.	Running	OctetString	Состояние виртуальной машины

Открытое средство для просмотра MIB находится по адресу *https://www.ireasoning.com/mibbrowser.shtml.*

Для просмотра текущей SNMP конфигурации сервера необходимо запустить в CLI команду

system snmp_conf

3.13.2.3. SMTP

3.13.2.3.1. В окне «Настройки» – «Контроллер» – «SMTP» имеется возможность настроить SMTP-сервер. Для этого необходимо нажать кнопку «Настроить SMTP-сервер» и в открывшемся окне заполнить следующие поля:

– адрес сервера;

– порт;

– имя SMTP пользователя | e-mail;

– e-mail для отправки текстового сообщения;

– e-mail для получения текстового сообщения;

– пароль SMTP приложения;

– включить (выключить) опцию «Без аутентификации»;

– включить (выключить) опцию «Использовать сохраненные имя/email и пароль»;

– включить (выключить) опцию TLS;

– включить (выключить) опцию SSL.

После заполнения всех полей необходимо подтвердить операцию, нажав кнопку «Сохранить».

Также существует возможность проверки соединения с SMTP-сервером по кнопке «Проверить соединение с SMTP сервером». При нажатии данной кнопки в открывшемся окне необходимо выбрать настройки сервера и почтовый адрес, на который уйдет тестовое сообщение. После этого необходимо подтвердить операцию, нажав кнопку «Проверить».

3.13.2.3.2. Существует несколько сценариев работы с сервисом SMTP:

1) работа с внешним SMTP сервером. Для работы с внешним SMTP сервером переключатель «Без аутентификации» должен быть выключен. Обязательными к заполнению в данном режиме при первоначальной настройке являются только поля «Адрес сервера», «Порт», «Имя SMTP пользователя | email», «Пароль SMTP приложения». Выполнив первичную настройку и нажав кнопку «Сохранить» можно переходить либо к тестированию отдельных e-mail адресов, либо непосредственно к работе с SMTP-сервисом.

При повторном конфигурировании или при отправке тестового сообщения для использования ранее сконфигурированных параметров (имя, пароль и далее) можно выбрать переключатель «Использовать сохранённые имя/email и пароль». Данный переключатель позволяет изменять и тестировать различные конфигурации SMTP-сервера без необходимости повторного набора всего множества полей. Проверка соединения путём отправки тестового сообщения выполняется по кнопке «Проверить соединение».

Отдельно стоит отметить логику работы, связанную с полем «Email для отправки текстового сообщения». Если в поле «Имя SMTP пользователя | email» было введено имя пользователя, то для правильной работы необходимо заполнить поле «Email для отправки текстового сообщения». Если в поле «Имя SMTP пользователя | email» был введён e-mail, то он автоматически продублируется и в поле «Email для отправки текстового сообщения»;

2) работа с внутренним сервером. При условии, что SMTP сервер развернут в пользовательской сети (не используются внешние типа *smtp.mail.ru*) необходимо активировать переключатель «Без аутентификации». Это приведёт к сокращению количества активных полей до необходимого минимума.

Примечания:

1. Не забудьте обеспечить доступ контроллера к SMTP-серверу.

2. Удалить абсолютно все данные, связанные с конфигурацией SMTP-сервиса, можно по кнопке «Сбросить настройки».

3.13.2.4. ПО и сервисы

3.13.2.4.1. В окне «Настройки» – «Контроллер» – «ПО и сервисы» – «ПО» содержатся версии всех компонентов установленного ПО контроллера. Также в данном окне присутствуют кнопки запуска процесса обновления ПО контроллера:

– только на контроллере «Обновление ПО контроллера»;

– на контроллере и всех серверах «Обновление ПО контроллера+серверов».

При запуске обновлений в открывшемся окне отобразится список пакетов, готовых к обновлению, после чего следует нажать кнопку «Обновить все пакеты ПО».

3.13.2.4.2. В окне «Настройки» – «Контроллер» – «ПО и сервисы» – «Сервисы» содержатся сервисы контроллера и их статус.

Также в данном окне присутствует кнопка «Действия над сервисами контроллера», которая позволяет настроить сервисы.

При нажатии на кнопку «Действия над сервисами контроллера» в открывшемся окне необходимо выбрать из раскрывающегося списка сервис и действие для него («start», «stop» или «restart»). После внесения изменений необходимо подтвердить операцию, нажав кнопку «Изменить».

3.13.2.5. Системный журнал

3.13.2.5.1. В окне «Настройки» – «Контроллер» – «Syslog» можно настроить доставку системных сообщений системы управления в rsyslog, ArcSight logger и другие системы, поддерживающие прием событий в форматах «syslog» и «cef» (common event format). Для этого необходимо нажать кнопку «Добавление получателя» и в открывшемся окне заполнить следующие поля:

– имя получателя;

– тип получателя (выбор из раскрывающегося списка). Может принимать значения «syslog» и «cef»;

– сетевой адрес получателя;

– порт получателя;

– информация о протоколе передачи сообщений;

– уровень сообщений (выбор из раскрывающегося списка). Может принимать значения «CRITICAL», «ERROR», «WARNING», «INFO», «DEBUG» или «NOTSET».

После заполнения полей необходимо подтвердить операцию, нажав кнопку «Добавить».

Выбор источника и уровня сообщений осуществляется в соответствии с правилами, принятыми для ОС семейства Linux:

– при уровне «NOTSET» будут отправляться все сообщения;

– для других уровней будут отправляться сообщения указанного уровня и все сообщения уровнем выше по критичности (для «WARNING» – «WARNING», «ERROR» и «CRITICAL»).

Отдельно выведена кнопка редиректа (автоматическое перенаправление) на сервис «Kibana», находящийся на контроллере. «По умолчанию» сервис выключен, а включить/выключить его можно из CLI командой

kibana start|*stop*

«Kibana» позволяет удобно просматривать и фильтровать все журналы системы.

Описание стека журналирования смотрите в руководстве системного программиста ДСБР.30001-01 32 01. Подробности фильтрации смотрите на официальном сайте «Kibana».

Индексы в Elasticsearch группируются логически в пять групп:

– cli-[one for the every day];

– node-[one for the every day];

– controller-[one for the every day];

– system.syslog-[one for the every day];

– fluent-[one for the every day].

Для первоначальной настройки «Kibana» необходимо создать нужный паттерн индекса. В зависимости от того, что нужно, выберите наиболее близкие индексы для создания паттерна. Выберите имя поля временного фильтра (обычно «@timestamp»). После создания паттерна можно смотреть журналы созданного паттерна и фильтровать их по нужным полям.

3.13.2.6. Контроллеры

3.13.2.6.1. В окне «Настройки» – «Контроллер» – «Контроллеры» можно добавить другие контроллеры для управления ими из интерфейса.

Для этого необходимо нажать кнопку «Добавить контроллер» и в открывшемся окне заполнить следующие поля:

– имя;

– сетевой адрес;

– ключ интеграции, созданный на другом контроллере для выбранного пользователя.

После заполнения полей необходимо подтвердить операцию, нажав кнопку «Добавить». При добавлении будет осуществлена проверка аутентификации и в случае неудачи добавление не произойдет.

Поддерживается добавление до 15 контроллеров.

3.13.2.7. Репликация

3.13.2.7.1. В окне «Настройки» – «Контроллер» – «Репликация» отображаются настройки резервного контроллера и статус репликации параметров кластера. Настройка резервного контроллера и репликации производится из CLI-интерфейса контроллера. Более полное описание приведено в разделе 3 руководства системного программиста ДСБР.30001-01 32 01.

3.13.3. Лицензирование

3.13.3.1. В разделе «Настройки» – «Лицензирование» основного меню содержится информация по действующим лицензионным ключам SpaceVM и их стекируемому результату. Также имеется возможность обновления, загрузки файлов новых ключей и удаления старых.

3.13.3.2. Загрузка лицензионного ключа производится нажатием кнопки «Выбрать файл лицензии». При этом открывается стандартное окно загрузки файлов, где необходимо выбрать файл и нажать на кнопку «Открыть».

3.13.3.3. Информация о лицензии содержит следующие поля:

– лицензия на ПО;

– e-mail;

– название компании;

– количество серверов (максимальное количество серверов для добавления к контроллеру);

– количество дней до окончания лицензии;

– количество дней до окончания сервисной поддержки;

– дата завершения лицензии;

– дата завершения сервисной поддержки.

Если пользователь имеет бессрочную лицензию, то ограничений по времени использования лицензии не будет и будет отражаться следующая информация:

– дней до окончания лицензии – «0»;

– дней до окончания сервисной поддержки – «0»;

– дата завершения лицензии – «--»;

– дата завершения сервисной поддержки – «--».

Примечания:

1. Количество используемых физических процессоров на сервере программными средствами не ограничено. При этом количество процессоров не может быть менее количества установленных на сервере и более количества сокетов на сервере.

2. Если были загружены лицензии с одинаковыми ID, то только первая из них будет учитываться.

3. Итоговые даты завершения лицензии и даты завершения сервисной поддержки берутся по наиболее поздней из них.

3.13.3.4. Также в окне с лицензиями имеются сообщения о работе с лицензиями с возможностью их сортировки по признакам – «По всем типам», «Ошибки», «Предупреждения», «Информационные», возможность отображения только непрочитанных сообщений и просмотр событий по дате с выбором интервала дат.

3.13.3.4.1. Правила использования лицензионных соглашений:

1) лицензирование при использовании нескольких контроллеров.

На каждом контроллере SpaceVM независимо от наличия сетевой связанности между ними, кроме случаев использования механизма репликации, должна быть уникальная лицензия на контроллер, а также уникальные лицензии на соответствующее количество серверов виртуализации Node.

ВНИМАНИЕ! Не разрешается повторное использование уникальной лицензии на нескольких несвязанных репликацией контроллерах. Повторное использование уникальной лицензии в данном случае является нарушением Лицензионного соглашения!

2) лицензирование при использовании механизма репликации.

При наличии механизма репликации для каждой пары контроллеров, связанных механизмом репликации (один контроллер с ролью «master» и один контроллер с ролью «slave» объединены связанностью), используется одна уникальная лицензия на контроллер и необходимое количество лицензий на серверы виртуализации. То есть, если два контроллера SpaceVM связаны механизмом репликации и имеют роли «master» и «slave», то на этих двух контроллерах должен быть использован одинаковый набор лицензий, включающий одну лицензию на контроллер и необходимое количество лицензий на серверы виртуализации Node**.**

После инициализация связанности между основным и резервным контроллерами и назначения им соответствующих ролей, лицензии с основного контроллера «master» будут скопированы на резервный контроллер «slave». Это означает, что не требуется никаких действий для переноса лицензий с основного контроллера на резервный, и при наступлении нештатной ситуации и переводе резервного контроллера «slave» в основной «master», в том числе при использовании свидетеля, лицензии останутся доступными.

ВНИМАНИЕ! Разрешается использование одного набора уникальных лицензий на нескольких связанных репликацией контроллерах;

3) лицензирование при использовании комбинированной схемы.

При наличии комбинированной схемы (несколько объединенных сетевой связанностью контроллеров, для которых используется механизм репликации) на каждый управляющий контроллер с ролью «master**»** или «alone» должна использоваться своя уникальная лицензия. На контроллерах с ролью **«**slave» должна использоваться та же лицензия, которая используется на связанном репликацией контроллере с ролью **«**master»**.**

3.13.4. Теги

3.13.4.1. Раздел «Настройки» – «Теги» основного меню предназначен для централизованного управления метками (тегами), которые можно применять ко всем объектам системы. Теги, созданные в системе управления для любого объекта системы, будут отображены в данном разделе. Также созданные в данном разделе теги станут доступными для установки на любой объект системы.

Теги предназначены для формирования привязок между объектами системы. Например, ВМ, отмеченная тегом node, при срабатывании ВД будет перезапущена на том сервере кластера с ВД, который имеет такой же тег. Теги не являются обязательными к применению, они формируют «магнетизм» между объектами кластера.

Таким образом, если ни один сервер кластера не имеет тегов, то при переносе ВМ приоритетов не будет, но может сработать тег, присвоенный виртуальному коммутатору. При этом наличие тегов на объектах кластера при работе механизмов ВД и DRS является блокирующим.

3.13.4.2. Создание нового тега производится с помощью кнопки «Создать» и заполнения следующих полей:

– название тега;

– идентификатор тега (Slug);

– цвет тега из открывающейся палитры.

При выборе цвета необходимо подтвердить изменения, нажав кнопку «ОК», либо выйти без сохранения изменений, нажав кнопку «Отмена».

После заполнения полей необходимо подтвердить операцию, нажав кнопку «ОК».

3.13.4.3. Система контроля повторяемости тегов не позволяет создавать теги с одинаковым именем или идентификатором (Slug).

3.13.4.4. Также существует возможность обновления названия и цвета.

3.13.4.5. Для удаления тега (метки) необходимо выбрать его в списке тегов и в открывшемся окне выбрать одну из следующих операций:

1) удалить тег. При нажатии на кнопку «Удалить тег» в открывшемся окне подтвердить операцию, нажав «Да»;

2) удалить метку. Для этого раскрыть список «Сущности» и нажать на кнопку  . В открывшемся окне «Удаление метки» подтвердить операцию, нажав «Да».

3.13.5. Системные

3.13.5.1. Раздел «Настройки» – «Системные» основного меню предназначен для управления настройками приложения контроллера.

3.13.5.2. В данном разделе содержится следующая общая информация:

1) настройки контроллера:

– возможность перемещать виртуальные машины (вкл/выкл) (редактируемый параметр). При выключении будет запрещена миграция ВМ;

– журналирование действий с ограниченным доступом (вкл/выкл) (редактируемый параметр).

При включении будут создаваться события безопасности для всех попыток действий пользователя, на которые у него нет доступа;

– журналирование некорректных действий пользователей (вкл/выкл) (редактируемый параметр). При включении будут создаваться события с некорректными действиями пользователей.

Например, пользователь захотел создать ВМ с 1000 vCPU, ему вернулась ошибка «Убедитесь, что это значение меньше либо равно 255», и сразу создастся событие с этой ошибкой;

– возможность удаления пользователей (вкл/выкл) (редактируемый параметр). При включении будет возможность удалять пользователей.

После изменения поля необходимо подтвердить операцию, нажав кнопку «Сохранить» и перезагрузить сервисы контроллера в CLI командами *services restart controller-web-api* и *services restart controller-engine*;

2) системные настройки:

– системный язык (редактируемый параметр). Можно выбрать «Russian» или «English» При нажатии кнопки редактирования в открывшемся окне отобразится информация о выбранном на данный момент языке. Также имеется возможность смены языка из раскрывающегося списка и предупреждение о необходимости перезагрузки контроллера для смены языка. Перезагрузка контроллера выполняется в окне «Настройки» – «Контроллер» – «ПО и Сервисы» – «Сервисы» по кнопке «Действия над сервисами контроллера», где необходимо выбрать сервис «controller-engine» и действие «restart»;

– период жизни токена – ключа доступа (редактируемый параметр). Это период (дни), по истечению которого токен пользователя удалится из системы, если этим токеном не пользоваться;

– период возможности обновления токена (редактируемый параметр). Это период (дни), в течении которого возможно обновлять токен, чтобы избежать удаление этого токена из системы.

Пример – период жизни токена 1 день, период возможности обновления токена 30 дней. При таких настройках токен пользователя будет храниться в системе в течении 30 дней при условии его использования минимум раз в 1 день;

– количество одновременных сессий (редактируемый параметр). Это максимальное количество активных сессий во всей системе;

– время жизни сессионных cookie (редактируемый параметр). По истечению этого времени происходит удаление cookie-файлов пользователя, при этом токен пользователя остается в системе;

– тестовый режим (вкл/выкл) (редактируемый параметр). Включает (выключает) вывод сообщений отладчика в журнал, открывает тестовые Endpoint, открывает Swagger Web по URL;

– отладка подсказок (редактируемый параметр). Включает (выключает) режим редактирования подсказок;

– тайм-аут бездействия пользователя (редактируемый параметр). При превышении тайм-аута происходит автоматический выход из системы. Бездействие – отсутствие действий устройств ввода («мышь», клавиатура) на странице. Выход из системы включает в себя и выход из сессий терминалов.

4. СООБЩЕНИЯ ОПЕРАТОРУ

4.1. Сообщения оператору, выдаваемые на экран во время настройки и выполнения программы в виде всплывающих сообщений, информируют о задачах, выполнение которых было прервано.

Список задач и событий в системе регистрируются в журналах системы управления. Подробнее работа с журналами описана в подразделе 3.11 данного руководства.

ПРИЛОЖЕНИЕ 1

ПАРАМЕТРЫ ОБЪЕКТОВ ИНФРАСТРУКТУРЫ SPACEVM

1. В таблице 1.1 приведены допустимые пределы для контролера.

Таблица 1.1

Параметр	Предел
Узлы на контроллере	2500
ВМ на контроллере	35000
Включенные ВМ на контроллере	30000
Другие контроллеры на контроллере	15

2. В таблице 1.2 приведены допустимые пределы для кластера.

Таблица 1.2

Параметр	Предел
Узлы на кластере	96
Узлы с кластерным транспортом ocfs2 или gfs2 на кластере	32
ВМ на кластере	10000
Включенные ВМ на кластере	8000

3. В таблице 1.3 приведены допустимые пределы и значения для вычислительного узла.

Таблица 1.3

Параметр	Предел/значение
ВМ на узле	1024
Физические интерфейсы на узле	98
Объем гипервизора (Мбайт)	50
Поддержка сетевых карт со скоростью передачи данных (Гбит/сек)	40
Поддержка серверов с количеством процессоров	512 (x86_64)
Поддержка серверов с количеством логических процессоров	1024 (x86_64)

Параметр	Предел/значение
Поддержка серверов с количеством RAM (TiB)	128

4. В таблице 1.4 приведены допустимые пределы для виртуальной машины.

Таблица 1.4

Параметр	Предел
Интерфейсы на ВМ	10
Максимум процессоров на ВМ	255
Минимальный размер слота памяти на ВМ (Мбайт)	256
Максимальный размер слота памяти на ВМ	Размер памяти сервера
Максимум слотов памяти на ВМ	16
Максимальный размер видеопамяти на ВМ (Мбайт)	524288
Минимальный размер памяти на ВМ (Мбайт)	50

5. В таблице 1.5 приведены допустимые пределы для хранилища.

Таблица 1.5

Параметр	Предел
Максимальный размер виртуального диска (TiB)	64
Поддержка томов системы хранения (TiB)	360
Максимум виртуальных дисков на lvm (thinlvm) пул данных	255

6. В таблице 1.6 приведен предел для интерфейса.

Таблица 1.6

Параметр	Предел
Количество одновременных сессий	100

7. В таблице 1.7 приведен предел для меток.

Таблица 1.7

Параметр	Предел
Максимальное количество тегов на сущность	15

ПРИЛОЖЕНИЕ 2

ДОПУСТИМЫЕ ФОРМАТЫ ФАЙЛОВ ДЛЯ ЗАГРУЗКИ

1. Допустимые форматы файлов для загрузки приведены в таблице 2.1.

Таблица 2.1

Расширение	Тип	Применение
vmdk	Vmware4 disk image	Диск для ВМ (импорт на диск)
vhdx	Microsoft Disk Image eXtended	Диск для ВМ (импорт на диск)
qcow2	QEMU QCOW2 Image	Диск для ВМ (импорт на диск)
qcow	QEMU QCOW Image	Диск для ВМ (импорт на диск)
raw	raw image	Диск для ВМ (импорт на диск)
img	raw image	Диск для ВМ (импорт на диск)
bin	raw image	Диск для ВМ (импорт на диск)
ova	POSIX tar archive	Восстановление ВМ из ova
ovf	Open virtualization format	Восстановление ВМ из ovf
xml	XML document	Восстановление ВМ из xml
tar	POSIX tar archive	Резервная копия ВМ (восстановление ВМ из резервной копии)
run	POSIX shell script executable (binary data)	Резервная копия узла
json	text	Профиль узла (применение конфигурации к узлу)
zst	Zstandard compressed data	Сжатая резервная копия ВМ (восстановление ВМ из резервной копии)
vfd	Virtual Floppy Device	Виртуальный гибкий диск для ВМ
key	ASCII text	Ключи активации
rdp	Unicode	Файлы RDP
deb	Debian binary package	Deb-пакет
rpm	RPM	RPM-пакет
yaml	ASCII text	Файлы конфигураций
yaml	ASCII text	Файлы конфигураций
pub	OpenSSH	Открытые SSH-ключи

Для импорта файла на диск необходимо:

1) загрузить файл через Web-интерфейс одним из способов:

– перейти в раздел «Хранилища» – «Пулы данных» основного меню, выбрать нужный пул данных, перейти во вкладку «Файлы» и нажать кнопку «Загрузить из файловой системы» или «Загрузить по URL»;

– включить «vsftpd» сервис на сервере, где должен лежать этот файл, загрузить его по FTP в каталог файлов нужного пула данных ([Абсолютный путь к пулу данных]/_LIBRARY/), просканировать пул данных во вкладке «Файлы»;

– скопировать файл через SCP на сервер в каталог файлов ([Абсолютный путь к пулу данных]/_LIBRARY/) и просканировать пул данных во вкладке «Файлы»;

2) далее перейти в раздел «Хранилища» – «Файлы» основного меню, выбрать файл и нажать кнопку «Импортировать».

Перечень принятых сокращений

АРМ	– автоматизированное рабочее место
БД	– база данных
ВД	– высокая доступность
ВК	– виртуальный коммутатор
ВМ	– виртуальная машина
ЛВС	– локальная вычислительная сеть
МК	– менеджер конфигурации
МСЭ	– межсетевой экран
НЖМД	– накопитель на жестком магнитном диске
ОЕ	– организационная единица
ОС	– операционная система
ПО	– программное обеспечение
ПЭВМ	– персональная электронно-вычислительная машина
СХД	– система хранения данных
ФС	– файловая система
ЦОД	– центр обработки данных
ЦСХД	– централизованная система хранения данных
AD	– Active Directory (активный каталог)
API	– Application Programming Interface (программный интерфейс приложения)
BMC	– Baseboard Management Controller (модуль, обеспечивающий управление сервером по IPMI)
CLI	– Command Line Interface (интерфейс командной строки)
CPU	– Central Processing Unit (центральное процессорное устройство)
DNS	– Domain Name System (система доменных имен)
DRS	– динамическое управление ресурсами
FC	– Fiber Channel (оптическая сеть блочного доступа)
IPMI	– Intelligent Platform Management Interface (независимый от ОС интерфейс управления сервером)

LDAP – Lightweight Directory Access Protocol (облегченный протокол доступа к каталогам)

LLDP – Link Layer Discovery Protocol (протокол канального уровня)

LVM – Logical Volume Manager (менеджер логических томов)

LUN – Logical Unit Number (адрес дискового устройства в сетях хранения)

MS AD – Microsoft Active Directory (служба каталогов, разработанная Microsoft для доменных сетей Windows)

NPIV – N_Port ID Virtualization (технология для сетей Fibre Channel)

NUMA – Non-Uniform Memory Access (способ взаимодействия одного процессора с блоками памяти второго процессора)

OID – Object Identifier (идентификатор объекта)

OUI – Organizational Unique Identifier (уникальный идентификатор организации)

RAM – Random Access Memory (оперативная память)

SNMP – Simple Network Management Protocol (простой протокол сетевого управления)

STP – Spanning Tree Protocol (сетевой протокол, работающий на втором уровне модели OSI)

VDI – Virtual Desktop Infrastructure (инфраструктура виртуальных рабочих столов)

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	Номер документа	Входящий номер сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					