КИБЕРПРОТЕКТ

КИБЕР Инфраструктура

Версия 5.5

Руководство администратора

Редакция: 24.04.2024

Заявление об авторских правах

Содержание

1 Добро пожаловать в Кибер Инфраструктура! 11

2 Об инфраструктуре 12

2.1 О кластере хранилища данных 12

2.1.1 Архитектура кластера хранилища данных 13

2.2 Об архитектуре кэша хранилища 15

2.2.1 Поведение чтения и записи 15

2.2.2 Преимущества кэширования 16

2.3 О хранилище резервных копий 16

2.3.1 Архитектура хранилища резервных копий 17

2.4 О хранилище блочных данных 17

2.4.1 Пример блочного хранилища 18

2.5 О хранилище объектов 19

2.5.1 Архитектура хранилища объектов 20

2.5.2 Пример хранилища объектов 21

2.6 О файловом хранилище 21

2.7 О вычислительном кластере 22

2.7.1 Архитектура вычислительного кластера 23

2.7.2 Архитектура вычислительных сетей 23

3 Понятия и функции 27

3.1 Высокая доступность 27

3.1.1 Высокая доступность для служб 27

3.1.2 Высокая доступность и вычислительный кластер 29

3.2 Избыточность данных 29

3.2.1 Избыточность посредством репликации 30

3.2.2 Избыточность посредством избыточного кодирования 31

3.2.3 Без избыточности 31

3.2.4 Режимы избыточности 32

3.3 Области отказа 35

3.4 Уровни хранения данных 36

3.4.1 Ручной запуск миграции данных между уровнями (по умолчанию) 36

3.4.2 Автоматическая миграция данных между уровнями 36

3.5 Политики хранения 37

3.6 Перестроение кластера 38

3.7 Автоматическая балансировка данных 40

3.8 Мультитенантность ... 40
3.9 Типы трафика ... 42
3.9.1 Эксклюзивные типы трафика ... 42
3.9.2 Обычные типы трафика ... 43
3.9.3 Пользовательские типы трафика ... 44
4 Требования к системе ... 45
4.1 Рекомендации по оборудованию ... 45
4.2 Рекомендуемое оборудование ... 45
4.2.1 Сетевые карты для RDMA ... 45
4.2.2 Сетевые карты для DPDK ... 46
4.2.3 Серверы ... 46
4.3 Требования к серверу ... 46
4.3.1 Общие требования ... 46
4.3.2 Количество серверов ... 49
4.3.3 Требования к хранилищу резервных копий ... 50
4.3.4 Требования для вычислительного кластера ... 54
4.3.5 Требования для хранилища объектов ... 56
4.4 Требования к дискам ... 58
4.4.1 Типы и роли дисков ... 58
4.4.2 Емкость диска ... 58
4.4.3 Бюджетные твердотельные накопители ... 59
4.4.4 Контроллеры RAID и HBA ... 59
4.4.5 Количество дисков на сервер ... 60
4.4.6 Конфигурация с жесткими дисками и твердотельными накопителями ... 61
4.4.7 Рекомендации для конфигурации серверов с несколькими дисками ... 64
4.4.8 Использование SSD-накопителей ... 65
4.4.9 Расчет размера журнала записи ... 66
4.4.10 Конфигурация кэша ... 67
4.4.11 Защита данных во время отключений электроэнергии ... 71
4.4.12 Проверка функций сброса данных на диски ... 71
4.5 Требования к сети и рекомендации ... 73
4.5.1 Требования к сети ... 73
4.5.2 Рекомендации по сети ... 76
4.5.3 Сетевые порты ... 78
4.6 Требования для панели администрирования ... 80
5 Установка ... 81

5.1 Подготовка загрузочного носителя ... 81
5.1.1 Создание загрузочного USB-накопителя ... 82
5.1.2 Присоединение виртуального диска IPMI ... 84
5.1.3 Настройка PXE-сервера ... 87
5.2 Подключение к серверу с помощью консоли VNC ... 89
5.3 Создание файла kickstart ... 91
5.3.1 Параметры kickstart ... 91
5.3.2 Сценарии kickstart ... 92
5.3.3 Пример файла kickstart ... 94
5.4 Установка в ручном режиме ... 96
5.5 Установка в автоматическом режиме ... 103
5.6 Поиск и устранение неисправностей установки ... 106
5.6.1 Установка в базовом графическом режиме ... 106
5.6.2 Загрузка в режиме аварийного восстановления ... 106
6 Развертывание и настройка ... 108
6.1 Использование интерфейса командной строки ... 108
6.1.1 Предоставление учетных данных для vinfra ... 109
6.1.2 Управление заданиями vinfra ... 110
6.2 Настройка сетей ... 110
6.2.1 Настройка сетей для хранилища резервных копий ... 110
6.2.2 Настройка сетей для блочного хранилища ... 111
6.2.3 Настройка сетей для хранилища объектов ... 112
6.2.4 Настройка сетей для файлового хранилища ... 113
6.2.5 Настройка сетей в вычислительном кластере ... 113
6.3 Настройка сетевых интерфейсов серверов ... 117
6.3.1 Изменение сетевых интерфейсов ... 117
6.3.2 Создание объединений сетевых интерфейсов ... 127
6.3.3 Создание интерфейсов VLAN ... 131
6.3.4 Настройка устройств InfiniBand ... 134
6.3.5 Настройка устройств RoCE ... 136
6.4 Включение RDMA ... 136
6.4.1 Проверка сетевой инфраструктуры RDMA ... 137
6.4.2 Настройка RDMA ... 139
6.5 Добавление внешних DNS-серверов ... 139
6.6 Развертывание кластера хранилища данных ... 141
6.7 Включение высокой доступности сервера управления ... 146

6.8 Подготовка пространства для хранилища резервных копий к работе ... 150
6.8.1 Создание хранилища резервных копий в локальном кластере ... 151
6.8.2 Создание хранилища резервных копий в публичном облаке ... 154
6.8.3 Создание хранилища резервных копий на внешнем томе NFS ... 163
6.8.4 Добавление хранилищ резервных копий в Кибер Бэкап и Кибер Бэкап Облачный ... 167
6.9 Подготовка вычислительных ресурсов к работе ... 168
6.9.1 Создание вычислительного кластера ... 169
6.9.2 Настройка модели ЦП виртуальных машин ... 178
6.9.3 Установка доменного имени для API вычислений ... 180
6.9.4 Защита трафика API OpenStack с помощью SSL ... 181
6.9.5 Настройка мультитенантности ... 182
6.9.6 Обеспечение доступа к панели самообслуживания ... 190
6.9.7 Подготовка к работе балансировщиков нагрузки ... 191
6.9.8 Подготовка к работе кластеров Kubernetes ... 192
6.9.9 Подготовка к работе учета и биллинга ... 193
6.9.10 Настройка быстрой сети DPDK для виртуальных машин ... 194
6.10 Подготовка пространства для блочного хранилища к работе ... 197
6.10.1 Настройка инструмента командной строки для управления блочным хранилищем 199
6.10.2 Создание групп целевых устройств ... 199
6.10.3 Создание томов ... 204
6.10.4 Присоединение томов к группам целевых устройств ... 205
6.11 Подготовка пространства для хранилища объектов ... 207
6.11.1 Создание кластера S3 ... 208
6.11.2 Добавление пользователей S3 ... 214
6.11.3 Масштабирование хранилища объектов ... 215
6.11.4 Увеличение количества шлюзов S3 на серверах кластера S3 ... 215
6.12 Подготовка пространства для файлового хранилища ... 217
6.12.1 Создание кластера NFS ... 217
6.12.2 Создание томов NFS ... 218
6.12.3 Создание экспортов NFS ... 220
6.12.4 Масштабирование файлового хранилища ... 223
6.13 Настройка пользовательских режимов избыточности данных ... 224
7 Управление ... 225
7.1 Управление инфраструктурой ... 225
7.1.1 Управление серверами инфраструктуры ... 225
7.1.2 Масштабирование кластера хранилища ... 240

7.1.3 Управление сетями инфраструктуры ... 245
7.1.4 Управление доменами, пользователями и проектами ... 273
7.1.5 Настройка панели самообслуживания ... 314
7.1.6 Управление безопасностью ... 316
7.1.7 Управление лицензиями ... 322
7.1.8 Управление уведомлениями ... 326
7.1.9 Отправка уведомлений по электронной почте ... 329
7.1.10 Настройка параметров памяти для сервисов хранилища ... 331
7.1.11 Управление паролем кластера хранилища ... 336
7.1.12 Управление токенами ... 337
7.1.13 Управление технологией Fast Path ... 338
7.1.14 Настройка производительности дисков NVMe ... 339
7.1.15 Управление автоматической балансировкой нагрузки на уровни хранилища ... 341
7.2 Управление хранилищем резервных копий ... 350
7.2.1 Добавление узлов в хранилище резервных копий ... 350
7.2.2 Обновление сертификата для хранилища резервных копий ... 351
7.2.3 Повторная регистрация хранилища резервных копий в новом экземпляре Кибер Бэкап ... 352
7.2.4 Изменение схемы избыточности для хранилища резервных копий ... 354
7.2.5 Управление георепликацией для хранилища резервных копий ... 356
7.2.6 Настройка прокси для хранилища резервных копий ... 363
7.2.7 Настройка параметров TLS для хранилища резервных копий ... 365
7.2.8 Просмотр и изменение параметров хранилища резервных копий ... 367
7.2.9 Высвобождение серверов из хранилища резервных копий ... 370
7.3 Управление блочным хранилищем ... 372
7.3.1 Управление группами целевых устройств ... 373
7.3.2 Управление целевыми устройствами и их порталами ... 376
7.3.3 Управление томами ... 379
7.3.4 Ограничение доступа к группам целевых устройств ... 383
7.3.5 Управление серверами в группах целевых устройств ... 389
7.3.6 Управление представлениями LUN ... 393
7.4 Управление хранилищем объектов ... 395
7.4.1 Поддерживаемые функции Amazon S3 ... 395
7.4.2 Добавление серверов в кластер S3 ... 400
7.4.3 Управление пользователями S3 ... 401
7.4.4 Управление корзинами S3 ... 403

7.4.5 Рекомендации по использованию S3 в продукте Кибер Инфраструктура ... 404
7.4.6 Определение классов хранения объектов ... 407
7.4.7 Репликация данных S3 между центрами обработки данных ... 408
7.4.8 Настройка параметров TLS для хранилища объектов ... 415
7.4.9 Освобождение серверов из кластеров S3 ... 416
7.5 Управление хранилищем файлов ... 417
7.5.1 Добавление серверов в кластер NFS ... 417
7.5.2 Настройка аутентификации и авторизации пользователей ... 418
7.5.3 Управление томами NFS ... 422
7.5.4 Управление экспортами NFS ... 424
7.5.5 Удаление серверов из кластера NFS ... 426
7.6 Управление вычислительным кластером ... 427
7.6.1 Изменение параметров вычислительного кластера ... 427
7.6.2 Управление виртуальными машинами ... 435
7.6.3 Управление вычислительной сетью ... 529
7.6.4 Управление вычислительным хранилищем ... 602
7.6.5 Управление кластерами Kubernetes ... 628
7.6.6 Управление вычислительными серверами ... 641
7.6.7 Использование учета для вычислительных ресурсов ... 656
7.6.8 Управление автоматической балансировкой нагрузки на вычислительные серверы 664
8 Мониторинг ... 667
8.1 Просмотр оповещений ... 667
8.1.1 Оповещения инфраструктуры ... 669
8.1.2 Оповещения основного хранилища ... 675
8.1.3 Оповещения хранилища объектов ... 678
8.2 Просмотр журнала аудита ... 681
8.3 Просмотр журналов кластера ... 683
8.4 Мониторинг серверов инфраструктуры ... 686
8.4.1 Мониторинг производительности сервера ... 688
8.4.2 Мониторинг дисков сервера ... 688
8.4.3 Мониторинг сетевых интерфейсов сервера ... 704
8.5 Мониторинг кластера хранилища данных ... 706
8.5.1 Мониторинг серверов метаданных ... 710
8.5.2 Мониторинг серверов фрагментов данных ... 711
8.5.3 Мониторинг клиентов ... 716
8.5.4 Мониторинг физических дисков ... 718

8.5.5 Мониторинг журналов событий ... 720
8.5.6 Мониторинг параметров репликации ... 724
8.5.7 Диаграммы активности ввода-вывода ... 725
8.5.8 Диаграмма «Сервисы» ... 726
8.5.9 Диаграмма «Фрагменты данных» ... 727
8.5.10 Диаграмма «Физическое пространство» ... 730
8.5.11 Диаграмма «Логическое пространство» ... 732
8.5.12 Мониторинг нагрузки на уровни хранилища ... 734
8.5.13 Мониторинг объектов кластера с помощью SNMP ... 739
8.6 Удаленный мониторинг кластера ... 751
8.6.1 Использование встроенного Prometheus для мониторинга ... 751
8.6.2 Использование внешнего Prometheus для мониторинга ... 753
8.6.3 Настройка политики хранения для метрик Prometheus ... 755
8.6.4 Использование Alertmanager для оповещений ... 756
8.6.5 Метрики Prometheus ... 757
8.7 Мониторинг хранилища резервных копий ... 765
8.7.1 Расширенный мониторинг Backup Gateway с помощью Grafana ... 766
8.8 Мониторинг блочного хранилища ... 768
8.8.1 Расширенный мониторинг iSCSI с помощью Grafana ... 769
8.9 Мониторинг хранилища объектов ... 771
8.9.1 Расширенный мониторинг кластера S3 с помощью Grafana ... 771
8.10 Мониторинг файлового хранилища ... 773
8.11 Мониторинг вычислительного кластера ... 775
8.11.1 Диаграмма «Выделено вЦП» ... 777
8.11.2 Диаграмма «Выделено ОЗУ» ... 778
8.11.3 Диаграмма «Выделено хранилища» ... 782
8.11.4 Диаграмма «Статус ВМ» ... 783
8.11.5 Диаграмма «Список ВМ с наибольшим потреблением ресурсов» ... 784
8.11.6 Диаграмма «Оповещения» ... 785
8.11.7 Мониторинг вычислительных узлов ... 786
8.11.8 Мониторинг виртуальных машин ... 787
8.11.9 Мониторинг балансировщиков нагрузки ... 788
8.11.10 Мониторинг нагрузки на вычислительные серверы ... 789
9 Обслуживание ... 798
9.1 Установка обновлений ... 798
9.2 Выполнение обслуживания сервера ... 805

9.3 Резервное копирование и восстановление базы данных управления ... 811
9.3.1 Резервное копирование базы данных управления ... 812
9.3.2 Восстановление базы данных управления из резервной копии ... 813
9.3.3 Восстановление базы данных управления в вычислительном кластере ... 814
9.4 Управление конфигурацией высокой доступности ... 815
9.5 Замена дисков серверов ... 817
9.5.1 Автоматическая настройка новых дисков хранилища ... 817
9.5.2 Освобождение дисков сервера ... 819
9.5.3 Настройка новых дисков вручную ... 820
9.6 Выключение и запуск кластера ... 823
9.7 Освобождение серверов из кластера хранилища ... 824
9.8 Удаление неназначенных серверов ... 825
9.9 Повторное добавление неназначенных серверов ... 826
9.10 Возможные ошибки при входе в систему ... 827
10 Получение технической поддержки ... 830
Указатель ... 832

1 Добро пожаловать в Кибер Инфраструктура!

Продукт Кибер Инфраструктура, ранее известный как Acronis Infrastructure – это гиперконвергентное решение, которое предоставляет ресурсы хранилища, вычислительные и сетевые ресурсы для предприятий и поставщиков услуг в следующих целях:

- Обеспечить файловое хранилище для любых корпоративных данных, объектное хранилище S3 для приложений и облачных сервисов и блочное хранилище для работы виртуальных машин или баз данных с целевыми устройствами iSCSI.
- Создавать частные и публичные облака и управлять ими с помощью решения для аварийного восстановления.
- Сохранять резервные копии из решений Кибер Бэкап локально, в общедоступных облаках или на устройствах NAS с помощью Backup Gateway.
- Создавать виртуальные машины и программно определяемые сети и управлять ими.
- Запускать облачные приложения в производственных средах, включая сервисы «Kubernetes как услуга», «Балансировщик нагрузки как услуга» и постоянное хранилище для Kubernetes.
- Обеспечить высокую доступность для критически важных бизнес-приложений.

2 Об инфраструктуре

При установке на выделенные физические серверы без ПО Кибер Инфраструктура объединяет их в единый кластер, который можно легко масштабировать путем добавления дисков или узлов. Кластер управляется через веб-панель администрирования с высокой доступностью и через интерфейс командной строки. Панель администрирования обеспечивает всесторонний мониторинг всех компонентов. Обзорные панели мониторинга интегрируются в решения Prometheus, Grafana, SNMP и Zabbix, обеспечивая предоставление полезной информации о состоянии инфраструктуры. Кроме того, система оповещений позволяет администратору быть в курсе неправильных конфигураций, сбоев и других проблем.

Кластеризация помогает избежать потери данных благодаря репликации и помехоустойчивому кодированию. При включенной высокой доступности отсутствует единая точка отказа для кластера и служб. Кластер хранилища обладает возможностями самовосстановления: при отказе узла или диска кластер автоматически пытается восстановить утерянные данные. Также благодаря последовательному обновлению без перерывов в работе данные остаются доступными даже во время обновления узлов. В случае обслуживания узла или применения исправлений рабочая нагрузка переносится на другие доступные узлы.

В этом разделе описываются основные компоненты инфраструктуры и их архитектура: это кластеры хранилища и вычислительные кластеры, а также хранилища резервных копий, блочные хранилища, хранилища объектов и файловые хранилища.

2.1 О кластере хранилища данных

Кластер хранилища обеспечивает наиболее эффективное использование оборудования благодаря помехоустойчивому кодированию (технология Erasure Coding), встроенному кэшированию на твердотельных накопителях, автоматической балансировке нагрузки и поддержке RDMA/InfiniBand. Пространство кластера можно использовать для хранилищ следующих типов:

- Блочное хранилище iSCSI (горячие данные и виртуальные машины).
- Объектное хранилище S3 (защищено с помощью георепликации между ЦОД).
- Файловое хранилище (NFS).

Кроме того, Кибер Инфраструктура интегрирована с решениями Кибер Бэкап, что позволяет хранить резервные копии в кластере, отправлять их в облачные сервисы (такие как Yandex.Cloud) либо сохранять их на устройстве NAS по протоколу NFS. Георепликация доступна для шлюзов Backup Gateway, установленных на различных внутренних хранилищах: это может быть локальный кластер хранилища, том NFS или публичное облако.

Политики хранения данных можно настроить в зависимости от сценариев использования: каждый том данных может иметь свои настройки режима избыточности, уровня хранилища и области отказов. Также данные могут шифроваться по стандарту AES-256.

2.1.1 Архитектура кластера хранилища данных

Базовым компонентом продукта Кибер Инфраструктура является кластер хранилища – это группа физических серверов, связанных посредством сети. Основное хранилище состоит из сетевых дисков, каждому из которых назначаются одна или несколько ролей. Обычно на каждом сервере в кластере выполняются основные службы хранилища, которые соответствуют следующим дисковым ролям:

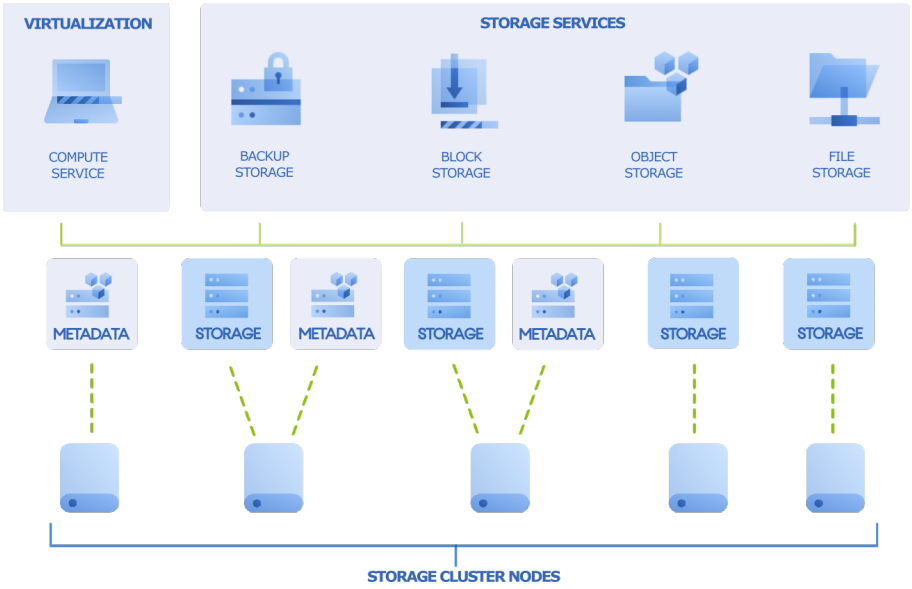
- Метаданные
  На узлах метаданных работают службы метаданных. На них хранятся метаданные кластера, также они управляют тем, как пользовательские файлы разделяются на фрагменты и где сохраняются эти фрагменты. Узлы метаданных также обеспечивают наличие достаточного количества реплик для фрагментов. Наконец, на них регистрируются в журналах все важные события, происходящие в кластере. Для обеспечения надежности системы Кибер Инфраструктура использует алгоритм консенсуса Паксос. Он гарантирует отказоустойчивость при работоспособности большинства узлов, на которых работают службы метаданных.
  Чтобы обеспечить высокую доступность метаданных в производственной среде, службы метаданных должны выполняться как минимум на трех узлах кластера. В этом случае при отказе одной службы остающиеся две продолжат контролировать кластер. Однако рекомендуется применять максимум пять служб метаданных, чтобы кластер мог выдержать одновременный отказ двух узлов без потери данных.
  Первичный узел метаданных является ведущим узлом в кворуме метаданных. В случае отказа ведущего узла с MDS в качестве ведущего выбирается другой доступный узел с MDS.
- Хранилище
  На узлах хранения выполняются службы фрагментов данных (CS). Эти узлы хранят данные в виде фрагментов фиксированного размера и предоставляют доступ к этим фрагментам. Все фрагменты данных реплицируются, и реплики размещаются на разных узлах хранения для обеспечения высокой доступности данных. При отказе одного из узлов хранения оставшиеся исправные узлы продолжат предоставлять доступ к фрагментам данных, которые хранились на отказавшем узле. Роль хранилища можно назначить только серверу с дисками определенной емкости.
  Узлы хранения также могут реализовывать преимущества кэширования данных и подсчета контрольных сумм.
  - Кэширование данных улучшает производительность кластера путем размещения часто используемых данных на твердотельном накопителе.
  - При контрольном суммировании данных контрольные суммы создаются при каждом изменении данных в кластере. Когда эти данные в дальнейшем считываются, вычисляется новая контрольная сумма, которая сравнивается со старой. Если две суммы не совпадают, операция чтения повторяется, что обеспечивает повышенную надежность и целостность данных.
    Если на узле имеется твердотельный (SSD) накопитель, он будет автоматически настроен на хранение контрольных сумм при добавлении узла в кластер. Это рекомендуемая настройка.

Однако если на узле нет твердотельного накопителя, контрольные суммы по умолчанию будут храниться на диске с вращающимися пластинами. Это значит, что данному диску придется обрабатывать двойной объем ввода-вывода, поскольку на каждую операцию чтения/записи данных будет приходиться дополнительная операция чтения/записи соответствующей контрольной суммы. Поэтому на узлах без твердотельных накопителей может потребоваться отключение контрольного суммирования, чтобы повысить производительность за счет отказа от контрольных сумм. Это может быть особенно результативно для хранилища горячих данных.

- Дополнительные роли:
  - Журнал и кэш на твердотельном накопителе
    Повышает производительность чтения/записи фрагментов данных путем создания кэша записи на выбранных твердотельных накопителях (SSD). Такие накопители также рекомендуется использовать для размещения метаданных. Использование журналов записи может более чем вдвое увеличить скорость записи в кластере.
  - Система
    Один диск на узел, зарезервированный для операционной системы и недоступный для хранения данных.

    Обратите внимание на следующее.
    - Отменить назначение роли «Система» диску невозможно.
    - Если физический сервер содержит системный диск емкостью более 100 ГБ, этому диску можно дополнительно назначить роль «Метаданные» или «Хранилище».
    - Рекомендуется назначать роль «Система+Метаданные» твердотельному накопителю. Назначение обеих этих ролей жесткому диску приведет к посредственной производительности, подходящей только для холодных данных (например, архивов).
    - Роль «Система» не может сочетаться с ролями «Кэш» или «Метаданные+Кэш». Причина состоит в том, что операции ввода-вывода, создаваемые операционной системой и приложениями, будут конкурировать с операциями ввода-вывода при ведении журнала, что нивелирует преимущества твердотельного накопителя по производительности.

Наряду с основными службами хранения на серверах выполняются точки доступа к хранилищам, которые обеспечивают доступ к серверу хранения данных для служб виртуализации высокого уровня и служб хранилищ.



Кроме того, на сервере, присоединенном к кластеру хранения данных, не могут выполняться ни службы метаданных, ни службы фрагментов данных. В этом случае на узле будут выполняться только точки доступа к хранилищу, он также может играть роль клиента кластера хранения данных.

2.2 Об архитектуре кэша хранилища

Термины «кэш» и «журнал» иногда используются как синонимы. Однако в кластере хранения кэш относится к быстрому аппаратному устройству (например, на базе SSD, в том числе NVMe), которое используется для хранения журнала обслуживания фрагментов. Журнал, в свою очередь, представляет собой буфер, который используется сервисом фрагментов и хранится в кэш-устройстве. Поскольку несколько сервисов фрагментов могут совместно использовать одно и то же устройство кэширования, один кэш может содержать несколько журналов.

Таким образом, кэширование не считается дополнительным уровнем хранения в кластере. Вместо этого каждое кэш-устройство может быть связано с несколькими службами фрагментов, назначенными разным уровням и используемыми для хранения журналов данных.

По умолчанию служба фрагментов хранит свой журнал на том же устройстве, что и данные. Эта конфигурация называется «внутренним кэшем». Чтобы использовать быстрое кэш-устройство, служба фрагментов должна быть настроена на использование «внешнего кэша».

2.2.1 Поведение чтения и записи

В кластере хранения кэш в основном используется для записи данных: когда новые данные поступают в систему, они временно сохраняются в кэше. Поскольку кэш-устройство быстрее, чем емкое, запись данных на кэш-устройство повышает производительность. В течение определенного времени данные существуют только в кэше с удаленными репликами на других узлах кластера, если удаленная репликация настроена. В течение этого времени все операции чтения попадают в

кэш и также выигрывают от прироста производительности. При восстановлении кэша и удалении из него данных все последующие операции чтения перенаправляются на устройство емкости.

Журнал используется как кольцевой буфер: он хранит данные до тех пор, пока не возникнет необходимость освободить место и освободить место для новых данных. Когда это происходит, данные выгружаются на устройство емкости в порядке поступления (FIFO).

2.2.2 Преимущества кэширования

Кэширование помогает значительно повысить скорость записи и задержку записи при незначительном увеличении стоимости системы. Системы с кэш-памятью могут извлечь выгоду из высокой емкости недорогих и малопроизводительных жестких дисков (HDD), обеспечивая при этом быстрый доступ для записи с помощью флэш-устройств, таких как твердотельные накопители (SSD), в том числе устройства NVMe. Хотя стоимость устройств кэш-памяти выше, чем стоимость устройств емкости, требуется лишь несколько устройств кэш-памяти, что делает общую стоимость системы в целом низкой. Более того, прирост производительности часто оправдывает такое обновление.

Выгода из использования кэша возможна в следующих сценариях:

- «Горячее» хранение данных
- Случайные записи
- Меньшие размеры блоков или файлы меньшего размера
- Базы данных и среды с несколькими клиентами/потоками

С другой стороны, сценарии, которые обычно имеют небольшое преимущество при использовании кэша, включают:

- «Холодное» хранение данных
- Рабочие нагрузки с постоянной пропускной способностью, такие как запись видеонаблюдения
- Последовательная запись очень больших файлов
- Рабочие нагрузки с интенсивным чтением

В этих случаях можно использовать решение, состоящее только из жестких дисков, которое обеспечит ту же производительность при меньших затратах; или решение all-flash, если цель – повысить производительность.

2.3 О хранилище резервных копий

Хранилище резервных копий использует шлюз Backup Gateway в качестве точки доступа к хранилищу. Эта функциональность предназначена для поставщиков услуг, которые используют Кибер Бэкап и/или Кибер Бэкап Облачный и хотят хранить резервные копии клиентских данных в локальном кластере, в облаке (например, Yandex Object Storage, VK Cloud Storage и SberCloud OBS) или на устройстве NAS (по протоколу NFS).

Хранилище резервных копий позволяет поставщикам услуг легко настраивать хранение данных в собственном формате с поддержкой дедупликации, который используется продуктами Киберпротект. Кроме того, можно включить георепликацию данных хранилища.

Хранилище резервных копий поддерживает следующие места назначения:

- Кластеры хранилища Кибер Инфраструктура с помехоустойчивым кодированием, которое обеспечивает избыточность данных.
- Тома NFS.
- Публичные облачные сервисы, включая ряд решений S3, а также Yandex Object Storage, VK Cloud Storage и SberCloud OBS.

Хотя ваш выбор должен основываться на конкретных требованиях и сценарии использования, рекомендуется хранить данные резервных копий в локальном кластере хранилища Кибер Инфраструктура. В этом случае достигается наилучшая производительность благодаря оптимизации каналов WAN и локальности данных. Хранение резервных копий на томе NFS или в публичном облаке предполагает постоянную передачу данных и другие дополнительные нагрузки, что снижает общую производительность. Кроме того, при использовании внешних мест назначения избыточность должна обеспечиваться внешним хранилищем. Само хранилище резервных копий не обеспечивает избыточности данных и не производит дедупликации.

2.3.1 Архитектура хранилища резервных копий

Точка доступа к хранилищу резервных копий Backup Gateway работает в виде службы на узлах Кибер Инфраструктура. Ее рекомендуется развернуть на двух или более узлах для обеспечения высокой доступности.

2.4 О хранилище блочных данных

Кибер Инфраструктура можно использовать как внутреннее хранилище блочных данных, доступное по протоколу iSCSI. Хранилище блочных данных оптимизировано для работы с данными, к которым нужно часто осуществлять доступ и которые нужно изменять. Оно идеально подходит для горячих данных и виртуальных машин.

Блочное хранилище позволяет управлять данными в виде блоков, в отличие от файлов в файловых системах или объектов в хранилище S3. Эти блоки могут храниться в разных операционных системах подобно сети SAN.

Кибер Инфраструктура позволяет создавать группы избыточных целевых устройств, работающих на разных серверах хранилища. К каждой группе целевых устройств можно присоединить множество томов хранения данных с собственной избыточностью, обеспечиваемой уровнем хранилища. Целевые устройства экспортируют эти тома как устройства LUN.

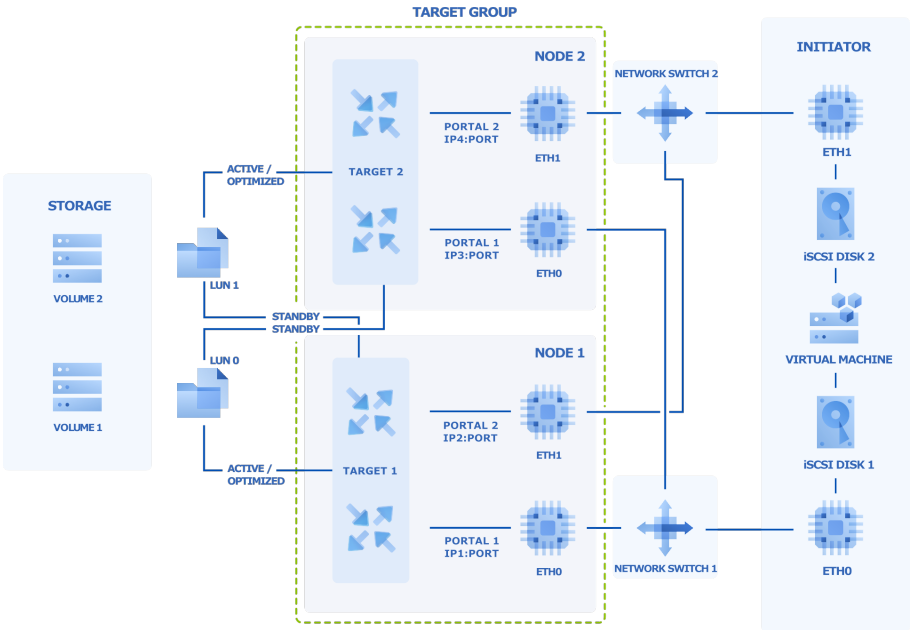
Можно создать несколько групп целевых устройств на одних и тех же серверах. Однако том в любой момент времени можно присоединить только к одной группе целевых устройств.

На каждом сервере в группе целевых устройств может размещаться одно целевое устройство для этой группы. Если один из серверов в группе выйдет из строя вместе со своими целевыми устройствами, то исправные целевые устройства из этой же группы продолжат предоставлять доступ к устройствам LUN, которые ранее обслуживались отказавшими целевыми устройствами.

Доступ к группам целевых устройств можно настраивать с использованием авторизации CHAP или ACL.

2.4.1 Пример блочного хранилища

На рисунке ниже показана типичная настройка для экспорта дискового пространства Кибер Инфраструктура через iSCSI.



На рисунке показаны два тома, расположенные в избыточном хранилище, предоставляемом продуктом Кибер Инфраструктура. Тома присоединены как LUN к группе из двух целевых устройств, работающих на серверах Кибер Инфраструктура. Каждое целевое устройство содержит два портала, по одному на каждый сетевой интерфейс с типом трафика iSCSI, что составляет в целом четыре обнаруживаемые конечные точки с разными IP-адресами. Каждое целевое устройство предоставляет доступ ко всем LUN, присоединенным к группе.

Целевые устройства работают в режиме ALUA, поэтому один путь к тому является предпочтительным и считается активным/оптимизированным, а другой – резервным. В норме активный/оптимизированный путь выбирается инициатором (явный режим ALUA). Если инициатор не поддерживает этот путь или истекает время ожидания, то путь выбирается самим хранилищем (неявный режим ALUA).

Сетевые интерфейсы **eth0** и **eth1** на каждом сервере подключены к разным коммутаторам для избыточности. Инициатор, например VMware ESXi, также подключается к обоим коммутаторам и предоставляет тома в качестве дисков iSCSI 1 и 2 виртуальной машине по разным сетевым путям.

Если активный/оптимизированный путь по какой-либо причине станет недоступен (например, при отказе сервера с целевым объектом или сетевого коммутатора), для подключения к тому вместо него будет использоваться резервный путь через другое целевое устройство. После восстановления активного/оптимизированного пути он будет использоваться снова.

2.5 О хранилище объектов

Кибер Инфраструктура позволяет экспортировать дисковое пространство кластера для клиентов в форме S3-подобного хранилища на основе объектов.

Кибер Инфраструктура реализует API-интерфейс, подобный интерфейсу Amazon S3, который является одним из самых распространенных API-интерфейсов объектного хранилища. Конечные пользователи могут работать с продуктом Кибер Инфраструктура так же, как они работают с Amazon S3. Можно использовать привычные приложения для S3 и продолжать работу с ними после миграции данных из Amazon S3 в решение Кибер Инфраструктура.

Хранилище объектов представляет собой архитектуру хранения данных, которая позволяет управлять данными в виде объектов (как в хранилище данных типа «ключ-значение»), в противоположность файлам в файловых системах или блокам в блочном хранилище. Кроме данных, каждый объект содержит метаданные, которые его описывают, а также уникальный идентификатор, позволяющий найти объект в хранилище. Хранилище объектных данных оптимизировано для хранения миллиардов объектов, в частности для хранения приложений, хостинга статического веб-контента, сервисов хранения данных в Интернете, «больших данных» и резервных копий. Все эти сценарии реализуются хранилищем объектов благодаря сочетанию очень высокой масштабируемости с доступностью и согласованностью данных.

По сравнению с другими типами хранилищ ключевое отличие хранилища объектных данных в том, что части объекта нельзя изменить, поэтому при изменении объекта вместо этого формируется его новая версия. Такой подход крайне важен для поддержания доступности и согласованности данных. Прежде всего, изменение объекта как единого целого устраняет проблему конфликтов. То есть объект с самой недавней меткой времени считается текущей версией и является таковой. В результате объекты всегда согласованы, то есть их состояние является релевантным и соответствующим.

Особенностью георепликированного хранилища объектов является согласованность в конечном счете. Согласованность в конечном счете не гарантирует, что операции чтения будут возвращать новое состояние во всех центрах обработки данных (ЦОД) после выполнения записи на одном из них. Читатели могут наблюдать старое состояние на одном из ЦОД в течение неопределенного периода времени, пока запись не будет распространена на все ЦОДы. Это очень важно для обеспечения доступности хранилища, так как географически удаленные ЦОДы могут не иметь возможности выполнять обновление данных синхронно (например, из-за сетевых проблем), а само обновление также может быть медленным из-за того, что ожидание подтверждений от всех реплик данных на больших расстояниях может занимать сотни миллисекунд. Поэтому согласованность в конечном счете помогает скрывать задержки связи при операциях записи ценой вероятного старого состояния, наблюдаемого читателями. Однако во многих случаях это вполне допустимо.

2.5.1 Архитектура хранилища объектов

Инфраструктура хранилища объектных данных состоит из следующих сущностей: объектных серверов (OS), серверов имен (NS), шлюзов S3 (GW) и внутреннего хранилища блочного уровня.

Эти сущности выполняются в виде служб на узлах Кибер Инфраструктура. Каждая служба должна быть развернута на нескольких узлах Кибер Инфраструктура для обеспечения высокой доступности.

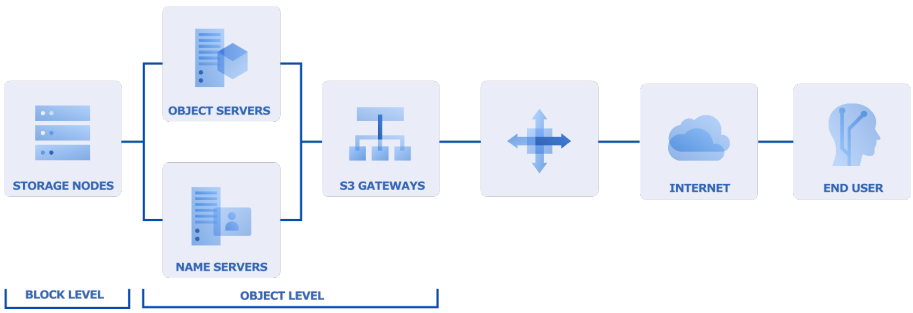
Службы OS и NS – это службы с высокой доступностью: система автоматически поддерживает эти службы в активном состоянии, пока в кластере S3 работает хотя бы одна машина. При отказе службы NS или OS весь кластер S3 не сможет правильно работать.

По умолчанию на каждый узел в кластере S3 может приходиться до 10 экземпляров службы NS и 10 экземпляров службы OS, но на весь кластер S3 может приходиться не более 24 экземпляров службы OS и 16 экземпляров службы NS.

Примеры:

- Кластер S3 из одного узла содержит 10 экземпляров сервиса OS и 10 экземпляров сервиса NS.
- Кластер S3 из двух узлов содержит 20 экземпляров сервиса OS и 16 экземпляров сервиса NS.
- Кластер S3 из трех узлов содержит 24 экземпляров сервиса OS и 16 экземпляров сервиса NS.

Количество экземпляров служб определяется при развертывании кластера S3. Последующее добавление узлов не меняет развернутый кластер S3.



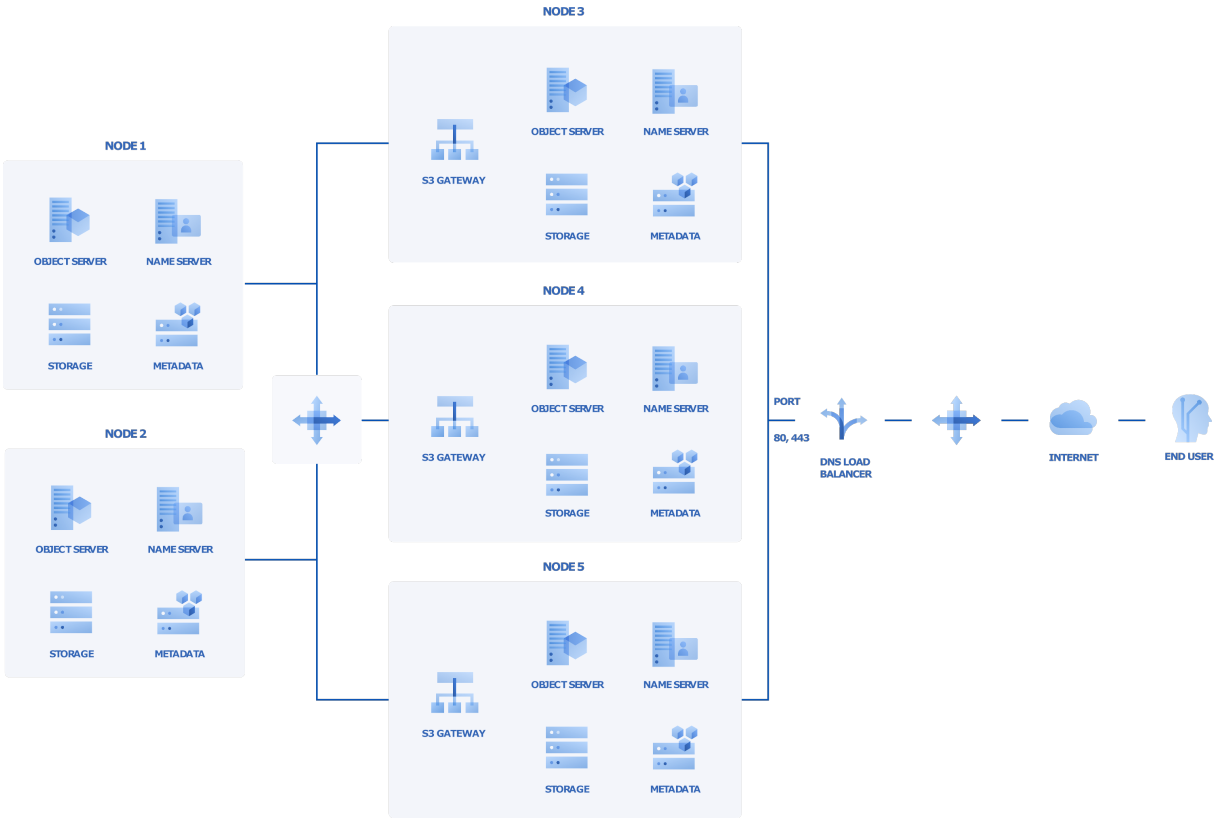
- Объектный сервер хранит актуальные данные объектов, полученные от шлюза S3. Эти данные упаковываются в специальные контейнеры для достижения высокой производительности. Контейнеры являются избыточными, причем режим избыточности можно указать при настройке хранилища объектов. Объектный сервер также хранит собственные данные в блочном хранилище со встроенной высокой доступностью.
- Сервер имен хранит метаданные объектов, полученные от шлюза S3. Метаданные включают в себя имя объекта, его размер, ACL (список управления доступом), расположение, владельца и т. п. Сервер имен (NS) также хранит собственные данные в блочном хранилище со встроенной высокой доступностью.
- Шлюз S3 представляет собой прокси данных между службами хранилища объектов и конечными пользователями. Он получает и обрабатывает запросы протокола Amazon S3,

а также выполняет аутентификацию пользователей S3 и проверку ACL. Шлюз S3 использует веб-сервер NGINX для внешних подключений и не имеет собственных данных (то есть работает без состояний).

- Внутреннее хранилище блочного уровня представляет собой блочное хранилище с высокой доступностью служб и данных. Поскольку службы хранилища объектных данных выполняются на хостах, для хранилища объектных данных не требуются виртуальные среды (а следовательно, и лицензии).

2.5.2 Пример хранилища объектов

В этом разделе показан пример хранилища объектов, развернутого поверх кластера хранилища из пяти узлов, на которых выполняются различные службы. Окончательная конфигурация показана на рисунке ниже.



2.6 О файловом хранилище

Файловое хранилище – это архитектура хранения данных, которая использует протокол NFS (Network File System) для управления данными в виде файлов. Кибер Инфраструктура позволяет организовать серверы в кластер NFS высокой доступности, в котором можно создавать тома NFS. Том NFS – это точка доступа для тома, которой можно назначить IP-адрес или доменное имя. Для тома в свою очередь можно назначить схему избыточности, уровень хранения и область отказа. В каждом томе NFS можно создать несколько экспортов NFS, представляющих собой фактические экспортированные каталоги для пользовательских данных. Каждый экспорт, помимо прочих

свойств, получает путь, который в сочетании с IP-адресом тома уникальным образом идентифицирует экспорт в сети и позволяет подключить его с помощью стандартных инструментов.

С технической стороны тома NFS основаны на хранилище объектов. Помимо обеспечения высокой доступности и масштабируемости, хранилище объектов устраняет ограничение на количество файлов и размер данных, которые можно хранить в кластере NFS. Каждый том отлично подходит для хранения миллиардов файлов любого размера. Однако такая масштабируемость предполагает дополнительный расход ресурсов ввода-вывода при изменении размера файлов и перезаписи. По этой причине кластер NFS представляет собой идеальное «холодное» и «теплое» хранилище файлов, но не рекомендуется в качестве «горячего» и высокопроизводительного хранилища, а также для часто перезаписываемых данных (например, для работы виртуальных машин). В частности, интеграцию продукта Кибер Инфраструктура с решениями VMware лучше всего выполнять через iSCSI для достижения лучшей производительности.

Примечание
Кибер Инфраструктура поддерживает только NFS версии 4 и выше. Начиная с версии Кибер Инфраструктура 4.0, pNFS больше не поддерживается.

2.7 О вычислительном кластере

Вычислительный кластер обеспечивает управление виртуализацией для виртуальных машин и программно определяемых сетей. В продукте Кибер Инфраструктура используются виртуальные машины на базе технологии с открытым исходным кодом, которые могут работать с гостевыми операционными системами Windows и Linux. Эти виртуальные машины также обеспечивают высокую доступность, и возможен их перенос в активном состоянии без остановки. Кроме того, моментальные снимки томов ВМ создаются с учетом согласованности приложений.

Кибер Инфраструктура обеспечивает наиболее эффективное использование вычислительных ресурсов с помощью сервисов «Kubernetes как услуга», «Балансировщик нагрузки как услуга» и учета для вычислительных ресурсов. Для выделения пространства для виртуальных машин и выбора различных режимов избыточности к томам ВМ применяются политики хранения. Эти политики также могут ограничивать пропускную способность и количество операций ввода-вывода в секунду (IOPS), чтобы обеспечить прогнозируемый уровень производительности для дисков ВМ. Также в целях распределения нагрузки между узлами можно настроить размещение виртуальных машин в зависимости от характеристик узла.

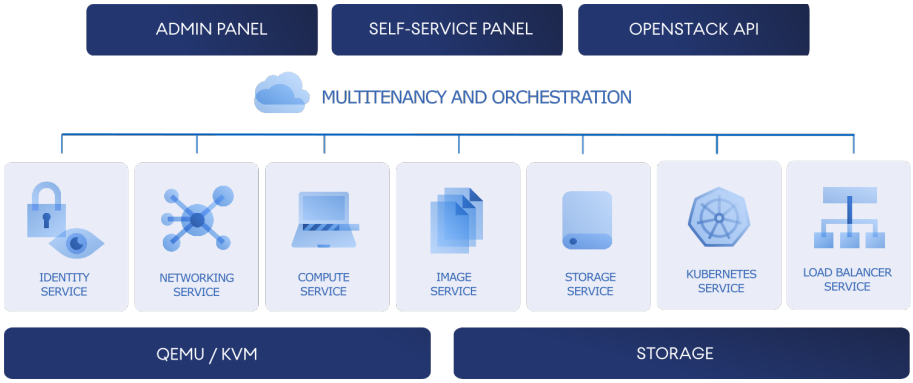
В продукте Кибер Инфраструктура администраторы могут создавать множество доменов, тенантов и пользователей и распределять ресурсы в соответствии с квотами тенантов. Кроме того, можно создавать собственные публичные или частные облачные хранилища и предлагать их под собственной маркой. При этом независимые конечные пользователи вычислительных ресурсов будут изолированы и защищены на собственных порталах самообслуживания.

Кибер Инфраструктура защищает и изолирует виртуальные сети для виртуальных машин с помощью инкапсуляции VXLAN. Распределенная виртуальная коммутация и маршрутизация упрощают конфигурацию сетей на ВМ, а встроенный брандмауэр повышает их защищенность.

Интегрированный DHCP-сервер, а также управление IP-адресами и DNS обеспечивают эффективную конфигурацию сети.

2.7.1 Архитектура вычислительного кластера

На следующей схеме показаны основные вычислительные компоненты продукта Кибер Инфраструктура.



- Служба идентификации предоставляет функции проверки подлинности и авторизации для продукта Кибер Инфраструктура.
- Служба вычислений дает пользователям возможность создавать, запускать виртуальные машины и управлять ими. Эта служба работает на основе модифицированного гипервизора QEMU/KVM.
- Сетевая служба реализует функции физических и виртуальных сетей для виртуальных машин.
- Служба образов дает пользователям возможность отправлять, хранить и использовать образы поддерживаемых гостевых операционных систем и виртуальных дисков. Эта служба зависит от базового кластера хранилища в плане обеспечения избыточности данных.
- Служба хранилища предоставляет виртуальные диски виртуальным машинам. Эта служба зависит от базового кластера хранилища в плане обеспечения избыточности данных.
- Служба Kubernetes дает пользователям возможность развертывать кластеры Kubernetes в виртуальных машинах.
- Служба балансировщика нагрузки распределяет входящий сетевой трафик между виртуальными машинами в пуле балансировки.

2.7.2 Архитектура вычислительных сетей

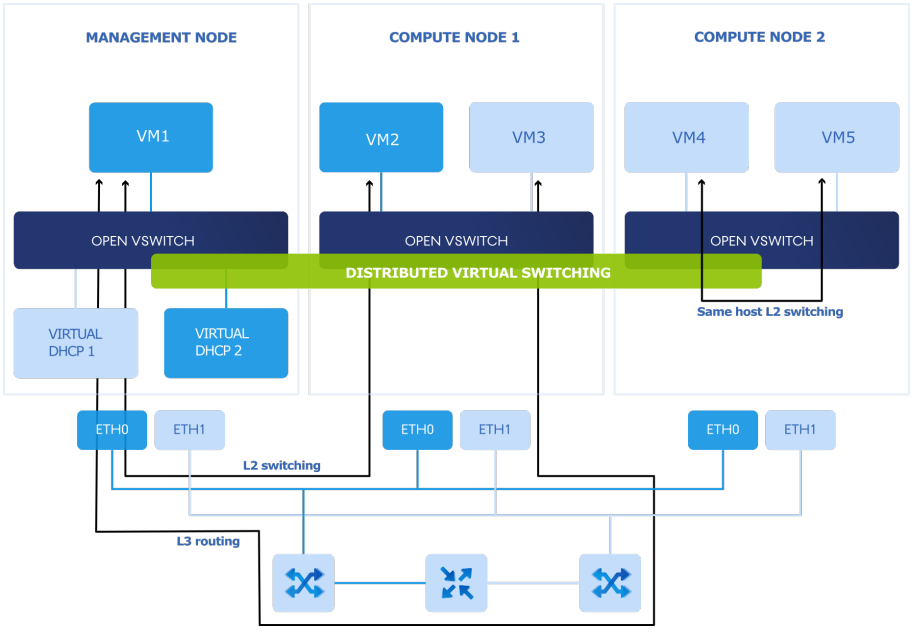
Кибер Инфраструктура поддерживает распределенную виртуальную коммутацию на базе Open vSwitch. Коммутатор Open vSwitch запускается на каждом вычислительном узле и перенаправляет сетевой трафик между виртуальными машинами на этом узле, а также между виртуальными машинами и сетями инфраструктуры. Распределенная виртуальная коммутация обеспечивает централизованный мониторинг и управление конфигурацией виртуальной сети на всех узлах вычислительного кластера.

Распределенная виртуальная маршрутизация, используемая для виртуальных сетевых подключений, позволяет размещать виртуальные маршрутизаторы на вычислительных узлах и перенаправлять трафик ВМ непосредственно с узлов размещения. В сценарии с использованием DNAT плавающий IP-адрес напрямую назначается сетевому интерфейсу ВМ. Если используется SNAT, трафик перенаправляется через узлы управления.

2.7.2.1 Подключение физических сетей

Физические сети подключаются к инфраструктурным сетям на уровне 2.

Физическое представление подключения физических сетей можно изобразить следующим образом.



На рисунке выше:

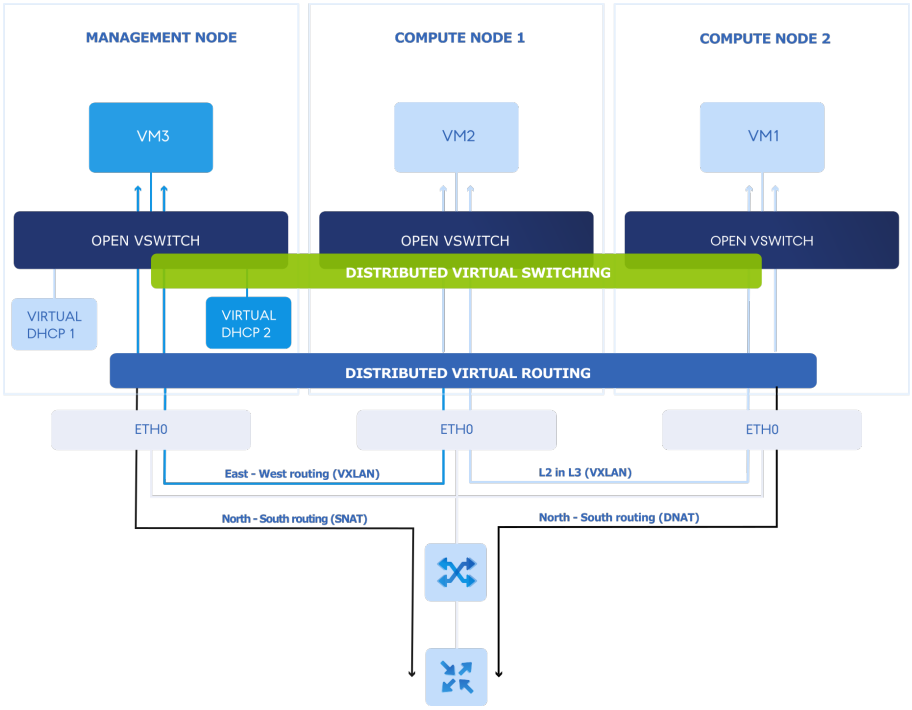
- Пять виртуальных машин распределены по вычислительному кластеру и подключены к двум нетегированным физическим сетям через два физических коммутатора **VM1** и **VM2**, которые принадлежат одной физической сети, а **VM3**, **VM4** и **VM5** – другой.
- Для каждой вычислительной сети на узле управления работает DHCP-сервер.
- Вычислительные узлы подключены к одному физическому коммутатору через сетевые интерфейсы **eth0**, а к другому физическому коммутатору – через **eth1**, причем они располагаются в двух отдельных сегментах L2.
- Сетевые интерфейсы **eth0** и **eth1** подключены к инфраструктурным сетям с типом трафика **ВМ внешн.**
- Физический маршрутизатор соединяет между собой две физические сети, созданные поверх инфраструктурных, и обеспечивает доступ к внешним сетям, например к Интернету.

Логически схему физической сети можно представить следующим образом.

2.7.2.2 Подключение виртуальных сетей

Технология VXLAN, используемая для виртуальных сетей, позволяет создавать логические сети L2 в сетях L3 путем инкапсуляции (туннелирования) кадров Ethernet поверх пакетов UDP.

Физическое представление подключения виртуальных сетей можно изобразить следующим образом.

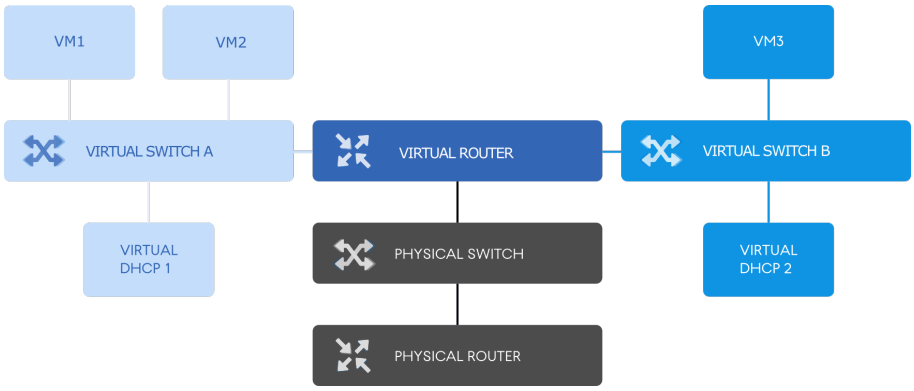


На рисунке выше:

- Три виртуальные машины распределены по вычислительному кластеру и подключены к двум виртуальным сетям через два виртуальных коммутатора: **VM1** и **VM2** принадлежат одной виртуальной сети, **VM3** – другой.
- Для каждой вычислительной сети на узле управления работает DHCP-сервер.
- Распределенный виртуальный маршрутизатор соединяет виртуальные сети и нетегированную физическую сеть, созданную поверх сети инфраструктуры.
- Вычислительные узлы подключены к физическому коммутатору через сетевые интерфейсы **eth0** и располагаются в одном сегменте L2.

- Сетевые интерфейсы **eth0** подключены к инфраструктурной сети с типами трафика **ВМ внутр.** и **ВМ внешн.**
- Физический маршрутизатор обеспечивает доступ к внешним сетям, например к Интернету.

Логически схему виртуальной сети можно представить следующим образом.



3 Понятия и функции

В этом разделе описываются ключевые понятия и функции Кибер Инфраструктура. Эта информация поможет вам понять принцип работы данного продукта.

3.1 Высокая доступность

Высокая доступность поддерживает работу служб Кибер Инфраструктура даже в случае отказа узла, на котором они расположены. В таких случаях службы с отказавшего узла перемещаются на исправные узлы в соответствии с алгоритмом консенсуса Raft. Высокая доступность обеспечивается следующими методами:

- Избыточность метаданных. Для функционирования кластера хранилища достаточно работы не всех, а лишь большинства серверов метаданных. Если настроить несколько серверов метаданных в кластере, то в случае сбоя одного сервера остальные серверы метаданных продолжат управлять кластером.

  Нужное количество серверов метаданных развертывается автоматически в зависимости от рекомендуемой конфигурации оборудования.
- Избыточность данных. Копии каждого фрагмента данных размещаются на разных узлах хранилища, что обеспечивает доступность данных, даже если некоторые узлы хранилища окажутся недоступны. Дополнительные сведения см. в "Избыточность данных" на странице 29.
- Мониторинг работоспособности узла.

Примечание
Для проверки высокой доступности вместо обычной команды reboot необходимо использовать следующие команды:

```
# echo 1 > /proc/sys/kernel/sysrq
# echo b > /proc/sysrq-trigger
```

Выполнение указанных команд приводит к принудительной перезагрузке узлов кластера.

3.1.1 Высокая доступность для служб

Кибер Инфраструктура дополнительно обеспечивает высокую доступность следующих сервисов:

- Панель администрирования. Если сервер управления выйдет из строя или станет недоступен по сети, экземпляр панели администрирования на другом сервере возьмет на себя сервис панели, чтобы он оставался доступным по тому же выделенному IP-адресу. Перемещение сервиса может занять несколько минут. Высокая доступность панели администрирования включается вручную вместе с высокой доступностью сервера управления.

- Виртуальные машины. Если вычислительный сервер выйдет из строя или станет недоступен по сети, размещенные на нем виртуальные машины будут эвакуированы на другие исправные вычислительные серверы в зависимости от их свободных ресурсов. По умолчанию высокая доступность для виртуальных машин включается автоматически после создания вычислительного кластера, и ее можно при необходимости отключить вручную.

  Примечание
  По умолчанию вычислительный кластер может продолжать работу при отказе только одного сервера. Для подготовки вычислительного кластера к одномоментному отказу нескольких серверов используйте процедуру, описанную в статье Подготовка сервисов кластера Кибер Инфраструктуры к одномоментному отказу двух и более узлов.

- Сервис iSCSI. Если произойдет сбой по активному пути к томам, экспортированным через iSCSI (например, сервер хранения с активными целевыми устройствами iSCSI выйдет из строя или станет недоступен по сети), активный путь будет перенаправлен через целевые устройства, расположенные на исправных серверах. Тома, экспортированные через iSCSI, остаются доступны, пока к ним существует хотя бы один путь.
- Сервис S3. Если сервер S3 выйдет из строя или станет недоступен по сети, будет выполнена автоматическая балансировка и миграция расположенных на нем компонентов сервера имен и сервера объектов между другими серверами S3. Миграция шлюзов S3 не выполняется автоматически, поскольку их высокая доступность основана на записях DNS. Необходимо поддерживать актуальность записей DNS вручную при добавлении или удалении шлюзов S3. Высокая доступность для сервиса S3 включается автоматически после включения высокой доступности сервера управления и создания кластера S3 из трех или большего количества серверов. Кластер S3 из трех серверов может потерять один сервер и продолжать работать.
- Сервис Backup Gateway. Если сервер, входящий в кластер Backup Gateway, выйдет из строя или станет недоступен по сети, другие серверы в кластере Backup Gateway продолжат предоставлять доступ к выбранному внутреннему хранилищу. Миграция шлюзов Backup Gateway не выполняется автоматически, поскольку их высокая доступность основана на записях DNS. Необходимо поддерживать актуальность записей DNS вручную при добавлении или удалении шлюзов Backup Gateway. Высокая доступность для Backup Gateway включается автоматически после создания кластера Backup Gateway из двух или большего количества серверов. Доступ к внутреннему хранилищу сохраняется, пока исправен хотя бы один сервер в кластере Backup Gateway.
- Тома NFS. Если сервер хранилища выйдет из строя или станет недоступен по сети, выполняется миграция размещенных на нем томов NFS между другими серверами NFS. Высокая доступность для томов NFS на сервере хранилища включается автоматически после создания кластера NFS.

Примечание
Для проверки высокой доступности вместо обычной команды reboot необходимо использовать следующие команды:

```
# echo 1 > /proc/sys/kernel/sysrq
# echo b > /proc/sysrq-trigger
```

Выполнение указанных команд приводит к принудительной перезагрузке узлов кластера.

3.1.2 Высокая доступность и вычислительный кластер

Высокая доступность узла управления и вычислительный кластер тесно связаны, поэтому изменение узлов в одной составляющей обычно влияет на другую. Обратите внимание на следующее.

- Каждый узел в конфигурации высокой доступности должен соответствовать требованиям к узлу управления, перечисленным в разделе "Требования к серверу" на странице 46. Если предстоит создать вычислительный кластер, необходимо также добавить его аппаратные требования.
- Если конфигурация высокой доступности была создана до вычислительного кластера, все узлы в ней будут добавлены в вычислительный кластер.
- Если вычислительный кластер был создан до конфигурации высокой доступности, в эту конфигурацию можно добавить только узлы вычислительного кластера. Поэтому, чтобы добавить узел в конфигурацию высокой доступности, сначала добавьте его в вычислительный кластер.
- Если как конфигурация высокой доступности, так и вычислительный кластер содержат одни и те же три узла, то одиночные узлы нельзя будет удалить из вычислительного кластера. В таком случае вычислительный кластер можно полностью уничтожить, но конфигурация высокой доступности сохранится. Верно и обратное: конфигурацию высокой доступности можно удалить, а вычислительный кластер продолжит работать.

3.2 Избыточность данных

Кибер Инфраструктура защищает каждый фрагмент данных путем обеспечения его избыточности. Это означает, что копии каждого фрагмента данных размещаются на разных узлах хранения, чтобы гарантировать доступность этих данных, даже если часть узлов окажется недоступна.

Кибер Инфраструктура автоматически поддерживает требуемое количество копий внутри кластера и обеспечивает актуальность этих копий. Если узел хранилища окажется недоступен, копии данных с него заменяются новыми копиями, распределенными по исправным узлам. Если через некоторое время узел хранилища снова становится доступен, устаревшие копии данных на нем обновляются.

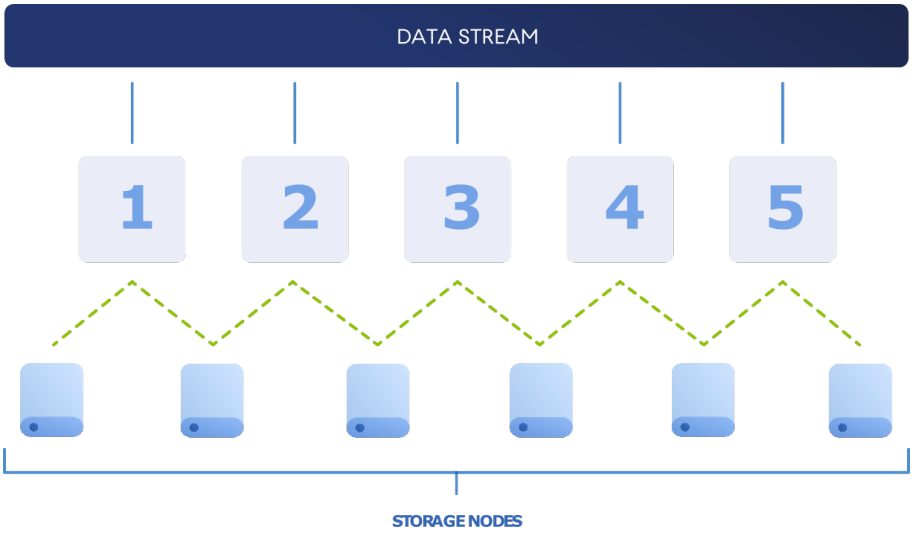
Избыточность достигается одним из двух методов: репликацией или избыточным кодированием. От выбранного метода зависит размер фрагмента данных и количество копий фрагмента, которое будет храниться в кластере. В целом репликация обеспечивает лучшую производительность,

в то время как избыточное кодирование оставляет больше доступного пространства для хранения данных (см. таблицу).

3.2.1 Избыточность посредством репликации

При использовании репликации Кибер Инфраструктура разбивает входящий поток данных на фрагменты размером 256 МБ. Каждый фрагмент реплицируется, и реплики размещаются на разных узлах хранилища так, чтобы на каждом узле хранилась только одна реплика определенного фрагмента.

На следующей схеме показан режим избыточности с двумя репликами.



Репликация в продукте Кибер Инфраструктура похожа на процесс перестроения RAID-массива, но с двумя ключевыми отличиями.

- Репликация в продукте Кибер Инфраструктура выполняется намного быстрее, чем обычная перестройка RAID 1/5/10 в режиме онлайн. Причиной является то, что Кибер Инфраструктура реплицирует фрагменты параллельно на несколько узлов хранения.
- Чем больше узлов хранения в кластере, тем быстрее кластер восстановится после отказа диска или узла.

Высокая производительность репликации сводит к минимуму периоды пониженной избыточности в кластере. Производительность репликации зависит от следующих условий.

- Количество доступных узлов хранилища. Репликация выполняется параллельно, поэтому чем больше доступно источников и мест назначения репликации, тем больше ее скорость.
- Производительность дисков на узлах хранения.
- Производительность сети. Все реплики перемещаются между узлами хранилища по сети. Например, пропускная способность 1 Гбит/с может стать узким местом системы (см. раздел «Требования к сети и рекомендации для каждого узла»).

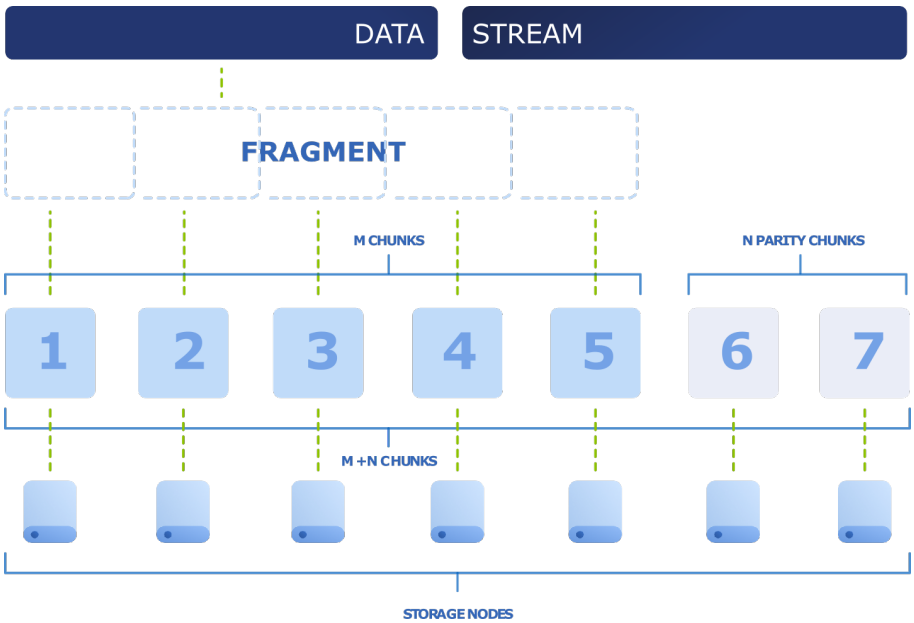
- Распределение данных в кластере. На некоторых узлах хранения может быть больше данных для репликации, чем на других, что может привести к их перегрузке при репликации.
- Активность ввода-вывода в кластере во время репликации.

3.2.2 Избыточность посредством избыточного кодирования

При использовании избыточного кодирования (технология Erasure Coding) Кибер Инфраструктура разбивает входящий поток данных на фрагменты определенного размера, затем разбивает каждый фрагмент на определенное количество (M) блоков размером 1 мегабайт и создает определенное количество (N) блоков четности для обеспечения избыточности. Все блоки распределяются по узлам хранилища M+N, то есть по одному блоку на узел. На узлах хранилища блоки хранятся в обычных фрагментах по 256 МБ, но такие фрагменты не реплицируются, поскольку избыточность уже достигнута. Кластер может выдержать отказ любых N узлов хранилища без потери данных.

Значения M и N указаны в названиях режимов помехоустойчивого кодирования. Например, в режиме 5+2 входящие данные разбиваются на фрагменты размером 5 МБ, каждый фрагмент разбивается на пять блоков размером 1 МБ и добавляются два паритетных блока размером 1 МБ для избыточности. Кроме того, если N равно 2, то данные кодируются с использованием схемы RAID6, а если N больше 2, то применяются помехоустойчивые коды.

На схеме ниже показан режим 5+2.



3.2.3 Без избыточности

Предупреждение
Риск потери данных!

Без обеспечения избыточности одиночные фрагменты данных размещаются на узлах хранения по одному фрагменту на узел. При отказе узла или диска данные могут быть утеряны. Такой режим настоятельно не рекомендуется применять, независимо от сценария использования, за исключением случаев, когда вы хотите опробовать продукт Кибер Инфраструктура на одном сервере.

3.2.4 Режимы избыточности

Кибер Инфраструктура поддерживает несколько режимов для каждого из методов обеспечения избыточности. В панели администрирования доступны лишь предопределенные режимы избыточности. В следующей таблице показаны накладные расходы ресурсов данных для различных режимов избыточности. Первые четыре строки представляют репликацию, а остальные – избыточное кодирование.

Количество узлов, указанное в таблице, обозначает лишь требуемое число для каждого из методов обеспечения избыточности, а не количество узлов, необходимое для кластера Кибер Инфраструктура. Минимальные и рекомендуемые конфигурации кластеров описаны в разделе "Количество серверов" на странице 49.

Максимально возможный режим избыточности с помощью кодирования – 61+3.

Режим избыточности	Число узлов, требуемое для хранения копий данных	Сколько узлов могут отказать без потери данных	Доп. затраты ресурсов хранилища, %	Физическое пространство, необходимое для хранения 100 ГБ данных
1 реплика (без избыточности)	1	0	0	100 ГБ
2 реплики	2	1	100	200 ГБ
3 реплики	3	2	200	300 ГБ
4 реплики	4	3	300	400 ГБ
Кодирование 1+0 (без избыточности)	1	0	0	100 ГБ
Кодирование 1+1	2	1	100	200 ГБ
Кодирование 1+2	3	2	200	300 ГБ
Кодирование 3+1	4	1	33	133 ГБ
Кодирование 3+2	5	2	67	167 ГБ

Режим избыточности	Число узлов, требуемое для хранения копий данных	Сколько узлов могут отказать без потери данных	Доп. затраты ресурсов хранилища, %	Физическое пространство, необходимое для хранения 100 ГБ данных
Кодирование 5+2	7	2	40	140 ГБ
Кодирование 7+2	9	2	29	129 ГБ
Кодирование 9+2	11	2	22	122 ГБ
Кодирование 11+3	14	3	28	128 ГБ
Кодирование 13+3	16	3	23	123 ГБ
Кодирование 15+3	18	3	20	120 ГБ
Кодирование 17+3	20	3	18	118 ГБ

Примечание

Режимы кодирования 1+0, 1+1, 1+2 и 3+1 предназначены для небольших кластеров, в которых недостаточно узлов для других режимов кодирования, но которые будут расширяться в будущем. Поскольку выбранный тип обеспечения избыточности нельзя изменить (с репликации на избыточное кодирование или наоборот), этот режим позволяет выбрать избыточное кодирование, даже если кластер меньше рекомендуемого. После расширения кластера можно будет выбрать более благоприятные режимы избыточности.

Режим избыточности данных можно выбрать при настройке служб хранилища и создании томов хранения данных для виртуальных машин. Независимо от того, какой режим вы выберете, настоятельно рекомендуется обеспечить достаточную защиту на случай одновременного отказа двух узлов, поскольку это часто происходит в реальных условиях.

Для настройки режима избыточности данных, который недоступен в панели администрирования, используйте интерфейс командной строки, как описано в разделе "Настройка пользовательских режимов избыточности данных" на странице 224.

По умолчанию все режимы кодирования, кроме 1+0, разрешают операции записи, когда недоступен один сервер или диск хранилища. Если избыточность равна 1, то есть при использовании режима кодирования M+1, то при недоступности двух серверов хранилища данные могут стать недоступны даже для чтения и существует большой риск потери данных. Поэтому настоятельно рекомендуется использовать режимы кодирования M+2 или M+3.

Кибер Инфраструктура также поддерживает нестандартные режимы избыточности, которые предназначены для кластеров с уменьшенными областями отказа. О том, как можно использовать эти режимы, см. в статье базы знаний Применение схем избыточного кодирования с уменьшенной областью отказа для построения эффективных кластеров из нескольких ЦОД. В следующей таблице показаны накладные расходы ресурсов данных для различных нестандартных режимов избыточности.

Режим избыточности	Число узлов, требуемое для хранения копий данных	Сколько узлов могут отказать без потери данных	Доп. затраты ресурсов хранилища, %	Физическое пространство, необходимое для хранения 100 ГБ данных
Кластер на 3 ЦОД с уменьшенной областью отказа				
Кодирование 3+3 (по две стойки в ЦОД)	6	3	100	200 ГБ
Кодирование 5+4 (по три стойки в ЦОД)	9	4	80	180 ГБ
Кодирование 7+5 (по четыре стойки в ЦОД)	12	5	72	172 ГБ
Кодирование 9+6 (по пять стоек в ЦОД)	15	6	67	167 ГБ
Кодирование 11+7 (по шесть стоек в ЦОД)	18	7	64	164 ГБ
Кластер на 2 ЦОД с уменьшенной областью отказа				
1+3 (по две стойки в ЦОД)	4	3	300	400 ГБ
2+4 (по три стойки в ЦОД)	6	4	200	300 ГБ
3+5 (по четыре стойки в ЦОД)	8	5	167	267 ГБ
4+6 (по пять стоек в ЦОД)	10	6	150	250 ГБ
5+7 (по шесть стоек в ЦОД)	12	7	140	240 ГБ

3.3 Области отказа

Под областью отказа подразумевается область (например, серверная стойка), которая может отказать, в то время как ее данные останутся доступны. Если выбрать стойку в качестве области отказа, то данные в кластере выдержат отказ одной стойки, так как другие стойки обеспечат доступность данных. Если выбрать хост в качестве области отказа, то потеря целого сервера не приведет к потере доступности данных.

Чтобы обеспечить высокую доступность, Кибер Инфраструктура равномерно распределяет реплики данных по областям отказа в соответствии с политикой размещения реплик. Доступны следующие политики:

- Диск, наименьшая возможная область отказа. При использовании этой политики Кибер Инфраструктура никогда не размещает больше одной реплики данных на одном диске. Несмотря на защиту от отказов дисков, этот вариант может привести к потере данных, если реплики будут расположены на разных дисках одного хоста, который откажет. Эту политику следует применять в кластерах с одним узлом.
- Хост как область отказа. При использовании этой политики Кибер Инфраструктура никогда не размещает больше одной реплики данных на одном хосте. Поэтому, если один из узлов хранилища откажет (сбой операционной системы) и все его диски станут недоступны, данные по-прежнему будут доступны с исправных узлов.
- Стойка как область отказа. При использовании этой политики Кибер Инфраструктура никогда не размещает больше одной реплики данных на одну стойку. Поэтому, если одна из стоек откажет (сбой коммутатора, обслуживающего стойку) и все узлы в ней станут недоступны, данные по-прежнему будут доступны из других стоек.
- Ряд стоек как область отказа. При использовании этой политики Кибер Инфраструктура никогда не размещает больше одной реплики данных в одном ряду. Поэтому, если один ряд откажет (сбой одного источника питания) и все стойки в нем станут недоступны, данные по-прежнему будут доступны из других рядов.
- Серверная комната как область отказа. При использовании этой политики Кибер Инфраструктура никогда не размещает больше одной реплики данных на одну комнату. Поэтому, если одна комната откажет (отключение электричества) и все ряды стоек в ней станут недоступны, данные по-прежнему будут доступны из других комнат.

При выборе области отказа учитывайте следующие рекомендации.

- Убедитесь, что службы метаданных распределены по областям. Например, если вы выбрали комнату как область отказа и равномерно распределили данные по нескольким комнатам, необходимо также распределить службы метаданных. Если разместить все службы метаданных в одной серверной комнате, то при ее отказе из-за отключения электричества кластер не сможет нормально работать.
- Для выбора какой-либо области отказа необходимо иметь несколько областей этого типа, чтобы службы или данные могли перемещаться между ними, например из одной стойки в другую. Например, если вы хотите выбрать стойку как область отказа с уровнем избыточности

2 реплики или **кодирование 1+1**, убедитесь, что кластеру назначено как минимум две стойки с исправными узлами.

- Дисковое пространство должно быть равномерно распределено между областями отказа. Например, если выбрать стойку в качестве области отказа, в каждой стойке должно быть равное количество доступного дискового пространства. Распределяемое дисковое пространство в каждой стойке соответствует размеру дискового пространства наименьшей стойки. Это необходимо, поскольку в каждой стойке должна храниться одна реплика фрагмента данных. Поэтому, когда дисковое пространство наименьшей стойки закончится, в кластере больше не смогут создаваться фрагменты данных, пока не будет добавлена новая стойка или не будет уменьшен коэффициент репликации. Огромные области отказа более чувствительны к дисбалансу общего дискового пространства. Например, если в области 5 стоек с общим дисковым пространством 10, 20, 30, 100 и 100 ТБ, невозможно будет распределить (10+20+30+100+100)/3 = 86 ТБ данных в трех репликах. Вместо этого только 60 ТБ будет доступно для распределения, поскольку место в стойках низкой емкости закончится раньше. При этом в самых больших стойках (по 100 ТБ) будет оставаться свободное пространство, недоступное для распределения.

3.4 Уровни хранения данных

В терминологии продукта Кибер Инфраструктура уровнями называются группы дисков, которые позволяют организовать рабочие нагрузки хранилища по определенными критериям. Например, можно использовать уровни для разделения нагрузок клиентов. Либо можно создать уровень из быстрых твердотельных накопителей для служебных процессов или виртуальных сред и уровень из жестких дисков большой емкости для хранения резервных копий.

3.4.1 Ручной запуск миграции данных между уровнями (по умолчанию)

При необходимости запустить миграцию данных между уровнями можно вручную. Убедитесь, что на целевом уровне достаточно свободного места и выберите его в настройках текущей политики хранения.

3.4.2 Автоматическая миграция данных между уровнями

В режиме автоматической миграции при заполнении текущего уровня данные автоматически переносятся на более низкий. Автоматическая миграция по умолчанию отключена. Включить ее можно командой vstorage -c <cluster_name> set-config mds.alloc.strict_tier=0.

При назначении дисков уровням (это можно сделать в любое время) учитывайте, что более быстрые накопители следует назначать на высшие уровни хранения. Например, уровень 0 можно использовать для резервных копий и других холодных данных (CS без кэша на твердотельных накопителях), уровень 1 – для виртуальных сред, то есть большого объема холодных данных, но с быстрыми операциями произвольной записи (CS с кэшем на твердотельных накопителях), уровень 2 – для горячих данных (CS на твердотельных накопителях), кэшей, конкретных дисков и т. п.

Эта рекомендация связана с тем, как Кибер Инфраструктура работает с пространством хранилища в режиме автоматической миграции. Если на каком-либо уровне хранения заканчивается свободное место, Кибер Инфраструктура попытается временно использовать пространство более низких уровней вплоть до низшего. Если заполнен и низший уровень, Кибер Инфраструктура попытается задействовать более высокий уровень. Если позже добавить пространства на исходный уровень, то данные, временно хранящиеся в другом месте, будут снова перемещены на него. Например, при попытке записать данные на уровень 2, который заполнен, Кибер Инфраструктура попытается записать эти данные на уровень 1, а затем на уровень 0. Если позже добавить пространства на уровень 2, вышеупомянутые данные, теперь хранящиеся на уровне 1 или 0, будут перемещены обратно на уровень 2, где они должны были храниться изначально.

3.5 Политики хранения

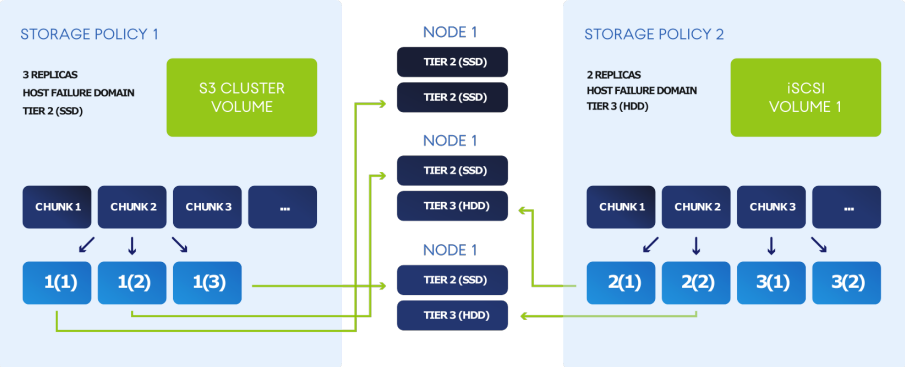
Широко используемая в Кибер Инфраструктура единица данных – это том. При создании тома для него необходимо определить режим обеспечения избыточности, уровень и область отказов. Эти параметры составляют политику хранения, которая определяет, насколько избыточным должен быть том и где он должен располагаться.

Чтобы лучше понять политику хранения, рассмотрим ее основные компоненты (уровни, области отказа и избыточность) на примере сценария. Например, у вас есть три узла с некоторым количеством дисков для хранения данных: быстрыми твердотельными накопителями и жесткими дисками большой емкости. На узле 1 есть только твердотельные накопители, на узлах 2 и 3 есть как твердотельные накопители, так и жесткие диски. Вы хотите экспортировать дисковое пространство через iSCSI и S3, поэтому вам необходимо определить подходящую политику хранения для каждой рабочей нагрузки.

- Первый параметр, уровень, определяет группу дисков, объединенных по какому-либо критерию (как правило, это тип накопителя) и ориентированных на конкретную рабочую нагрузку хранилища. В этом примере можно сгруппировать твердотельные накопители в уровень 2, а жесткие диски – в уровень 3. Диск можно назначить на уровень при создании кластера хранилища или добавлении в него узлов. Обратите внимание, что только узлы 2 и 3 имеют жесткие диски и будут использоваться для уровня 3. Твердотельные накопители первого узла не могут использоваться для уровня 3.
- Второй параметр, область отказа, определяет область, внутри которой несколько служб могут отказать взаимосвязанным образом. По умолчанию областью отказа является хост. Каждый фрагмент данных копируется на разные узлы хранилища, по одной копии на узел. При отказе одного узла данные останутся доступны с исправных узлов. Областью отказа также может быть диск, но это имеет смысл только в кластерах, состоящих из одного узла. Поскольку в этом сценарии у вас три узла, рекомендуем выбрать хост как область отказа.
- Третий параметр, избыточность, следует настроить в соответствии с доступными дисками и уровнями. В этом тестовом примере у вас есть три узла и на всех имеются твердотельные накопители на уровне 2. Таким образом, если выбрать уровень 2 в политике хранения, можно использовать три узла для 1, 2 или 3 реплик. Но только на двух узлах есть жесткие диски

на уровне 3. Таким образом, если выбрать уровень 3 в политике хранения, можно хранить только 1 или 2 реплики на двух узлах. В обоих случаях также можно применять кодирование, но для тестового сценария мы будем использовать только репликацию: 3 реплики для твердотельных накопителей и 2 реплики для жестких дисков.

В результате получатся следующие политики хранения:



3.6 Перестроение кластера

Кластер хранилища является самовосстанавливающимся. При отказе узла или диска кластер автоматически попытается восстановить потерянные данные, то есть перестроить себя.

3.6.0.1 Предварительные требования для перестроения

Для успешной перестройки кластер должен иметь как минимум:

- столько исправных узлов, сколько требуется для установленного режима избыточности;
  В кластере, который работает в режиме избыточного кодирования 5+2 и состоит из семи узлов (то есть минимального количества), каждый фрагмент пользовательских данных распределен по 5+2 узлам для избыточности, то есть задействованы все узлы. При отказе одного или двух узлов данные не будут потеряны, но производительность кластера снизится, а перестройка будет невозможна, пока не будут исправны как минимум семь узлов (то есть пока вы не добавите недостающие узлы). Для сравнения: в кластере, который работает в режиме избыточного кодирования 5+2 и состоит из десяти узлов, каждый фрагмент пользовательских данных распределен по произвольным 5+2 узлам из десяти для равномерной нагрузки на серверы хранения фрагментов (CS-серверы). Даже если откажут сразу три узла, в таком кластере останется достаточно узлов для перестройки.
- достаточно свободного пространства для размещения данных с любого узла.
  В кластере с десятью узлами по 10 ТБ следует оставить свободным как минимум 1 ТБ на каждом узле, чтобы при отказе одного узла 9 ТБ данных можно было восстановить на оставшихся девяти узлах. Однако если в кластере десять узлов по 10 ТБ и один узел на 20 ТБ, на каждом из меньших узлов должно быть свободно не менее 2 ТБ на случай сбоя большого узла (при этом на большом узле достаточно оставить свободным 1 ТБ).

3.6.0.2 Процесс перестроения

Процесс перестроения включает несколько этапов. Каждый сервер хранения фрагментов отправляет heartbeat-сообщение на один из MDS-серверов (серверов метаданных) каждые пять секунд. Если сообщение не отправлено, сервер хранения фрагментов считается неактивным и MDS-сервер направляет всем компонентам кластера указание прекратить операции с запросами к данным на этом сервере хранения фрагментов. Если heartbeat-сообщения не поступают от сервера хранения фрагментов в течение 15 минут, то MDS-сервер считает его недоступным и начинает перестройку кластера (при соблюдении указанных ниже условий). В процессе перестройки MDS-сервер находит серверы хранения фрагментов, на которых нет фрагментов (реплик) потерянных данных, и восстанавливает эти данные по одному фрагменту (реплике) за раз следующим образом.

- Если используется репликация, существующие реплики потерянного фрагмента блокируются (чтобы обеспечить идентичность всех реплик) и одна из них копируется на новый сервер хранения фрагментов. Если в это время клиенту нужно прочитать данные, которые еще не были восстановлены, он читает эти данные из любой оставшейся реплики.
- Если используется избыточное кодирование, новый сервер хранения фрагментов запрашивает практически все оставшиеся фрагменты данных для восстановления недостающих фрагментов. Если в это время клиенту нужно прочитать данные, которые еще не были восстановлены, эти данные восстанавливаются вне очереди и возвращаются клиенту.

Самовосстановление требует больше сетевого трафика и ресурсов ЦП, если используется репликация. С другой стороны, перестроение с избыточным кодированием выполняется медленнее.

Примечание
Если узел или диск становится недоступен во время обслуживания, самовосстановление кластера задерживается для экономии ресурсов. По умолчанию задержка составляет 30 минут. Это время можно настроить, задав значение параметра mds.wd.offline_tout_mnt в миллисекундах с помощью команды vstorage -c <cluster_name> set-config.

3.6.0.3 Рекомендации по перестроению кластера

Две рекомендации, которые помогут уменьшить дополнительный расход ресурсов при перестроении:

- Чтобы упростить перестройку, используйте одинаковое количество дисков одной емкости на всех узлах.
- Перестройка сопровождается дополнительной нагрузкой на сеть и увеличивает задержку операций чтения и записи. Чем больше пропускная способность сети в кластере, тем быстрее будет завершена перестройка и высвобождены ресурсы.

3.7 Автоматическая балансировка данных

Для обеспечения максимальной производительности ввода-вывода сервисов фрагментов данных в кластере хранилища данных выполняется автоматическая балансировка нагрузки на эти сервисы: каждые 60 секунд горячие фрагменты данных перемещаются с горячих сервисов фрагментов данных на более холодные.

Сервис фрагментов данных считается горячим, если средняя длина его очереди запросов превышает среднюю длину очереди запросов во всем кластере на 40 % или больше. Фрагмент данных считается горячим, если к нему часто обращаются.

Насколько сервис фрагментов данных является горячим, можно оценить с помощью команд vstorage top и vstorage stat. Например:

```
...
 IO QDEPTH: 0.1 aver, 1.0 max; 1 out of 1 hot CS balanced    46 sec ago
...
 CSID STATUS    SPACE  AVAIL  REPLICAS   UNIQUE IOWAIT IOLAT(ms) QDEPTH HOST
BUILD_VERSION
 1025 active    1007.3 156.8G    7142      0   10%    1/117    0.3 10.31.240.167 6.0.11-10
 1026 active    1007.3 156.8G    7267      0   11%    0/225    0.1 10.31.240.167 6.0.11-10
 1027 active    1007.3 156.8G    7151      0    2%     0/10    0.1 10.31.240.167 6.0.11-10
 1028 active    1007.3 156.8G    7285      0   13%    1/141    1.0 10.31.240.167 6.0.11-10
...
```

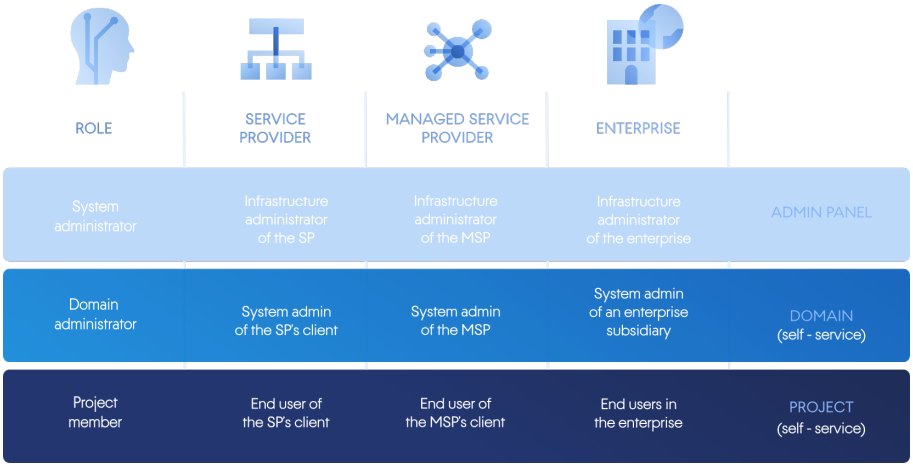
В выводе этих команд колонка QDEPTH содержит среднюю длину очереди запросов для каждого сервиса фрагментов данных за последние 5 секунд, а строка IO QDEPTH содержит среднюю длину очереди запросов и максимальную длину очереди запросов во всем кластере за последние 60 секунд.

3.8 Мультитенантность

В продукте Кибер Инфраструктура используется административная иерархия доменов и проектов (тенантов) с контролем доступа на основе ролей (RBAC) для управления виртуальными объектами вычислительного кластера, такими как виртуальные машины, тома и виртуальные сети. Домен представляет собой изолированный контейнер проектов и пользователей с назначенными ролями. Каждый проект и пользователь могут принадлежать только одному домену. Проект представляет собой изолированный контейнер виртуальных объектов с назначенными пользователями и заданными ограничениями для виртуальных ресурсов, таких как виртуальные ЦП, ОЗУ, хранилище и плавающие IP-адреса. Роль является глобальной и определяет все возможные задачи, которые может выполнять пользователь на уровне всей инфраструктуры, определенного домена или проекта.

В соответствии с этими уровнями в продукте Кибер Инфраструктура предусмотрены три роли пользователей: системный администратор, администратор домена и участник проекта.
На следующей схеме показаны стандартные пользователи с этими ролями, которые являются

сотрудниками поставщиков услуг и предприятий, а также их рабочие области — панели администрирования или самообслуживания.



- Системные администраторы могут выполнять задачи по администрированию системы в соответствии с назначенными им разрешениями, у них также есть доступ к панели администрирования. Это единственная роль, которая позволяет создавать проекты и определять для них квоты. Помимо этого, системный администратор с разрешениями для домена может управлять доменом Default (по умолчанию) с панели самообслуживания.

  Системными администраторами обычно являются администраторы инфраструктуры поставщика услуг или поставщика управляемых услуг либо главного ИТ-подразделения корпорации (в зависимости от ситуации на вашем конкретном предприятии).
- Администраторы домена отвечают за собственный домен, работая с ним с панели самообслуживания. Администратору домена можно назначить только один домен, и он может управлять виртуальными объектами во всех проектах в рамках этого домена. Эта роль также позволяет создавать пользователей и назначать их проектам.

  Администраторами домена обычно являются системные администраторы клиента поставщика услуг или поставщика управляемых услуг либо ИТ-отдела дочернего подразделения корпорации (в зависимости от ситуации на вашем конкретном предприятии).
- Участник проекта играет роль администратора проекта в определенном домене на панели самообслуживания. Участника проектов можно назначить сразу на несколько проектов, тогда он будет управлять виртуальными объектами во всех этих проектах.

  Участниками проекта обычно являются конечные пользователи клиента поставщика услуг или поставщика управляемых услуг либо конечные пользователи в корпорации (в зависимости от ситуации на вашем конкретном предприятии).

Такая реализация обеспечивает среду администрирования с собственными пользователями и виртуальными объектами, а также их изоляцию от других пользователей и виртуальных объектов.

3.9 Типы трафика

Для балансировки и оптимизации сетевых подключений в Кибер Инфраструктура можно назначить отдельным сетям разные типы трафика. Назначение сети определенного типа трафика означает, что на подключенных к этой сети узлах настраивается брандмауэр, на сетевых интерфейсах открываются определенные порты и задаются необходимые правила iptables. Например, серверы, подключенные к сети только с типом трафика **S3 внешн.**, будут принимать входящие подключения только на портах 80 и 443.

В следующих трех подразделах описаны все типы трафика, которые можно назначить сетям.

3.9.1 Эксклюзивные типы трафика

Эксклюзивность означает, что такой тип трафика можно добавить только в одну сеть.

Управление системными сервисами

Внутреннее управление кластером и перенос данных мониторинга узлов на панель администрирования. Без этого типа трафика администратор не может контролировать и отслеживать состояние кластера, хотя кластер продолжит работать. Используется любой доступный порт.

Хранилище

Внутренние операции переноса фрагментов данных, служебные heartbeat-сообщения высокой доступности, а также самовосстановление данных. Это самый важный тип трафика, который определяет производительность хранилища и обеспечивает высокую доступность кластера. Используется любой доступный порт.

OSTOR внутр.

Внутренний обмен данными между несколькими службами S3/NFS. Используется любой доступный порт.

Резервное копирование (ABGW) внутр.

Управление системными службами и обмен данными между несколькими службами хранилищ резервных копий.

ВМ внутр.

Сетевой трафик между виртуальными машинами в частных виртуальных сетях и трафик консоли VNC. Виртуальные сети реализуются как сети VXLAN, оверлейное сетевое подключение полностью изолируется на уровне L2. Открывает UDP-порт 4789 и TCP-порты 15900-16900.

API вычислений

Внешний доступ к стандартным конечным точкам OpenStack API. Открывает следующие порты:

- TCP 5000 — API идентификации, версия 3
- TCP 6080 — noVNC Websocket Proxy
- TCP 8004 — API сервиса оркестрации, версия 1
- TCP 8041 — API Gnocchi (сервис учета и биллинга)
- TCP 8774 — API вычислений
- TCP 8776 — API блочного хранилища, версия 3
- TCP 8780 — API размещения
- TCP 9292 — API службы образов, версия 2
- TCP 9313 — API управления ключами, версия 1
- TCP 9513 — API управления контейнерной инфраструктурой (служба Kubernetes)
- TCP 9696 — сетевой API, версия 2
- TCP 9888 — API Octavia, версия 2 (сервис балансировщика нагрузки)

Резервные копии ВМ

Внешний доступ к оконечным точкам NBD. Сторонние системы управления резервным копированием могут извлекать резервные копии ВМ, используя этот тип трафика. Для доступа к агентам резервного копирования, установленным на виртуальных машинах, назначьте этот тип трафика вместе с типом **ВМ внешн.** Открывает TCP-порты 49300-65535.

3.9.2 Обычные типы трафика

Трафик с обычными типами трафика можно добавлять во многие сети.

S3 внешн.

Внешний обмен данными с точкой доступа S3. Использует порты TCP 80 и 443.

iSCSI

Внешний обмен данными с точкой доступа iSCSI. Использует порт TCP 3260.

NFS

Внешний обмен данными с точкой доступа NFS. Использует порты TCP/UDP 111, 892 и 2049.

Резервное копирование (ABGW) внеш.

Внешний обмен данными с агентами Кибер Бэкап и Кибер Бэкап Облачный. Использует порты TCP 40440-44445.

Панель администрирования

Внешний доступ к панели администрирования. Использует порт TCP 8888.

ВМ внешн.

Внешний обмен данными между виртуальными машинами и внешними сетями (например, Интернетом). При назначении сети сетевого интерфейса узла с этим типом трафика на соответствующем сетевом интерфейсе создается мост Open vSwitch.

SSH

Удаленный доступ к узлам по протоколу SSH. Использует порт TCP 22.

SNMP

Внешний доступ к статистике мониторинга кластера хранилища данных по протоколу SNMP. Открывает порт UDP 161.

Панель самообслуживания

Внешний доступ к панели самообслуживания. Открывает порт TCP 8800.

3.9.3 Пользовательские типы трафика

Пользовательские типы трафика создаются системным администратором, чтобы открыть нужные порты TCP.

4 Требования к системе

Кибер Инфраструктура работает на стандартном оборудовании, поэтому можно создать кластер, используя обычные серверы, диски и сетевые карты. Тем не менее для оптимальной производительности необходимо соблюдение некоторых условий и рекомендаций.

Для промышленных сред можно запускать продукт Кибер Инфраструктура на физическом сервере или внутри виртуальной машины, чтобы использовать хранилище резервных копий в публичном облаке. Требования к оборудованию и рекомендуемое количество серверов в кластере зависят от развертываемых сервисов.

Если вы не уверены в выборе оборудования, можете использовать готовые программно-аппаратные комплексы с Кибер Инфраструктурой.

4.1 Рекомендации по оборудованию

- Продукт Кибер Инфраструктура работает на том же оборудовании, которое рекомендуется для Red Hat Enterprise Linux 7, включая процессоры AMD EPYC: серверы, компоненты.
- Хотя кластер можно создать поверх различного оборудования, использование серверов со сходной аппаратной конфигурацией обеспечит лучшую производительность, мощность и балансировку кластера.
- В производственной среде не рекомендуется использовать продукт Кибер Инфраструктура на оборудовании SAN/NAS с собственными механизмами обеспечения избыточности. Это может отрицательно сказаться на производительности и доступности данных.
- Рекомендуется использовать UEFI вместо BIOS, если позволяет оборудование. Особенно это рекомендуется при использовании дисков NVMe.
- Любая кластерная инфраструктура должна быть основательно протестирована перед развертыванием в производственной среде. Всегда следует тщательно проверять частые точки отказа, такие как твердотельные накопители и объединенные сетевые адаптеры.

Список оборудования, протестированного для использования с продуктом Кибер Инфраструктура, предоставлен в отдельном документе, который доступен по ссылке https://docs.cyberprotect.ru/ru-RU/CyberInfrastructure/5.5/testedhardware/.

4.2 Рекомендуемое оборудование

4.2.1 Сетевые карты для RDMA

- Mellanox MT27710 [ConnectX-4 Lx], MT27800 [ConnectX-5]
- Broadcom BCM57416 NetXtreme-E Dual-Media 10G RDMA
- Intel E810-XXV, X722 for 10GbE

4.2.2 Сетевые карты для DPDK

- Intel 82599ES 10-Gigabit, E810-XXV, X722 for 10GbE

4.2.3 Серверы

- GOOXI G4DCL
- Supermicro H12SSW-NT (AS -1014S-WTRT), B11SPE-CPU-TF (SBI-6119P-T3N)
- Gigabyte R182-N20-UNI
- Delta Computers DSS-C621LTG
- Dell PowerEdge R640, R740, R750, XC640
- HPE ProLiant DL360 Gen10
- Lenovo ThinkSystem SR650

4.3 Требования к серверу

Требования к оборудованию и рекомендуемое количество серверов в кластере зависят от сервисов, которые будут развернуты в этом кластере.

4.3.1 Общие требования

Проверьте, что все серверы, которые должны быть присоединены к кластеру, соответствуют общим требованиям, приведенным ниже.

4.3.1.1 Требования к хранилищу

В следующей таблице приведены минимальные и рекомендуемые требования к хранилищу в соответствии с ролями дисков (см. раздел "О кластере хранилища данных" на странице 12).

Роль диска	Количество	Емкость	Тип	Износостойкость
Система	Один диск на сервер	Минимум 100 ГБ Рекомендуется 250 ГБ	Минимум жесткий диск SATA/SAS Рекомендуется твердотельный накопитель SATA/SAS	
Метаданные	Один диск на сервер Рекомендуется пять дисков	100 ГБ	Твердотельный накопитель корпоративного класса с защитой	Минимум 1 DWPD

Роль диска	Количество	Емкость	Тип	Износостойкость
	на один кластер		от перебоев питания	
Кэш	Дополнительно Один твердотельный накопитель на 4-12 жестких дисков	100+ ГБ	Твердотельный накопитель корпоративного класса с защитой от перебоев питания и скоростью последовательной записи 75 МБ/с на обслуживаемый жесткий диск	Минимум 1 DWPD Рекомендуется 10 DWPD
Хранилище	Как минимум один на кластер	Минимум 100 ГБ Для физического сервера максимальный размер неограничен, для виртуальной машины не более 10 ТБ	Жесткий диск SATA/SAS или твердотельный накопитель SATA/SAS/NVMe (корпоративного класса с защитой от перебоев питания)	Минимум 1 DWPD

4.3.1.2 Резервирование ОЗУ и ЦП

В следующей таблице приведен объем ОЗУ и количество ядер ЦП, которые будут зарезервированы на одном сервере, в соответствии с сервисами, которые вы будете использовать.

Сервис	Сервер управления		Подчиненный сервер	
	ОЗУ[1]	Кол-во ядер ЦП[2]	ОЗУ[3]	Кол-во ядер ЦП[4]
Система	4,5 ГБ	3,3 ядра	1,5 ГБ	1,1 ядра

[1]Используйте только память с коррекцией ошибок (ECC), чтобы избежать повреждения данных.
[2]Ядро ЦП здесь означает физическое ядро в многоядерном процессоре (гиперпоточность не учитывается).
[3]Используйте только память с коррекцией ошибок (ECC), чтобы избежать повреждения данных.
[4]Ядро ЦП здесь означает физическое ядро в многоядерном процессоре (гиперпоточность не учитывается).

Сервис		Сервер управления		Подчиненный сервер	
		ОЗУ[1]	Кол-во ядер ЦП[2]	ОЗУ[3]	Кол-во ядер ЦП[4]
Сервисы хранилища: каждый диск с ролью Metadata, Storage или Cache (любого размера)[5]		0,5 ГБ	0,2 ядра	0,5 ГБ	0,2 ядра
Служба вычислений[6]		10 ГБ	4 ядра		
Балансировщик нагрузки		1,5 ГБ	0,5 ядра		
Kubernetes		1 ГБ	0,5 ядра		
Backup Gateway[7]		1 ГБ	0,5 ядра	1 ГБ	0,5 ядра
S3[8]	Шлюз S3	256 МБ	1 ядро	256 МБ	1 ядро
	Объектный сервер	256 МБ	0,1 ядра	256 МБ	0,1 ядра
	Сервер имен	512 МБ	0,2 ядра	512 МБ	0,2 ядра
NFS	Сервис	4 ГБ	1 ядро	4 ГБ	1 ядро
	Каждый том NFS[9]	до 9 ГБ	до 8 ядер	до 9 ГБ	до 8 ядер
iSCSI		1 ГБ	1 ядро	1 ГБ	1 ядро

В этих таблицах указаны минимальные значения. Чем больше ресурсов вы выделите для кластера, тем лучше он будет работать. Дополнительная оперативная память используется для

---

[1]Используйте только память с коррекцией ошибок (ECC), чтобы избежать повреждения данных.
[2]Ядро ЦП здесь означает физическое ядро в многоядерном процессоре (гиперпоточность не учитывается).
[3]Используйте только память с коррекцией ошибок (ECC), чтобы избежать повреждения данных.
[4]Ядро ЦП здесь означает физическое ядро в многоядерном процессоре (гиперпоточность не учитывается).
[5]Для кластеров с размером физического пространства более 1 ПБ добавьте еще 0,5 ГБ ОЗУ на каждый сервис метаданных.
[6]Рекомендуемая конфигурация для сервера в кластере вычислений начинается с 64+ ГБ и 16+ ядер.
[7]При работе с публичным облаком и NFS шлюз Backup Gateway потребляет столько же ОЗУ и ресурсов ЦП, сколько и с локальным хранилищем.
[8]Производительность и потребление ресурсов определяются во время начальной настройки кластера S3. Добавление дополнительных серверов в кластер S3 не влияет на эти параметры. Резервирование ресурсов ЦП и объема ОЗУ зависит от количества серверов S3. В целом чем больше кластер S3, тем меньше ресурсов ЦП и объема ОЗУ резервируется на каждом сервере.
[9]Резервирование объема ОЗУ для тома NFS зависит от количества серверов в кластере NFS. Чем больше кластер NFS, тем меньший объем ОЗУ резервируется на каждом сервере.

кэширования операций чтения с диска, а дополнительные ядра ЦП повышают производительность и уменьшают задержку.

4.3.1.3 Ограничения ОЗУ и ЦП

В следующей таблице приведены актуальные ограничения по объему ОЗУ и количеству ЦП для серверов продукта Кибер Инфраструктура.

Оборудование	Теоретически	Сертификация
ОЗУ	64 ТБ	1 ТБ
ЦП	5120 логических ЦП[1]	384 логических ЦП[2]

4.3.1.4 Рекомендации для ЦП

- Минимальная частота ЦП для серверов Кибер Инфраструктура – 2 ГГц. Рекомендуемая – не ниже 2,4 ГГц.
- Частота ЦП влияет на производительность кластера. При более высокой частоте показатель задержки снижается практически линейно, что способствует увеличению производительности. При прочих равных параметрах ЦП более высокая частота предпочтительнее большего количества ядер.
- Для серверов, на которых размещаются сервисы метаданных, следует устанавливать ЦП с высокой частотой, так как эти сервисы оказывают большую нагрузку на процессор.

4.3.1.5 Требования к сетевому интерфейсу

Рекомендуется как минимум 2 интерфейса 10 GbE для внутреннего и внешнего трафика, еще лучше – 25, 40 и 100 GbE. Лучше использовать объединенные каналы. Хотя для внешнего трафика можно начать с каналов 1 GbE, они могут ограничить пропускную способность кластера при современном уровне нагрузок.

[1]Логический ЦП – это ядро (поток) в многоядерном (многопоточном) процессоре.

[2]Логический ЦП – это ядро (поток) в многоядерном (многопоточном) процессоре.

4.3.2 Количество серверов

Масштабируемость – одно из отличительных преимуществ продукта Кибер Инфраструктура. Чем больше кластер, тем выше производительность продукта Кибер Инфраструктура.

Для наилучшей производительности оставьте свободными не менее 20 процентов ресурсов кластера.

4.3.2.1 Один сервер (для ознакомления с продуктом)

Хотя даже в минимальной конфигурации рекомендуется три сервера, можно начать тестировать продукт Кибер Инфраструктура всего с одним сервером и добавить остальные серверы позже.

Однако если вы хотите использовать только Backup Gateway, можно развернуть базовую инфраструктуру на одном виртуальном или физическом сервере. Хотя в этом случае может потребоваться обеспечение избыточности данных другими способами, так как существует риск потери пользовательских данных.

Как минимум в кластере хранилища должен работать один сервис метаданных и один сервис фрагментов данных. Однако такая конфигурация имеет два ключевых ограничения:

- Один сервер MDS будет единой точкой отказа. Если он откажет, весь кластер перестанет работать.
- Один сервер CS сможет хранить только одну реплику фрагмента данных. Если он откажет, данные будут потеряны.

Можно использовать конфигурацию, состоящую из одного сервера, для хранилища резервных копий с томом NFS или публичным облаком в качестве места назначения.

4.3.2.2 Три сервера (минимум для высокой доступности)

Для тестирования всех функций продукта требуется три сервера.

Эта минимальная конфигурация обеспечивает работу кластера без потери данных при отказе одного сервера. Эта конфигурация не предназначена для производственной среды.

Минимальная конфигурация должна содержать как минимум три работающих сервиса метаданных. Твердотельным накопителям можно одновременно назначить роли «Система», «Метаданные» и «Кэш», чтобы освободить больше дисков для роли «Хранилище».

4.3.2.3 Пять и более серверов (рекомендуется для высокой доступности и оптимальной совокупной стоимости владения)

Для производственной среды требуется не менее пяти серверов, чтобы гарантировать отсутствие потери данных при отказе двух серверов. В целях повышения надежности, производительности и отказоустойчивости рекомендуется создавать производственные кластеры с использованием не менее десяти серверов.

Кластер, готовый к использованию в производственной среде, можно создать всего из пяти серверов с рекомендуемым оборудованием. Однако рекомендуется вводить кластер в производственную эксплуатацию как минимум с десятью серверами, если вы хотите получить значительное повышение производительности по сравнению с напрямую подключаемым устройством хранения (DAS) или уменьшить время восстановления.

Рекомендуемая конфигурация кластера должна содержать 5 работающих сервисов метаданных и выделенные диски для кэша записи.

4.3.3 Требования к хранилищу резервных копий

Требования к хранилищу резервных копий зависят от его типа. Поддерживаются данные типы хранилищ:

- локальные кластеры Кибер Инфраструктура,
- тома NFS,
- публичные облачные сервисы, включая ряд решений S3, а также Yandex Object Storage, VK Cloud Storage и SberCloud OBS.

В последнем случае можно также размещать хранилища в виртуальных машинах.

4.3.3.1 Требования к хранилищам в локальных кластерах

Примечание
Общие требования перечислены в разделе Требования к физическим серверам.

Ниже приведены примеры резервирования ОЗУ и ЦП, если целевым хранилищем выбран локальный кластер.

Пример №1: Один физический сервер с одним диском для системы и метаданных и пятью дисками для хранения данных. Режим избыточности – 3+2, область отказа – диск (отказ хоста целиком может привести к потере данных).

Хранилище в локальном кластере из одного сервера

Сервис	Сервер
Система	4,5 ГБ, 3,3 ядра
Сервисы хранилища	5 дисков для хранения данных, 1 диск для системы и метаданных (0,5 ГБ и 0,2 ядра на каждый). Всего 3 ГБ и 1,2 ядра.
Backup Gateway	1 ГБ, 0,5 ядра
Зарезервировано для сервисов	**8,5 ГБ ОЗУ и 5 ядер**
Минимальная конфигурация	**12 ГБ ОЗУ и 6 ядер**
Рекомендуемая конфигурация	**16 ГБ**[1] Вся дополнительная память будет использована для кэширования операций чтения с диска. **ОЗУ и 6 ядер**

Пример №2: Пять серверов, на каждом по одному диску для системы, одному для метаданных и по 10 дисков для хранения данных. Включена высокая доступность сервера управления, поэтому три сервера соответствуют аппаратным требованиям для сервера управления.

Хранилище в локальном кластере из пяти серверов

Сервис	Серверы управления (1-3)	Подчиненные серверы (4-5)
Система	4,5 ГБ, 3,3 ядра	1,5 ГБ, 1,1 ядра
Сервисы хранилища	10 дисков для хранения данных и 1	10 дисков для хранения данных и 1 диск

Сервис	Серверы управления (1-3)	Подчиненные серверы (4-5)
	диск для метаданных (0,5 ГБ и 0,2 ядра на каждый). Всего 5,5 ГБ и 2,2 ядра.	для метаданных (0,5 ГБ и 0,2 ядра на каждый). Всего 5,5 ГБ и 2,2 ядра.
Backup Gateway	1 ГБ, 0,5 ядра	1 ГБ, 0,5 ядра
Зарезервировано под сервисы	**11 ГБ ОЗУ и 6 ядер**	**8 ГБ ОЗУ и 3,8 ядра**
Минимальная конфигурация	**12 ГБ ОЗУ и 6 ядра**	**8 ГБ ОЗУ и 4 ядра**
Рекомендуемая конфигурация	**24**[2] Вся дополнительная память будет использована для кэширования операций чтения с диска. **ГБ ОЗУ и 8 ядер**	**16 ГБ**[3] Вся дополнительная память будет использована для кэширования операций чтения с диска. **ОЗУ и 6 ядер**

4.3.3.2 Требования к хранилищам в томах NFS

Примечание
Общие требования перечислены в разделе Требования к физическим серверам.

Ниже приведен пример резервирования ОЗУ и ЦП, если целевым хранилищем выбраны тома NFS.

Пример: один физический сервер с одним диском для системы и метаданных и одним диском для хранения данных.

Хранилище в томе NFS

Сервис	Сервер
Система	4,5 ГБ, 3,3 ядра
Сервисы хранилища	1 диск для хранения данных[1] Хотя данные хранятся в удаленной папке, локально необходимо иметь диск емкостью от 100 ГБ с ролью "Хранилище"., 1 диск для системы и метаданных (0,5 ГБ и 0,2 ядра на каждый). Всего 1 ГБ и 0,4 ядра.
Backup Gateway	1 ГБ, 0,5 ядра
Зарезервировано для сервисов	**6,5 ГБ ОЗУ и 4,2 ядра**
Минимальная конфигурация	**8 ГБ ОЗУ и 4 ядра**
Рекомендуемая конфигурация	**8 ГБ ОЗУ и 6 ядер**

4.3.3.3 Требования к хранилищам в публичных облаках

Примечание
Общие требования перечислены в разделе Требования к физическим серверам.

Ниже приведены дополнительные требования:

- При работе с публичным облаком Backup Gateway использует локальное хранилище для промежуточного копирования, а также для хранения служебной информации. Это означает, что данные, предназначенные для загрузки в публичное облако, сначала сохраняются локально и только после этого отправляются в место назначения. По этой причине для сохранности данных крайне важно, чтобы локальное хранилище было постоянным и избыточным. Можно развернуть Backup Gateway на нескольких узлах кластера и выбрать подходящий режим резервирования. Если продукт Кибер Инфраструктура со шлюзом развернут на одном физическом узле, можно сделать локальное хранилище избыточным, реплицируя его между локальными дисками. Если продукт Кибер Инфраструктура со шлюзом развернут в виртуальной машине, убедитесь, что для него есть достаточный уровень резервирования со стороны виртуальной машины, на которой он работает.
- Убедитесь, что в локальном кластере хранилища достаточно логического пространства для промежуточного копирования. Например, при ежедневном резервном копировании обеспечьте достаточно места для резервных копий как минимум на 1,5 дня. Если размер ежедневной резервной копии составляет 2 ТБ, необходимо как минимум 3 ТБ логического пространства. Требуемый объем неформатированного пространства будет различаться в зависимости от режима кодирования: 9 ТБ (3 ТБ на сервер) в режиме 1+2, 5 ТБ (1 ТБ на сервер) в режиме 3+2 и т. д.
- Для каждого кластера хранилища резервных копий требуется отдельный контейнер объектов.
- Для хранения резервных копий в хранилищах объектов публичных облачных сервисов рекомендуется использовать предварительно настроенные шаблоны продукта Кибер Инфраструктура. Эти шаблоны предоставляют гибридную модель хранения резервных копий для продуктов Кибер Бэкап и Кибер Бэкап Облачный. Более того, с помощью этих шаблонов можно значительно сократить временные затраты на развертывание виртуальных машин в публичных облаках.

  Подробную информацию об использовании этих шаблонов см. в следующих документах:
  - Руководство пользователя приложения "Шлюз резервных копий СРК Кибер Бэкап" для Яндекс.Облака.

Ниже приведен пример резервирования ОЗУ и ЦП, если целевым хранилищем выбрано публичное облако.

Пример: одна виртуальная машина с одним диском для системы и метаданных и одним диском для хранения данных. Режим избыточности — 1+0, область отказа — диск. Фактическая избыточность обеспечивается решением виртуализации, на котором работает виртуальная машина.

Хранилище в публичном облаке

Сервис	Сервер
Система	4,5 ГБ, 3,3 ядра
Сервисы хранилища	1 диск для хранения данных[1] Используется для промежуточного копирования и хранения данных., 1 диск для системы и метаданных (0,5 ГБ и 0,2 ядра на каждый). Всего 1 ГБ и 0,4 ядра.
Backup Gateway	1 ГБ, 0,5 ядра
Зарезервировано для сервисов	**6,5 ГБ ОЗУ и 4,2 ядра**
Минимальная конфигурация	**8 ГБ ОЗУ и 4 ядра**
Рекомендуемая конфигурация	**16 ГБ**[2] **Вся дополнительная память будет использована для кэширования операций чтения с диска. ГБ ОЗУ и 6 ядер**

4.3.3.4 Требования к хранилищам в виртуальных машинах

VMware vSphere является одним из официально поддерживаемых гипервизоров для запуска Кибер Инфраструктура. Кроме VMware vSphere также поддерживаются KVM и Hyper-V.

Для запуска Кибер Инфраструктура на VMware vSphere убедитесь, что выполнены следующие требования:

- Версия VMware vSphere: 6.7 или новее.
- Версия ВМ: 14 или новее.
- Минимум 8 ГБ ОЗУ на хосте с Backup Gateway и одним диском для хранения данных.
- Минимум 464 ГБ дискового пространства для каждой виртуальной машины с Backup Gateway (два диска хранилища по 200 ГБ и системный диск на 64 ГБ). Шаблон продукта Кибер Инфраструктура также занимает около 3 ГБ. Рекомендуемый максимальный размер одного виртуального диска – 16 ТБ.

Внимание
Планируйте размер виртуальных дисков заранее и резервируйте достаточно пространства для ожидаемого увеличения объема данных. Размер дисков нельзя изменить позже, но можно добавить новые диски (см. Руководство по быстрому старту Backup Gateway для VMware vSphere).

4.3.4 Требования для вычислительного кластера

Примечание
Общие требования перечислены в разделе "Общие требования" на странице 46.

Обратите внимание на эти дополнительные требования для вычислительного кластера:

- Для развертывания и работы с вычислительным кластером устанавливайте продукт Кибер Инфраструктура на физических серверах.
- Используйте 64-разрядные x86 процессоры AMD-V или Intel VT с включенными аппаратными расширениями виртуализации. Для процессоров Intel включите поддержку unrestricted guest и VT-x с расширенными таблицами страниц (EPT) в BIOS.
- Используйте одинаковую модель ЦП на всех серверах во избежание проблем при динамической миграции ВМ. Если требуется использовать разные модели ЦП в одном кластере, создайте отдельное размещение для каждой группы вычислительных серверов одной модели.
- Если вы планируете использовать перераспределение памяти для виртуальных машин, убедитесь, что на системном диске достаточно места для файла подкачки и есть дополнительные 100 ГиБ свободного пространства.

Для лучшего понимания, как рассчитать конфигурацию оборудования для вычислительного кластера, рассмотрите пример ниже с перераспределением ресурсов ОЗУ и ЦП.

Пример: Если есть в наличии 10 серверов (на каждом по одному диску для системы, одному диску для метаданных, одному диску для кэша и по 10 дисков для хранения данных) и необходимо использовать их для вычислительного кластера, см. таблицу ниже для расчета. В этом примере три сервера используются для обеспечения высокой доступности сервера управления, поэтому эти три сервера соответствуют аппаратным требованиям для сервера управления.

Вычислительный кластер из 10 серверов с высокой доступностью сервера управления

Сервис	Серверы управления (1-3)	Подчиненные серверы (4-10)
Система	4,5 ГБ, 3,3 ядра	1,5 ГБ, 1,1 ядра
Сервисы хранилища	10 дисков для хранения данных, один диск для метаданных, один диск для кэша (0,5 ГБ и 0,2 ядра на каждый). Всего 6 ГБ и 2,4 ядра.	10 дисков для хранения данных, один диск для метаданных, один диск для кэша (0,5 ГБ и 0,2 ядра на каждый). Всего 6 ГБ и 2,4 ядра.
Вычисления	10 ГБ, 4 ядра	
Балансировщик нагрузки	1,5 ГБ, 0,5 ядра	
Kubernetes	1 ГБ, 0,5 ядра	
Зарезервировано для сервисов	**23 ГБ ОЗУ и 10,7 ядра**	**7,5 ГБ ОЗУ и 3,5 ядра**
Рекомендуемая конфигурация	**64 ГБ**[1] Вся дополнительная память используется для виртуальных машин. **ОЗУ и 16 ядер**	**64 ГБ**[2] Вся дополнительная память используется для виртуальных машин. **ОЗУ и 16 ядер**

4.3.5 Требования для хранилища объектов

Примечание
Общие требования перечислены в разделе "Общие требования" на странице 46.

Обратите внимание на эти дополнительные требования для хранилища объектов:

- Для развертывания и работы с хранилищем объектов, устанавливайте продукт Кибер Инфраструктура на физических серверах.
- Хранилище объектов требует больше пространства, чем суммарно занимают все объекты S3. Это происходит потому, что служба S3 также сохраняет внутренние метаданные об объектах и их распределении по серверам объектов. Для этих метаданных обычно требуется 0,5-1[1] процента пространства, используемого данными S3. Кроме того, начиная с версии 4.6, Кибер Инфраструктура предоставляет резервные копии метаданных объектов, которые увеличивают размер метаданных дополнительно на 0,5 процента. У этих резервных копий задаются автоматические параметры хранения, и они не требуют какого-либо вмешательства системного администратора. Метаданные и резервные копии используют одну и ту же схему избыточности, которая настроена для кластера S3.
- Хранилище объектов резервирует дополнительную оперативную память и ядра ЦП на случай возможного отказа сервера. Размер дополнительного резерва зависит от количества серверов кластера. На каждом сервере S3 работает сервис hostd, шлюз S3, до 10 сервисов объектов (OS), до 10 сервисов имен (NS). При этом один кластер S3 не может вместить более 24 OS и 16 NS.
  Объем ОЗУ, резервируемой на сервере S3, рассчитывается по следующей формуле:

  ```
  HOSTD * 256 МБ + S3GW * 256 МБ + (total_OS * 256 МБ + total_NS * 512 МБ) / (S3_nodes_number - nodes_that_can_fail_number)
  ```

  Количество процессорных ядер, резервируемых на сервере S3, рассчитывается по следующей формуле:

  ```
  S3GW * 1 ядро + (total_OS * 0,1 ядра + total_NS * 0,2 ядра) / (S3_nodes_number - nodes_that_can_fail_number)
  ```

  Например, в кластере S3 из пяти серверов может работать 24 OS, 16 NS. Такой кластер может потерять один сервер без потери данных. В таком случае на каждом сервере будет зарезервировано 4 ГБ ОЗУ: 256 МБ + 256 МБ + (24 * 256 МБ + 16 * 512 МБ) / (5 - 1), а также 2,4 процессорных ядра: 1 ядро + (24 * 0,1 ядра + 16 * 0,2 ядра) / (5 - 1).

Ниже приведены дополнительные примеры расчета объема ОЗУ и количества процессорных ядер для хранилища объектов.

---

[1]Метаданные объектов могут занимать больше места, если все объекты в кластере S3 занимают менее 100 КБ или если пользователь S3 дополнительно устанавливает метаданные при передаче объекта в хранилище.

Пример №1. Три сервера, на каждом по одному диску для системы и метаданных и по пять дисков для хранения данных. Режим избыточности с тремя репликами, область отказа – хост. Включена высокая доступность сервера управления, поэтому каждый сервер соответствует аппаратным требованиям для сервера управления.

Кластер S3 из трех серверов

Сервис	Серверы управления
Система	4,5 ГБ, 3,3 ядра
Сервисы хранилища	5 дисков для хранения данных, 1 диск для системы и метаданных (0,5 ГБ и 0,2 ядра на каждый). Всего 3 ГБ и 1,2 ядра.
S3	7,7 ГБ, 3,8 ядра
Зарезервировано под сервисы	**15,2 ГБ ОЗУ и 8,3 ядра**
Мин. конфигурация	**16 ГБ ОЗУ и 8 ядер**
Рекомендуемая конфигурация	**32 ГБ ОЗУ и 16 ядер**

Пример №2. Пять серверов, на каждом по одному диску для системы и метаданных, по одному SSD-диску для кэша и по 10 дисков для хранения данных. Включена высокая доступность сервера управления, поэтому три сервера соответствуют аппаратным требованиям для сервера управления.

Кластер S3 из пяти серверов

Сервис	Серверы управления (1-3)	Подчиненные серверы (4-5)
Система	4,5 ГБ, 3,3 ядра	1,5 ГБ, 1,1 ядра
Сервисы хранилища	10 дисков для хранения данных, один диск для системы и метаданных, один диск для кэша (0,5 ГБ и 0,2 ядра на каждый). Всего 6 ГБ и 2,4 ядра.	10 дисков для хранения данных, один диск для системы и метаданных, один диск для кэша (0,5 ГБ и 0,2 ядра на каждый). Всего 6 ГБ и 2,4 ядра.
S3	4 ГБ, 2,4 ядра	4 ГБ, 2,4 ядра
Зарезервировано под сервисы	**12,6 ГБ ОЗУ и 8,1 ядра**	**9,6 ГБ ОЗУ и 5,9 ядра**
Мин. конфигурация	**16 ГБ ОЗУ и 8 ядер**	**12 ГБ ОЗУ и 6 ядер**
Рекомендуемая конфигурация	**48 ГБ ОЗУ и 16 ядер**	**48 ГБ ОЗУ и 16 ядер**

4.4 Требования к дискам

4.4.1 Типы и роли дисков

- Экономичнее использовать жесткие диски SATA с одним твердотельным накопителем для кэширования, чем только жесткие диски SAS без такого накопителя.
- Использование твердотельных накопителей NVMe или SAS для кэширования записи повышает производительность произвольного ввода-вывода и настоятельно рекомендуется для всех рабочих нагрузок с большим количеством операций произвольного доступа (например, для томов iSCSI). Диски SATA лучше всего подходят для конфигураций только с твердотельными накопителями, но не для кэширования записи.
- Работа сервисов метаданных на твердотельных накопителях повышает производительность кластера. Для снижения капитальных затрат можно использовать те же накопители для кэширования записи.
- Жесткие диски с черепичной магнитной записью (SMR) можно использовать только для хранения данных и только при условии, что на сервере установлен SSD-накопитель для кэширования.
- Если основной целью является запас емкости и при этом необходимо хранить редко используемые данные, выбирайте диски SATA. Если основной целью является производительность, предпочтительнее будут диски NVMe или SAS.
- Размер блока на диске (например, 512 байт или 4 КБ) не имеет значения и не влияет на производительность.
- Максимально поддерживаемый размер физического раздела – 254 ТиБ.

4.4.2 Емкость диска

- На системном диске должно быть не менее 100 ГБ пространства.
- В одном кластере можно использовать диски разного размера. Однако учтите, что при одинаковом значении IOPS небольшие диски обеспечивают более высокую производительность на терабайт данных по сравнению с большими дисками. Рекомендуется группировать диски с одинаковым IOPS на терабайт на одном уровне хранилища.
- Емкость жестких дисков и твердотельных накопителей измеряется и указывается с использованием десятичных, а не двоичных приставок, поэтому «ТБ» в спецификациях диска обычно означает «терабайт». Однако операционная система отображает емкость дисков с использованием двоичных приставок, то есть «ТБ» означает «тебибайт», который представляет собой заметно большее число. В результате диски могут отображаться с меньшей емкостью, чем заявлено производителем. Например, диск емкостью 6 ТБ по спецификации может иметь фактический объем дискового пространства 5,45 ТБ в продукте Кибер Инфраструктура. Пять процентов дискового пространства резервируются под экстренные нужды. Таким образом, при добавлении в кластер диска размером 6 ТБ доступное физическое пространство должно увеличиться примерно на 5,2 ТБ.

- Производительность твердотельных накопителей может зависеть от их размера. Диски меньшей емкости (100-400 ГБ) могут работать значительно медленней (иногда в десять раз), чем диски большой емкости (1,9-3,8 ТБ). Проверьте характеристики производительности и стойкости дисков перед покупкой.
- Для всех данных всегда включено экономное распределение, которое нельзя настроить по-другому.

4.4.3 Бюджетные твердотельные накопители

- Бюджетные накопители рассчитаны на очень небольшое количество операций перезаписи. Накопители, предназначенные для кластеров хранения, должны иметь стойкость минимум 1 DWPD (рекомендуется 10 DWPD). Чем выше это значение, тем реже придется заменять накопители и тем ниже будет совокупная стоимость владения.
- Бюджетные твердотельные накопители обычно имеют нестабильную производительность и не рассчитаны на продолжительные производственные нагрузки. По этой причине при выборе накопителей обращайте внимание на результаты тестирования с продолжительной нагрузкой.
- Многие бюджетные твердотельные накопители могут игнорировать сброс данных на диск и отправлять операционной системе ложный отчет о выполненной записи данных, когда в действительности данные не были записаны. Примерами таких накопителей являются OCZ Vertex 3, Intel 520, Intel X25-E и Intel X-25-M G2. Эти накопители считаются ненадежными в плане фиксации данных, их не следует использовать с базами данных, и они могут легко повредить файловую систему при сбое питания. По этой причине следует использовать накопители корпоративного класса, которые подчиняются правилам сброса данных (подробнее см. здесь: "Защита данных во время отключений электроэнергии" на странице 71).

4.4.4 Контроллеры RAID и HBA

- Создайте аппаратные или программные тома RAID1 для системных дисков с использованием контроллеров RAID или HBA соответственно, чтобы обеспечить их высокую производительность и доступность.
- Используйте контроллеры HBA, поскольку они дешевле и проще в управлении, чем контроллеры RAID.
- Отключите все функции кэширования контроллера RAID для твердотельных накопителей. Современные твердотельные накопители имеют хорошую производительность, которую может снизить кэш чтения и записи контроллера RAID. Рекомендуется отключить кэширование для твердотельных накопителей и оставить его только для жестких дисков.
- Если вы используете контроллеры RAID, не создавайте тома RAID из жестких дисков, предназначенных для хранения данных. Каждый жесткий диск хранилища должен распознаваться продуктом Кибер Инфраструктура как отдельное устройство.
- Если вы используете контроллеры RAID с кэшированием, их следует оснастить резервными аккумуляторами (BBU) для защиты от потери данных кэша при отключении питания.

4.4.5 Количество дисков на сервер

На каждом сервере управления должно быть не менее двух дисков (один для системы и метаданных, один для хранилища). На каждом подчиненном сервере должно быть не менее двух дисков (один для системы, один для хранилища). Для метаданных рекомендуется использовать от трех до пяти дисков на кластер.

Чем больше дисков на сервер, тем меньше капитальные затраты. Например, кластер из десяти серверов с двумя дисками на каждом сервере будет стоить дешевле, чем кластер из двадцати серверов с одним диском на сервер.

Обычно кластер со множеством серверов и небольшим количеством дисков на сервер обеспечивает более высокую производительность, в то время как кластер с минимальным количеством серверов (3) и большим количеством дисков на сервер стоит дешевле. Подробнее см. в таблице ниже.

Рекомендации по составу кластера

Аспекты проектирования	Минимум серверов (3), много дисков на сервер	Много серверов, мало дисков на сервер (конфигурация с полным флеш-массивом)
Оптимизация	Меньше стоимость.	Больше производительность.
Резерв свободного дискового пространства	Требуется резервировать больше места для перестройки кластера, так как меньше исправных серверов должны будут хранить данные с отказавшего сервера.	Требуется резервировать меньше места для перестройки кластера, так как больше исправных серверов должны будут хранить данные с отказавшего сервера.
Избыточность	Меньше вариантов избыточного кодирования.	Больше вариантов избыточного кодирования.
Балансировка кластера и скорость перестройки	Хуже балансировка и медленнее перестройка.	Лучше балансировка и быстрее перестройка.
Пропускная способность сети	Требуется большая пропускная способность для поддержки производительности кластера во время перестройки.	Требуется меньшая пропускная способность для поддержки производительности кластера во время перестройки.
Предпочтительный тип данных	Холодные данные (например, резервные копии).	Горячие данные (например, виртуальные среды).
Пример конфигурации сервера	Supermicro SSG-6047R-E1R36L (ЦП Intel© Xeon E5-2620 v1/v2, 32 ГБ ОЗУ, 36 жестких дисков по 12 ТБ, системный диск 500 ГБ).	Supermicro SYS-2028TP-HC0R-SIOM (4 ЦП Intel E5-2620 v4, 4 ОЗУ 16 ГБ, 4 твердотельных накопителя Samsung PM1643 1,9 ТБ).

Обратите внимание на следующие моменты:

- Эти аспекты применимы, только если областью отказа является хост.
- Кибер Инфраструктура поддерживает сотни дисков на сервер. Если вы планируете использовать более 36 дисков на сервер, обратитесь к нашим специалистам отдела продаж, которые помогут вам спроектировать более эффективный кластер.

4.4.6 Конфигурация с жесткими дисками и твердотельными накопителями

4.4.6.1 Только жесткие диски

В этой базовой конфигурации требуется выделенный диск для каждого сервера метаданных.

Конфигурация только с жесткими дисками

Серверы 1-5 (база)			Серверы 6+ (расширение)		
№ диска	Тип диска	Роли дисков	№ диска	Тип диска	Роли дисков
1	HDD	Система	1	HDD	Система
2	HDD	MDS	2	HDD	CS
3	HDD	CS	3	HDD	CS
...	...	...	...	...	...
N	HDD	CS	N	HDD	CS

4.4.6.2 Жесткие диски + системные твердотельные накопители (без кэширования)

Эта конфигурация подходит для кластеров, ориентированных на емкость.

Конфигурация с жесткими дисками и системными твердотельными накопителями (без кэширования)

Серверы 1-5 (база)			Серверы 6+ (расширение)		
№ диска	Тип диска	Роли дисков	№ диска	Тип диска	Роли дисков
1	SSD	Система, MDS	1	SSD	Система
2	HDD	CS	2	HDD	CS
3	HDD	CS	3	HDD	CS
...	...	...	...	...	...
N	HDD	CS	N	HDD	CS

4.4.6.3 HDD + SSD

Эта конфигурация подходит для кластеров, ориентированных на производительность.

Конфигурация с жесткими дисками и твердотельными накопителями

Серверы 1-5 (база)			Серверы 6+ (расширение)		
№ диска	**Тип диска**	**Роли дисков**	**№ диска**	**Тип диска**	**Роли дисков**
1	HDD	Система	1	HDD	Система
2	SSD	MDS, кэш	2	SSD	Кэш
3	HDD	CS	3	HDD	CS
...	...	...	...	...	...
N	HDD	CS	N	HDD	CS

4.4.6.4 Только твердотельные накопители

В этой конфигурации не требуются твердотельные накопители для кэширования.

Примечание

В этой конфигурации сетевая задержка определяет больше половины общей производительности, поэтому убедитесь, что задержка минимальна. Как вариант, рекомендуется установить один коммутатор на 10 Гбит/с между каждыми двумя серверами в кластере.

Конфигурация только с твердотельными накопителями

Серверы 1-5 (база)			Серверы 6+ (расширение)		
№ диска	**Тип диска**	**Роли дисков**	**№ диска**	**Тип диска**	**Роли дисков**
1	SSD	Система, MDS	1	SSD	Система
2	SSD	CS	2	SSD	CS
3	SSD	CS	3	SSD	CS
...	...	...	...	...	...
N	SSD	CS	N	SSD	CS

4.4.6.5 Жесткие диски + твердотельные накопители (без кэширования), 2 уровня

В этом примере конфигурации уровень 1 предназначен для жестких дисков без кэширования, а уровень 2 – для твердотельных накопителей. На уровне 1 могут храниться холодные данные (например, резервные копии), а на уровне 2 – горячие данные (например, высокопроизводительные виртуальные машины).

2-уровневая конфигурация с жесткими дисками и твердотельными накопителями (без кэширования) для серверов 1-5 (база)

№ диска	Тип диска	Роли дисков	Уровень
1	SSD	Система, MDS	
2	SSD	CS	2
3	HDD	CS	1
...	...	...	...
N	HDD/SSD	CS	1/2

2-уровневая конфигурация с жесткими дисками и твердотельными накопителями (без кэширования) для серверов 6+ (расширение)

№ диска	Тип диска	Роли дисков	Уровень
1	SSD	Система	
2	SSD	CS	2
3	HDD	CS	1
...	...	...	...
N	HDD/SSD	CS	1/2

4.4.6.6 Жесткие диски + твердотельные накопители, 3 уровня

В этом примере конфигурации уровень 1 предназначен для жестких дисков без кэширования, уровень 2 – для жестких дисков с кэшированием, а уровень 3 – для твердотельных накопителей. На уровне 1 могут храниться холодные данные (например, резервные копии), на уровне 2 – обычные виртуальные машины, а на уровне 3 – высокопроизводительные виртуальные машины.

3-уровневая конфигурация с жесткими дисками и твердотельными накопителями для серверов 1-5 (база)

№ диска	Тип диска	Роли дисков	Уровень
1	HDD/SSD	Система	
2	SSD	MDS, кэш T2	
3	HDD	CS	1
4	HDD	CS	2
5	SSD	CS	3
...	...	...	...
N	HDD/SSD	CS	1/2/3

3-уровневая конфигурация с жесткими дисками и твердотельными накопителями для серверов 6+ (расширение)

№ диска	Тип диска	Роли дисков	Уровень
1	HDD/SSD	Система	
2	SSD	Кэш T2	
3	HDD	CS	1
4	HDD	CS	2
5	SSD	CS	3
…	…	…	…
N	HDD/SSD	CS	1/2/3

4.4.7 Рекомендации для конфигурации серверов с несколькими дисками

Если серверы, которые планируется включить в кластер Кибер Инфраструктура, имеют несколько дисков, следуйте следующим рекомендациям:

1. **(Рекомендуется для конфигураций с твердотельными накопителями) Конфигурация без использования RAID-массива.**
   Настройте сервер для каждого жесткого диска таким образом, чтобы каждый фрагмент данных имел две или более реплики. Такая конфигурация обеспечивает отказоустойчивость, а репликация сервера обеспечит надежность, близкую к схеме RAID 1. Использование твердотельных накопителей для хранения журнала обслуживания фрагментов также повышает производительность.
2. **(Рекомендуется для конфигураций со всеми типами накопителей) Конфигурация с отдельными дисками, подключенными к контроллеру RAID (прямое подключение, без использования схем RAID 0/1/10/5/6).**
   Эта конфигурация гораздо более производительна, чем предыдущая. Для контроллеров RAID с кэшированием рекомендуется использовать отдельные диски с резервными аккумуляторами (BBU). Кэширование обратной записи RAID значительно улучшает операции произвольного ввода-вывода, а также производительность базы данных. Использование твердотельных накопителей оптимизирует операции ввода-вывода, особенно операции чтения.
3. **(Не рекомендуется) Конфигурация с локальной схемой RAID 0 для фрагментов данных с двумя или более репликами.**
   Такая конфигурация снижает надежность кластера, так как сбой одного диска приведет к сбою всего массива RAID 0, что вынудит кластер реплицировать больше данных каждый раз, когда происходит сбой. Тем не менее, это незначительная проблема, поскольку кластеры Кибер Инфраструктура выполняют параллельное восстановление с нескольких серверов, что намного быстрее, чем восстановление при схеме RAID 1.

Использование твердотельных накопителей для кэширования и журналирования повысит производительность и даст возможность проверки контрольных сумм для повышения надежности кластера.

4. **(Не рекомендуется) Конфигурация с локальной схемой RAID 1 для фрагментов данных с одной или несколькими репликами.**
   Конфигурация кластера с одной репликой на каждый фрагмент данных не обеспечивает высокую доступность в случае сбоя нескольких серверов. Кроме того, такие конфигурации не приносят экономии дискового пространства, так как они эквивалентны зеркальному отображению кластера, а локальный RAID просто удваивает коэффициент репликации данных и экономит сетевой трафик кластера.
5. **(Категорически не рекомендуется) Конфигурация с локальными схемами RAID 1, 5 или 6 для фрагментов данных с двумя или более репликами.**
   Избегайте конфигурации Кибер Инфраструктура на избыточных схемах RAID (1, 5 или 6) поверх локального хранилища. В этом случае одна операция записи может повлиять на значительное количество жестких дисков, что приведет к очень низкой производительности. Например, для трех реплик Кибер Инфраструктура и схемы RAID 5 на серверах с 5 жесткими дисками каждая операция записи может привести к 15 операциям ввода-вывода.

4.4.8 Использование SSD-накопителей

Для оптимизации производительности SSD-накопителей необходимо проводить регулярную очистку неиспользуемых блоков посредством передачи SSD-накопителям команды TRIM. Без этого у большинства SSD-накопителей после полной перезаписи данных может значительно деградировать скорость записи.

Примечание
Некоторые современные SSD-накопители, такие как Intel SSD DC S3700, не нуждаются в команде TRIM.

Каждое воскресенье на всех узлах Кибер Инфраструктуры автоматически запускается процесс очистки неиспользуемых блоков SSD-накопителей. Для минимизации нагрузки на хранилище запуск на разных узлах происходит с разбросом по времени, составляющим от 0 до 999 минут. Время запуска и величина разброса заданы в конфигурационном файле /etc/cron.d/fstrim.

Наряду с конфигурациями All-Flash, в которых SSD-накопители используются для хранения фрагментов данных, Кибер Инфраструктура также поддерживает гибридные кластеры, в которых диски SSD используются для журналирования записи. Диск SSD можно подключить к серверу кластеров на основе жесткого диска и настроить для хранения журнала записи, повысив производительность операций записи в кластере до двух и более раз.

Обратите внимание:

- Не все твердотельные накопители подчиняются семантике сброса и фиксируют данные в соответствии с протоколом. Это может привести к произвольной потере или повреждению данных в случае сбоя питания. Всегда проверяйте твердотельные накопители с помощью

инструмента vstorage-hwflush-check.

- Рекомендуется использовать накопители Intel SSD DC S3700. Однако допустимо использование Samsung SM1625, Intel SSD 710, Kingston SSDNow E или любого другого SSD-накопителя с поддержкой защиты данных при отключении питания. Некоторые названия данной технологии: Enhanced Power Loss Data Protection (Intel), Cache Power Protection (Samsung), Power-Failure Support (Kingston), Complete Power Fail Protection (OCZ).

4.4.9 Расчет размера журнала записи

Использование SSD-накопителей для ведения журнала записи поможет сократить задержки записи, тем самым повысив общую производительность кластера. При наличии нескольких серверов фрагментов на одном хосте, создайте отдельный журнал SSD для каждого CS.

Чтобы определить размер каждого журнала CS на SSD, следуйте приведенным ниже рекомендациям.

1. Узнайте, сколько жестких дисков может обслуживать твердотельный накопитель, исходя из требований к оборудованию. Также можно использовать данную формулу:

   ```
   SSD_SSWS * 0.8 / HDD_SSWS
   ```

   Где:

   - SSD_SSWS – это устойчивая скорость последовательной записи на диск SSD.
   - HDD_SSWS – это устойчивая скорость последовательной записи на жесткий диск (при условии, что в соответствии с рекомендациями используются идентичные модели жестких дисков).
   - 0,8 – приблизительный процент погрешности.

   Примечание
   Поддерживаемая скорость последовательной записи – это средняя скорость последовательной записи, измеренная в течение 60 секунд.

2. Для полноценной работы SSD-накопителя 20% его объема должны быть свободными и использоваться для хранения метаданных при необходимости. Оставляйте 1 ГБ свободного объема на диске SSD для контрольных сумм на каждый 1 ТБ объема на жестком диске. Избегайте полного заполнения SSD-накопителя, иначе его производительность ухудшится.
3. Разделите оставшиеся 80% объема диска SSD на разрешенное количество HDD.

Например, диск SSD на 512 ГБ со скоростью SSWS 1500 МБ/с сможет обслуживать 1500 * 0,8 / 150 = 8 HDD с SSWS 150 МБ/с. А размер журнала для каждого HDD будет (512 - 20%)/8 = 51 ГБ.

В следующей таблице приведены несколько примеров моделей твердотельных накопителей и количество жестких дисков, которые они могут обслуживать:

Тип твердотельного накопителя	Количество твердотельных накопителей
Твердотельный накопитель Intel серии 320, твердотельный накопитель Intel серии 710, корпоративная серия Kingston SSDNow E или другие модели твердотельных накопителей SATA 3 Гбит/с, обеспечивающие последовательную запись произвольных данных со скоростью 150-200 МБ/с.	1 SSD на 3 жестких диска
Твердотельные накопители Intel серии DC S3700, корпоративные серии Samsung SM1625 или другие модели твердотельных накопителей SATA 6 Гбит/с, обеспечивающие последовательную запись произвольных данных со скоростью не менее 300 МБ/с.	1 SSD на 5-6 HDD

4.4.10 Конфигурация кэша

4.4.10.1 Поддерживаемые типы устройств

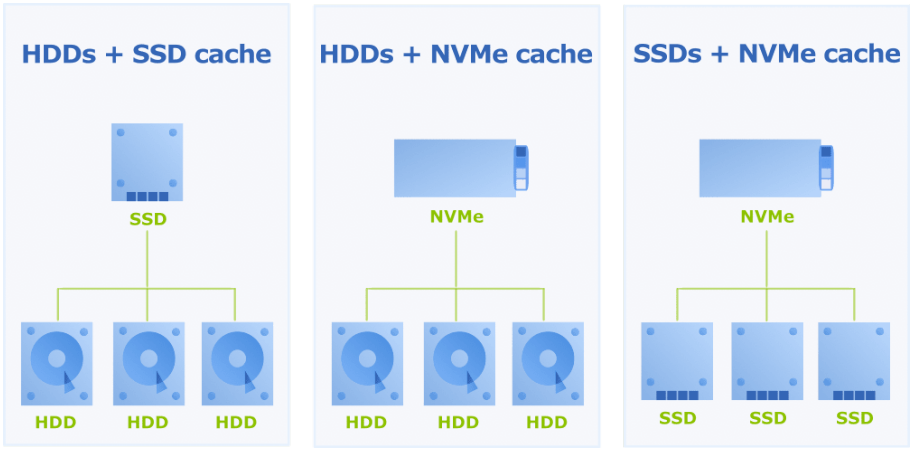
В настоящее время поддерживаемые диски включают HDD и SSD, в том числе устройства NVMe. Их характеристики описаны в таблице ниже.

Тип	Стоимость	Производительность	Интерфейс и форм-фактор
Жесткие диски (HDD)	Низкая	До 200 МБ/с Десятки/сотни IOPS	SAS или SATA
Твердотельные накопители (SSD)	Средняя	До 600 МБ/с Десятки тысяч IOPS	SAS или SATA
Твердотельные накопители NVMe (SSD NVMe)	Высокая	От 1 до 10 ГБ/с Сотни тысяч IOPS	2.5" U.2, карта расширения PCIe (AIC) или M.2

Примечание
Поддержка устройств PMem или NVRAM не проверялась.

Количество и тип устройств кэширования, поддерживаемых в вашем кластере, следует проверять для каждого узла кластера. Для того, чтобы кэширование имело смысл, устройства, обеспечивающие ускорение, должны быть быстрее базовых (основных) устройств.

По причине, изложенной выше, возможны следующие комбинации устройств кэш-памяти и емкости:



Примечание
Поддержка кэш-устройств, настроенных как RAID 1, не проверялась.

Рекомендуется, чтобы все устройства емкости на одном уровне хранения были идентичны с точки зрения технологии и размера. В противном случае возможны непредсказуемые производительность и поведение в случае аппаратного сбоя. Более того, все узлы кластера должны предлагать одинаковый объем хранилища. Если это требование не выполняется, пространство для хранения в кластере будет ограничено наименьшим узлом.

Аналогичная рекомендация относится к устройствам кэширования. Поскольку скорость записи ограничена самым медленным устройством в кластере, настоятельно рекомендуется использовать устройства кэширования той же технологии и размера.

4.4.10.2 Выбор кэш-устройства

Поскольку все данные, поступающие в систему, проходят через устройства кэширования, выбор устройства кэширования должен основываться не только на скорости, но и на долговечности устройства. Выносливость устройства измеряется двумя способами:

- Число операций записи на диск в день (DWPD) показывает, сколько раз устройство может быть полностью перезаписано каждый день, чтобы достичь ожидаемого конца срока службы устройства (обычно пять лет).
- Записанные терабайты (TBW) показывают ожидаемый объем данных, который может быть записан до того, как устройство выйдет из строя.

Оба параметра эквивалентны и должны быть тщательно оценены. Например, у вас есть флеш-накопитель на 1 ТБ с 1 DPWD, это означает, что вы можете записывать на него 1 ТБ каждый день в течение всего срока его службы. Если гарантийный срок накопителя равен пяти годам, то суммарно за это время получается 1 ТБ в день * 365 дней в году * 5 лет = 1825 ТБ совокупных операций записи, после чего диск обычно приходится заменять. Таким образом, TBW накопителя будет 1825.

DWPD типичного SSD-накопителя потребительского уровня может составлять всего 0,1, в то время как высокопроизводительный флеш-накопитель для центров обработки данных может иметь до 60 DWPD. Для устройства кэширования рекомендуемый минимум составляет 10 DWPD.

Еще одним параметром, который следует учитывать, является защита устройства от потери питания. Известно, что некоторые флеш-накопители потребительского уровня молча игнорируют запросы на сброс данных, что может привести к потере данных в случае отключения электроэнергии. Примеры таких дисков включают OCZ Vertex 3, Intel 520, Intel X25-E и Intel X-25-M G2. Рекомендуется избегать этих дисков (или протестировать их с помощью инструмента vstorage-hwflush-check) и использовать вместо них устройства корпоративного уровня или уровня центра обработки данных.

4.4.10.3 Предоставление устройств кэширования

Минимальное количество устройств кэширования на узел равно одному. Однако обратите внимание, что в этом случае, если кэширование используется для всех устройств емкости, кэш-устройство становится единой точкой отказа, что может привести к недоступности всего узла. Во избежание этого рекомендуется как минимум три устройства кэширования на узел.

Использование нескольких устройств кэширования также обеспечивает следующие улучшения:

- Больше емкости. Это может быть полезно, если данные записываются длинными пакетами или если кэш не может разгрузиться на базовое устройство.
- Повышение производительности. При наличии достаточного параллелизма на стороне клиента рабочую нагрузку можно разделить между несколькими устройствами кэширования, что увеличивает общую пропускную способность.
- Высокая доступность. С меньшим количеством устройств емкости на устройство кэш-памяти или зеркалированием RAID можно снизить вероятность простоя или его последствия.

Рекомендуется выделять одно устройство кэширования на каждые 4–12 устройств емкости. Однако скорость кэш-устройства должна быть как минимум в два раза выше, чем скорость базовых устройств вместе взятых.

Размер журнала

Независимо от размера устройства кэширования размер его журнала может быть разным в зависимости от доступного пространства и количества сервисов фрагментов, совместно использующих устройство кэширования. Существуют сценарии, когда использование журнала меньшего размера, чем доступная емкость, приводит к повышению производительности.

С одной стороны, если размер всех журналов меньше объема доступной оперативной памяти, то журнал будет использоваться только для хранения метаданных. Это позволит системе хранить журнал в ОЗУ, избегая всех операций чтения из журнала и приводя к меньшему количеству операций ввода-вывода. В конечном итоге это снизит нагрузку на устройства кэширования и может повысить общую производительность.

С другой стороны, если размер всех журналов больше, чем объем доступной оперативной памяти, то журнал также будет использоваться для хранения временных данных и будет служить кэшем

для чтения и записи. Это повысит производительность запросов на чтение и запись. Однако в этом случае устройство кэширования должно быть как минимум в два раза быстрее, чем все устройства базовой емкости вместе взятые, чтобы повысить общую производительность. Если это не так, предпочтительнее иметь журнал меньшего размера. Поскольку скорость также во многом зависит от рабочей нагрузки, это может быть неочевидно.

Размер кэша

Чтобы принять решение о размере устройства кэш-памяти, нужно учесть коэффициент выносливости конкретного устройства и размер его журнала.

Если вы используете кэш для пользовательских данных, то кэш-устройство должно выдерживать устойчиво высокую пропускную способность столько времени, сколько необходимо, не заполняясь. Содержимое кэша должно периодически выгружаться на базовое (основное) устройство, и этот процесс зависит от скорости базового устройства. Если устройство кэширования переполняется, производительность системы снижается до скорости базовых устройств, что сводит на нет преимущества кэширования. Следовательно, если ожидаемая рабочая нагрузка возникает в виде всплесков определенной продолжительности (например, в рабочее время), в кэше должна быть возможность хранить как минимум тот объем данных, который был записан за этот период времени.

4.4.10.4 Риски и возможные сбои

Хотя устройства кэширования могут значительно повысить производительность кластера, необходимо учитывать их возможные сбои. Флеш-устройства обычно имеют более короткий срок службы, и их использование в этом контексте подвергает их большему износу по сравнению с устройствами емкости.

Кроме того, поскольку одно устройство кэширования может использоваться для хранения нескольких журналов, все устройства емкости, связанные с устройством кэширования, станут недоступными, если это устройство кэширования выйдет из строя.

Возможные проблемы при использовании устройств кэширования:

- Потеря данных. Сбой устройства кэширования может привести к потере данных, если данные не имеют реплик или не настроено использование RAID 1.
- Снижение производительности. Если устройство кэширования выйдет из строя, система будет использовать другие устройства для хранения данных, что может привести к ограничениям производительности или запуску процесса повторной балансировки данных для восстановления избыточности данных. Это, в свою очередь, приведет к увеличению использования диска и сети и снижению производительности кластера.
- Низкая доступность. При отказе устройства кэширования избыточность данных может ухудшиться, что в тяжелых случаях может привести к созданию кластера, доступного только для чтения или нечитаемого.
- Меньшая емкость. Если устройство кэширования выйдет из строя, несколько устройств емкости могут стать недоступными, что приведет к нехватке места на диске для записи новых данных.

Чтобы предотвратить данные проблемы, используйте оптимальные политики избыточности и несколько устройств кэширования в вашей системе. Кроме того, возможно использование локальной репликации (например, RAID 1) поверх распределенной репликации, особенно в системах с низким коэффициентом репликации (1 реплика или кодировка 1+0).

4.4.11 Защита данных во время отключений электроэнергии

Для защиты Кибер Инфраструктура в случае отключения электроэнергии рекомендуется использовать источник бесперебойного питания для всех серверов и сетевых коммутаторов. Кроме того, чтобы предотвратить потерю данных и обеспечить их целостность, можно использовать следующие способы.

- Отключите кэширование записи для жестких дисков. Большинство жестких дисков не оборудованы функцией сброса данных, поэтому для них следует отключить кэширование записи. В противном случае при отключении электроэнергии данные могут быть утеряны.
- Используйте твердотельные накопители корпоративного класса с защитой от отключения питания. В отличие от жестких дисков такие накопители легко переносят сбои электроснабжения. Твердотельные накопители корпоративного класса, которые работают правильно, обычно имеют функцию защиты от перебоев питания, указанную в технических характеристиках. Некоторые рыночные названия этой технологии: Enhanced Power Loss Data Protection (Intel), Cache Power Protection (Samsung), Power-Failure Support (Kingston), Complete Power Fail Protection (OCZ). Проверьте функции сброса данных для всех ваших дисков, как описано в разделе "Проверка функций сброса данных на диски" ниже.

4.4.12 Проверка функций сброса данных на диски

Настоятельно рекомендуем убедиться, что все устройства хранения, которые вы планируете включить в кластер, могут сбрасывать данные из кэша на диск при незапланированном отключении питания. Таким образом вы определите устройства, которые могут потерять данные при сбое питания.

Кибер Инфраструктура поставляется с инструментом vstorage-hwflush-check, который проверяет, как устройство хранения сбрасывает данные на диск в аварийной ситуации. Инструмент реализован в виде клиентской/серверной утилиты.

- Клиент непрерывно записывает блоки данных на устройство хранения. После записи блока данных клиент увеличивает значение специального счетчика и отправляет его на сервер для сохранения.
- Сервер отслеживает значения счетчика, получаемые от клиента, и всегда знает следующее значение. Если на сервер приходит меньшее значение счетчика, чем уже существующее (например, когда из-за сбоя питания устройство хранения не сбросило кэшированные данные на диск), то сервер сообщает об ошибке.

Чтобы убедиться, что устройство хранения успешно сбрасывает данные на диск при сбое питания, выполните следующую процедуру.

1. На одном сервере запустите сервер:

   ```
   # vstorage-hwflush-check -l
   ```

2. На другом сервере, где расположено тестируемое устройство хранения, запустите клиент, например:

   ```
   # vstorage-hwflush-check -s vstorage1.example.com -d /vstorage/stor1-ssd/test -t 50
   ```

   где:

   - vstorage1.example.com – имя узла сервера:
   - /vstorage/stor1-ssd/test – каталог для тестирования сброса данных. Во время выполнения клиент создает в этом каталоге файл, в который записывает блоки данных.
   - 50 – количество потоков для записи клиентом данных на диск. У каждого потока есть собственный файл и счетчик. Можно увеличить количество потоков (до 200), чтобы протестировать систему в более сложных условиях. Также можно указать другие параметры при запуске клиента. Дополнительные сведения о доступных параметрах см. на справочной странице vstorage-hwflush-check.

3. Подождите как минимум 10-15 секунд, отключите питание на сервере клиента (нажмите кнопку питания или отсоедините шнур), а затем снова включите.
4. Перезапустите клиент.

```
# vstorage-hwflush-check -s vstorage1.example.com -d /vstorlage/stor1-ssd/test -t 50
```

После запуска клиент прочитает все ранее записанные данные, определит версию данных на диске и перезапустит тестирование с последнего действительного значения счетчика. Затем он отправит это значение на сервер, а сервер сравнит его с последним, полученным ранее. Будут выведены данные вида:

id<N>:<counter_on_disk> -> <counter_on_server>

что означает один из следующих вариантов.

- Если значение счетчика на диске меньше значения на сервере, то устройству хранения не удалось сбросить данные на диск. Это устройство лучше не использовать в производственной среде, особенно для CS или журналов, поскольку вы рискуете потерять данные.
- Если значение счетчика на диске больше значения на сервере, то устройство хранения сбросило данные на диск, но клиенту не удалось сообщить об этом серверу. Возможно, что скорость сети недостаточна либо устройство хранения работает слишком быстро для заданного количества потоков и следует увеличить количество. Это устройство хранения можно использовать в производственной среде.
- Если значения счетчиков равны, то устройство хранения сбросило данные на диск и клиент сообщил об этом серверу. Это устройство хранения можно использовать в производственной среде.

На всякий случай повторите процедуру несколько раз. Проверив первое устройство хранения, выполните проверку всех устройств, которые планируется использовать в кластере. Необходимо протестировать все устройства: твердотельные накопители, используемые для журналов CS, диски, используемые для журналов MDS, и серверы фрагментов данных.

4.5 Требования к сети и рекомендации

При планировании сети для кластера убедитесь, что она соответствует общим сетевым требованиям и рекомендациям. Дополнительные требования к сети зависят от сервисов, которые вы будете развертывать.

4.5.1 Требования к сети

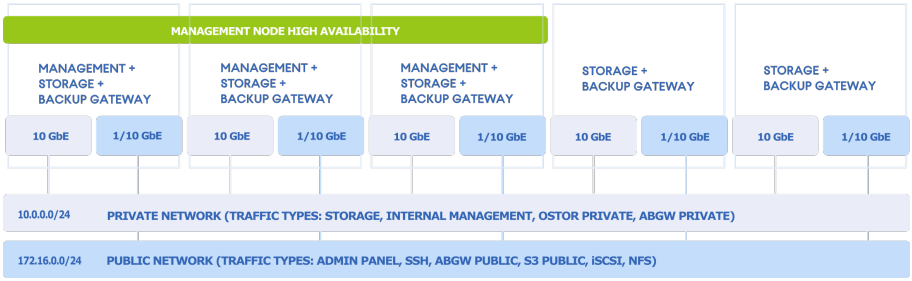
Общие требования к сети заключаются в следующем:

- Все сетевые интерфейсы на сервере должны быть подключены к разным подсетям. Сетевой интерфейс может представлять собой логический интерфейс с меткой VLAN, объединенный интерфейс без метки либо канал Ethernet.
- Сеть для внутреннего трафика может быть немаршрутизируемой с минимальной пропускной способностью 10 Гбит/с.
- Серверы добавляются в кластеры по IP-адресам, а не доменным именам. При изменении IP-адреса сервера в кластере этот сервер удаляется из кластера. Если вы планируете использовать в кластере DHCP, убедитесь, что IP-адреса привязаны к MAC-адресам сетевых интерфейсов серверов.
- Каждый сервер должен иметь доступ к Интернету для установки обновлений.
- Для правильной статистики необходима синхронизация времени по сети. Она включена по умолчанию посредством сервиса chronyd. Если вы хотите использовать ntpdate или ntpd, сначала остановите и отключите chronyd.

4.5.1.1 Требования к сети для хранилища резервных копий

Примечание
Общие требования к сети и рекомендации перечислены в разделах "Требования к сети" выше и "Рекомендации по сети" на странице 76.

Если вы хотите использовать только Backup Gateway и сервисы хранилища, настройте две сети: для внутреннего и внешнего трафика.



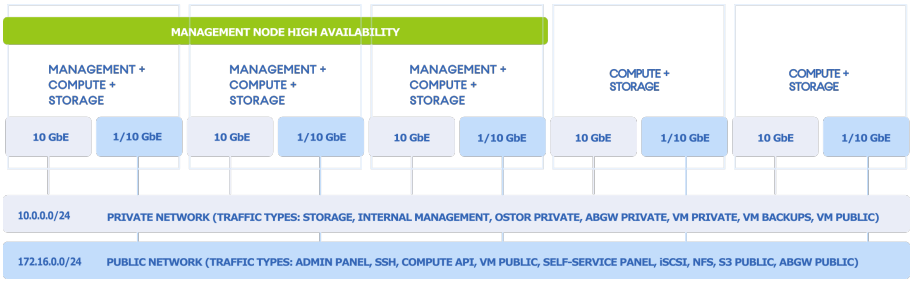
4.5.1.2 Требования к сети для вычислительного кластера

Примечание
Общие требования и рекомендации перечислены в разделах "Требования к сети" на предыдущей странице и "Рекомендации по сети" на странице 76.

Можно создать минимальную сетевую конфигурацию в целях тестирования либо расширить ее до более сложной конфигурации, рекомендуемой для производственной среды.

Минимальная сетевая конфигурация для вычислительного кластера

Минимальная конфигурация включает две сети: для внутреннего и внешнего трафика.



Примечание
Минимальная сетевая конфигурация не может быть использована для настройки быстрой сети DPDK для виртуальных машин.

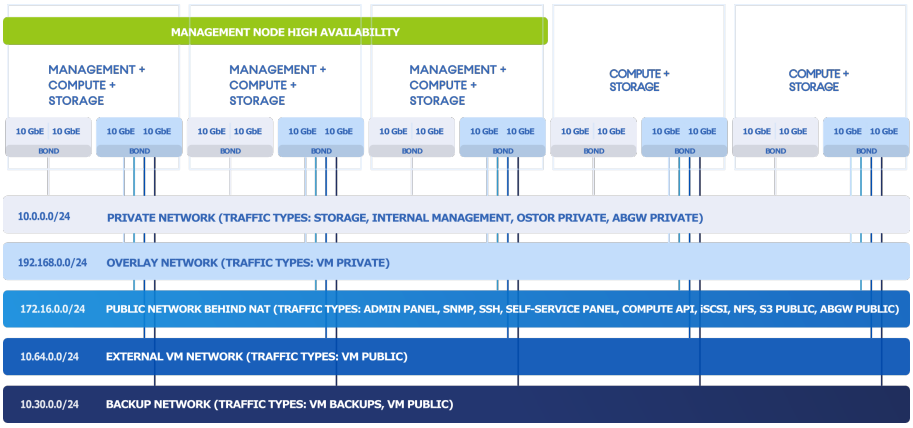
Рекомендуемая сетевая конфигурация для вычислительного кластера

Рекомендуемая конфигурация расширена до пяти сетей, подключенных к логическим сетевым интерфейсам.

Без поддержки быстрой сети DPDK для виртуальных машин

- Одно объединенное соединение для управления системными сервисами и внутреннего трафика хранилища
- Одно объединенное соединение с четырьмя VLAN поверх него:
  - Для оверлейного сетевого трафика между ВМ
  - Для управления через панели администрирования и самообслуживания, API вычислений, SSH и SNMP, а также для внешнего экспорта данных iSCSI, NFS, S3 и Backup Gateway

- Для внешнего трафика ВМ
- Для сбора резервных копий ВМ сторонними системами управления резервным копированием



С поддержкой быстрой сети DPDK для виртуальных машин

- Одно объединенное соединение для управления системными сервисами и внутреннего трафика хранилища
- Одно объединенное соединение с тремя VLAN поверх него:
  - Для оверлейного сетевого трафика между ВМ
  - Для управления через панели администрирования и самообслуживания, API вычислений, SSH и SNMP, а также для внешнего экспорта данных iSCSI, NFS, S3 и Backup Gateway
  - Для сбора резервных копий ВМ сторонними системами управления резервным копированием
- Одно объединенное соединение для внешнего трафика ВМ

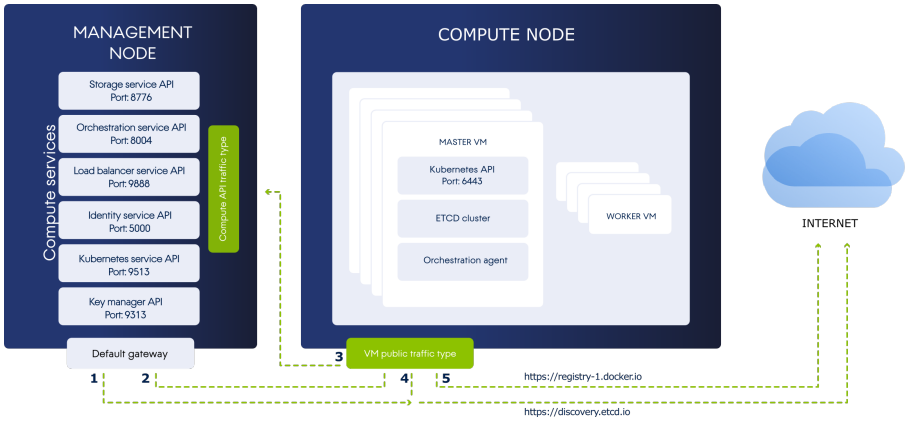
4.5.1.3 Требования к сети для компонента «Kubernetes как услуга»

Чтобы можно было развертывать кластеры Kubernetes в вычислительном кластере и работать с ними, убедитесь, что конфигурация вашей сети позволяет сервисам Kubernetes и вычислительным сервисам отправлять следующие сетевые запросы:

1. Запрос на начальную загрузку кластера etcd во внешнем сервисе обнаружения – со всех серверов управления на https://discovery.etcd.io через внешнюю сеть.
2. Запрос на получение файла kubeconfig – со всех серверов управления через внешнюю сеть:
   - Если высокая доступность (HA) для мастер-ВМ включена, запрос отправляется на публичный или плавающий IP-адрес ВМ балансировщика нагрузки, привязанный к API Kubernetes, через порт 6443.
   - Если высокая доступность для мастер-ВМ отключена, запрос отправляется на публичный или плавающий IP-адрес мастер-ВМ Kubernetes через порт 6443.
3. Запросы от мастер-ВМ Kubernetes к вычислительным API (тип трафика **API вычислений**) через сеть с типом трафика **ВМ внешн.** (через публично доступный сетевой интерфейс ВМ или виртуальный маршрутизатор с включенным преобразованием SNAT). По умолчанию API вычислений открывается через IP-адрес сервера управления (или его виртуальный IP-адрес

при включенной высокой доступности). Но доступ к API вычислений также можно получить через доменное имя.

4. Запрос на обновление состояния для участника кластера etcd во внешнем сервисе обнаружения – от мастер-ВМ Kubernetes на https://discovery.etcd.io через сеть с типом трафика **ВМ внешн.** (через публично доступный сетевой интерфейс ВМ или виртуальный маршрутизатор с включенным преобразованием SNAT).
5. Запрос на загрузку образов контейнеров из публичного репозитория Docker Hub – от мастер-ВМ Kubernetes на https://registry-1.docker.io через сеть с типом трафика **ВМ внешн.** (через публично доступный сетевой интерфейс ВМ или виртуальный маршрутизатор с включенным преобразованием SNAT).



Также необходимо, чтобы сеть, в которой создается кластер Kubernetes, не накладывалась на эти стандартные сети:

- 10.100.0.0/24 – используется для сетевого взаимодействия на уровне подов.
- 10.254.0.0/16 – используется для назначения IP-адресов кластера Kubernetes.

4.5.2 Рекомендации по сети

4.5.2.1 Рекомендации для сетевого оборудования

- Сетевая задержка существенно снижает производительность кластера. Используйте качественное сетевое оборудование с низким значением задержки. Не используйте бюджетные сетевые коммутаторы.
- Не используйте такие сетевые адаптеры для настольных компьютеров, как Intel EXPI9301CTBLK или Realtek 8129, поскольку они не предназначены для высоких нагрузок и могут не поддерживать полнодуплексные каналы. Также следует использовать неблокирующие коммутаторы Ethernet.
- Для RDMA рекомендуется использовать адаптеры Broadcom NetXtreme-E, Intel серий E800 (E810-C, E810-XXV, E823) и X722, Mellanox ConnectX-4, Mellanox ConnectX-5. Если вы хотите использовать другие адаптеры, обратитесь в службу технической поддержки.
- Если на серверах используются адаптеры Mellanox и ЦП AMD Epyc Rome, убедитесь, что в BIOS включена технология SR-IOV. В противном случае может произойти потеря данных.

- Не рекомендуется устанавливать адаптеры, которые используют драйвер BNX2X, такие как Broadcom Limited BCM57840 NetXtreme II 10/20-Gigabit Ethernet / 2-портовый адаптер HPE FlexFabric 10Gb 536FLB. Они ограничивают MTU до 3616, что отрицательно влияет на производительность кластера.
- RDMA не поддерживается для вычислительного кластера. Таким образом, сеть с вычислительным кластером и сеть хранилища (сеть с типом трафика **Хранилище**) должны использовать разные сетевые адаптеры. Рекомендуется использовать одну сетевую карту с двумя объединенными сетевыми интерфейсами для сети с вычислительным кластером и одну сетевую карту с двумя объединенными сетевыми интерфейсами для сети хранилища. Про использование магистральных (транковых) интерфейсов см. раздел "Подключение виртуальных коммутаторов к магистральным интерфейсам" на странице 530.
- Для быстрой сети DPDK для виртуальных машин следует использовать сетевые адаптеры Intel, поддерживающие технологию DPDK и следующие скорости передачи данных: от 10 Гбит/с и выше (в составе сетевого объединения), от 25 Гбит/с и выше (при независимом использовании).

4.5.2.2 Рекомендации по сетевой безопасности

- Используйте отдельные сети (и в идеале, хотя это и необязательно, отдельные сетевые адаптеры) для внутреннего и публичного трафика. Таким образом публичный трафик не будет влиять на производительность ввода-вывода кластера, а также будут исключены возможные DoS-атаки из внешней сети.
- Во избежание вторжений Кибер Инфраструктура должна быть развернута в выделенной внутренней сети, недоступной извне.
- Хотя на серверах кластера настроены необходимые правила iptables, рекомендуется использовать внешний брандмауэр для непроверенных публичных сетей, таких как Интернет.

4.5.2.3 Рекомендации по сетевой производительности

- Используйте один канал со скоростью 1 Гбит/с на каждые два жестких диска в сервере (с округлением в большую сторону). Для одного или двух жестких дисков в сервере все же рекомендуются два объединенных сетевых интерфейса для высокой доступности сети. Причина этой рекомендации состоит в том, что сети Ethernet со скоростью 1 Гбит/с могут обеспечить пропускную способность 110-120 МБ/с, что приближается к производительности последовательного ввода-вывода одного диска. Поскольку несколько дисков на сервере могут обеспечить более высокую пропускную способность, чем Ethernet-канал со скоростью 1 Гбит/с, передача данных по сети может стать узким местом системы.
- Для максимальной производительности последовательного ввода-вывода используйте один канал со скоростью 1 Гбит/с на каждый жесткий диск или один канал со скоростью 10 Гбит/с на сервер. Хотя в реальных условиях чаще всего выполняются операции произвольного ввода-вывода, последовательный ввод-вывод важен при резервном копировании.
- Для максимальной общей производительности используйте один канал со скоростью 10 Гбит/с на сервер (или два объединенных канала для высокой доступности сети).
- Не рекомендуется устанавливать для сетевых адаптеров со скоростью 1 Гбит/с нестандартные значения MTU (например, 9000-байтные jumbo-кадры). Такие параметры требуют

дополнительной настройки коммутаторов и часто приводят к пользовательским ошибкам. Сетевые адаптеры со скоростью 10+ Гбит/с, напротив, следует настроить на использование крупных кадров для достижения максимальной производительности. Для каждого маршрутизатора и коммутатора в сети требуется настроить одинаковое значение MTU (см. руководства по сетевому оборудованию), а также для сетевой карты каждого сервера, каждого объединенного интерфейса или интерфейса VLAN. По умолчанию для MTU установлено значение 1500.

4.5.2.4 Сетевые рекомендации для клиентов

В следующей таблице приведены максимальные показатели производительности сети, которые клиент может получить с указанным сетевым интерфейсом. Для клиентов рекомендуется использовать сетевое оборудование со скоростью передачи данных 10 Гбит/с между любыми двумя серверами кластера, а также свести к минимуму сетевую задержку, особенно при использовании твердотельных накопителей.

Максимальная производительность клиентской сети

Сетевой интерфейс хранилища	Макс. скорость ввода-вывода сервера	Макс. скорость ввода-вывода ВМ (репликация)	Макс. скорость ввода-вывода ВМ (избыточное кодирование)
1 Гбит/с	100 МБ/с	100 МБ/с	70 МБ/с
2 × 1 Гбит/с	~175 МБ/с	100 МБ/с	~130 МБ/с
3 × 1 Гбит/с	~250 МБ/с	100 МБ/с	~180 МБ/с
10 Гбит/с	1 ГБ/с	1 ГБ/с	700 МБ/с
2 × 10 Гбит/с	1,75 ГБ/с	1 ГБ/с	1,3 ГБ/с

4.5.3 Сетевые порты

Порты, которые будут открыты на серверах кластера, зависят от сервисов, которые будут работать на сервере, и от связанных с ними типов трафика. Перед включением определенного сервиса на сервере кластера необходимо назначить сети, к которой подключен этот сервер, соответствующий тип трафика. При назначении типа трафика сети выполняется настройка брандмауэра на серверах, подключенных к этой сети, открываются определенные порты на сетевых интерфейсах сервера и задаются необходимые правила iptables.

Если Кибер Инфраструктура используется в качестве гибридного партнерского хранилища для Кибер Бэкап Облачный, убедитесь, что кластеру предоставлен доступ к центру обработки данных.

В таблице ниже перечислены все необходимые порты и связанные с ними сервисы.

Сервис	Тип трафика	Порт	Описание
Веб-панель управления	Панель администрирования[1]	TCP 8888	Внешний доступ к панели администрирования.

Сервис	Тип трафика	Порт	Описание
	Панель самообслуживания	TCP 8800	Внешний доступ к панели самообслуживания.
Управление	Управление системными сервисами	любой доступный порт	Внутреннее управление кластером и перенос данных мониторинга серверов на панель администрирования.
Сервис метаданных	Хранилище	любой доступный порт	Внутренний обмен данными между сервисами MDS, а также с сервисами и клиентами CS.
Сервис фрагментов данных		любой доступный порт	Внутренний обмен данными с сервисами и клиентами MDS.
Клиент		любой доступный порт	Внутренний обмен данными с сервисами MDS и CS.
Backup Gateway	Резервное копирование (ABGW) внеш.	TCP 40440, 44445	Внешний обмен данными между агентами Кибер Бэкап и Кибер Бэкап Облачный.
	Резервное копирование (ABGW) внутр.	любой доступный порт	Внутреннее управление сервисами хранилища резервных копий и обмен данными между ними.
iSCSI	iSCSI	TCP 3260	Внешний обмен данными с точкой доступа iSCSI.
S3	S3 внешн.	TCP 80, 443	Внешний обмен данными с точкой доступа S3.
	OSTOR внутр.	любой доступный порт	Внутренний обмен данными между несколькими сервисами S3.
NFS	NFS	TCP/UDP 111, 892, 2049	Внешний обмен данными с точкой доступа NFS.
	OSTOR внутр.	любой доступный порт	Внутренний обмен данными между несколькими сервисами NFS.
Вычисления	API вычислений[2]		Внешний доступ к стандартным оконечным точкам OpenStack API:
		TCP 5000	API идентификации, версия 3
		TCP 6080	noVNC Websocket Proxy

Сервис	Тип трафика	Порт	Описание
		TCP 8004	API сервиса оркестрации, версия 1
		TCP 8041	API Gnocchi (сервис учета и биллинга)
		TCP 8774	API вычислений
		TCP 8776	API блочного хранилища, версия 3
		TCP 8780	API размещения
		TCP 9292	API сервиса образов, версия 2
		TCP 9313	API управления ключами, версия 1
		TCP 9513	API управления контейнерной инфраструктурой (сервис Kubernetes)
		TCP 9696	Сетевой API, версия 2
		TCP 9888	API Octavia, версия 2 (сервис балансировщика нагрузки)
	ВМ внутр.	UDP 4789	Сетевой трафик между ВМ в виртуальных вычислительных сетях.
		TCP 15900-16900	Трафик консоли VNC.
	Резервные копии ВМ	TCP 49300-65535	Внешний доступ к оконечным точкам NBD.
SSH	SSH	TCP 22	Удаленный доступ к серверам по протоколу SSH.
SNMP	SNMP[3]	UDP 161	Внешний доступ к статистике мониторинга кластера хранилища по протоколу SNMP.

[1]Порты для этого типа трафика должны быть открыты только на серверах управления.

[2]Порты для этого типа трафика должны быть открыты только на серверах управления.

[3]Порты для этого типа трафика должны быть открыты только на серверах управления.

4.6 Требования для панели администрирования

- Для правильного отображения панели администратора требуется монитор с разрешением Full HD.
- Панель администратора протестирована в работе с разрешением 1280 × 720 и выше в следующих веб-браузерах: последняя версия Firefox, Chrome, Safari.

5 Установка

В этом разделе описан процесс установки продукта Кибер Инфраструктура.

Ограничения

- Для программы установки требуется разрешение экрана не менее 800×600. Однако с этим разрешением могут возникнуть проблемы в пользовательском интерфейсе. Например, некоторые элементы могут быть недоступны. Рекомендуется разрешение не менее 1024×768.
- Сервер может входить только в один кластер.

Предварительные требования

- Четкое понимание инфраструктуры (см. описание в разделе "Об инфраструктуре" на странице 12).
- Оборудование инфраструктуры соответствует требованиям, перечисленным в разделе "Требования к системе" на странице 45.

Общие сведения об установке

1. Получите ISO-образ дистрибутива. Для этого зайдите на страницу продукта и отправьте запрос на пробную версию. ISO-образ также можно скачать из Кибер Бэкап Облачный.
   a. Перейдите на портал управления и выберите **НАСТРОЙКИ** > **Хранилища** в меню слева.
   b. Нажмите **Добавить хранилище резервных копий** и в открывшемся окне нажмите кнопку **Загрузить ISO-образ**.
2. Подготовьте загрузочный носитель с помощью ISO-образа дистрибутива: создайте загрузочный USB-накопитель, подключите образ дистрибутива к виртуальному диску IPMI или настройте PXE-сервер.
3. Если разрешение дисплея сервера меньше 800×600, подключитесь к серверу с удаленной машины с помощью консоли VNC.
4. Если планируется автоматическая установка, создайте файл kickstart.
5. Установите Кибер Инфраструктура на все серверы в автоматическом или ручном режиме.

5.1 Подготовка загрузочного носителя

Установку продукта Кибер Инфраструктура можно выполнить с помощью следующих загрузочных носителей:

- USB-накопителей при наличии физического доступа к серверу;
- виртуальных дисков Intelligent Platform Management Interface (IPMI), если сервер настроен для внешнего удаленного управления через порты IPMI;
- сервера Preboot Execution Environment (PXE) для загрузки по сети.

5.1.1 Создание загрузочного USB-накопителя

Предварительные требования

- USB-накопитель размером не менее 4 ГБ.

Чтобы копировать образ дистрибутива на USB-накопитель в системе Linux

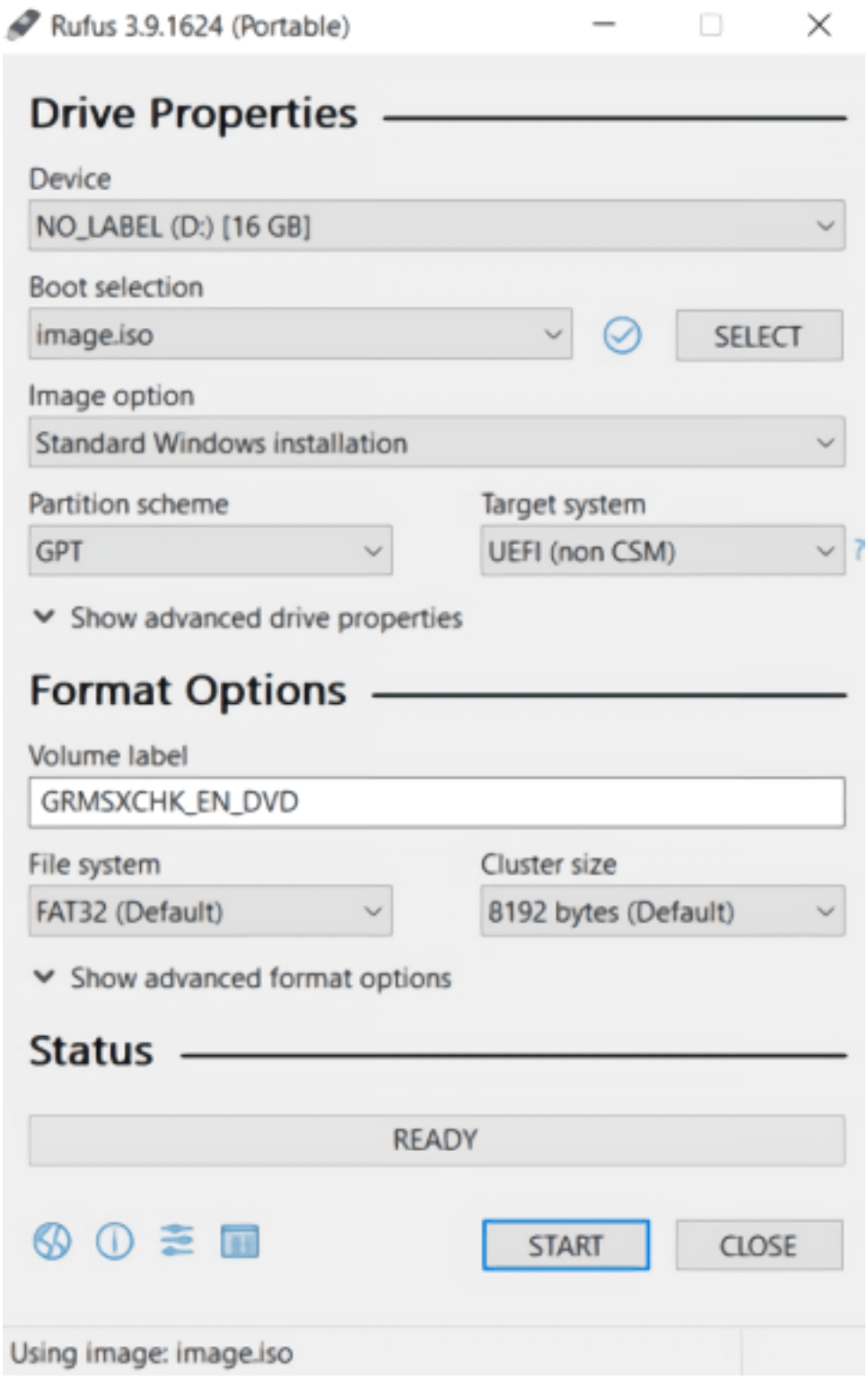
Используйте утилиту dd.

```
# dd if=image.iso of=/dev/sdb
```

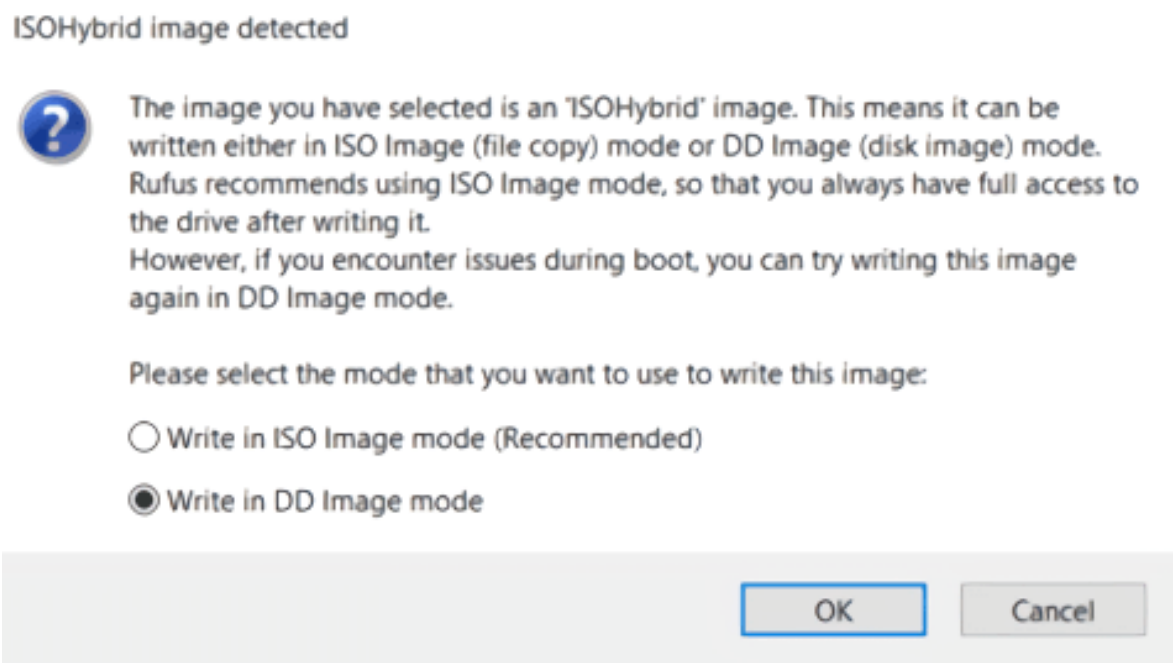
Внимание
Убедитесь, что указан правильный диск для переноса образа.

Чтобы копировать образ дистрибутива на USB-накопитель в системе Windows

1. Зайдите на сайт https://rufus.ie/ и загрузите переносимую версию.
2. Запустите Rufus.
3. В разделе **Drive Properties** (Свойства диска) выберите флеш-накопитель в раскрывающемся меню **Device** (Устройство) и нажмите **SELECT** (Выбрать). Затем выберите образ дистрибутива с локальной машины. При необходимости можно изменить другие параметры.
4. Нажмите **START** (Запустить).



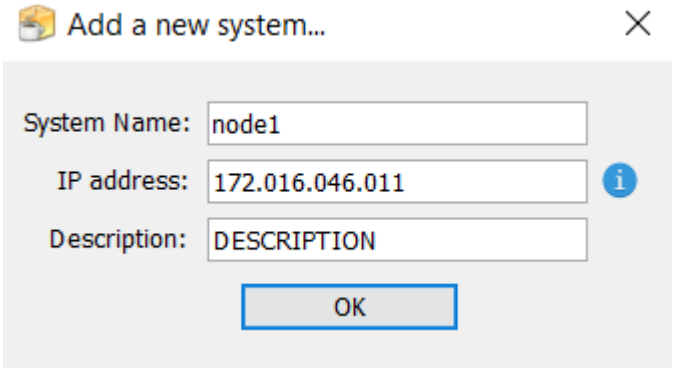
5. Во всплывающем окне выберите **Записать в режиме образа DD** и нажмите **OK**.



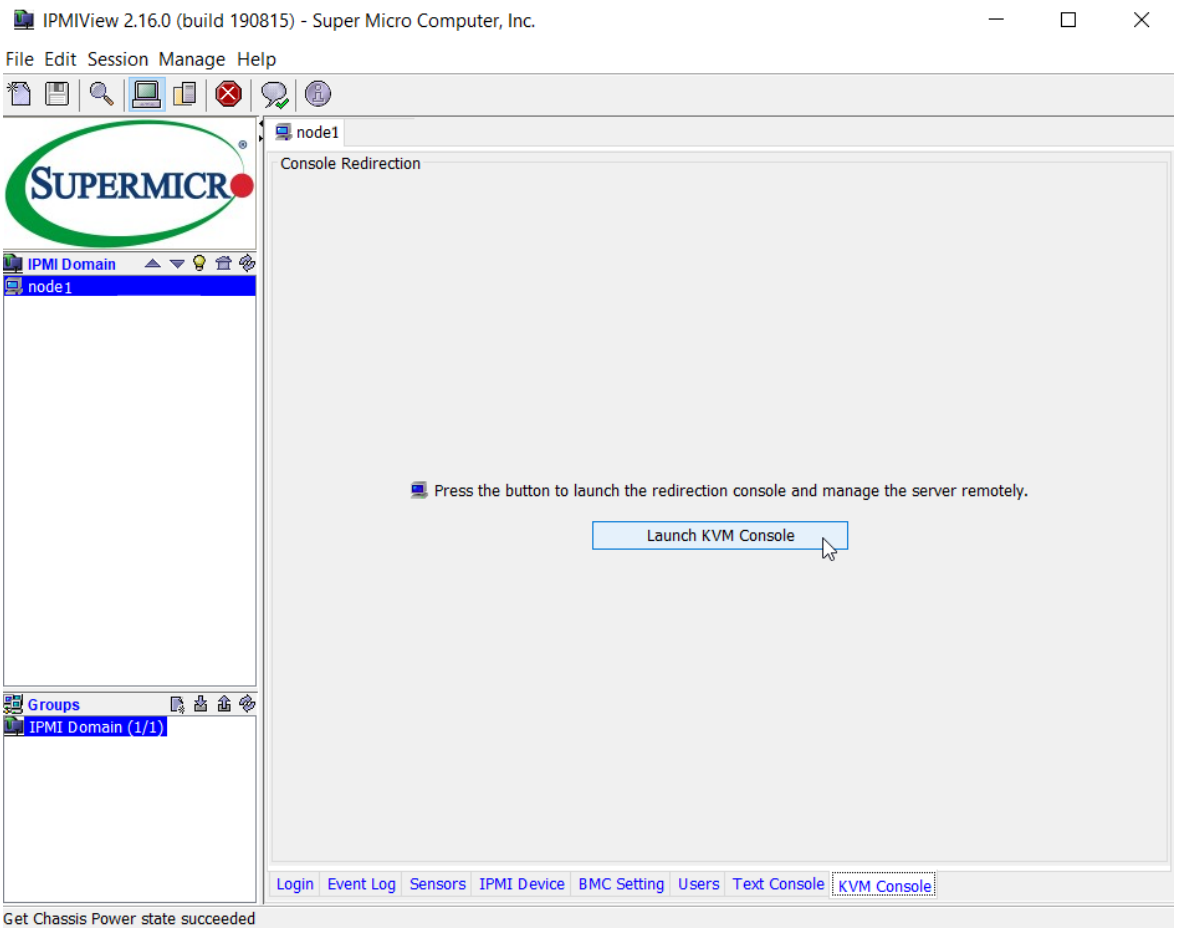
5.1.2 Присоединение виртуального диска IPMI

Чтобы присоединить виртуальный диск IPMI

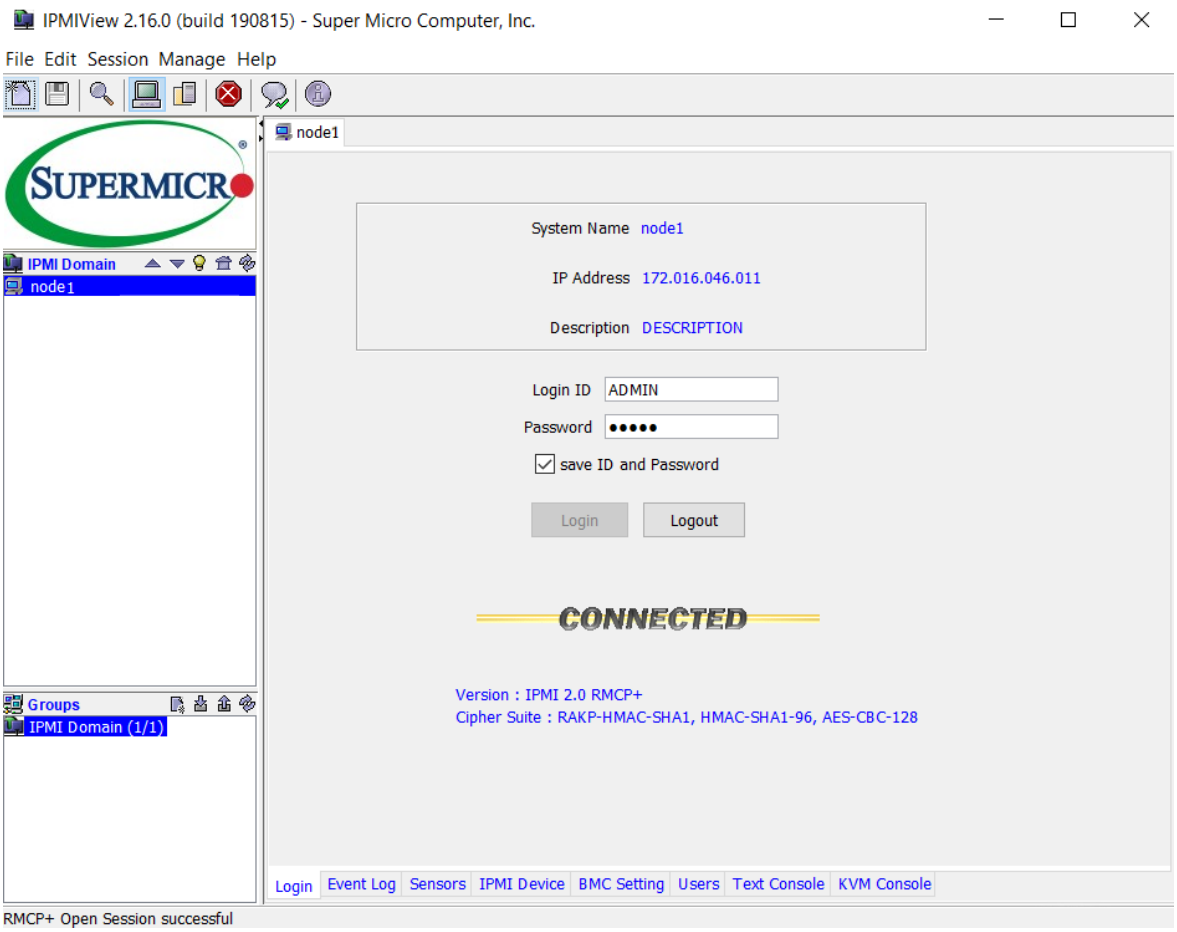
1. Загрузите приложение IPMIView (при необходимости) и запустите его.
2. Убедитесь, что сервер включен.
3. В окне **IPMIView** щелкните **File > New... > System** (Файл > Создать... > Система) и введите IP-адрес сервера IPMI. При необходимости можно изменить имя системы и добавить описание.



4. В разделе **IPMI Domain** (Домен IPMI) дважды щелкните по вновь добавленному имени системы.
5. После установки соединения перейдите на вкладку **KVM console** (Консоль KVM) и нажмите **Launch KVM console** (Запустить консоль KVM).

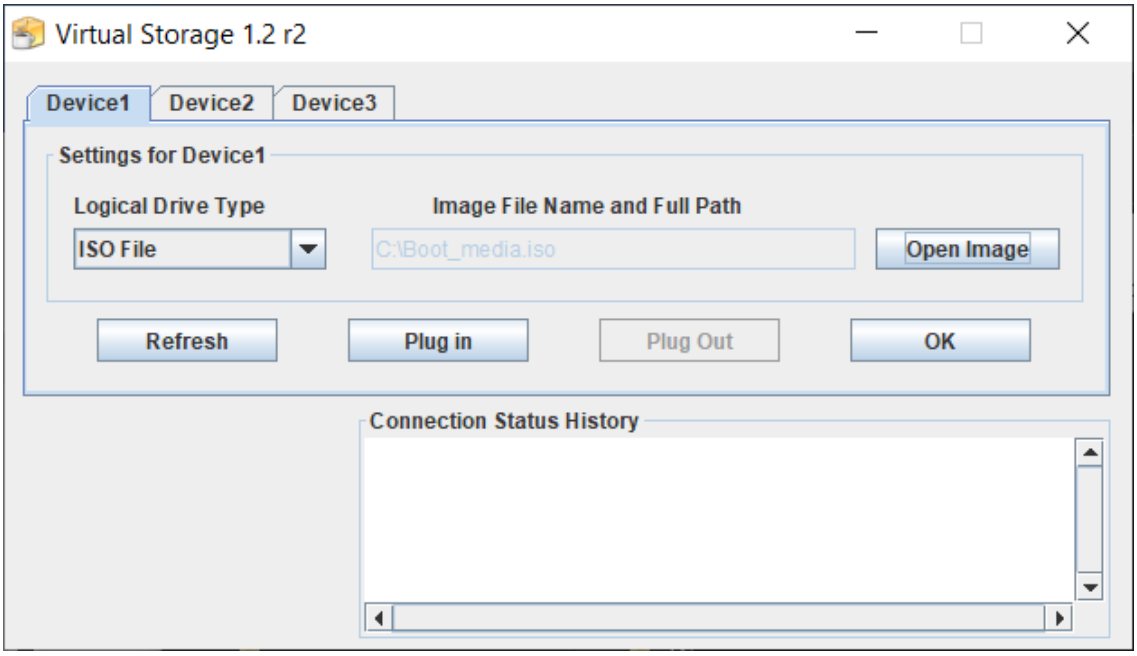


6. На вкладке **Login** (Вход в систему) укажите имя входа и пароль для доступа к серверу. Затем нажмите кнопку **Login** (Войти).



7. В окне **Java iKVM Viewer** прикрепите образ к серверу в качестве виртуального CD-ROM.
   a. Нажмите **Virtual Media** > **Virtual Storage** (Виртуальный носитель > Виртуальное хранилище).
   b. В окне **Virtual Storage** (Виртуальное хранилище) выберите **ISO File** (ISO-файл) в разделе **Local Drive Type** (Тип локального диска), щелкните **Open Image** (Открыть образ) и выберите образ дистрибутива на локальной машине.

c. Нажмите **OK**.



8. Перезагрузите сервер, щелкнув **Power Control** > **Set Power Reset** (Управление питанием > Установить сброс питания).

5.1.3 Настройка PXE-сервера

Требуется установить и настроить следующие компоненты:

- TFTP-сервер. Это машина, которая позволяет вашим серверам загрузиться и установить продукт Кибер Инфраструктура по сети. TFTP-сервером может быть любая Linux-совместимая машина, доступная по сети.
- DHCP-сервер. Это стандартная машина DHCP, передающая параметры TCP/IP компьютерам в вашей сети.
- HTTP-сервер. Это машина, передающая установочные файлы продукта Кибер Инфраструктура по сети.

  Дистрибутив продукта Кибер Инфраструктура также можно разместить на FTP-сервере (например, vsftpd) или томе NFS.

Чтобы установить компоненты PXE

Выполните следующую команду:

```
# yum install tftp-server syslinux httpd dhcp
```

Также можно использовать серверы, уже присутствующие в инфраструктуре. Например, можно пропустить httpd и dhcp, если у вас уже есть серверы HTTP и DHCP.

Настройка TFTP-сервера

Примечание

В этом разделе приводятся инструкции по настройке TFTP-сервера для систем на базе BIOS. Для получения сведений о настройке сервера в системах на базе EFI см. Руководство Red Hat Enterprise Linux.

1. На сервере откройте файл /etc/xinetd.d/tftp и введите следующие данные:

```
service tftp
{
disable       = no
socket_type    = dgram
protocol       = udp
wait          = yes
user          = root
server        = /usr/sbin/in.tftpd
server_args    = -v -s /tftpboot
per_source     = 11
cps           = 100 2
flags         = IPv4
}
```

   Завершив редактирование, сохраните файл.

2. Создайте каталог /tftpboot и скопируйте в него следующие файлы: vmlinuz, initrd.img, menu.c32, pxelinux.0.

   Эти файлы необходимы для запуска установки. Первые два можно найти в каталоге /images/pxeboot дистрибутива продукта Кибер Инфраструктура. Последние два файла расположены в каталоге syslinux (обычно /usr/share/syslinux или /usr/lib/syslinux).

3. Создайте каталог /tftpboot/pxelinux.cfg и создайте в нем файл default.

```
# mkdir /tftpboot/pxelinux.cfg
# touch /tftpboot/pxelinux.cfg/default
```

4. Добавьте следующие строки в файл default:

```
default menu.c32
prompt 0
timeout 100
ontimeout INSTALL
menu title Boot Menu
label INSTALL
      menu label Install
      kernel vmlinuz
      append initrd=initrd.img ip=dhcp
```

   Подробные сведения о параметрах, которые можно указать в этом файле, см. в документации по Syslinux.

5. Перезапустите сервис xinetd.

```
# /etc/init.d/xinetd restart
```

6. При необходимости настройте в брандмауэре разрешение доступа к TFTP-серверу (порт 69 по умолчанию).

   При запуске TFTP-сервера может возникнуть ошибка «Отказано в разрешении». В этом случае можно попытаться исправить проблему, выполнив команду # restorecon -Rv /tftboot/.

Настройка DHCP-сервера

Добавьте следующие строки в файл dhcpd.conf, который обычно расположен в каталоге /etc или /etc/dhcp:

```
next-server <PXE_server_IP_address>;
filename "/pxelinux.0";
```

Чтобы настроить DHCP-сервер для установки в системах на базе EFI, укажите filename "/bootx64.efi" вместо filename "/pxelinux.0" в файле dhcpd.conf, где /bootx64.efi – каталог, в который вы скопировали загрузочные образы EFI при настройке TFTP-сервера.

Чтобы предоставить доступ к файлам на HTTP-сервере

1. Настройте HTTP-сервер (или измените конфигурацию существующего).
2. Скопируйте содержимое образа дистрибутива в произвольный каталог на HTTP-сервере (например, /var/www/html/distrib).
3. На PXE-сервере укажите путь к установочным файлам в строке append в файле /tftpboot/pxelinux.cfg/default.

   В системах на базе EFI файл, который необходимо изменить, называется /tftpboot/pxelinux.cfg/efidefault или /tftpboot/pxelinux.cfg/<PXE_server_IP_address>.

   Например, если HTTP-сервер расположен по адресу 198.123.123.198, файлы установки находятся в /var/www/html/distrib/, а для DocumentRoot установлено значение /var/www/html, то файл default может выглядеть так:

```
default menu.c32
prompt 0
timeout 100
ontimeout INSTALL
menu title Boot Menu
label INSTALL
      menu label Install
      kernel vmlinuz
      append initrd=initrd.img ip=dhcp inst.repo=http://198.123.123.198/distrib
```

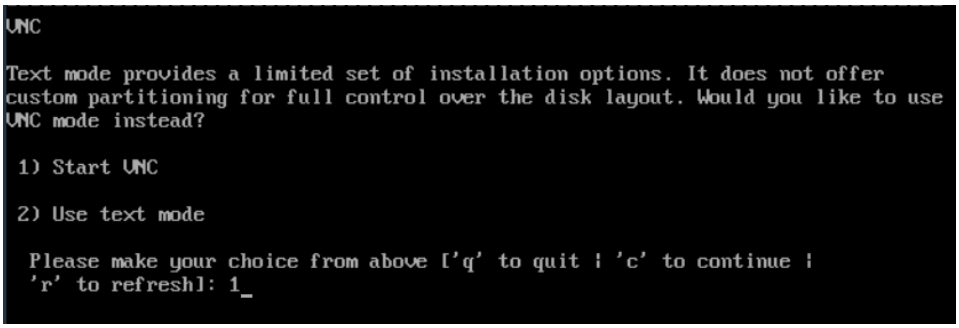
5.2 Подключение к серверу с помощью консоли VNC

Чтобы настроить сервер для подключения VNC

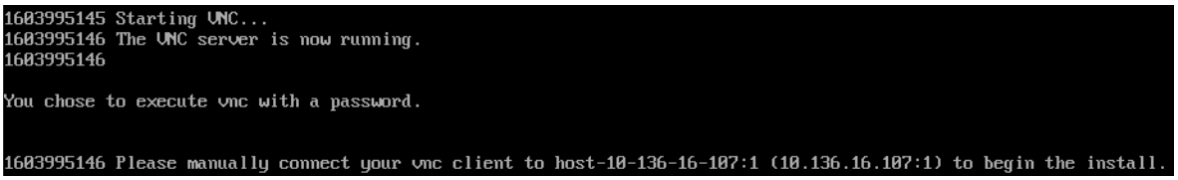
1. Выполните загрузку с загрузочного носителя и дождитесь **экрана приветствия**.
2. Выберите **Установить Кибер Инфраструктура** и нажмите клавишу **E**, чтобы изменить пункт меню.
3. Добавьте text в конце строки, начинающейся с linux /images/pxeboot/vmlinuz, например:

   ```
   linux /images/pxeboot/vmlinuz inst.stage2=hd:LABEL=<ISO_img> quiet ip=dhcp logo.nologo=1
   text
   ```

4. Нажмите **Ctrl+X**, чтобы начать загрузку с выбранным вариантом установки.
5. Чтобы запустить VNC, нажмите **1**, а затем клавишу **Enter** (Ввод).

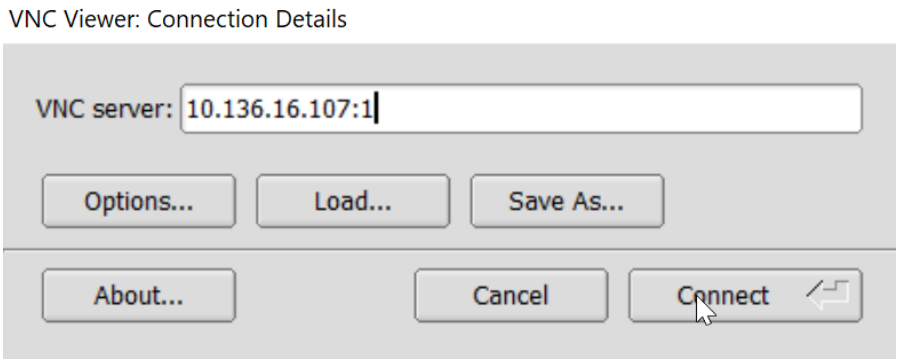


6. Дважды введите пароль VNC и нажмите клавишу **Enter** (Ввод).
7. В выходных данных найдите имя хоста или IP-адрес и порт VNC для подключения, например:

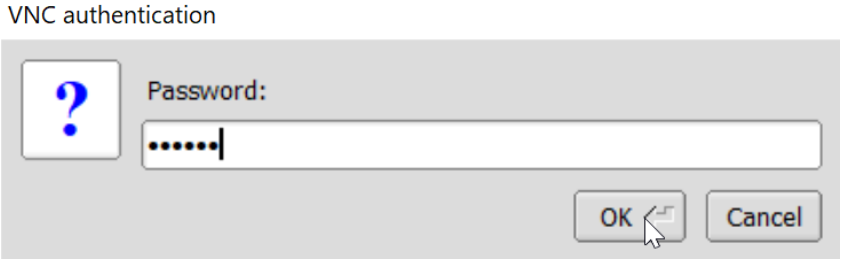


Чтобы подключиться к серверу с удаленной машины

1. На выбранной машине установите клиент VNC по своему усмотрению (например, TigerVNC Viewer) и запустите его.
2. Укажите адрес электронной почты и порт VNC и нажмите **Connect** (Подключить).



3. После того как клиент VNC подключится к серверу, введите пароль VNC и нажмите **OK**.



Откроется окно с установленным подключением VNC для дальнейшей настройки Кибер Инфраструктура с помощью графического пользовательского интерфейса.

5.3 Создание файла kickstart

Кибер Инфраструктура использует тот же синтаксис файла kickstart, что и Red Hat Enterprise Linux.

В следующих разделах описываются параметры и сценарии, которые следует включить в файл kickstart, а также приводится базовый пример файла.

5.3.1 Параметры kickstart

Хотя файл kickstart может содержать любые стандартные параметры, рекомендуется использовать только параметры, перечисленные в этом разделе. Они являются обязательными и должны быть включены в файл kickstart.

auth --enableshadow --passalgo=sha512

Указывает параметры проверки подлинности для физического сервера продукта Кибер Инфраструктура.

autopart --type=lvm

Автоматически разбивает на разделы системный диск, то есть sda. Этот параметр должен следовать за clearpart --all.

Остальные диски будут разбиты на разделы автоматически при создании кластера.

bootloader

Указывает параметры установки загрузчика.

clearpart --all

Удаляет все разделы с распознанных дисков.

Предупреждение
Этот параметр стирает все данные на всех дисках, доступных программе установки!

keyboard <layout>

Задает тип клавиатуры компьютера.

lang <lang>

Задает язык, используемый во время установки, и язык по умолчанию для установленной системы.

logvol

Создает логический том для группы управления логическими томами (LVM).

network <options>

Настраивает сетевые устройства и создает объединенные интерфейсы и интерфейсы VLAN.

raid

Создает том программного RAID-массива.

part

Создает раздел на сервере.

Примечание
Размер раздела /boot должен быть не меньше 1 ГБ.

rootpw --iscrypted <passwd>

Задает пароль привилегированного пользователя для сервера. Значение представляет собой хеш пароля, полученный с помощью алгоритма, указанного в параметре --passalgo. Например, чтобы создать из пароля хеш SHA-512, выполните команду python -c 'import crypt; print(crypt.crypt("yourpassword"))'.

selinux --disabled

Отключает систему SElinux, поскольку она мешает правильной работе виртуализации.

services --enabled="chronyd"

Включает синхронизацию времени по протоколу NTP.

timezone <timezone>

Задает часовой пояс системы. Чтобы просмотреть список часовых поясов, выполните команду timedatectl list-timezones.

volgroup

Создает группу управления логическими томами (LVM).

zerombr

Инициализирует диски с недопустимыми таблицами разделов.

Предупреждение
Этот параметр стирает все данные на всех дисках, доступных программе установки!

5.3.2 Сценарии kickstart

Указав параметры, добавьте в файл kickstart сценарии для установки группы обязательных пакетов и компонентов кластера.

Установка обязательных пакетов

В теле сценария %packages укажите группу пакетов hci для установки на сервере.

```
%packages
@^hci
%end
```

Установка обязательных компонентов на главный сервер

Чтобы выполнить развертывание главного сервера, необходимы панель администрирования и компонента хранилища. Эти компоненты можно настроить во время установки продукта. Однако таким образом будут раскрыты пароль суперадминистратора и токен хранилища в файле kickstart. Чтобы избежать этого, добавьте скрипт %addon com_vstorage в файл kickstart:

```
%addon com_vstorage --management --internal-iface=<private_iface> --external-iface=<public_
iface> --password=<password>
%end
```

где:

- <password> — пароль учетной записи суперадминистратора для панели управления;
- <private_iface> — имя интерфейса частной сети (который вы бы выбрали для сети управления при ручной установке);
- <public_iface> — имя интерфейса общедоступной сети (который вы бы выбрали для сети панели администратора при ручной установке).

Если вы не хотите использовать конфиденциальную информацию в файле kickstart, настройте компоненты после установки. Для этого добавьте сценарий %addon com_vstorage в файл kickstart следующим образом.

```
%addon com_vstorage --management --bare
%end
```

Установка обязательных компонентов на подчиненный сервер

Для развертывания подчиненных серверов требуется только компонент хранилища, который установлен по умолчанию. Однако чтобы добавить узел в инфраструктуру, вам потребуется токен хранилища и IP-адрес сервера управления.

Получите токен и адрес сервера управления на панели администрирования.

1. Войдите на панель администрирования по ее IP-адресу и порту 8888.
   При необходимости добавьте сертификат безопасности в исключения браузера.
2. На панели администрирования откройте раздел **Инфраструктура** > **Серверы** и нажмите **Подключить сервер**, чтобы вызвать экран с адресом сервера управления и токеном.

Эти компоненты нужны для последующей регистрации сервера на панели администрирования. Их можно настроить во время установки продукта. Однако таким образом токен хранилища будет

раскрыт в файле kickstart. Чтобы избежать этого, добавьте скрипт %addon com_vstorage в файл kickstart.

```
%addon com_vstorage --storage --token=<token> --mgmt-node-addr=<MN_IP_address>
%end
```

где:

- <token> – это полученный токен;
- <MN_IP_address> – это полученный адрес сервера управления.

Если вы не хотите использовать конфиденциальную информацию в файле kickstart, выполните регистрацию сервера после установки.

5.3.3 Пример файла kickstart

Ниже приведен пример файла kickstart, который можно использовать для установки и настройки продукта Кибер Инфраструктура в автоматическом режиме. На базе этого примера вы можете создать собственные файлы kickstart.

Внимание
Этот файл kickstart указывает программе установки очистить от данных и автоматически разбить на разделы все диски, которые распознаются программой. Не забудьте отсоединить все диски с нужной информацией перед установкой!

```
# Use the SHA-512 encryption for user passwords and enable shadow passwords.
auth --enableshadow --passalgo=sha512
# Use the US English keyboard.
keyboard --vckeymap=us --xlayouts='us'
# Use English as the installer language and the default system language.
lang en_US.UTF-8
# Specify the encrypted root password for the node.
rootpw --iscrypted xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
# Disable SELinux.
selinux --disabled
# Enable time synchronization via NTP.
services --enabled="chronyd"
# Set the system time zone.
timezone Europe/Moscow
# Specify a hostname for the node.
# NOTE: The only way to change the host name later is via the technical support.
network --hostname=<hostname>
# Configure network interfaces via DHCP.
network --device=<iface1> --activate
network --device=<iface2> --activate
# Alternatively, assign static addresses to network interfaces.
#network --device=<iface1> --activate --bootproto=static --ip=<IP_addr> \
#--netmask=<mask> --gateway=<gw> --nameserver=<ns1>[,<ns2>,...]
#network --device=<iface2> --activate --bootproto=static --ip=<IP_addr> \
#--netmask=<mask> --gateway=<gw> --nameserver=<ns1>[,<ns2>,...]
```

```
# If needed, uncomment and specify network interfaces to create a bond.
#network --device=bond0 --bondslaves=<iface1>,<iface2> \
#--bondopts=mode=balance-xor,miimon=100,xmit_hash_policy=layer3+4
# Erase all partitions from all recognized disks.
# WARNING: Destroys data on all disks that the installer can reach!
clearpart --all --initlabel
zerombr
# Automatically partition the system disk, which is 'sda'.
autopart --type=lvm
# Install the required packages on the node.
%packages
@^hci
%end
# Uncomment to install the admin panel and storage components.
# Specify an internal interface for the management network and
# an external interface for the admin panel network.
#%addon com_vstorage --management --internal-iface=eth0 \
#--external-iface=eth1 --password=xxxxxxxxx
#%end
# Uncomment to install the storage component. To register the node,
# specify the token as well as the IP address of the admin panel.
#%addon com_vstorage --storage --token=xxxxxxxxx --mgmt-node-addr=10.37.130.1
#%end
```

5.3.3.1 Пример системного раздела на программном массиве RAID1

Рекомендуется создавать массив RAID1 из дисков одного размера, поскольку размер тома будет соответствовать размеру наименьшего диска.

Чтобы создать системный раздел на томе программного массива RAID1, не используйте параметр autopart в файле kickstart. Следующий пример для сервера на базе BIOS разбивает на разделы диски sda и sdb, собирает программный массив RAID1 и создает расширяемый том подкачки и корневые тома LVM:

```
# Create partitions on sda.
part biosboot   --size=1     --ondisk=sda --fstype=biosboot
part raid.sda1  --size=1024   --ondisk=sda --fstype=ext4
part raid.sda2  --size=101376 --ondisk=sda --grow
# Create partitions on sdb.
part biosboot   --size=1     --ondisk=sdb --fstype=biosboot
part raid.sdb1  --size=1024   --ondisk=sdb --fstype=ext4
part raid.sdb2  --size=101376 --ondisk=sdb --grow
# Create software RAID1 from sda and sdb.
raid /boot --level=RAID1 --device=md0 --fstype=ext4 raid.sda1 raid.sdb1
raid pv.01 --level=RAID1 --device=md1 --fstype=ext4 raid.sda2 raid.sdb2
# Make LVM volumes for swap and root partitions.
volgroup vgsys pv.01
logvol swap --fstype=swap --name=swap --vgname=vgsys --recommended
logvol /    --fstype=ext4 --name=root --vgname=vgsys --size=10240 --grow
# Set the RAID device md0 as the first drive in the BIOS boot order.
```

```
bootloader --location=mbr --boot-drive=sda --driveorder=md0
bootloader --location=mbr --boot-drive=sdb --driveorder=md0
```

Для установки на серверах на базе EFI укажите раздел /boot/efi вместо biosboot.

```
part /boot/efi --size=200 --ondisk={sda|sdb} --fstype=efi
```

5.4 Установка в ручном режиме

Ограничения

- Жесткие диски с черепичной магнитной записью (SMR) нельзя использовать для установки системы, поэтому программа установки не отображает их.

Предварительные требования

- Загрузочный носитель USB, виртуальный диск IPMI или PXE-сервер, подготовленный в соответствии с инструкциями в разделе "Подготовка загрузочного носителя" на странице 81.
- Время синхронизировано посредством NTP на всех серверах одного кластера, и серверы имеют доступ к серверу NTP.
- Если вам нужно изменить MTU по умолчанию, он должен быть настроен на аппаратном обеспечении сети.

Установка в ручном режиме

1. Настройте сервер на загрузку с выбранного носителя.
2. Загрузите сервер и дождитесь **экрана приветствия**.
3. На **экране приветствия** выберите **Установить** Кибер Инфраструктура.
4. На шаге 1 прочитайте и примите условия лицензионного соглашения с конечным пользователем.
5. На шаге 2 выполните настройку сети.
   a. Укажите уникальное имя хоста: либо полное доменное имя (**<hostname>.<domainname>**), либо краткое имя (**<hostname>**).

      Внимание
      Позже можно будет изменить имя хоста, только обратившись в техническую поддержку.

   b. Настройте сетевые карты. Обычно сеть настраивается автоматически (через DHCP). Если требуется ручная настройка, выберите сетевую карту, нажмите **Configure...** (Настроить...) и укажите необходимые параметры.
   c. Настройте MTU для всех карт. По умолчанию для этого параметра установлено значение 1500, однако рекомендуется увеличить его до 9000.

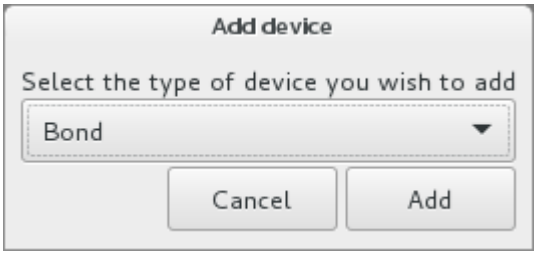
Внимание
Значение MTU должно быть одинаковым по всей сети.

- При интеграции Кибер Инфраструктура в существующую сеть, используйте значение MTU этой сети.
- При развертывании Кибер Инфраструктура в новой сети установите рекомендуемое значение MTU, равное 9000.

d. [Необязательно] В соответствии с сетевыми рекомендациями можно создать интерфейсы виртуальных локальных сетей (VLAN) и объединенные интерфейсы, чтобы повысить уровень безопасности и производительности сети.

- Создание объединенных соединений
  Объединенные соединения обеспечивают более высокую пропускную способность, чем отдельные сетевые карты, и улучшенную избыточность данных.

  i. Нажмите кнопку плюс внизу страницы, выберите **Bond** (Агрегация) из раскрывающегося списка и нажмите **Add** (Добавить).

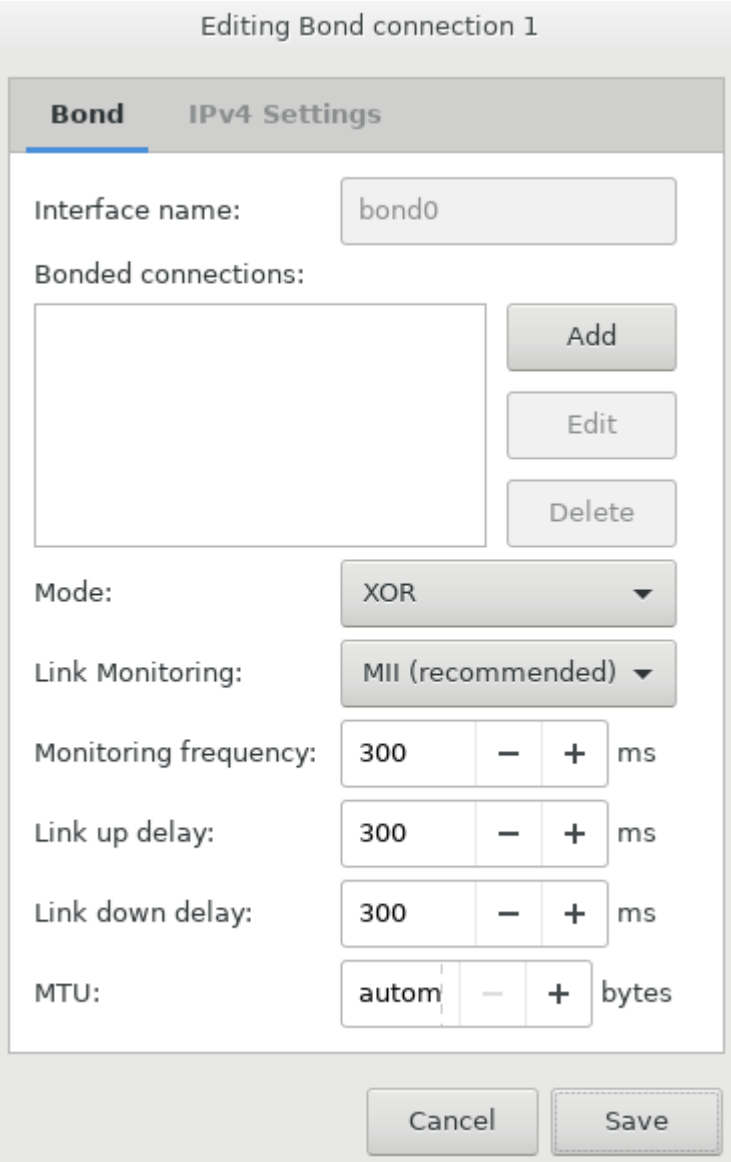


  ii. В окне **Editing Bond connection<N>** (Изменение объединенного соединения) установите следующие параметры для объединенного интерфейса Ethernet:

  A. **Mode** (Режим) согласно требованиям сети

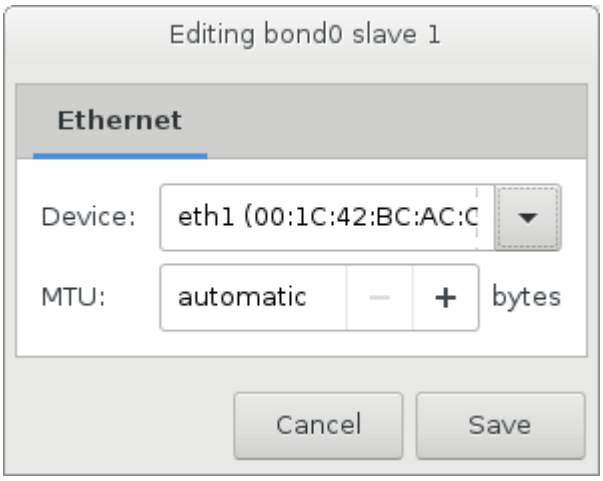
  B. **Link Monitoring** (Мониторинг каналов) – **MII (рекомендуется)**

  C. **Monitoring frequency** (Частота мониторинга), **Link up delay** (Задержка при установке соединения) и **Link down delay** (Задержка при разрыве соединения) – 300



iii. В разделе **Bonded connections** (Объединенные соединения) на вкладке **Bond** (Агрегация) нажмите **Добавить**.

iv. В окне **Editing bond<N> slave<N>** (Изменение подчиненного интерфейса агрегации) выберите сетевой интерфейс для объединения в списке **Device** (Устройство).



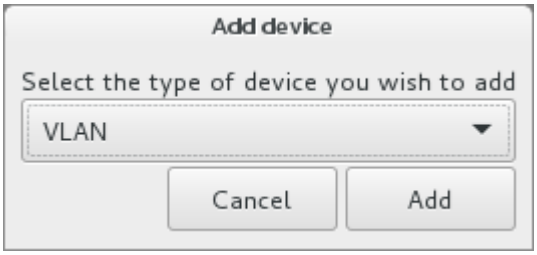
v. При необходимости настройте значение MTU и нажмите кнопку **Save** (Сохранить).

vi. Повторите шаги 3-5 для каждого сетевого интерфейса, который необходимо добавить в объединенное соединение.

vii. При необходимости настройте параметры IPv4 и нажмите кнопку **Save** (Сохранить).

- Создание интерфейсов VLAN

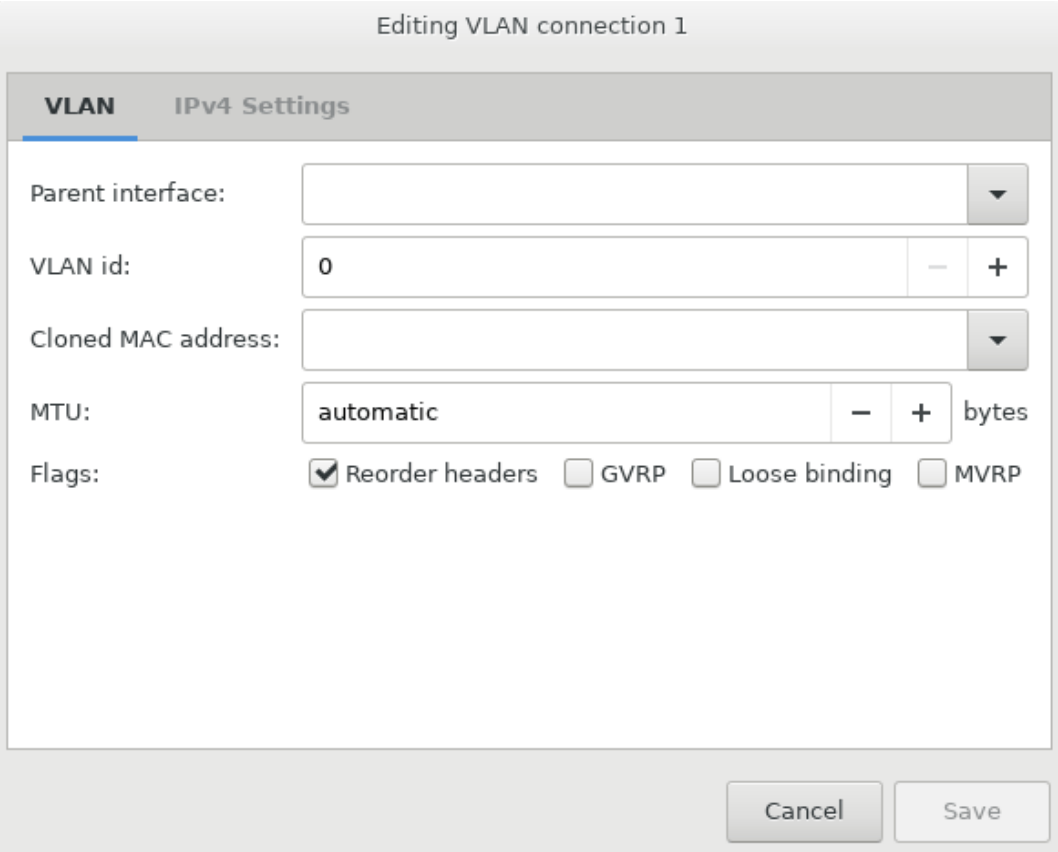
  i. Нажмите кнопку плюс внизу страницы, выберите **VLAN** и нажмите **Add** (Добавить).



  ii. В окне **Editing VLAN connection<N>** (Изменение соединения VLAN) выполните следующие действия.

    A. В раскрывающемся списке **Родительский интерфейс** выберите физический адаптер или объединенное соединение, на базе которого будет создан адаптер VLAN.

    B. Укажите идентификатор адаптера VLAN в поле **VLAN ID**. Значение должно находиться в диапазоне 1-4094.

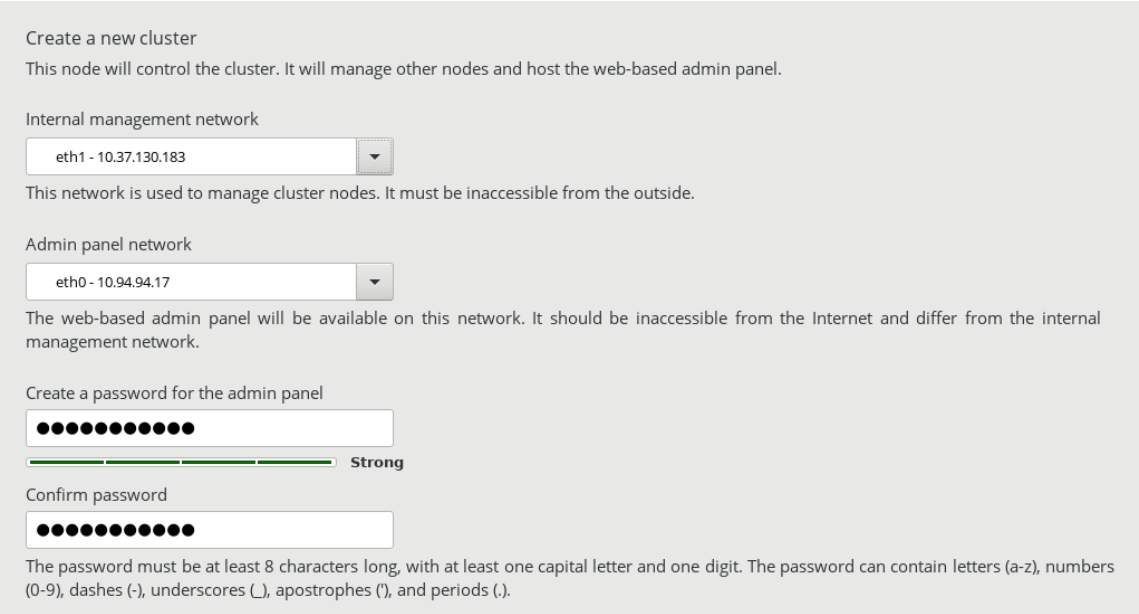


iii. При необходимости настройте параметры MTU и IPv4 и нажмите кнопку **Save** (Сохранить).

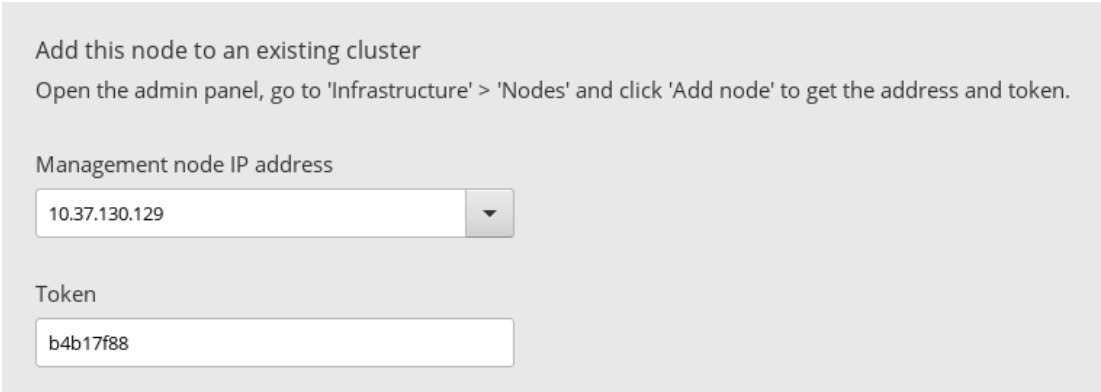
6. На шаге 3 выберите часовой пояс. Дата и время будут заданы посредством NTP. Для выполнения синхронизации потребуется подключение к Интернету.

Внимание
Настоятельно рекомендуется использовать часовой пояс UTC.

7. На шаге 4 необходимо указать тип устанавливаемого сервера.
   - Для установки на главный сервер
     Главный сервер, также называемый сервером управления, – это первый узел в инфраструктуре. На нем будут размещены сервисы управления кластером и панель администратора. Он также выступит в качестве сервера хранения данных. Только главный сервер является необходимым для установки.
     a. Выберите **Yes, create a new cluster** (Да, создать новый кластер).
     b. В списке **Internal management network** (Сеть управления системными сервисами) выберите сетевой интерфейс для управления системными сервисами и настройки.
     c. В списке **Admin panel network** (Сеть панели администратора) выберите сетевой интерфейс для доступа к панели управления.
     d. Создайте и подтвердите пароль для учетной записи суперадминистратора панели управления.



- Для установки на подчиненный сервер
  Подчиненный сервер – это сервер, который добавляется в уже существующую инфраструктуру. Такие серверы будут использоваться для сервисов, связанных с хранением данных, и будут добавлены в инфраструктуру во время установки.
  a. Выберите **No, add it to an existing cluster** (Нет, добавить сервер в существующий кластер).
  b. Получите токен и адрес сервера управления на панели администрирования.
     i. Войдите на панель администрирования по ее IP-адресу и порту 8888.
        При необходимости добавьте сертификат безопасности в исключения браузера.
     ii. На панели администрирования откройте раздел **Инфраструктура** > **Серверы** и нажмите **Подключить сервер**, чтобы вызвать экран с адресом сервера управления и токеном.
     Один токен можно использовать для параллельного развертывания нескольких подчиненных серверов. При необходимости можно создать новый токен, при этом старый маркер станет недействительным.
  c. На экране установки выберите частный IP-адрес сервера управления и введите токен.

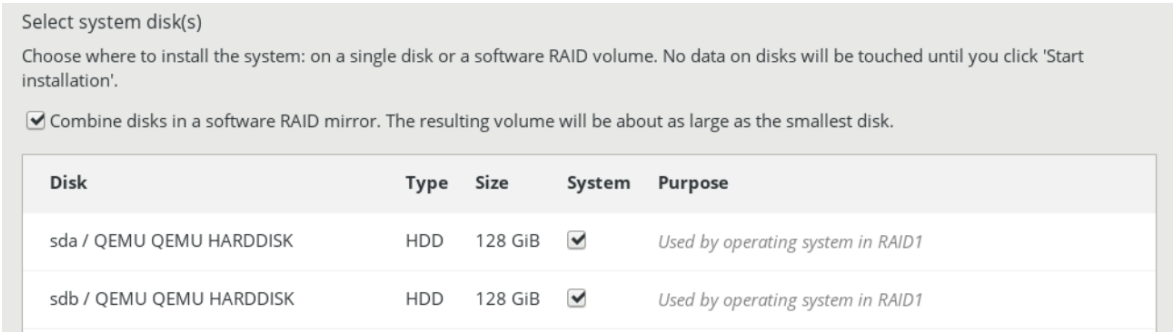


- Чтобы зарегистрировать сервер на панели администратора вручную после установки, выберите **Skip cluster configuration** (Пропустить настройку кластера).

8. На шаге 5 необходимо выбрать диск для операционной системы. Диску будет назначена дополнительная роль **System** (Система), хотя его можно будет настроить для хранения данных на панели администратора.

   Предупреждение
   Вся информация на дисках, распознанных программой установки, будет стерта.

   Чтобы обеспечить высокую производительность и доступность системного диска, можно создать программный массив RAID.
   Для этого установите флажок RAID и выберите как минимум два диска. Рекомендуется создавать массив RAID из дисков одного размера, поскольку размер тома будет соответствовать размеру наименьшего диска.

9. На шаге 6 укажите, нужно ли подготовить сервер для поддержки быстрой сети DPDK для виртуальных машин. Подготовку также можно выполнить после установки (см. раздел "Настройка быстрой сети DPDK для виртуальных машин" на странице 194).

   Примечание
   Шаг отображается только тогда, когда у сервера есть хотя бы один сетевой интерфейс, поддерживающий DPDK.

10. На шаге 7 введите и подтвердите пароль для учетной записи пользователя root и нажмите **Start installation** (Начать установку).

После завершения установки сервер автоматически перезагрузится. IP-адрес панели администрирования будет отображен в строке приветствия.

Что дальше?

- После развертывания главного сервера можно приступить к развертыванию нужного количества подчиненных серверов.
- Убедитесь, что все серверы отображаются на панели администратора на экране **Infrastructure** > **Nodes** (Инфраструктура > Серверы) со статусом **Unassigned** (Без назначения), и перейдите к созданию кластера хранилища, как описано в разделе "Развертывание и настройка" на странице 108.
- Если вы пропустили настройку кластера на шаге 4 и хотите добавить сервер без назначения вручную, выполните следующие действия.

- Настройка главного сервера
  1. На сервере выполните следующую команду от имени привилегированного пользователя, чтобы настроить компонент панели администрирования:

     ```
     echo <password> | /usr/libexec/vstorage-ui-backend/bin/configure-backend.sh -i <private_iface> -x <public_iface>
     ```

     где:
     - <password> – пароль для учетной записи суперадминистратора панели управления;
     - <private_iface> – имя частного сетевого интерфейса для управления системными сервисами и настройки;
     - <public_iface> – имя внешнего сетевого интерфейса для доступа к панели управления.
  2. Запустите сервис панели администрирования на сервере.

     ```
     # systemctl start vstorage-ui-backend
     ```
  3. Зарегистрируйте сервер на панели администрирования.

     ```
     # /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <MN_IP_address> -x <public_iface>
     ```

     где:
     - <MN_IP_address> – IP-адрес частного сетевого интерфейса сервера;
     - <public_iface> – имя внешнего сетевого интерфейса.

  Теперь можно приступить к развертыванию подчиненных серверов.
- Настройка подчиненного сервера
  Выполните следующий скрипт на сервере, чтобы зарегистрировать сервер на панели администрирования:

  ```
  # /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <MN_IP_address> -t <token>
  ```

  где:
  - <MN_IP_address> – IP-адрес частного сетевого интерфейса на сервере с панелью администрирования;
  - <token> – токен, полученный на панели администрирования.

5.5 Установка в автоматическом режиме

Если планируется автоматическая установка продукта Кибер Инфраструктура, можно использовать файл kickstart. Он автоматически отправит в программу установки параметры, которые выбираются вручную при обычной установке.

Предварительные требования

- Сервер PXE подготовлен в соответствии с инструкциями в разделе "Настройка PXE-сервера" на странице 87.
- Создан файл kickstart с использованием параметров и скриптов, перечисленных в разделе "Создание файла kickstart" на странице 91.

Установка в автоматическом режиме

1. Предоставьте доступ к файлу kickstart для всех компонентов сети.
   a. Скопируйте файл kickstart в тот же каталог на HTTP-сервере, где расположены установочные файлы продукта Кибер Инфраструктура (например, в /var/www/html/stor).
   b. Добавьте следующую строку в файл /tftpboot/pxelinux.cfg/default на PXE-сервере:

      ```
      inst.ks=<HTTP_server_address>/<path_to_kickstart_file>
      ```

      В системах на базе EFI файл, который необходимо изменить, называется /tftpboot/pxelinux.cfg/efidefault или /tftpboot/pxelinux.cfg/<PXE_server_IP_address>.

      Например, если HTTP-сервер имеет IP-адрес 198.123.123.198, для каталога DocumentRoot установлено значение /var/www/html, а полный путь к файлу kickstart на этом сервере — /var/www/html/stor/ks.cfg, то файл default может выглядеть следующим образом.

      ```
      default menu.c32
      prompt 0
      timeout 100
      ontimeout ASTOR
      menu title Boot Menu
      label ASTOR
            menu label Install
            kernel vmlinuz
            append initrd=initrd.img ip=dhcp inst.repo=http://198.123.123.198/stor
      inst.ks=http://198.123.123.198/stor/ks.cfg
      ```

2. Настройте сервер на загрузку с выбранного носителя.
3. Загрузите сервер и дождитесь **экрана приветствия**.
4. На **экране приветствия** выберите **Install Кибер Инфраструктура** (Установить) и нажмите клавишу **E**, чтобы изменить пункт меню.
5. Добавьте расположение файла kickstart в строку linux /images/pxeboot/vmlinuz и нажмите **Ctrl+X**, например:

   ```
   linux /images/pxeboot/vmlinuz inst.stage2=hd:LABEL=<ISO_img> quiet ip=dhcp logo.nologo=1
   inst.ks=<URL>
   ```

Установка будет выполнена автоматически. После ее завершения сервер автоматически перезагрузится. IP-адрес панели администрирования будет отображен в строке приветствия.

Что дальше?

- После установки на главный сервер
  Если вы установили компоненты панели администратора и хранилища, не раскрывая пароль суперадминистратора и токен хранилища в файле kickstart, выполните следующие действия.
  1. На сервере выполните следующую команду от имени привилегированного пользователя, чтобы настроить компонент панели администрирования:

     ```
     echo <password> | /usr/libexec/vstorage-ui-backend/bin/configure-backend.sh -i <private_iface> -x <public_iface>
     ```

     где:
     - <password> – пароль для учетной записи суперадминистратора панели управления;
     - <private_iface> – имя частного сетевого интерфейса для управления системными сервисами и настройки;
     - <public_iface> – имя внешнего сетевого интерфейса для доступа к панели управления.
  2. Запустите сервис панели администрирования на сервере.

     ```
     # systemctl start vstorage-ui-backend
     ```
  3. Зарегистрируйте сервер на панели администрирования.

     ```
     # /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <MN_IP_address> -x <public_iface>
     ```

     где:
     - <MN_IP_address> – IP-адрес частного сетевого интерфейса сервера;
     - <public_iface> – имя внешнего сетевого интерфейса.

  Теперь можно приступить к развертыванию подчиненных серверов.
- После установки на подчиненный сервер
  Если вы установили компоненты панели администратора и хранилища, не раскрывая пароль суперадминистратора и токен хранилища в файле kickstart, выполните на сервере следующий скрипт, чтобы зарегистрировать сервер на панели администратора:

  ```
  # /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <MN_IP_address> -t <token>
  ```

  где:
  - <MN_IP_address> – IP-адрес частного сетевого интерфейса на сервере с панелью администрирования;
  - <token> – токен, полученный на панели администрирования.
- Убедитесь, что все серверы отображаются на панели администратора на экране **Infrastructure** > **Nodes** (Инфраструктура > Серверы) со статусом **Unassigned** (Без назначения), и перейдите к созданию кластера хранилища, как описано в разделе "Развертывание и настройка" на странице 108.

5.6 Поиск и устранение неисправностей установки

В этой главе описываются способы устранения неисправностей установки продукта Кибер Инфраструктура.

5.6.1 Установка в базовом графическом режиме

Если программе установки не удается загрузить нужный драйвер для графического адаптера, можно попробовать установить продукт Кибер Инфраструктура в базовом графическом режиме, однако в этом режиме могут возникнуть проблемы с пользовательским интерфейсом. Например, некоторые элементы могут не помещаться на экране.

Сам процесс не отличается от установки в стандартном графическом режиме.

Выбор базового графического режима

На экране приветствия выберите **Troubleshooting->** (Поиск и устранение неисправностей), а затем**Install in basic graphics mode** (Установка в базовом графическом режиме).

5.6.2 Загрузка в режиме аварийного восстановления

При возникновении проблем с системой можно загрузить ее в режиме аварийного восстановления для поиска и устранения неисправностей. При входе в этот режим установленный продукт Кибер Инфраструктура подключается в каталог /mnt/sysimage. Можно перейти в этот каталог и внести необходимые изменения в систему.

Чтобы войти в режим аварийного восстановления

1. Загрузите систему из образа дистрибутива.
2. На экране приветствия нажмите **Troubleshooting** (Поиск и устранение неисправностей) -> **Rescue system** (Восстановить систему).
3. После того как Кибер Инфраструктура загрузится в аварийном режиме, нажмите **Ctrl+D** для загрузки среды аварийного восстановления.
4. В среде аварийного восстановления можно выбрать один из следующих вариантов:
   - Продолжить (нажмите **1**). Подключение установленного продукта Кибер Инфраструктура в режиме чтения и записи в каталог /mnt/sysimage.
   - Подключить только для чтения (нажмите **2**). Подключение установленного продукта Кибер Инфраструктура в режиме только для чтения в каталог /mnt/sysimage.
   - Пропустить и перейти к оболочке (нажмите **3**). Загрузка командной оболочки, если файловую систему нельзя подключить, например в случае, если она повреждена.
   - Выйти (Перезагрузить) (нажмите **4**). Перезагрузка сервера.
5. При выборе любого варианта, кроме **4**, появится приглашение оболочки. Выполните в ней команду chroot /mnt/sysimage, чтобы сделать каталог установки продукта Кибер Инфраструктура корневым. Теперь можно выполнять другие команды и попытаться исправить возникшие проблемы.

6. Исправив проблему, выполните команду exit для выхода из среды chroot, а затем команду reboot для перезапуска системы.

6 Развертывание и настройка

Рабочий процесс Кибер Инфраструктура включает настройку инфраструктуры и подготовку служб к работе. После настройки инфраструктуры у вас будет кластер хранилища данных с настроенной сетью и узлом управления с высокой доступностью. Поверх кластера хранилища можно развернуть и настроить различные службы для подготовки их для работы с конечными пользователями. Можно подготовить хранилище резервных копий, блочное хранилище, хранилище объектов и пространство хранения файлов, а также вычислительные ресурсы. Все эти задачи можно выполнить либо на панели администрирования, либо с помощью инструмента командной строки vinfra.

Предварительные требования

- Кибер Инфраструктура должен быть установлен на каждом из серверов, как описано в разделе "Установка" на странице 81.

Обзор настройки инфраструктуры

1. Если вы планируете использовать интерфейс командной строки, предоставьте ваши учетные данные для инструмента vinfra.
2. Настройте сети в соответствии со службой, которую необходимо подготовить к работе.
3. Настройте сетевые интерфейсы узлов.
4. Настройте внешний сервер DNS.
5. При необходимости включите RDMA.
6. Разверните кластер хранилища.
7. Если у вас имеется три узла или более в кластере, включите высокую доступность для узла управления.

После настройки инфраструктуры можно переходить к подготовке к работе хранилища резервных копий, блочного хранилища, хранилища объектов или пространства хранения файлов, а также вычислительных ресурсов.

6.1 Использование интерфейса командной строки

Для управления продуктом Кибер Инфраструктура из консоли и автоматизации подобных задач можно использовать инструмент командной строки vinfra. Чтобы посмотреть список всех поддерживаемых команд и их описания, запустите vinfra help. Чтобы получить справку по конкретной команде, выполните команду vinfra <command> help или vinfra <command> --help.

Обратите внимание, что следующие операции нельзя выполнять из командной строки:

- Настройка пользовательских путей для служб продукта Кибер Инфраструктура, в частности:
  - Создание кластеров S3 только в /mnt/vstorage/vols/s3
  - Создание целей iSCSI только в /mnt/vstorage/vols/iscsi

- Монтирование кластеров или изменение параметров монтирования кластера
- Настройка системы безопасности с помощью firewall-cmd
- Переименование сетевых подключений
- Управление службами метаданных и хранения
- Управление разделами, LVM или программным RAID
- Изменение файлов в каталогах /mnt/vstorage/vols и /mnt/vstorage/webcp/backup
- Настройка кодирования или репликации корня кластера

6.1.1 Предоставление учетных данных для vinfra

Инструмент vinfra требует следующей информации:

- IP-адрес или имя хоста узла управления (по умолчанию установлено backend-api.svc.vstoragedomain)
- Имя пользователя (по умолчанию admin)
- Пароль (указывается при установке продукта Кибер Инфраструктура)
- Доменное имя для аутентификации (по умолчанию Default)
- Идентификатор проекта для аутентификации (по умолчанию admin)

Данная информация может быть предоставлена с помощью следующих параметров командной строки с каждой командой:

- --vinfra-portal <portal>
- --vinfra-username <username>
- --vinfra-password <password>
- --vinfra-domain <domain>
- --vinfra-project <project>

Также вы можете указать собственные учетные данные, установив следующие переменные среды (например, в вашем ~/.bash_profile): VINFRA_PORTAL, VINFRA_USERNAME, VINFRA_PASSWORD, VINFRA_DOMAIN и VINFRA_PROJECT. В этом случае вы сможете запустить этот инструмент без вышеупомянутых параметров командной строки.

Поскольку vinfra обычно запускается с узла управления от имени администратора, единственная переменная, которую нужно установить, – это пароль. Например:

```
# export VINFRA_PASSWORD=12345
```

Если вы установили vinfra на удаленную машину и/или запустили ее от имени другого системного администратора, вам нужно будет установить VINFRA_PORTAL и/или VINFRA_USERNAME на этой машине в дополнение к VINFRA_PASSWORD.

Кроме того, если вы хотите аутентифицироваться в другом проекте и/или домене, вам нужно будет установить еще две переменные среды: VINFRA_PROJECT и/или VINFRA_DOMAIN.

6.1.2 Управление заданиями vinfra

Программа командной строки vinfra выполняет некоторые команды сразу, а для других команд (выполнение которых может занять некоторое время) создает системные задания, которые ставятся в очередь. Примеры действий, выполняемых посредством заданий: создание кластера хранилища или вычислительного кластера и добавление в него серверов.

Для отслеживания заданий, выполняемых программой vinfra, используйте команды vinfra task list и vinfra task show. Например:

```
# vinfra task list
+---------------+---------+-----------------------------------------------+
| task_id       | state   | name                                          |
+---------------+---------+-----------------------------------------------+
| 8fc27e7a-<...> | success | backend.tasks.cluster.CreateNewCluster  |
| e61377db-<...> | success | backend.tasks.disks.ApplyDiskRoleTask   |
| a005b748-<...> | success | backend.tasks.node.AddNodeInClusterTask |
+---------------+---------+-----------------------------------------------+
# vinfra task show 8fc27e7a-ba73-471d-9134-e351e1137cf4
+---------+---------------------------------------+
| Field   | Value                                 |
+---------+---------------------------------------+
| args    | - stor1                               |
|         | - 7ffa9540-5a20-41d1-b203-e3f349d62565 |
|         | - null                                |
|         | - null                                |
| kwargs  | {}                                    |
| name    | backend.tasks.cluster.CreateNewCluster |
| result  | cluster_id: 1                         |
| state   | success                               |
| task_id | 8fc27e7a-ba73-471d-9134-e351e1137cf4   |
+---------+---------------------------------------+
```

6.2 Настройка сетей

По умолчанию имеется две предварительно настроенные сети, которые называются **Внешняя (Public)** и **Частная (Private)** в соответствии с типом. Их можно рассматривать как шаблоны, которые можно изменять для создания нужной (рекомендуемой) конфигурации.

6.2.1 Настройка сетей для хранилища резервных копий

Предварительные требования

- Топология вашей сети должна соответствовать требованиям, приведенным в разделе "Требования к сети для хранилища резервных копий" на странице 73.

- Четкое понимание концепции "Типы трафика" на странице 42.

Рекомендуемая сетевая конфигурация для Backup Gateway включает две сети: для внутреннего и внешнего трафика. Можно оставить без изменений стандартные сети **Внешняя** и **Частная**. В этом случае следует назначить этим сетям типы трафика в соответствии со следующей таблицей.

Рекомендуемая сетевая конфигурация для Backup Gateway

Сеть	Типы трафика
Частная (Private)	Хранилище, Управление системными сервисами, OSTOR внутр., Резервные копии (ABGW) внутр.
Внешняя (Public)	Панель администрирования, SSH, S3 внешн., iSCSI, NFS, Резервные копии (ABGW) внешн.

Чтобы создать конфигурацию сети для хранилища резервных копий

Панель администратора

1. Проверьте конфигурацию сети на экране **Инфраструктура** > **Сети**.
2. Если планируется использовать RDMA поверх InfiniBand, переведите тип трафика **Хранилище** в выделенную сеть и назначьте эту сеть интерфейсу IB.
3. Настройте сетевые интерфейсы на узлах, которые планируется присоединить к хранилищу резервных копий.

Интерфейс командной строки

Проверьте конфигурацию сети с помощью следующей команды:

```
# vinfra cluster network list -c id -c name -c traffic_types
+--------------------------------------+---------+-------------------------------------------------------------------------+
| id                                   | name    | traffic_types                                                           |
+--------------------------------------+---------+-------------------------------------------------------------------------+
| f50605a3-64f4-4f0c-b50e-9481ec221c72 | Private | Backup (ABGW) private,Internal management,OSTOR private,Storage |
| 955041d4-b059-47a1-ba4c-0be117e8cbd2 | Public  | Backup (ABGW) public,iSCSI,NFS,S3 public,Admin panel,SSH        |
+--------------------------------------+---------+-------------------------------------------------------------------------+
```

6.2.2 Настройка сетей для блочного хранилища

Предварительные требования

- Четкое понимание концепций из раздела "Типы трафика" на странице 42.

Чтобы создать конфигурацию сети для блочного хранилища

Панель администратора

1. Перейдите на экран **Инфраструктура** > **Сети** и убедитесь, что в вашей инфраструктуре имеется внешняя сеть с типом трафика **iSCSI**.

2. Если планируется использовать RDMA поверх InfiniBand, переведите тип трафика **Хранилище** в выделенную сеть и назначьте эту сеть интерфейсу IB.
3. Настройте сетевые интерфейсы на узлах, которые планируется добавить в группу целевых устройств iSCSI.

Интерфейс командной строки

Проверьте конфигурацию сети с помощью следующей команды:

```
# vinfra cluster network list -c id -c name -c traffic_types
+--------------------------------------+---------+-------------------------------------------------------------------------+
| id                                   | name    | traffic_types                                                           |
+--------------------------------------+---------+-------------------------------------------------------------------------+
| f50605a3-64f4-4f0c-b50e-9481ec221c72 | Private | Backup (ABGW) private,Internal management,OSTOR private,Storage |
| 955041d4-b059-47a1-ba4c-0be117e8cbd2 | Public  | Backup (ABGW) public,iSCSI,NFS,S3 public,Admin panel,SSH        |
+--------------------------------------+---------+-------------------------------------------------------------------------+
```

6.2.3 Настройка сетей для хранилища объектов

Предварительные требования

- Четкое понимание концепции "Типы трафика" на странице 42.

Чтобы создать конфигурацию сети для хранилища объектов

Панель администратора

1. Перейдите на экран **Инфраструктура** > **Сети** и убедитесь, что в вашей инфраструктуре имеются следующие сети:
   - Частная сеть с типом трафика **OSTOR внутр.**
   - Внешняя сеть с типом трафика **S3 внешн.**
2. Убедитесь, что доступ к внешней сети для узлов S3 балансируется внешним балансировщиком нагрузки DNS.
3. Если планируется использовать RDMA поверх InfiniBand, переведите тип трафика **Хранилище** в выделенную сеть и назначьте эту сеть интерфейсу IB.
4. Настройте сетевые интерфейсы на узлах, которые планируется присоединить к кластеру S3.

Интерфейс командной строки

Проверьте конфигурацию сети с помощью следующей команды:

```
# vinfra cluster network list -c id -c name -c traffic_types
+--------------------------------------+---------+-------------------------------------------------------------------------+
| id                                   | name    | traffic_types                                                           |
+--------------------------------------+---------+-------------------------------------------------------------------------+
| f50605a3-64f4-4f0c-b50e-9481ec221c72 | Private | Backup (ABGW) private,Internal management,OSTOR private,Storage |
```

```
| 955041d4-b059-47a1-ba4c-0be117e8cbd2 | Public  | Backup (ABGW) public,iSCSI,NFS,S3
public,Admin panel,SSH       |
+--------------------------------------+---------+-------------------------------------------------------------------------+
```

6.2.4 Настройка сетей для файлового хранилища

Предварительные требования

- Четкое понимание концепции "Типы трафика" на странице 42.

Чтобы создать конфигурацию сети для файлового хранилища

Панель администратора

1. Перейдите на экран **Инфраструктура** > **Сети** и убедитесь, что в вашей инфраструктуре имеются следующие сети:
   - Частная сеть с типом трафика **OSTOR внутр.**
   - Внешняя сеть с типом трафика **NFS внешн.**
2. Если планируется использовать RDMA поверх InfiniBand, переведите тип трафика **Хранилище** в выделенную сеть и назначьте эту сеть интерфейсу IB.
3. Настройте сетевые интерфейсы на узлах, которые планируется присоединить к кластеру NFS.

Интерфейс командной строки

Проверьте конфигурацию сети с помощью следующей команды:

```
# vinfra cluster network list -c id -c name -c traffic_types
+--------------------------------------+---------+-------------------------------------------------------------------------+
| id                                   | name    | traffic_types                                                           |
+--------------------------------------+---------+-------------------------------------------------------------------------+
| f50605a3-64f4-4f0c-b50e-9481ec221c72 | Private | Backup (ABGW) private,Internal
management,OSTOR private,Storage |
| 955041d4-b059-47a1-ba4c-0be117e8cbd2 | Public  | Backup (ABGW) public,iSCSI,NFS,S3
public,Admin panel,SSH       |
+--------------------------------------+---------+-------------------------------------------------------------------------+
```

6.2.5 Настройка сетей в вычислительном кластере

Предварительные требования

- Топология вашей сети должна соответствовать требованиям, приведенным в разделе "Требования к сети для вычислительного кластера" на странице 74.
- Четкое понимание концепции "Типы трафика" на странице 42.

6.2.5.1 Минимальная сетевая конфигурация для вычислительного кластера

Минимальная сетевая конфигурация для вычислительного сервиса, развернутого в целях тестирования, включает две сети: для внутреннего и внешнего трафика. Можно оставить без

изменений стандартные сети **Внешняя** и **Частная**. В таком случае следует назначить этим сетям типы трафика в соответствии со следующей таблицей.

Минимальная сетевая конфигурация для вычислений

Сеть	Типы трафика
Частная	Хранилище, Управление системными сервисами, OSTOR внутр., Резервные копии (ABGW) внутр., ВМ внутр., Резервные копии ВМ, ВМ внешн.
Внешняя	Панель управления, SNMP, SSH, Панель самообслуживания, API вычислений, ВМ внешн., iSCSI, NFS, S3 внешн., Резервные копии (ABGW) внешн.

Чтобы создать минимальную сетевую конфигурацию для вычислительного кластера

Панель администратора

1. Добавьте требуемые типы трафика (**API вычислений**, **ВМ внутр.**, **Резервные копии ВМ** и **ВМ внешн.**) в ваши сети инфраструктуры.
   a. На экране **Инфраструктура** > **Сети** щелкните по значку карандаша рядом с типом трафика в разделе **Эксклюзивные типы трафика** или рядом с разделом **Обычные типы трафика**.
   b. Добавьте нужный тип трафика в вашу сеть, установив соответствующий переключатель или флажок.
   c. Щелкните галочку, чтобы применить изменения.
2. Если планируется использовать RDMA поверх InfiniBand, переведите тип трафика **Хранилище** в выделенную сеть и назначьте эту сеть интерфейсу IB.
3. Настройте сетевые интерфейсы на узлах, которые планируется присоединить к вычислительному кластеру.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster network set-bulk --network <network>:<traffic-types>
```

--network <network>:<traffic-types>

Конфигурация сети в формате:

- <network> – идентификатор или название сети
- <traffic-types> – список имен типов трафика через запятую

Этот параметр можно использовать несколько раз.

Например, чтобы добавить необходимые типы трафика к сетям Private и Public, выполните:

```
# vinfra cluster network set-bulk --network Private:"Storage","Internal management",\
"OSTOR private","Backup (ABGW) private","VM private","VM backups","VM public" \
--network Public:"Admin panel","SNMP","SSH","Self-service panel","Compute API",\
"VM public","iSCSI","NFS","S3 public","Backup (ABGW) public"
```

6.2.5.2 Рекомендуемая сетевая конфигурация для вычислительного кластера

Рекомендуемая сетевая конфигурация для вычислительного сервиса, развернутого в производственной среде, предполагает создание дополнительных сетей.

Без поддержки быстрой сети DPDK для виртуальных машин

Требуются следующие сети:

- **Частная**, назначенная первому объединенному соединению;
- **Оверлейная**, назначенная интерфейсу VLAN, созданному на втором объединенном соединении;
- **Публичная**, назначенная интерфейсу VLAN, созданному на втором объединенном соединении;
- **Внешняя ВМ**, назначенная интерфейсу VLAN, созданному на втором объединенном соединении;
- **Резервная**, назначенная интерфейсу VLAN, созданному на втором объединенном соединении.

С поддержкой быстрой сети DPDK для виртуальных машин

Требуются следующие сети:

- **Частная**, назначенная первому объединенному соединению;
- **Оверлейная**, назначенная интерфейсу VLAN, созданному на втором объединенном соединении;
- **Публичная**, назначенная интерфейсу VLAN, созданному на втором объединенном соединении;
- **Резервная**, назначенная интерфейсу VLAN, созданному на втором объединенном соединении;
- **Внешняя ВМ**, назначенная третьему объединенному соединению.

Распределение типов трафика между сетями

Необходимые типы трафика следует распределить между этими сетями в соответствии со следующей таблицей.

Рекомендуемая сетевая конфигурация для вычислений

Сеть	Типы трафика
Частная	Хранилище, Управление системными сервисами, OSTOR внутр., Резервные копии (ABGW) внутр.
Оверлейная	ВМ внутр.
Внешняя	Панель управления, SSH, SNMP, API вычислений, Панель самообслуживания, S3 внешн., iSCSI, NFS, Резервные копии (ABGW) внешн.

Сеть	Типы трафика
Внешняя ВМ	ВМ внешн.
Резервные копии	Резервные копии ВМ, ВМ внешн.

Чтобы создать рекомендуемую сетевую конфигурацию для вычислительного кластера

Панель администратора

1. Добавьте еще три сети.
   a. На экране **Инфраструктура** > **Сети** нажмите **Создать сеть**.
   b. В окне **Новая сеть** укажите имя сети. Имена сетей должны быть длиной от 3 до 32 символов и содержать только буквы латинского алфавита, цифры и символы подчеркивания.
   c. Нажмите кнопку **Создать**.
2. Назначьте требуемые типы трафика в соответствии с рекомендуемой сетевой конфигурацией.
   a. На экране **Инфраструктура** > **Сети** щелкните по значку карандаша рядом с типом трафика в разделе **Эксклюзивные типы трафика** или рядом с разделом **Обычные типы трафика**.
   b. Добавьте нужный тип трафика в вашу сеть, установив соответствующий переключатель или флажок.
   c. Щелкните галочку, чтобы применить изменения.
3. Если планируется использовать RDMA поверх InfiniBand, переведите тип трафика **Хранилище** в выделенную сеть и назначьте эту сеть интерфейсу IB.
4. Создайте объединенные подключения и подключения VLAN на узлах, которые планируется присоединить к вычислительному кластеру.

Интерфейс командной строки

1. Добавьте еще три сети с помощью команды vinfra cluster network create. Например:
   - Чтобы создать сеть Overlay и добавить к ней тип трафика VM private, выполните:

     ```
     # vinfra cluster network create Overlay --traffic-types "VM private"
     ```

   - Чтобы создать сеть External VM и добавить к ней тип трафика VM public, выполните:

     ```
     # vinfra cluster network create "External VM" --traffic-types "VM public"
     ```

   - Чтобы создать сеть Backup и добавить к ней типы трафика VM backups и VM public, выполните:

     ```
     # vinfra cluster network create Backup --traffic-types "VM backups","VM public"
     ```

2. Добавьте типы трафика SNMP, Compute API, и Self-service panel к сети Public с помощью команды:

   ```
   # vinfra cluster network set Public --add-traffic-types "SNMP","Compute API","Self-service panel"
   ```

3. Проверьте конфигурацию сети с помощью следующей команды:

```
# vinfra cluster network list -c id -c name -c traffic_types
+--------------------------------------+-------------+-------------------------------------------------------------------------------
-----------+
| id                                   | name        | traffic_types                                                                 |
+--------------------------------------+-------------+-------------------------------------------------------------------------------
-----------+
| 0181a09c-3334-4b3b-a8d9-8c011de5c21c | Overlay     | VM private
          |
| 40dea510-d73c-497e-8cea-69bc52a5ae07 | External VM | VM public
              |
| 8b7d2be5-6cc5-4635-b3d9-16c6cc11275d | Backup      | VM backups,VM public
                    |
| f50605a3-64f4-4f0c-b50e-9481ec221c72 | Private     | Backup (ABGW) private,Internal
management,OSTOR private,Storage              |
| 955041d4-b059-47a1-ba4c-0be117e8cbd2 | Public      | Backup (ABGW) public,Compute
API,iSCSI,NFS,S3 public,Self-service ...<truncated> |
+--------------------------------------+-------------+-------------------------------------------------------------------------------
-----------+
```

6.3 Настройка сетевых интерфейсов серверов

Перед созданием кластера хранилища данных необходимо настроить сетевые интерфейсы на каждом из узлов. Задать параметры сети и назначить сети для сетевых интерфейсов можно посредством изменения сетевых интерфейсов.

В зависимости от ваших требований к сети также может понадобиться создать объединенные соединения или соединения VLAN. Вдобавок к этому, если сетевые адаптеры на вашем узле поддерживают RDMA, настройте сетевую инфраструктуру InfiniBand.

Предварительные требования

- Сетевое оборудование, соответствующее требованиям, приведенным в разделе "Требования к сети и рекомендации" на странице 73.

6.3.1 Изменение сетевых интерфейсов

Ограничения

- Сеть можно назначить только одному сетевому интерфейсу в каждом узле.

Предварительные требования

- Если вам нужно изменить MTU по умолчанию, он должен быть настроен на аппаратном обеспечении сети.

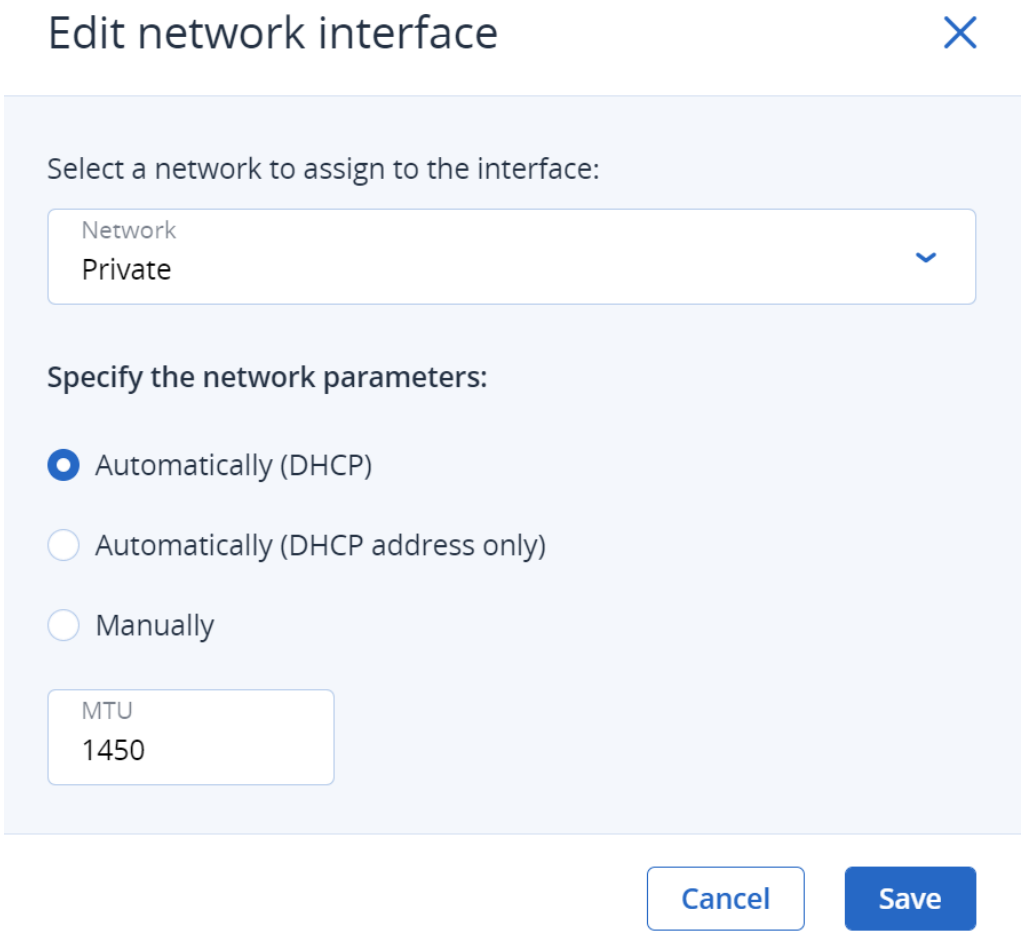
Чтобы изменить сетевой интерфейс

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по имени узла, перейдите на вкладку **Сетевые интерфейсы** и выберите сетевой интерфейс.
2. На правой панели интерфейса нажмите **Изменить**.
3. В окне **Изменить сетевой интерфейс** выберите сеть, которой нужно назначить интерфейс, затем укажите параметры сети.
   - Выберите **Автоматически (DHCP)**, чтобы получить IP-адрес, DNS и параметры маршрутизации от DHCP-сервера.
   - Выберите **Автоматически (DHCP, только адрес)**, чтобы получить только IP-адрес от DHCP-сервера.
   - Выберите **Вручную** и укажите IP-адрес в нотации CIDR, нажав кнопку **Добавить**.

   Предупреждение
   Динамическое выделение IP-адресов будет вызывать сетевые проблемы сразу же после изменения IP-адресов серверов кластера. Настройте статические IP-адреса с самого начала или сразу, как только это станет возможно.
4. [Необязательно] Укажите шлюз. Заданный шлюз станет шлюзом по умолчанию для узла.
5. Если вы задали пользовательское значение максимального размера передаваемого блока (MTU) на сетевом оборудовании, укажите то же значение в поле **MTU**.

   Предупреждение
   Установка пользовательского значения MTU на панели администрирования до его настройки на сетевом оборудовании приведет к сбою сети на сервере, и потребуется сброс вручную. Установка значения MTU, отличающегося от настроенного на сетевом оборудовании, может привести к отказу сети или низкой производительности.
6. Нажмите кнопку **Сохранить**, чтобы применить изменения.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra node iface set [--ipv4 <ipv4>] [--ipv6 <ipv6>]
                      [--gw4 <gw4>] [--gw6 <gw6>] [--mtu <mtu>]
                      [--dhcp4 | --no-dhcp4] [--dhcp6 | --no-dhcp6]
                      [--auto-routes-v4 | --ignore-auto-routes-v4]
                      [--auto-routes-v6 | --ignore-auto-routes-v6]
                      [--network <network> | --no-network]
                      [--connected-mode | --datagram-mode]
                      [--ifaces <ifaces>] [--bond-type <bond-type>]
                      [--node <node>] <iface>
```

--ipv4 <ipv4>

Разделенный запятыми список адресов IPv4

--ipv6 <ipv6>

Разделенный запятыми список адресов IPv6

--gw4 <gw4>

Адрес шлюза IPv4

--gw6 <gw6>

Адрес шлюза IPv6

--mtu <mtu>

Значение MTU (максимального размера передаваемого пакета) для интерфейса

--dhcp4

Включение DHCPv4

--no-dhcp4

Отключение DHCPv4

--dhcp6

Включение DHCPv6

--no-dhcp6

Отключение DHCPv6

--auto-routes-v4

Включить автоматические маршруты IPv4

--ignore-auto-routes-v4

Игнорировать автоматические маршруты IPv4

--auto-routes-v6

Включить автоматические маршруты IPv6

--ignore-auto-routes-v6

Игнорировать автоматические маршруты IPv6

--network <network>

Идентификатор или имя сети

--no-network

Удаление сети из интерфейса

--connected-mode

Включение подключенного режима (только для интерфейсов InfiniBand)

--datagram-mode

Включение режима дейтаграмм (только для интерфейсов InfiniBand)

--ifaces <ifaces>

Разделенный запятыми список имен сетевых интерфейсов, например: iface1,iface2...ifaceN

--bond-type <bond-type>

Тип объединения (balance-rr, balance-xor, broadcast, 802.3ad, balance-tlb, balance-alb)

Тип объединения для интерфейса OVS (balance-tcp, active-backup)

--node <node>

Идентификатор или имя хоста сервера (по умолчанию node001.vstoragedomain)

<iface>

Имя сетевого интерфейса

Пример 1. Назначение сети для сетевого интерфейса.

```
# vinfra node iface set eth2 --network MyNet --node node002
+---------+--------------------------------------+
| Field   | Value                                |
+---------+--------------------------------------+
| task_id | 8a378098-6760-4fe9-ac20-1f18a8ed9d2e |
+---------+--------------------------------------+
```

Эта команда создает задание, которое назначает сеть MyNet сетевому интерфейсу eth2, расположенному на сервере node002.

Результат выполнения задания:

```
# vinfra task show 8a378098-6760-4fe9-ac20-1f18a8ed9d2e
+---------+------------------------------------------------------------------+
| Field   | Value                                                            |
+---------+------------------------------------------------------------------+
| details |                                                                  |
| name    | backend.presentation.network.tasks.NetworkInterfaceChangeTask |
| result  | contained_in: null                                               |
|         | dhcp4: null                                                      |
|         | dhcp4_enabled: false                                             |
|         | dhcp6: null                                                      |
|         | dhcp6_enabled: false                                             |
|         | duplex: null                                                     |
|         | gw4: null                                                        |
|         | gw6: null                                                        |
|         | ignore_auto_routes_v4: true                                      |
|         | ignore_auto_routes_v6: true                                      |
|         | ipv4: []                                                         |
|         | ipv6: []                                                         |
|         | mac_addr: fa:16:3e:a7:fa:bc                                      |
|         | mtu: 1450                                                        |
|         | multicast: true                                                  |
|         | name: eth2                                                       |
|         | node_id: db83dc60-e34a-43d3-06fe-0caeb5ddaae2                    |
|         | plugged: true                                                    |
|         | roles_set: 7577efe8-33b5-44da-b54e-ab8f4419125b                  |
|         | rx_bytes: 7038                                                   |
|         | rx_dropped: 0                                                    |
|         | rx_errors: 0                                                     |
|         | rx_overruns: 0                                                   |
|         | rx_packets: 90                                                   |
|         | speeds:                                                          |
|         |   current: null                                                  |
|         |   max: null                                                      |
|         | state: up                                                        |
|         | tx_bytes: 356                                                    |
```

```
|       | tx_dropped: 0                                                  |
|       | tx_errors: 0                                                   |
|       | tx_overruns: 0                                                 |
|       | tx_packets: 4                                                  |
|       | type: iface                                                    |
| state   | success                                                        |
| task_id | 8a378098-6760-4fe9-ac20-1f18a8ed9d2e                           |
+---------+----------------------------------------------------------------+
```

Пример 2. Отмена назначения сети для сетевого интерфейса.

```
# vinfra node iface set eth2 --node node002 --no-network
+---------+--------------------------------------+
| Field   | Value                                |
+---------+--------------------------------------+
| task_id | c47837c4-e7a8-40d0-ab77-67c65375b86d |
+---------+--------------------------------------+
```

Эта команда создает задание, которое отменяет назначение сети сетевому интерфейсу eth2, расположенному на сервере node002.

Результат выполнения задания:

```
# vinfra task show c47837c4-e7a8-40d0-ab77-67c65375b86d
+---------+----------------------------------------------------------------+
| Field   | Value                                                          |
+---------+----------------------------------------------------------------+
| details |                                                                |
| name    | backend.presentation.network.tasks.NetworkInterfaceChangeTask |
| result  | contained_in: null                                             |
|       | dhcp4: null                                                    |
|       | dhcp4_enabled: false                                           |
|       | dhcp6: null                                                    |
|       | dhcp6_enabled: false                                           |
|       | duplex: null                                                   |
|       | gw4: null                                                      |
|       | gw6: null                                                      |
|       | ignore_auto_routes_v4: true                                    |
|       | ignore_auto_routes_v6: true                                    |
|       | ipv4: []                                                       |
|       | ipv6: []                                                       |
|       | mac_addr: fa:16:3e:a7:fa:bc                                    |
|       | mtu: 1450                                                      |
|       | multicast: true                                                |
|       | name: eth2                                                     |
|       | node_id: db83dc60-e34a-43d3-06fe-0caeb5ddaae2                  |
|       | plugged: true                                                  |
|       | roles_set: ''                                                  |
|       | rx_bytes: 7038                                                 |
|       | rx_dropped: 0                                                  |
|       | rx_errors: 0                                                   |
```

```
|       | rx_overruns: 0                                                  |
|       | rx_packets: 90                                                  |
|       | speeds:                                                         |
|       |   current: null                                                 |
|       |   max: null                                                     |
|       | state: up                                                       |
|       | tx_bytes: 356                                                   |
|       | tx_dropped: 0                                                   |
|       | tx_errors: 0                                                    |
|       | tx_overruns: 0                                                  |
|       | tx_packets: 4                                                   |
|       | type: iface                                                     |
| state   | success                                                         |
| task_id | c47837c4-e7a8-40d0-ab77-67c65375b86d                          |
+---------+-----------------------------------------------------------------+
```

Пример 3. Включение DHCP для сетевого интерфейса.

```
# vinfra node iface set eth2 --node node002 --dhcp4
+---------+--------------------------------------+
| Field   | Value                                |
+---------+--------------------------------------+
| task_id | 077ef0c2-de0b-4e6c-84d0-d7cafd390606 |
+---------+--------------------------------------+
```

Эта команда создает задание, которое включает назначение IP-адресов посредством DHCP для сетевого интерфейса eth2, расположенного на сервере node002.

Результат выполнения задания:

```
# vinfra task show 077ef0c2-de0b-4e6c-84d0-d7cafd390606
+---------+-----------------------------------------------------------------+
| Field   | Value                                                           |
+---------+-----------------------------------------------------------------+
| details |                                                                 |
| name    | backend.presentation.network.tasks.NetworkInterfaceChangeTask |
| result  | contained_in: null                                              |
|       | dhcp4: 192.168.30.192/24                                        |
|       | dhcp4_enabled: true                                             |
|       | dhcp6: null                                                     |
|       | dhcp6_enabled: true                                             |
|       | duplex: null                                                    |
|       | gw4: null                                                       |
|       | gw6: null                                                       |
|       | ignore_auto_routes_v4: true                                     |
|       | ignore_auto_routes_v6: false                                    |
|       | ipv4:                                                           |
|       | - 192.168.30.192/24                                             |
|       | ipv6: []                                                        |
|       | mac_addr: fa:16:3e:a7:fa:bc                                     |
|       | mtu: 1450                                                       |
```

```
|       | multicast: true                                                  |
|       | name: eth2                                                       |
|       | node_id: db83dc60-e34a-43d3-06fe-0caeb5ddaae2                    |
|       | plugged: true                                                    |
|       | roles_set: ''                                                    |
|       | rx_bytes: 8080                                                   |
|       | rx_dropped: 0                                                    |
|       | rx_errors: 0                                                     |
|       | rx_overruns: 0                                                   |
|       | rx_packets: 93                                                   |
|       | speeds:                                                          |
|       |   current: null                                                  |
|       |   max: null                                                      |
|       | state: up                                                        |
|       | tx_bytes: 1570                                                   |
|       | tx_dropped: 0                                                    |
|       | tx_errors: 0                                                     |
|       | tx_overruns: 0                                                   |
|       | tx_packets: 13                                                   |
|       | type: iface                                                      |
| state | success                                                          |
| task_id | 077ef0c2-de0b-4e6c-84d0-d7cafd390606                           |
+---------+------------------------------------------------------------------+
```

Пример 4. Отключение DHCP и настройка IP-адреса для сетевого интерфейса вручную.

```
# vinfra node iface set eth2 --node node002 --no-dhcp4 --ipv4 192.168.30.20/24
+---------+--------------------------------------+
| Field   | Value                                |
+---------+--------------------------------------+
| task_id | 95ab841c-3ce8-4ada-ab61-60ddcfc90d79 |
+---------+--------------------------------------+
```

Эта команда создает задание, которое отключает DHCP и назначает IP-адрес 192.168.30.20/24 для сетевого интерфейса eth2, расположенного на сервере node002.

Результат выполнения задания:

```
# vinfra task show 95ab841c-3ce8-4ada-ab61-60ddcfc90d79
+---------+------------------------------------------------------------------+
| Field   | Value                                                            |
+---------+------------------------------------------------------------------+
| details |                                                                  |
| name    | backend.presentation.network.tasks.NetworkInterfaceChangeTask |
| result  | contained_in: null                                               |
|       | dhcp4: null                                                      |
|       | dhcp4_enabled: false                                             |
|       | dhcp6: null                                                      |
|       | dhcp6_enabled: false                                             |
|       | duplex: null                                                     |
|       | gw4: null                                                        |
```

```
|        | gw6: null                                                    |
|        | ignore_auto_routes_v4: true                                  |
|        | ignore_auto_routes_v6: true                                  |
|        | ipv4:                                                        |
|        | - 192.168.30.20/24                                           |
|        | ipv6: []                                                     |
|        | mac_addr: fa:16:3e:a7:fa:bc                                  |
|        | mtu: 1450                                                    |
|        | multicast: true                                              |
|        | name: eth2                                                   |
|        | node_id: db83dc60-e34a-43d3-06fe-0caeb5ddaae2                |
|        | plugged: true                                                |
|        | roles_set: ''                                                |
|        | rx_bytes: 8164                                               |
|        | rx_dropped: 0                                                |
|        | rx_errors: 0                                                 |
|        | rx_overruns: 0                                               |
|        | rx_packets: 95                                               |
|        | speeds:                                                      |
|        |   current: null                                              |
|        |   max: null                                                  |
|        | state: up                                                    |
|        | tx_bytes: 1962                                               |
|        | tx_dropped: 0                                                |
|        | tx_errors: 0                                                 |
|        | tx_overruns: 0                                               |
|        | tx_packets: 19                                               |
|        | type: iface                                                  |
| state  | success                                                      |
| task_id | 95ab841c-3ce8-4ada-ab61-60ddcfc90d79                        |
+--------+--------------------------------------------------------------+
```

Пример 5. Изменение типа для сетевого объединения.

```
# vinfra node iface set bond0 --node node002 --bond-type balance-xor
+---------+--------------------------------------+
| Field   | Value                                |
+---------+--------------------------------------+
| task_id | 3a21b5b8-fe5e-432a-b143-43f80ec51b70 |
+---------+--------------------------------------+
```

Эта команда создает задание, которое меняет тип сетевого объединения bond0, расположенного на сервере node002, на balance-xor.

Результат выполнения задания:

```
# vinfra task show 3a21b5b8-fe5e-432a-b143-43f80ec51b70
+---------+--------------------------------------------------------------+
| Field   | Value                                                        |
+---------+--------------------------------------------------------------+
| details |                                                              |
```

```
| name   | backend.presentation.network.tasks.NetworkInterfaceChangeTask |
| result  | bond_type: balance-xor                                        |
|        | dhcp4: null                                                   |
|        | dhcp4_enabled: false                                          |
|        | dhcp6: null                                                   |
|        | dhcp6_enabled: false                                          |
|        | duplex: null                                                  |
|        | gw4: null                                                     |
|        | gw6: null                                                     |
|        | ifaces:                                                       |
|        | - eth2                                                        |
|        | - eth3                                                        |
|        | ignore_auto_routes_v4: true                                   |
|        | ignore_auto_routes_v6: true                                   |
|        | ipv4:                                                         |
|        | - 192.168.30.20/24                                            |
|        | ipv6: []                                                      |
|        | mac_addr: fa:16:3e:a7:fa:bc                                   |
|        | mtu: 1450                                                     |
|        | multicast: true                                               |
|        | name: bond0                                                   |
|        | node_id: db83dc60-e34a-43d3-06fe-0caeb5ddaae2                 |
|        | plugged: true                                                 |
|        | roles_set: ''                                                 |
|        | rx_bytes: 1326                                                |
|        | rx_dropped: 0                                                 |
|        | rx_errors: 0                                                  |
|        | rx_overruns: 0                                                |
|        | rx_packets: 17                                                |
|        | speeds:                                                       |
|        |   current: null                                               |
|        |   max: null                                                   |
|        | state: up                                                     |
|        | tx_bytes: 1586                                                |
|        | tx_dropped: 0                                                 |
|        | tx_errors: 0                                                  |
|        | tx_overruns: 0                                                |
|        | tx_packets: 21                                                |
|        | type: bonding                                                 |
| state   | success                                                       |
| task_id | 3a21b5b8-fe5e-432a-b143-43f80ec51b70                          |
+---------+---------------------------------------------------------------+
```

Сетевой интерфейс с измененными настройками будет показан в выводе команды vinfra node iface list:

```
# vinfra node iface list --node node002
+------+---------------+--------------------+-------+---------+
| name | node_id       | ipv4               | state | network |
+------+---------------+--------------------+-------+---------+
| eth0 | 4f96acf5-<...> | - 10.94.29.218/16  | up    | Public  |
```

```
| eth1 | 4f96acf5-<...> | - 10.37.130.101/24 | up    | Private |
| eth2 | 4f96acf5-<...> | - 192.168.30.20/24 | up    | MyNet   |
+------+----------------+--------------------+-------+---------+
```

6.3.2 Создание объединений сетевых интерфейсов

Объединение нескольких сетевых интерфейсов необязательно, но предоставляет следующие преимущества:

- Высокая доступность сети. В случае отказа одного из интерфейсов трафик будет автоматически перенаправлен через один или несколько работающих интерфейсов.
- Повышенная производительность сети. Например, два объединенных интерфейса Gigabit Ethernet обеспечат пропускную способность около 1,7 Гбит/с или до 200 МБ/с. Для узла хранения необходимое количество объединяемых сетевых интерфейсов может зависеть от количества дисков. Например, жесткий диск может выдавать данные со скоростью до 1 Гбит/с.

Ограничения

- Интерфейсы Ethernet и InfiniBand нельзя связывать между собой.
- Сетевые мосты и интерфейсы InfiniBand нельзя связывать между собой.
- Если вы связываете мост на основе Open vSwitch, используемый в вычислительном кластере, с другим сетевым интерфейсом, выберите один из следующих двух режимов связывания:
  - **balance-tcp**, при котором балансировка нагрузки производится на основе данных уровней L2-L4, таких как MAC-адрес назначения, IP-адрес и порт TCP. Для этого режима необходимо, чтобы на физическом коммутаторе, к которому подключен узел, был включен протокол LACP (Link Aggregation Control Protocol – протокол управления агрегированием каналов).
  - **active-backup**, при котором один из сетевых интерфейсов является активным, а все остальные сетевые интерфейсы пассивные. В случае отказа активного интерфейса один из пассивных сетевых интерфейсов становится активным.

Чтобы создать объединение

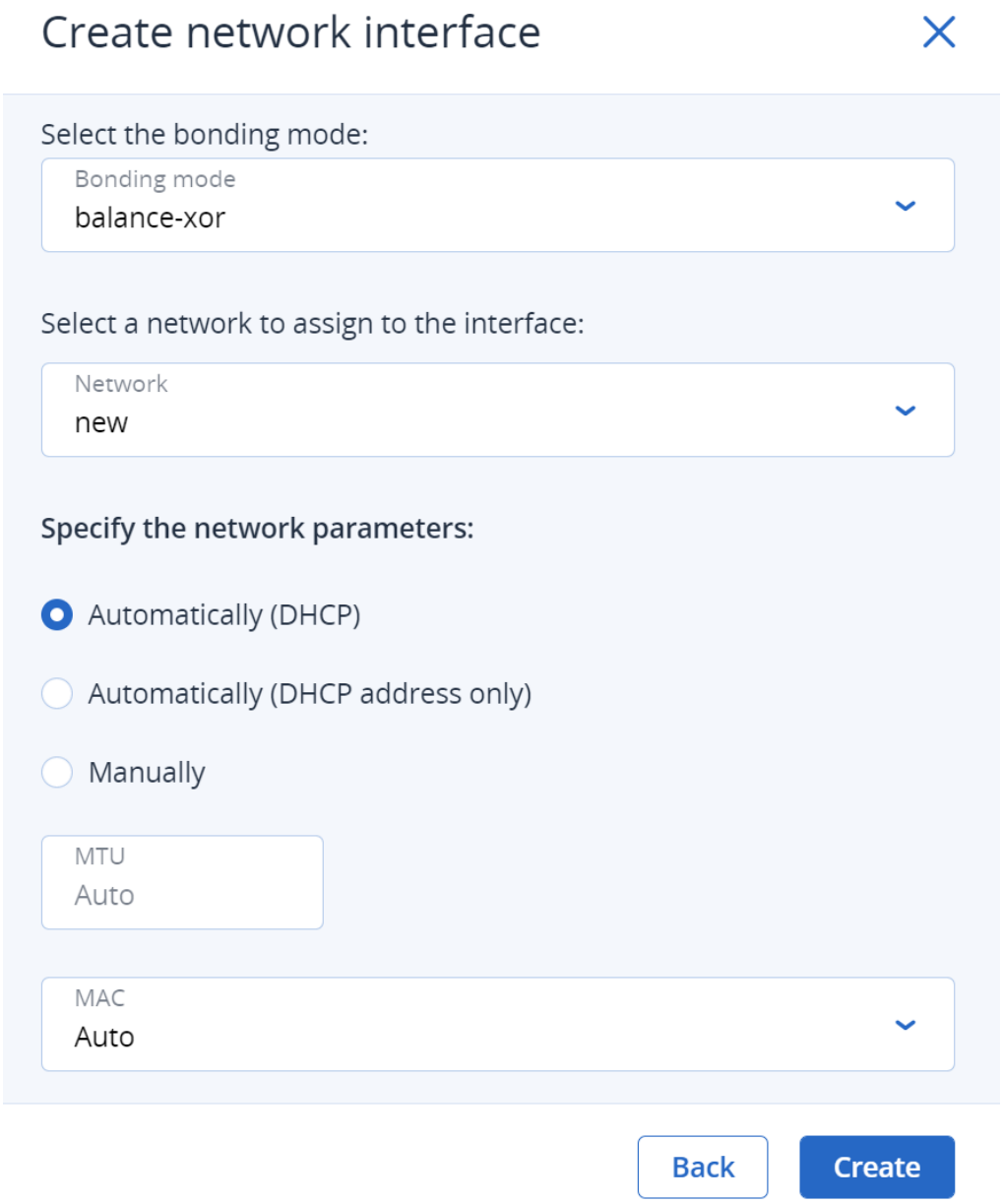
Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по имени узла, перейдите на вкладку **Сетевые интерфейсы** и нажмите **Создать**.
2. В окне **Создать сетевой интерфейс** выберите тип **Агрегация** и объединяемые сетевые интерфейсы, затем нажмите кнопку **Далее**.
3. Выберите режим объединения. Чтобы обеспечить и стойкость к отказам и хорошую производительность, рекомендуется установить режим **balance-xor**.
4. Выберите сеть, которой следует назначить объединение, затем укажите параметры сети.
   - Выберите **Автоматически (DHCP)**, чтобы получить IP-адрес, DNS и параметры маршрутизации от DHCP-сервера.

- Выберите **Автоматически (DHCP, только адрес)**, чтобы получить только IP-адрес от DHCP-сервера.
- Выберите **Вручную** и укажите IP-адрес в нотации CIDR, нажав кнопку **Добавить**.

Предупреждение
Динамическое выделение IP-адресов будет вызывать сетевые проблемы сразу же после изменения IP-адресов серверов кластера. Настройте статические IP-адреса с самого начала или сразу, как только это станет возможно.

5. [Необязательно] Укажите шлюз. Заданный шлюз станет шлюзом по умолчанию для узла.
6. [Необязательно] Введите требуемое значение MTU в поле **MTU**. Если оставить в этом поле значение **Автоматически**, будет использоваться размер блока MTU подчиненного интерфейса.
7. Выберите MAC-адрес в поле **MAC**. При выборе варианта **Автоматически** будет происходить автоматический выбор между MAC-адресами подчиненных интерфейсов, или можно выбрать один из них вручную.
8. Нажмите кнопку **Создать**.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra node iface create-bond [--ipv4 <ipv4>] [--ipv6 <ipv6>] [--gw4 <gw4>] [--gw6 <gw6>]
                              [--mtu <mtu>] [--dhcp4 | --no-dhcp4] [--dhcp6 | --no-dhcp6]
                              [--auto-routes-v4 | --ignore-auto-routes-v4]
                              [--auto-routes-v6 | --ignore-auto-routes-v6]
                              [--bonding-opts <bonding_opts>] [--network <network>]
                              [--node <node>] --bond-type <bond-type> --ifaces <ifaces>
```

--ipv4 <ipv4>

Разделенный запятыми список адресов IPv4

--ipv6 <ipv6>

Разделенный запятыми список адресов IPv6

--gw4 <gw4>

Адрес шлюза IPv4

--gw6 <gw6>

Адрес шлюза IPv6

--mtu <mtu>

Значение MTU (максимального размера передаваемого пакета) для интерфейса

--dhcp4

Включение DHCPv4

--no-dhcp4

Отключение DHCPv4

--dhcp6

Включение DHCPv6

--no-dhcp6

Отключение DHCPv6

--auto-routes-v4

Включить автоматические маршруты IPv4

--ignore-auto-routes-v4

Игнорировать автоматические маршруты IPv4

--auto-routes-v6

Включить автоматические маршруты IPv6

--ignore-auto-routes-v6

Игнорировать автоматические маршруты IPv6

--network <network>

Идентификатор или имя сети

--bonding-opts <bonding_opts>

Дополнительные параметры объединения

--bond-type <bond-type>

Тип объединения (balance-rr, active-backup, balance-xor, broadcast, 802.3ad, balance-tlb, balance-alb)

--node <node>

Идентификатор или имя хоста сервера (по умолчанию node001.vstoragedomain)

--ifaces <ifaces>

Разделенный запятыми список имен сетевых интерфейсов, например: iface1,iface2,...,iface<N>

Например, чтобы объединить сетевые интерфейсы eth2 и eth3 сервера node002 в объединение bond0 типа balance-xor, выполните:

```
# vinfra node iface create-bond --ifaces eth2,eth3 --bond-type balance-xor --dhcp4 --node node002
```

6.3.3 Создание интерфейсов VLAN

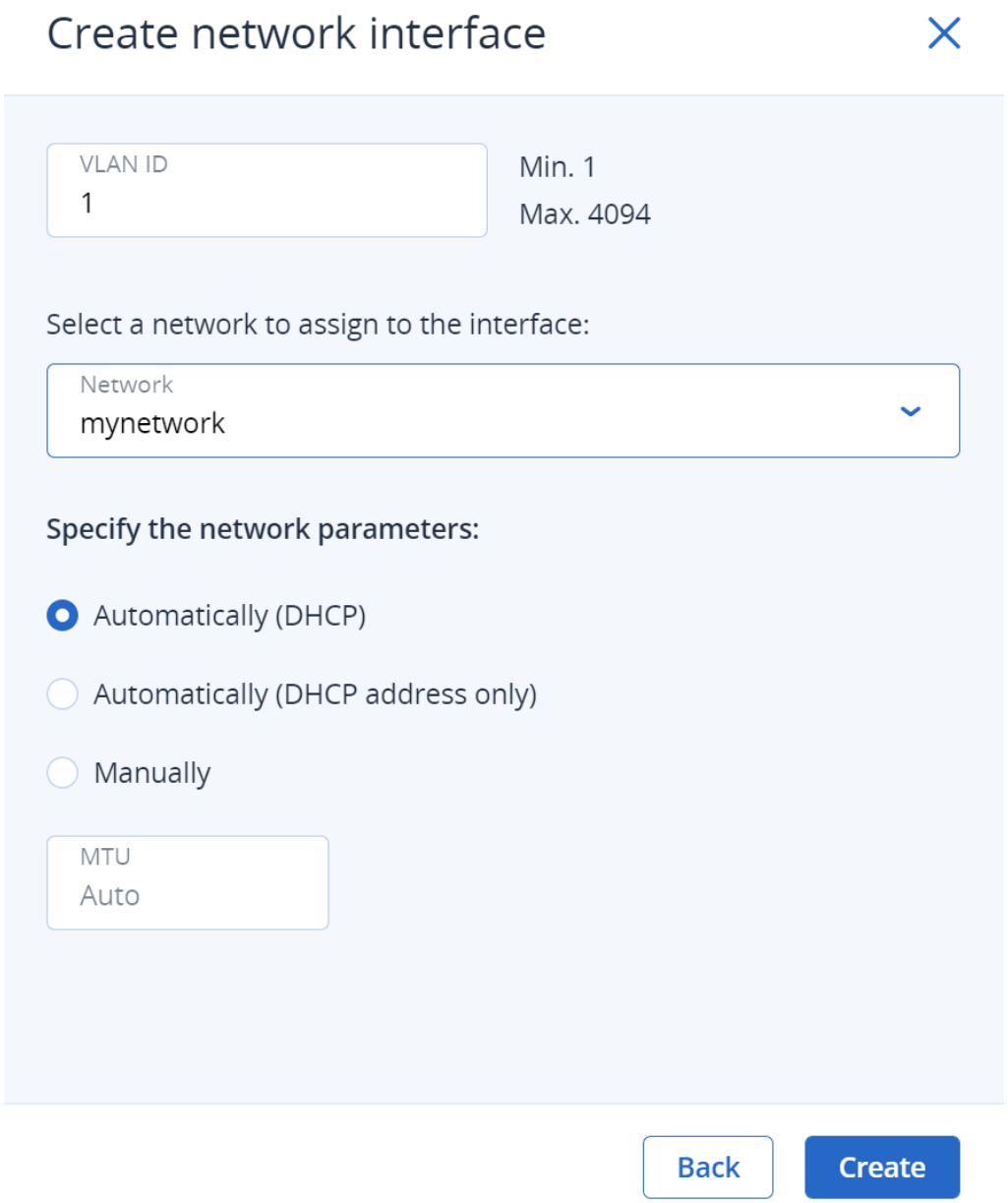
В соответствии с требованиями, приведенными в разделе "Требования для вычислительного кластера" на странице 54, рекомендуется настраивать интерфейсы VLAN поверх объединений сетевых интерфейсов для вычислительного кластера. Такие логические интерфейсы можно создать на вкладке **Сетевые интерфейсы** экрана узла. Кроме того, сетевые интерфейсы VLAN на вычислительных узлах можно создать с помощью автоматизированной процедуры, описанной в разделе "Подключение виртуальных коммутаторов к магистральным интерфейсам" на странице 530.

Чтобы создать интерфейс VLAN

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по имени узла, перейдите на вкладку **Сетевые интерфейсы** и выберите **Создать**.
2. В окне **Создать сетевой интерфейс** выберите тип **VLAN** и сетевой интерфейс, на основе которого нужно создать интерфейс VLAN, затем нажмите кнопку **Далее**.
3. Укажите номер сети VLAN в поле **Идентификатор VLAN**. Можно выбрать номер от 1 до 4094.
4. Выберите сеть, которой следует назначить VLAN, затем укажите параметры сети.
   - Выберите **Автоматически (DHCP)**, чтобы получить IP-адрес, DNS и параметры маршрутизации от DHCP-сервера.
   - Выберите **Автоматически (DHCP, только адрес)**, чтобы получить только IP-адрес от DHCP-сервера.
   - Выберите **Вручную** и укажите IP-адрес в нотации CIDR, нажав кнопку **Добавить**.

   Предупреждение
   Динамическое выделение IP-адресов будет вызывать сетевые проблемы сразу же после изменения IP-адресов серверов кластера. Настройте статические IP-адреса с самого начала или сразу, как только это станет возможно.
5. [Необязательно] Укажите шлюз. Заданный шлюз станет шлюзом по умолчанию для узла.
6. [Необязательно] Введите требуемое значение MTU в поле **MTU**. Если оставить в этом поле значение **Автоматически**, будет использоваться размер блока MTU родительского интерфейса.
7. Нажмите кнопку **Создать**.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra node iface create-vlan [--ipv4 <ipv4>] [--ipv6 <ipv6>] [--gw4 <gw4>] [--gw6 <gw6>]
                              [--mtu <mtu>] [--dhcp4 | --no-dhcp4] [--dhcp6 | --no-dhcp6]
                              [--auto-routes-v4 | --ignore-auto-routes-v4]
                              [--auto-routes-v6 | --ignore-auto-routes-v6]
                              [--network <network>] [--node <node>] --iface <iface> --tag <tag>
```

--ipv4 <ipv4>

Разделенный запятыми список адресов IPv4

--ipv6 <ipv6>

Разделенный запятыми список адресов IPv6

--gw4 <gw4>

Адрес шлюза IPv4

--gw6 <gw6>

Адрес шлюза IPv6

--mtu <mtu>

Значение MTU (максимального размера передаваемого пакета) для интерфейса

--dhcp4

Включение DHCPv4

--no-dhcp4

Отключение DHCPv4

--dhcp6

Включение DHCPv6

--no-dhcp6

Отключение DHCPv6

--auto-routes-v4

Включить автоматические маршруты IPv4

--ignore-auto-routes-v4

Игнорировать автоматические маршруты IPv4

--auto-routes-v6

Включить автоматические маршруты IPv6

--ignore-auto-routes-v6

Игнорировать автоматические маршруты IPv6

--network <network>

Идентификатор или имя сети

--node <node>

Идентификатор или имя хоста сервера (по умолчанию node001.vstoragedomain)

--iface <iface>

Имя интерфейса

--tag <tag>

Номер тега VLAN

Например, чтобы создать интерфейс VLAN с тегом 100 на сетевом интерфейсе eth2 сервера node002, выполните:

```
# vinfra node iface create-vlan --iface eth2 --tag 100 --dhcp4 --node node002
```

6.3.4 Настройка устройств InfiniBand

Ограничения

- Так как на панели администрирования показывается только состояние подключений по протоколу IP, но не показываются состояния подключений InfiniBand (IB), она может отображать подсоединенные, но еще не настроенные устройства IB со статусом **Отсоединено**. Статус изменится на **Готово**, как только такому устройству будет назначен IP-адрес.

Предварительные требования

- Тип трафика **Хранилище** должен быть перенесен в выделенную сеть.

Чтобы настроить устройства InfiniBand

Панель администратора

1. На экране **Инфраструктура** > **Сети** назначьте тип трафика **Хранилище** пустой сети (без любых других типов трафика). При необходимости создайте новую сеть, нажав **Создать сеть**.
2. На экране **Инфраструктура** > **Серверы** щелкните по имени узла, перейдите на вкладку **Сетевые интерфейсы** и выберите сетевой интерфейс.
3. На правой панели интерфейса нажмите **Изменить**.
4. В окне **Изменить сетевой интерфейс** укажите сеть с типом трафика **Хранилище**, выберите **Вручную**, затем укажите IP-адрес в записи бесклассовой адресации, нажав кнопку **Добавить**.
5. Укажите шлюз. Заданный шлюз станет шлюзом по умолчанию для узла.
6. Выберите **Подключенный режим**.
7. Введите значение 65520 в поле **MTU**.

   Предупреждение
   Установка пользовательского значения MTU на панели администрирования до его настройки на сетевом оборудовании приведет к сбою сети на сервере, и потребуется сброс вручную. Установка значения MTU, отличающегося от настроенного на сетевом оборудовании, может привести к отказу сети или низкой производительности.

8. Нажмите кнопку **Сохранить**, чтобы применить изменения.
9. Повторите эти шаги для каждого из устройств IB на узлах инфраструктуры.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node iface set [--ipv4 <ipv4>] [--ipv6 <ipv6>] [--gw4 <gw4>] [--gw6 <gw6>]
                      [--mtu <mtu>] [--dhcp4 | --no-dhcp4] [--dhcp6 | --no-dhcp6]
                      [--auto-routes-v4 | --ignore-auto-routes-v4]
                      [--auto-routes-v6 | --ignore-auto-routes-v6]
```

```
        [--network <network> | --no-network] [--connected-mode | --datagram-mode]
        [--node <node>] <iface>
```

--ipv4 <ipv4>

Разделенный запятыми список адресов IPv4

--ipv6 <ipv6>

Разделенный запятыми список адресов IPv6

--gw4 <gw4>

Адрес шлюза IPv4

--gw6 <gw6>

Адрес шлюза IPv6

--mtu <mtu>

Значение MTU (максимального размера передаваемого пакета) для интерфейса

--dhcp4

Включение DHCPv4

--no-dhcp4

Отключение DHCPv4

--dhcp6

Включение DHCPv6

--no-dhcp6

Отключение DHCPv6

--auto-routes-v4

Включить автоматические маршруты IPv4

--ignore-auto-routes-v4

Игнорировать автоматические маршруты IPv4

--auto-routes-v6

Включить автоматические маршруты IPv6

--ignore-auto-routes-v6

Игнорировать автоматические маршруты IPv6

--network <network>

Идентификатор или имя сети

--no-network

Удаление сети из интерфейса

--connected-mode

Включение подключенного режима (только для интерфейсов InfiniBand)

--datagram-mode

Включение режима дейтаграмм (только для интерфейсов InfiniBand)

--node <node>

Идентификатор или имя хоста сервера (по умолчанию node001.vstoragedomain)

<iface>

Имя сетевого интерфейса

Например, чтобы назначить сеть Storage сетевому интерфейсу ib2 сервера node002, включить подключенный режим, задать IP-адрес 192.168.30.20/24 и MTU 65520, выполните:

```
# vinfra node iface set ib2 --network Storage --node node002 --ipv4 192.168.30.20/24 \
--mtu 65520 --connected-mode
```

6.3.5 Настройка устройств RoCE

Настройка устройств Converged Ethernet (RoCE)

- На экране **Инфраструктура** > **Серверы** щелкните имя узла, перейдите на вкладку **Сетевые интерфейсы** и выберите устройство.
- Щелкните **Настроить**.
- Щелкните **Назначить сеть**.
- На панели **Назначить сеть** выберите сеть с типом трафика хранилища (и, возможно, с другими типами трафика, такими как **Внутреннее управление**, частный **OSTOR** и частный **ABGW**, а затем нажмите **Готово**.

6.4 Включение RDMA

Кибер Инфраструктура поддерживает удаленный прямой доступ к памяти (RDMA) по протоколам Converged Ethernet (RoCE), InfiniBand (IB) и Internet Wide Area RDMA Protocol (iWARP) для внутренней сети хранения данных. Технология RDMA позволяет серверам в этой сети обмениваться данными в основной памяти без задействования процессоров, кэша или операционных систем, высвобождая тем самым ресурсы и улучшая пропускную способность и производительность.

По умолчанию RDMA отключен. Включить RDMA можно в панели администратора или в интерфейсе командной строки.

Процедура настройки RDMA для сетевых адаптеров, использующих протокол iWARP, не отличается от процедуры настройки RDMA для адаптеров, использующих протокол RoCE.

Ограничения

- Включить RDMA можно только до создания кластера хранения данных.

- Рекомендуется использовать сетевые адаптеры Broadcom NetXtreme-E, Intel серий E800 (E810-C, E810-XXV, E823) и X722, Mellanox ConnectX-4, Mellanox ConnectX-5. Если вы хотите использовать другие адаптеры, обратитесь в службу технической поддержки.
- Для использования RDMA агрегация может быть сконфигурирована только путем объединения портов одной и той же сетевой карты.
- RDMA не поддерживается для вычислительного кластера. Таким образом, сеть с вычислительным кластером и сеть хранилища (сеть с типом трафика **Хранилище**) должны использовать разные сетевые адаптеры. Рекомендуется использовать одну сетевую карту с двумя агрегированными сетевыми интерфейсами для сети с вычислительным кластером и одну сетевую карту с двумя агрегированными сетевыми интерфейсами для сети хранилища. Про использование магистральных (транковых) интерфейсов см. раздел "Подключение виртуальных коммутаторов к магистральным интерфейсам" на странице 530.
- Включение или отключение RDMA может временно повлиять на доступность кластера.

Предварительные требования

- Сетевая инфраструктура RDMA должна быть готова перед установкой Кибер Инфраструктура.
- Каждый сетевой адаптер, подсоединенный к сети с типом трафика **Хранилище**, должен поддерживать RDMA. Если какой-либо сервер кластера хранилища данных не поддерживает RDMA, весь кластер необходимо переключить на TCP.
- Устройства InfiniBand и RoCE на всех узлах должны быть настроены, как описано в разделах "Настройка устройств InfiniBand" на странице 134 и "Настройка устройств RoCE" на предыдущей странице.

6.4.1 Проверка сетевой инфраструктуры RDMA

Для проверки состояния сетевой инфраструктуры RDMA вы можете использовать утилиты командной строки, предоставляемые производителем оборудования.

Чтобы проверить сетевое оборудование

Получите список устройств RDMA, доступных для использования:

```
# ibv_devices
    device                 node GUID
    ------              ----------------
    rdmao1              5e6f69fffe27b644
    rdmao2              5e6f69fffe27b645
```

Чтобы проверить сетевое соединение

Запустите утилиту rping в режиме сервера на любом узле:

```
# rping -s -C 10 -v
```

Запустите утилиту rping в режиме клиента на любом другом узле:

```
# rping -c -a <server_IP> -C 10 -v
```

Где <server_IP> – это IP-адрес узла с утилитой rping, запущенной в режиме сервера.

Пример вывода утилиты rping:

```
ping data: rdma-ping-0: ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqr
ping data: rdma-ping-1: BCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrs
ping data: rdma-ping-2: CDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrst
ping data: rdma-ping-3: DEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstu
ping data: rdma-ping-4: EFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuv
ping data: rdma-ping-5: FGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvw
ping data: rdma-ping-6: GHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwx
ping data: rdma-ping-7: HIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxy
ping data: rdma-ping-8: IJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz
ping data: rdma-ping-9: JKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyzA
client DISCONNECT EVENT...
```

Чтобы проверить пропускную способность сети

Запустите утилиту проверки пропускной способности ib_send_bw в режиме сервера на любом узле:

```
# ib_send_bw -d mlx4_0 -i 1 -F --report_gbits
```

Запустите утилиту проверки пропускной способности ib_send_bw в режиме клиента на любом другом узле:

```
# ib_send_bw -d mlx4_0 -i 1 -F --report_gbits <server_IP>
```

Где <server_IP> – это IP-адрес узла с утилитой ib_send_bw, запущенной в режиме сервера.

Пример вывода утилиты ib_send_bw:

```
Send BW Test
Dual-port : OFF Device : mlx4_0
Number of qps : 1 Transport type : IB
Connection type : RC
RX depth : 512
CQ Moderation : 100
Mtu : 1024[B]
Link type : Ethernet
Gid index : 0
Max inline data : 0[B]
rdma_cm QPs : OFF
Data ex. method : Ethernet
---------------------------------------------------------------------
local address: LID 0000 QPN 0x0065 PSN 0xc8f367
GID: 254:128:00:00:00:00:00:00:246:82:20:255:254:23:27:129
remote address: LID 0000 QPN 0x005d PSN 0x884d7d
GID: 254:128:00:00:00:00:00:00:246:82:20:255:254:23:31:225
```

```
---------------------------------------------------------------------------
#bytes #iterations BW peak[Gb/sec] BW average[Gb/sec] MsgRate[Mpps]
65536  1000       0.00          36.40           0.069428
```

6.4.2 Настройка RDMA

Ограничения

- Включить RDMA можно только до создания кластера хранения данных.

Предварительные требования

- Была проведена проверка сетевой инфраструктуры RDMA, как описано в разделе "Проверка сетевой инфраструктуры RDMA" на странице 137.

Чтобы включить или выключить RDMA

Панель администратора

Используйте переключатель на экране **Настройки** > **Настройки системы** > **RDMA**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cses-config change (--enable | --disable)
```

--enable
: Включение RDMA

--disable
: Выключение RDMA

Например, чтобы включить RDMA для кластера хранения данных, выполните:

```
# vinfra cses-config change --enable
```

Проверить статус настройки можно в выводе команды vinfra cses-config show:

```
# vinfra cses-config show
+-------+-----------------------------------------+
| Field | Value                                   |
+-------+-----------------------------------------+
| rdma  | true                                    |
+-------+-----------------------------------------+
```

6.5 Добавление внешних DNS-серверов

Продукт Кибер Инфраструктура оснащен встроенным DNS-сервером, который обеспечивает обнаружение всех его внутренних сервисов. Для разрешения внешних доменных имен можно

добавить DNS-серверы, уже существующие в вашей сетевой инфраструктуре.

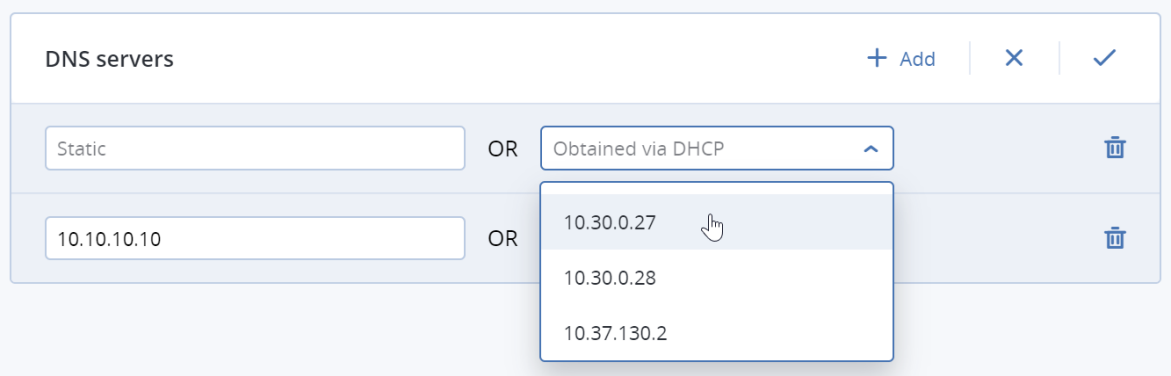
Ограничения

- Укажите сервер DNS, который принадлежит к внешней сети, чтобы получать доступ к внешним расположениям, например к репозиторию обновлений, а также к любым внешним (общедоступным) сетям.

Чтобы добавить внешние DNS-серверы

Панель администратора

1. Перейдите в раздел **Настройки** > **Настройки системы** > **DNS кластера**.
2. Нажмите **Добавить**, затем укажите статический IP-адрес DNS-сервера в поле **Статический** либо выберите IP-адрес DNS-сервера, предоставленный DHCP-сервером, из списка. Нажмите кнопку **Добавить** несколько раз, чтобы указать несколько внешних DNS-серверов.



3. Щелкните по галочке, чтобы сохранить изменения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster settings dns set --nameservers <nameservers>
```

--nameservers <nameservers>

Разделенный запятыми список DNS-серверов

Например, чтобы задать внешний DNS-сервер с IP-адресом 8.8.8.8, выполните:

```
# vinfra cluster settings dns set --nameservers 8.8.8.8
+-----------------+--------------+
| Field           | Value        |
+-----------------+--------------+
| dhcp_nameservers | - 10.10.0.10 |
|                 | - 10.10.0.11 |
|                 | - 10.37.130.2 |
| nameservers     | - 8.8.8.8    |
+-----------------+--------------+
```

Добавленный DNS-сервер появится в выводе команды vinfra cluster settings dns show:

```
# vinfra cluster settings dns show
+-----------------+---------------------------------+
| Field           | Value                           |
+-----------------+---------------------------------+
| dhcp_nameservers | 10.10.0.10,10.10.0.11,10.37.130.2 |
| nameservers     | 10.10.0.11,10.10.0.10           |
+-----------------+---------------------------------+
```

6.6 Развертывание кластера хранилища данных

Создайте кластер хранилища данных на одном (первом) узле, затем заполните его дополнительными узлами.

Ограничения

- Диску можно назначить роль, только если его размер превышает 1 ГиБ.
- Системному диску можно назначить дополнительную роль, только если его размер не меньше 100 ГиБ.
- Жесткие диски с черепичной магнитной записью (SMR) можно использовать только с ролью **Хранилище** и только в случае, если на сервере есть твердотельный диск с ролью **Кэш**.
- Нельзя использовать на одном уровне хранилища стандартные и SMR-диски.
- Нельзя одновременно назначить роли системным и несистемным дискам.

Предварительные требования

- Четкое понимание архитектуры кластера хранения данных и ролей дисков, которые разъясняются в разделе "О кластере хранилища данных" на странице 12.
- Четкое понимание концепции "Уровни хранения данных" на странице 36.
- Сети инфраструктуры должны быть настроены, как описано в разделе "Настройка сетей" на странице 110.
- Сетевые интерфейсы узла должны быть настроены согласно указаниям в разделе "Настройка сетевых интерфейсов серверов" на странице 117.
- Если поддерживается RDMA, этот режим должен быть включен, как описано в разделе "Включение RDMA" на странице 136.
- Внешние DNS-серверы должны быть добавлены автоматически во время установки или настроены вручную, как описано в разделе "Добавление внешних DNS-серверов" на странице 139.
- Все узлы должны отображаться на панели администрирования в разделе **Инфраструктура** > **Серверы** как имеющие состояние **Не назначен**.

Чтобы создать кластер хранилища на первом сервере

Панель администратора

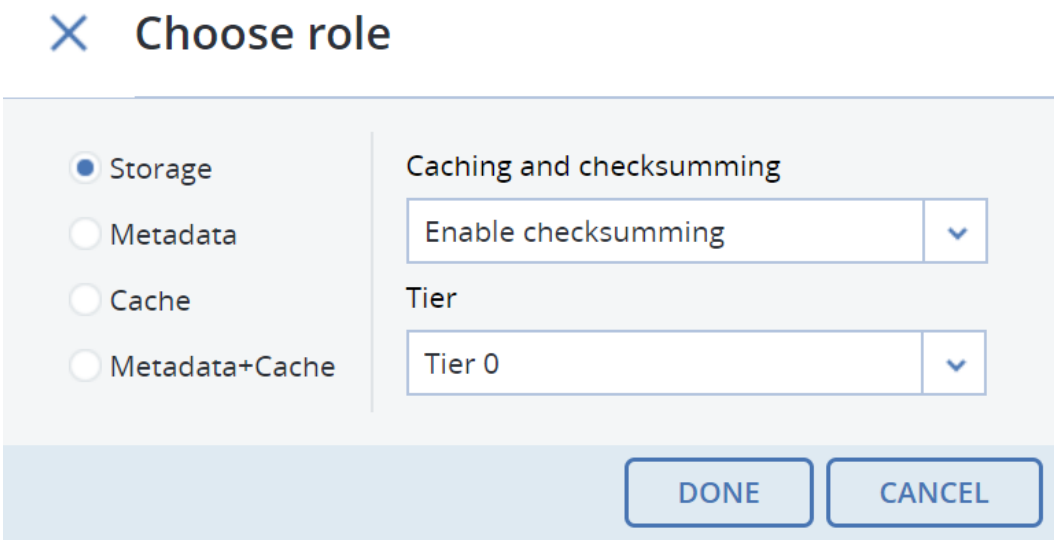
1. Откройте экран **Инфраструктура** > **Серверы** и нажмите **Создать кластер хранилища**.
2. [Необязательно] Чтобы настроить роли дисков или расположение сервера, нажмите значок шестерни.
   - Как настроить диски
     a. Выберите **Диски**.
     b. Выберите нужный диск и нажмите **Настроить**.
     c. В окне **Выбрать роль** выберите роль.
        - [Только для твердотельных накопителей] Как хранить кэш записи
          i. Выберите роль **Кэш**.
          ii. Выберите уровень хранилища, который следует кэшировать.

          Примечание
          Для того чтобы диски использовали кэш, роль **Кэш** необходимо назначить до назначения роли **Хранилище**.

        - Как организовать хранение данных
          i. Выберите роль **Хранилище**.
          ii. Выберите уровень хранилища для размещения данных. Чтобы повысить эффективность избыточности данных, не назначайте все диски сервера на один и тот же уровень. Вместо этого убедитесь, что каждый из уровней равномерно распределен по кластеру и на каждом сервере ему назначено по одному диску.
          iii. Включите кэширование данных и проверку контрольных сумм:
            - **Использовать диск SSD для кэширования и проверки контрольных сумм**. Доступно и рекомендуется только для серверов с твердотельными накопителями.
            - **Включить проверку контрольных сумм** (по умолчанию). Рекомендуется для серверов с жесткими дисками, так как обеспечивает повышенную надежность.
            - **Отключить проверку контрольных сумм**. Не рекомендуется для производственной среды. В среде оценки или тестирования можно отключить проверку контрольных сумм для серверов с жесткими дисками для повышения производительности.
        - Как хранить метаданные кластера
          Выберите роль **Метаданные**.

          Примечание
          Рекомендуется не больше одного сервиса метаданных на сервер и не больше пяти сервисов метаданных для кластера.

        - [Только для твердотельных накопителей] Как хранить метаданные и кэш записи
          i. Выберите роль **Метаданные+Кэш**.
          ii. Выберите уровень хранилища, который следует кэшировать.



d. Повторите предыдущие шаги для каждого диска, который будет использоваться в кластере хранилища, и нажмите **Готово**.

e. На экране **Итоговая конфигурация** проверьте количество дисков для каждой категории конфигурации и нажмите **Продолжить**.

- Как настроить расположение серверов
  По умолчанию серверы добавляются в стойку **Default rack** в ряду **Default row** в комнате **Default room**.

  a. Выберите **Расположение**.

  b. Для создания комнаты нажмите **Создать комнату** в окне **Переместить серверы**. Укажите имя комнаты и нажмите **Создать**.

  c. Чтобы добавить новый ряд, щелкните по созданной комнате. Нажмите **Создать ряд**, введите имя ряда и нажмите **Создать**.

  d. Чтобы добавить новую стойку, щелкните по созданному ряду. Нажмите **Создать стойку**, введите имя стойки и нажмите **Создать**.

  e. Щелкните по созданной стойке и нажмите **Переместить**.

3. Введите имя для кластера. Имя может содержать только буквы латинского алфавита (a-z, A-Z), цифры (0-9) и дефисы (-).
4. При необходимости включите шифрование.
5. Нажмите кнопку **Создать**.

Отслеживать создание кластера можно на экране **Инфраструктура** > **Серверы**. Создание может занять некоторое время в зависимости от количества настраиваемых дисков. Кластер будет создан после завершения настройки.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster create [--disk <disk>:<role>[:<key=value,…>]] [--tier-encryption {0,1,2,3}]
                      --node <node> <cluster-name>
```

--disk <disk>:<role>[:<key=value,…>]

Конфигурация диска в формате:

- <disk>: идентификатор или имя дискового устройства
- <role>: роль диска (cs, mds, journal, mds-journal, mds-system, cs-system, system)
- разделенные запятыми пары key=value с ключами (необязательно):
  - tier: уровень диска (0, 1, 2 или 3)
  - journal-tier: уровень диска журнала (кэша) (0, 1, 2 или 3)
  - journal-type: тип диска журнала (кэша) (no_cache – без кэша, inner_cache – внутренний кэш или external_cache – внешний кэш)
  - journal-disk: идентификатор или имя устройства диска журнала (кэша)
  - bind-address: IP-адрес привязки для сервиса метаданных

Например: sda:cs:tier=0,journal-type=inner_cache.
Этот параметр можно указывать несколько раз.

--tier-encryption {0,1,2,3}

Включение шифрования для определенных уровней кластера хранилища. По умолчанию шифрование отключено. Этот параметр можно указывать несколько раз.

--node <node>

Идентификатор сервера или имя хоста

<cluster-name>

Имя кластера хранилища данных

Например, чтобы создать кластер хранилища stor1 на сервере node001, выполните:

```
# vinfra cluster create stor1 --node node001
```

Поскольку роли дисков не указаны явно, они назначаются автоматически: mds-system для системного диска и cs для всех остальных дисков.

Просмотреть сведения о кластере хранилища можно в выводе команды vinfra cluster show:

```
# vinfra cluster show
+-------+-----------------------------------------+
| Field | Value                                   |
+-------+-----------------------------------------+
| id    | 1                                       |
| name  | stor1                                   |
| nodes | - host: node001.vstoragedomain          |
|       |   id: f59dabdb-bd1c-4944-8af2-26b8fe9ff8d4 |
```

```
|     |  is_installing: false                |
|     |  is_releasing: false                 |
+-------+--------------------------------------------+
```

Для удаления кластера хранилища используйте команду vinfra cluster delete.

Чтобы добавить узлы в кластер

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по неназначенному серверу.
2. На правой панели сервера нажмите **Присоединить к кластеру**.
3. Нажмите **Присоединить**, чтобы автоматически назначить роли дискам и добавить сервер в текущее расположение. Вместо этого можно нажать значок шестерни, чтобы вручную настроить роли дисков или расположение сервера.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node join [--disk <disk>:<role>[:<key=value,...>]] <node>
```

--disk <disk>:<role>[:<key=value,...>]

Конфигурация диска в формате:

- <disk>: идентификатор или имя дискового устройства
- <role>: роль диска (cs, mds, journal, mds-journal, mds-system, cs-system, system)
- разделенные запятыми пары key=value с ключами (необязательно):
  - tier: уровень диска (0, 1, 2 или 3)
  - journal-tier: уровень диска журнала (кэша) (0, 1, 2 или 3)
  - journal-type: тип диска журнала (кэша) (no_cache – без кэша, inner_cache – внутренний кэш или external_cache – внешний кэш)
  - journal-disk: идентификатор или имя устройства диска журнала (кэша)
  - bind-address: IP-адрес привязки для сервиса метаданных

Например: sda:cs:tier=0,journal-type=inner_cache.
Этот параметр можно указывать несколько раз.

<node>

Идентификатор сервера или имя хоста

Например, чтобы добавить сервер node002 в кластер хранилища и назначить дискам роли (mds-system для sda, cs для sdb и sdc), выполните:

```
# vinfra node join f59dabdb-bd1c-4944-8af2-26b8fe9ff8d4 --disk sda:mds-system \
--disk sdb:cs --disk sdc:cs
```

Добавленный сервер появится в выводе команды vinfra node list:

```
# vinfra node list
+--------------+--------------+------------+-----------+-------------+----------+
| id           | host         | is_primary | is_online | is_assigned | is_in_ha |
+--------------+--------------+------------+-----------+-------------+----------+
| 09bb6b8<...> | node001<...> | True       | True      | True        | False    |
| 187edb1<...> | node002<...> | False      | True      | True        | False    |
+--------------+--------------+------------+-----------+-------------+----------+
```

6.7 Включение высокой доступности сервера управления

Чтобы сделать инфраструктуру более устойчивой и избыточной, можно создать конфигурацию высокой доступности из трех серверов.

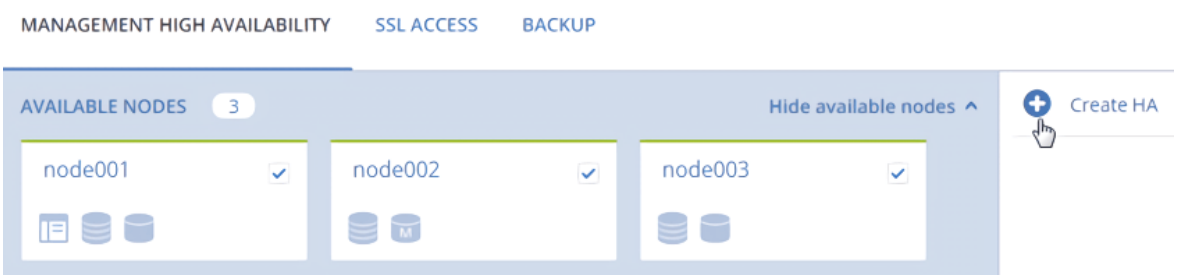
Предварительные требования

- Четкое понимание концепции "Высокая доступность" на странице 27.
- Каждый из узлов, добавляемых в конфигурацию высокой доступности, должен быть подключен к сети с типами трафика **Панель администрирования** и **Внутреннее управление**.
- Если вычислительный кластер (см. раздел "О вычислительном кластере" на странице 22) уже был создан, на каждом сервере необходим доступ к Интернету или к локальному зеркалу репозитория пакетов продукта. Подробную информацию см. в статье базы знаний Настройка локального зеркала репозитория Кибер Инфраструктуры.
- Кластер хранилища должен быть создан в соответствии с указаниями из раздела "Развертывание кластера хранилища данных" на странице 141.

Чтобы создать конфигурацию высокой доступности

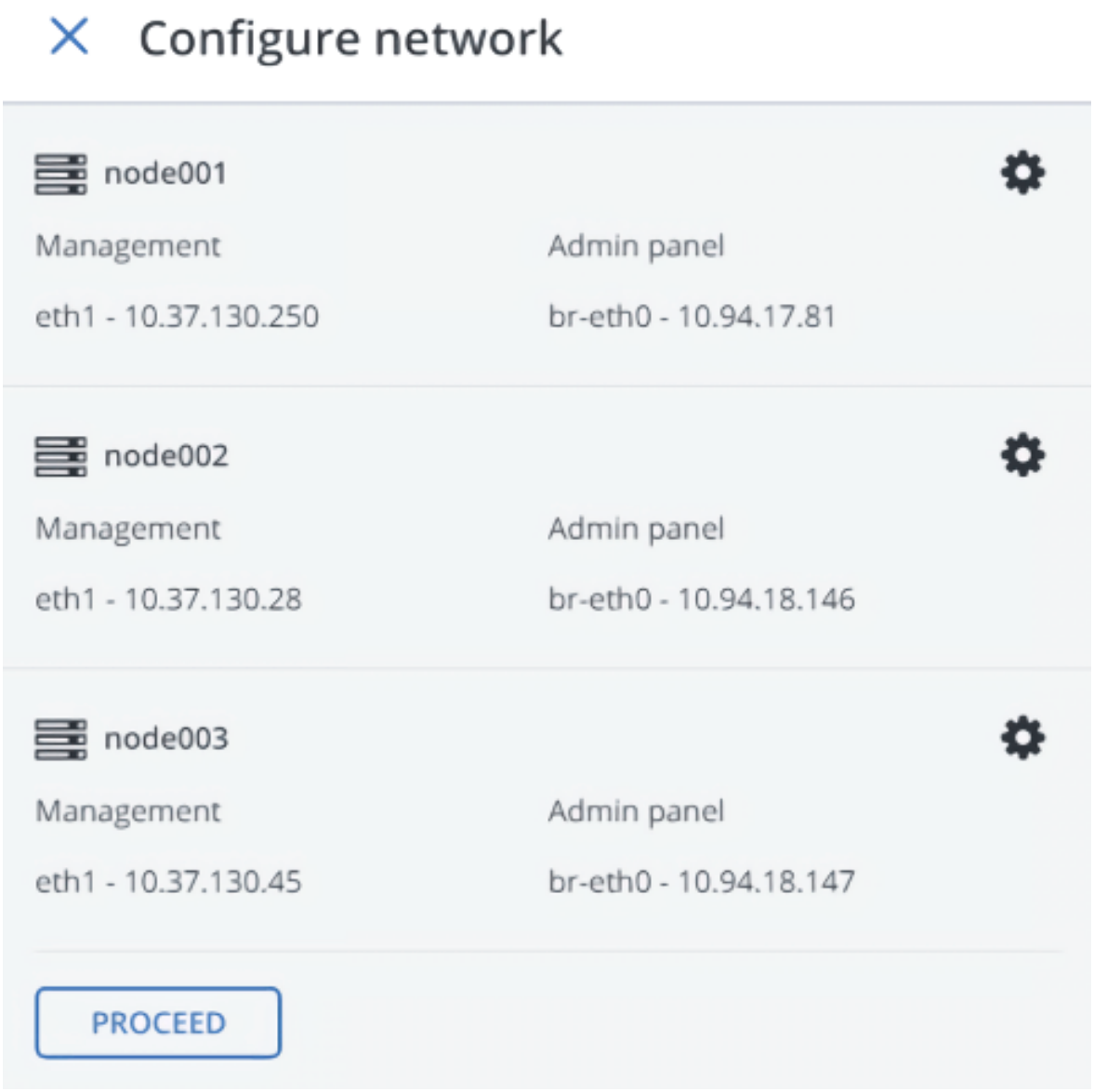
Панель администратора

1. На экране **Настройки** > **Сервер управления** откройте вкладку **Высокая доступность**.

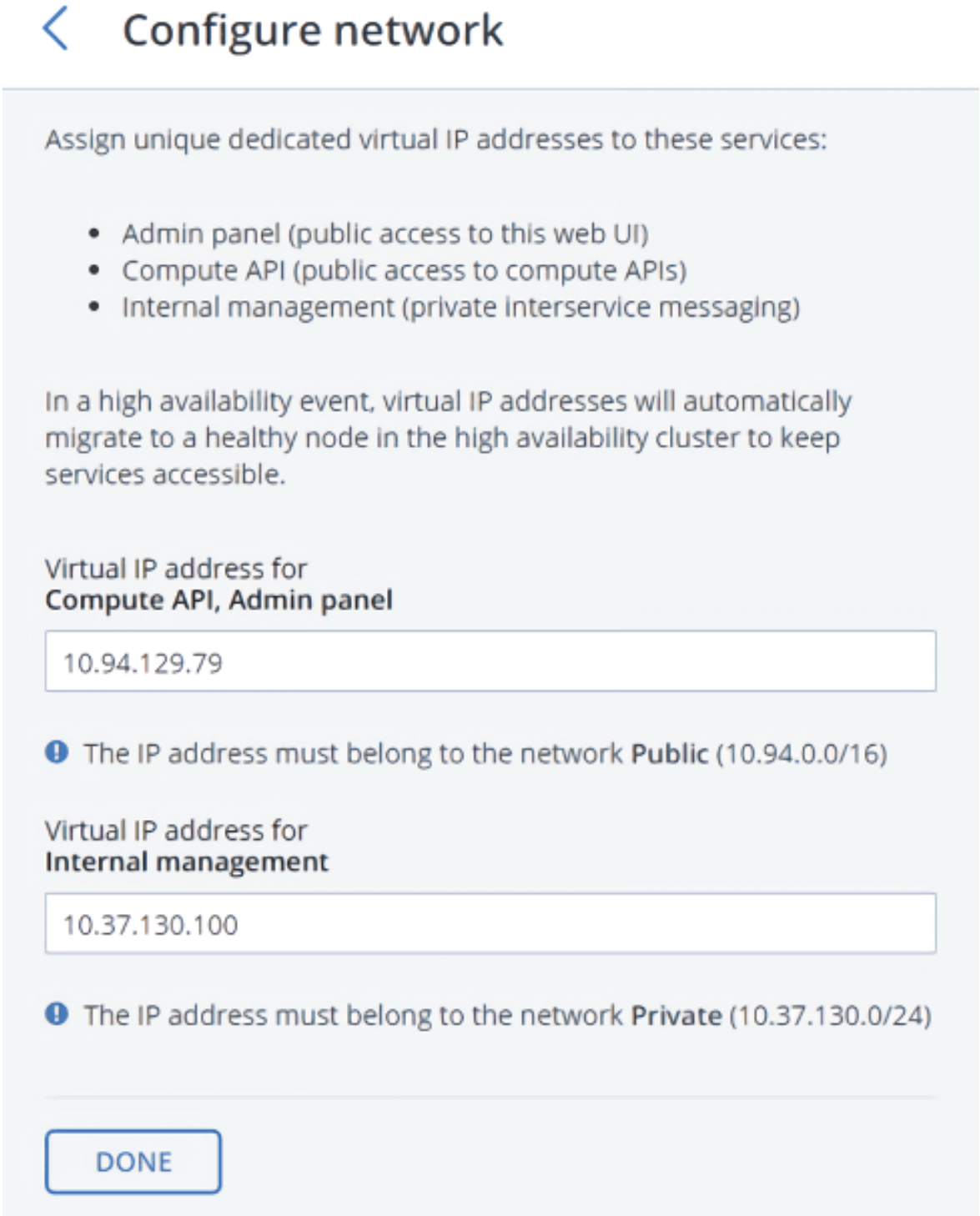


2. Выберите три сервера и нажмите **Создать конфигурацию высокой доступности**. Сервер управления будет выбран автоматически.
3. На шаге **Настройте сеть** убедитесь, что на каждом сервере выбраны правильные сетевые интерфейсы. Если это не так, щелкните по значку шестерни для сервера и назначьте его

сетевым интерфейсам сети с типами трафика **Управление системными сервисами** и **Панель администрирования**. Нажмите **Продолжить**.



4. На шаге **Настройте сеть** укажите один или несколько уникальных статических IP-адресов для панели администрирования с высокой доступностью, оконечной точки API вычислений и обмена сообщениями между сервисами. Нажмите **Готово**.



После того как высокая доступность сервера управления будет включена, можно выполнить вход на панель администрирования по указанному статическому IP-адресу (на том же порту 8888).

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster ha create --virtual-ip <network:ip> --nodes <nodes> [--force]
```

--virtual-ip <network:ip>

Сопоставление конфигурации высокой доступности в формате:

- network: сеть, включаемая в конфигурацию высокой доступности (должна включать по меньшей мере один из следующих типов трафика: Управление системными сервисами, Панель администрирования, Панель самообслуживания или API вычислений).
- ip: виртуальный IP-адрес, который будет использоваться в конфигурации высокой доступности.

Укажите этот параметр несколько раз, чтобы создать конфигурацию высокой доступности сразу для нескольких сетей.

--nodes <nodes>

Разделенный запятыми список идентификаторов или имен серверов

--force

Пропустить проверки на соответствие минимальным аппаратным требованиям

Например, чтобы создать кластер высокой доступности сервера управления из серверов node001, node002 и node003, выполните:

```
# vinfra cluster ha create --virtual-ip Private:10.37.130.200 \
--virtual-ip Public:10.94.129.79 --nodes node001,node002,node003
```

Эта команда задает сеть Private с типом трафика Управление системными сервисами и сеть Public с типом трафика Панель администрирования.

Посмотреть конфигурацию высокой доступности сервера управления можно в выводе команды vinfra cluster ha show:

```
# vinfra cluster ha show
+----------------------+-------------------------------------------------+
| Field                | Value                                           |
+----------------------+-------------------------------------------------+
| ha_cluster_location  | - https://10.94.129.79:8888                     |
| nodes                | - id: 94d58604-6f30-4339-8578-adb7903b7277      |
|                      |   ipaddr: 10.37.130.118                         |
|                      |   is_primary: false                             |
|                      | - id: f59dabdb-bd1c-4944-8af2-26b8fe9ff8d4      |
|                      |   ipaddr: 10.37.130.134                         |
|                      |   is_primary: true                              |
|                      | - id: 4b83a87d-9adf-472c-91f0-782c47b2d5f1      |
|                      |   ipaddr: 10.37.130.127                         |
|                      |   is_primary: false                             |
| primary_node_location | https://10.94.62.243:8888                      |
| virtual_ips          | - ip: 10.37.130.200                             |
|                      |   roles_set: 5a0401b5-9b42-4d8b-8372-71c747230033 |
```

```
|                | - ip: 10.94.129.79                          |
|                |   roles_set: 5f0adc1d-c10f-46c1-b7b8-dd1aacab613b |
+----------------------+-----------------------------------------------------+
```

Внимание

После создания кластера высокой доступности панель администрирования будет доступна только по заданному общедоступному IP-адресу. Выполните вход на этот адрес по протоколу SSH, чтобы продолжить управление Кибер Инфраструктура с помощью инструмента командной строки vinfra. Также может потребоваться снова установить переменную среды VINFRA_PASSWORD, поскольку теперь вы при каждом входе в систему будете осуществлять доступ к различным серверам кластера высокой доступности, а на некоторых из них она может быть не установлена.

6.8 Подготовка пространства для хранилища резервных копий к работе

Пространство хранилища для резервных копий из пакета продуктов Киберпротект подготавливается с помощью шлюза Backup Gateway, который соединяет Кибер Бэкап Облачный или Кибер Бэкап с целевым хранилищем. Целевое хранилище может быть одним из следующих:

- Локальный кластер Кибер Инфраструктура
- Внешний том NFS
- Публичное облако

Ограничения

- Чтобы можно было зарегистрировать Backup Gateway в Кибер Бэкап Облачный, для вашего тенанта партнера должна быть отключена двухфакторная проверка подлинности (2FA). Вы также можете отключить ее для выбранного пользователя в тенанте с поддержкой 2FA, как описано в Руководстве администратора партнера в разделе "Управление двухфакторной проверкой подлинности для пользователей", и указать учетные данные этого пользователя.

Предварительные требования

- Четкое понимание понятий, связанных с хранилищем резервных копий, которое описывается в разделе "О хранилище резервных копий" на странице 16.
- Оборудование, соответствующее требованиям, приведенным в разделе "Требования к хранилищу резервных копий" на странице 50.
- Сети инфраструктуры должны быть настроены, как описано в разделе "Настройка сетей для хранилища резервных копий" на странице 110.
- Кластер хранилища должен быть создан в соответствии с указаниями из раздела "Развертывание кластера хранилища данных" на странице 141.
- В Кибер Бэкап Облачный должна существовать учетная запись партнера.

- Если включен контроль входа для веб-интерфейса Кибер Бэкап Облачный, убедитесь, что внешний IP-адрес кластера хранилища резервных копий добавлен в список разрешенных IP-адресов, как описано в Руководстве администратора партнера в разделе "Ограничение доступа к веб-интерфейсу".

Обзор подготовки к работе

1. Создайте хранилище резервных копий в этом кластере, в томе NFS или в публичном облаке.
2. Настройте Кибер Бэкап Облачный на использование нового хранилища резервных копий.

6.8.1 Создание хранилища резервных копий в локальном кластере

Ограничения

- Избыточность за счет репликации не поддерживается для хранилищ резервных копий.

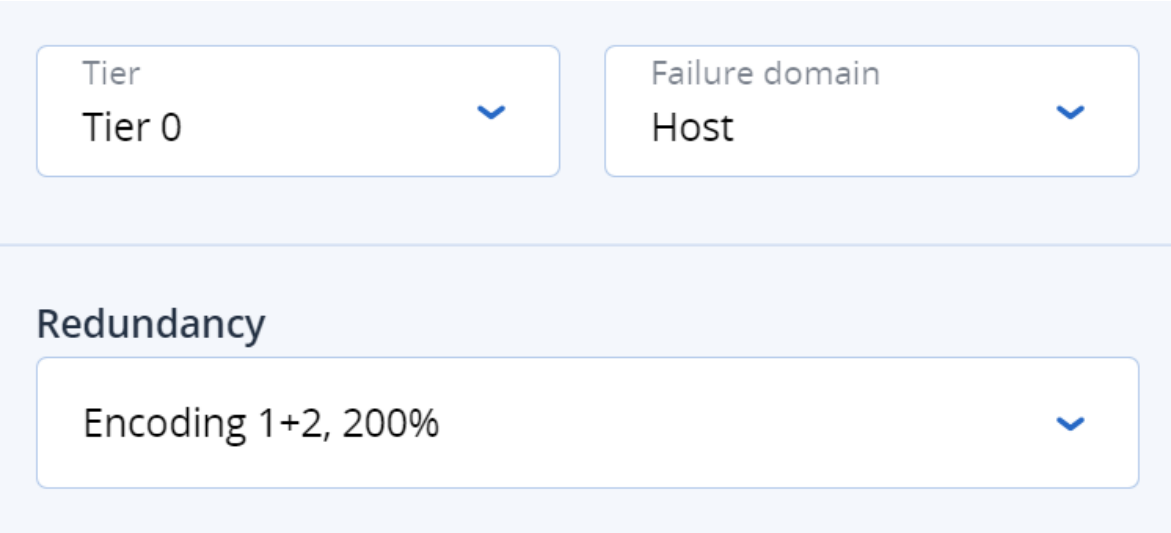
Предварительные требования

- В целевом хранилище достаточно места как для существующих, так и для новых резервных копий.
- Убедитесь, что на каждом сервере, который будет присоединен к кластеру хранилища резервных копий, открыт TCP-порт 44445 для исходящих подключений к Интернету, а также для входящих подключений от продукта Кибер Бэкап.

Как выбрать локальный кластер в качестве места назначения резервных копий

Панель администратора

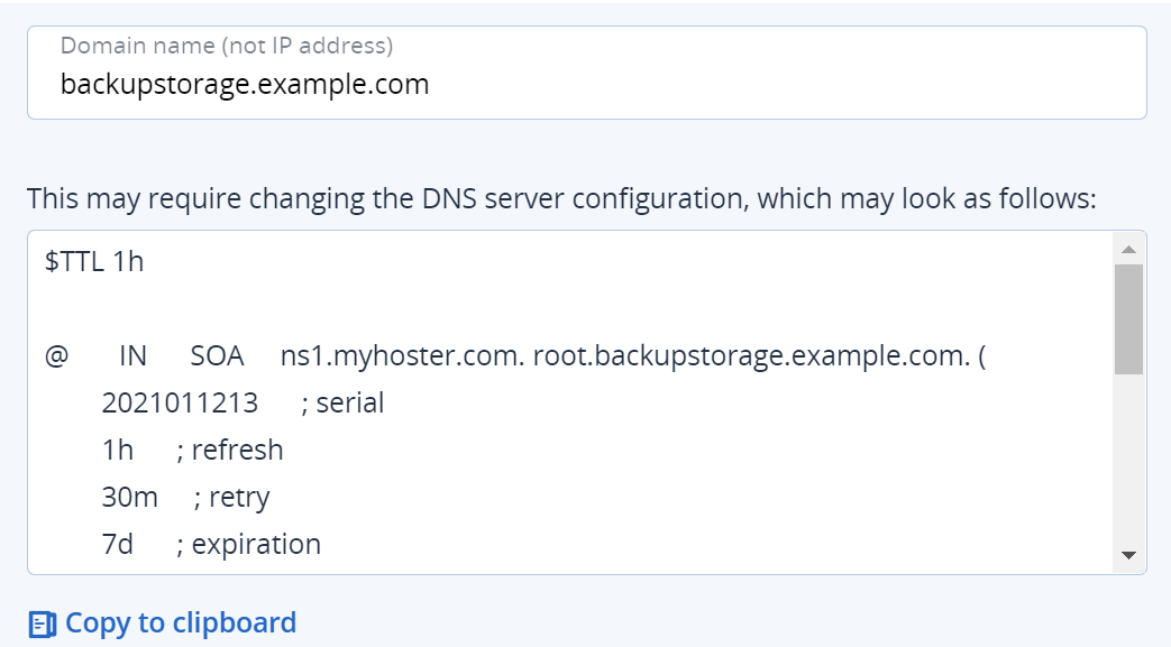
1. На экране **Инфраструктура** > **Сети** убедитесь, что в сети, которые вы собираетесь использовать, добавлены типы трафика **Резервное копирование (ABGW) внутр.** и **Резервное копирование (ABGW) внешн.**
2. Откройте экран **Сервисы хранилища** > **Резервные копии** и нажмите **Создать хранилище резервных копий**.
3. На шаге **Место назначения резервных копий** выберите **Кибер Инфраструктура кластер**.
4. На шаге **Серверы** выберите серверы, которые нужно добавить в кластер хранилища резервных копий, и нажмите **Далее**.
5. На шаге **Политика хранения** выберите нужный уровень, область отказов и режим избыточности данных. Затем нажмите кнопку **Далее**.



6. На шаге **DNS** укажите внешнее доменное имя для хранилища резервных копий, например **backupstorage.example.com**. Агенты резервного копирования будут использовать это доменное имя и TCP-порт 44445 для передачи данных в хранилище. Затем нажмите кнопку **Далее**.

Внимание

- Настройте свой DNS-сервер в соответствии с примером, приведенным на панели администратора.
- При каждом изменении сетевой конфигурации серверов в кластере хранилища резервных копий корректируйте записи DNS соответствующим образом.



Примечание

В сложных средах можно использовать HAProxy для создания масштабируемой избыточной платформы балансировки нагрузки, которую можно легко перемещать или переносить, независимо от продукта Кибер Инфраструктура. Дополнительные сведения см. в статье Как запустить хранилище за HAProxy.

7. На шаге **Учетная запись Киберпротект** укажите следующую информацию для вашего продукта Киберпротект:
   - URL-адрес портала управления облаком или имя хоста/IP-адрес и порт локального сервера управления (например, http://192.168.1.2:9877)
   - Данные партнерской учетной записи в облаке или учетные данные администратора организации на локальном сервере управления.
8. На шаге **Сводка** просмотрите конфигурацию и нажмите **Создать**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service backup cluster create --nodes <nodes> --domain <domain>
                                     --reg-account <reg-account>
                                     --reg-server <reg-server>
                                     --tier {0,1,2,3} --encoding <M>+<N>
                                     --failure-domain {0,1,2,3,4}
                                     --storage-type local [--stdin]
```

--nodes <nodes>

Список имен хостов или идентификаторов серверов через запятую

--domain <domain>

Имя домена для кластера хранилища резервных копий

--reg-account <reg-account>

Партнерская учетная запись в облаке или учетная запись администратора организации на локальном сервере управления

--reg-server <reg-server>

URL-адрес портала управления облаком или имя хоста/IP-адрес и порт локального сервера управления

--tier {0,1,2,3}

Уровень хранилища

--encoding <M>+<N>

Схема помехоустойчивого кодирования хранилища в формате:

- M: число блоков данных
- N: число паритетных блоков

--failure-domain {0,1,2,3,4}

Область отказа хранилища

--storage-type local

Тип хранилища. Укажите значение local.

--stdin

Используется для настройки пароля регистрации из stdin.

Например, чтобы создать кластер хранилища резервных копий, который будет состоять из трех серверов и использовать локальное хранилище, выполните:

```
# vinfra service backup cluster create --nodes node001,node002,node003 --storage-type local --
domain dns.example.com \
--tier 0 --encoding 1+2 --failure-domain 1 --reg-account account@example.com --reg-server
https://cloud.example.com/ --stdin
```

Эта команда также задает доменное имя, уровень хранилища, область отказа, регистрационную учетную запись и URL-адрес портала.

Просмотреть подробную информацию о кластере хранилища резервных копий можно в выводе команды vinfra service backup cluster show:

```
# vinfra service backup cluster show
+-----------------+--------------------------------------+
| Field           | Value                                |
+-----------------+--------------------------------------+
| abgw_address    | dns.example.com                      |
| account_server  | https://cloud.example.com            |
| dc_uid          | d2c8a676-102e-4d76-8da9-9b9a57847c9f |
| deployment_mode | standalone                           |
| hosts           | - node001.vstoragedomain             |
|                 | - node002.vstoragedomain             |
|                 | - node003.vstoragedomain             |
| migration       | dns: null                            |
|                 | ips: []                              |
|                 | running: false                       |
|                 | time_left: 0.0                       |
| reg_type        | abc                                  |
| storage_params  |                                      |
| storage_type    | local                                |
| upstreams       | []                                   |
+-----------------+--------------------------------------+
```

6.8.2 Создание хранилища резервных копий в публичном облаке

Backup Gateway позволяет Кибер Бэкап Облачный или Кибер Бэкап использовать для хранения резервных копий публичные облачные сервисы и локальные хранилища объектов:

- Yandex Object Storage
- VK Cloud Storage
- SberCloud OBS
- CloudMTS S3 Object Storage
- Amazon S3
- IBM Cloud
- Alibaba Cloud
- IIJ
- Cleversafe
- Cloudian
- Microsoft Azure
- Объектное хранилище Swift
- Softlayer (Swift)
- Google Cloud Platform
- Wasabi
- Другие решения, использующие S3

Однако по сравнению с локальными кластерами хранение данных резервных копий в публичном облаке увеличивает время задержки всех запросов ввода-вывода к резервным копиям и снижает производительность. По этой причине рекомендуется использовать в качестве внутреннего хранилища локальный кластер.

Резервные копии представляют собой холодные данные со специфической схемой доступа: к этим данным обращаются редко, но они должны быть немедленно доступны при обращении. Для этого сценария экономичным вариантом будут классы хранилищ, предназначенные для долгосрочного хранения редко используемых данных. Рекомендуются следующие классы хранилищ:

- **Ice** в Yandex Object Storage
- **Cold** в SberCloud OBS
- **Infrequent Access** в Amazon S3
- **Cool Blob Storage** в Microsoft Azure
- **Nearline** и **Coldline Storage** в Google Cloud Platform

Классы архивных хранилищ, такие как Amazon S3 Glacier, Azure Archive Blob или Google Archive, не могут использоваться для резервного копирования, поскольку не предоставляют мгновенного доступа к данным. Большая задержка при доступе (несколько часов) делает технически невозможным просмотр архивов, быстрое восстановление данных и создание инкрементных резервных копий. Хотя архивные хранилища, как правило, очень экономичны, следует учитывать, что существуют различные факторы, определяющие стоимость. В действительности общая стоимость публичного облачного хранилища складывается из платы за хранение данных,

операции, трафик, извлечение данных, досрочное удаление и т. д. Например, сервис архивного хранилища может брать полугодовую стоимость хранения всего за одну операцию восстановления данных. Если предполагается более частый доступ к данным, то добавочные расходы значительно повышают общую стоимость хранилища. Чтобы избежать низкой скорости извлечения данных и сократить расходы, рекомендуем использовать Кибер Бэкап Облачный для хранения данных резервного копирования.

Ограничения

- Избыточность за счет репликации не поддерживается для хранилищ резервных копий.

Предварительные требования

- В целевом хранилище достаточно места как для существующих, так и для новых резервных копий.
- Убедитесь, что на каждом сервере, который будет присоединен к кластеру хранилища резервных копий, открыт TCP-порт 44445 для исходящих подключений к Интернету, а также для входящих подключений от продукта Кибер Бэкап.

Как выбрать публичное облако в качестве места назначения резервных копий

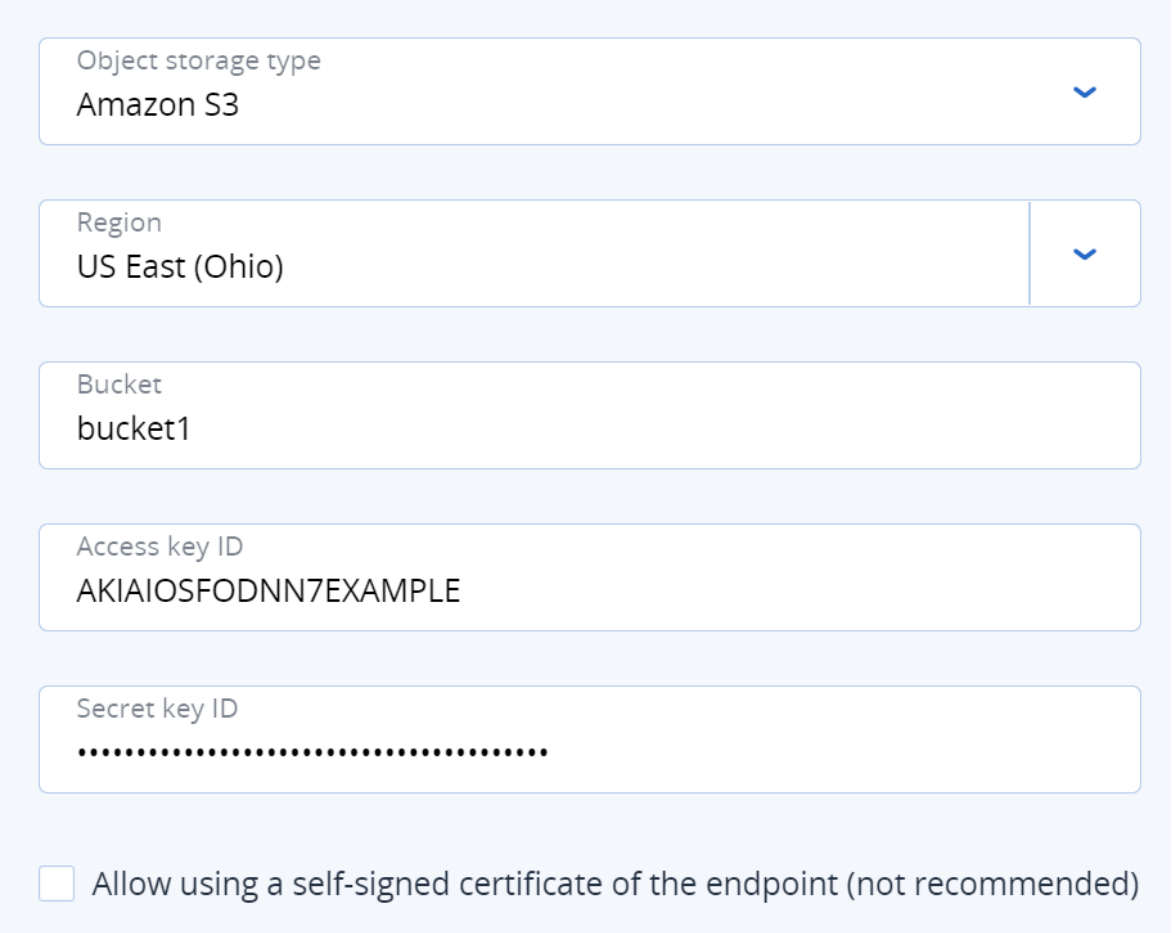
Панель администратора

1. На экране **Инфраструктура** > **Сети** убедитесь, что в сети, которые вы собираетесь использовать, добавлены типы трафика **Резервное копирование (ABGW) внутр.** и **Резервное копирование (ABGW) внешн.**
2. Откройте экран **Сервисы хранилища** > **Резервные копии** и нажмите **Создать хранилище резервных копий**.
3. На шаге **Место назначения резервной копии** выберите **Облачный сервис**.
4. На шаге **Серверы** выберите серверы, которые нужно добавить в кластер хранилища резервных копий, и нажмите **Далее**.
5. На шаге **Облачный сервис** укажите информацию, связанную с поставщиком облачного сервиса.
   a. Выберите поставщика облачного сервиса. Если ваш сервис совместим с S3, но отсутствует в списке, попробуйте **AuthV2-совместимый (S3)** или **AuthV4-совместимый (S3)** сервис.
   b. В зависимости от поставщика укажите **Регион**, **URL аутентификации (Keystone)** или **URL точки доступа**.
   c. При использовании **объектного хранилища Swift** укажите версию протокола аутентификации и необходимые для него атрибуты.
   d. Укажите учетные данные пользователя. При использовании **Google Cloud** выберите файл JSON с ключами для загрузки.
   e. Укажите папку (корзину, контейнер) для хранения резервных копий. Папка должна быть доступна для записи.
   f. Для объектного хранилища типа **AuthV4-совместимый (S3)** укажите, какую модель адресации необходимо использовать для доступа.

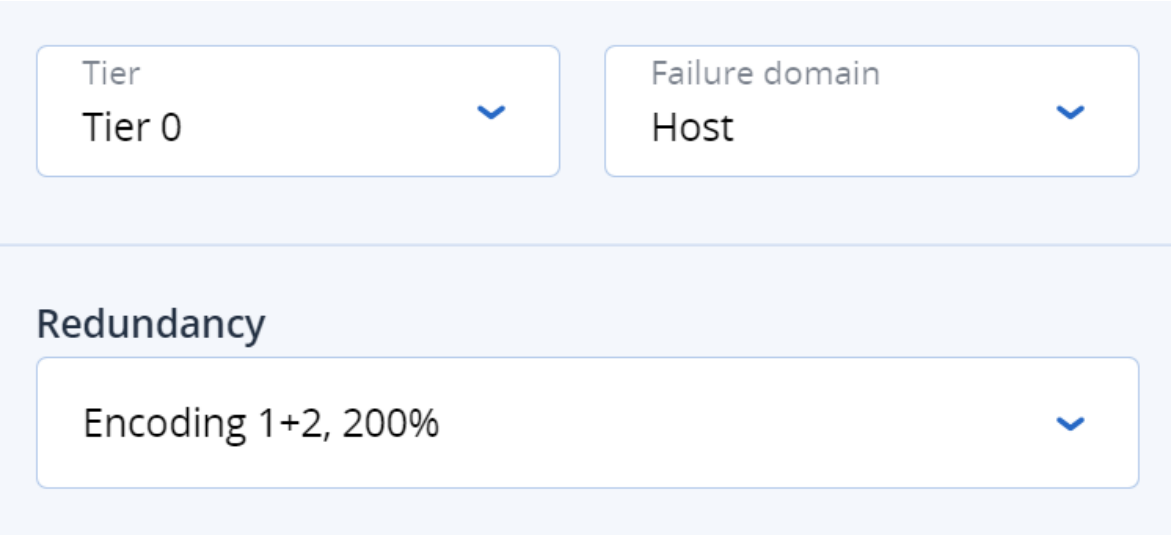
- Virtual-hosted style URLs. Адреса вида https://mybucket.s3.example.com/myobject.txt. Предназначена для облачных S3-хранилищ.
- Path-style URLs. Адреса вида https://s3.example.com/mybucket/myobject.txt. Предназначена для локальных S3-хранилищ.

Модель Virtual-hosted style URLs используется по умолчанию. Для использования модели Path-style URLs установите флажок **Использовать адресацию path-style**.

g. Нажмите кнопку **Далее**.



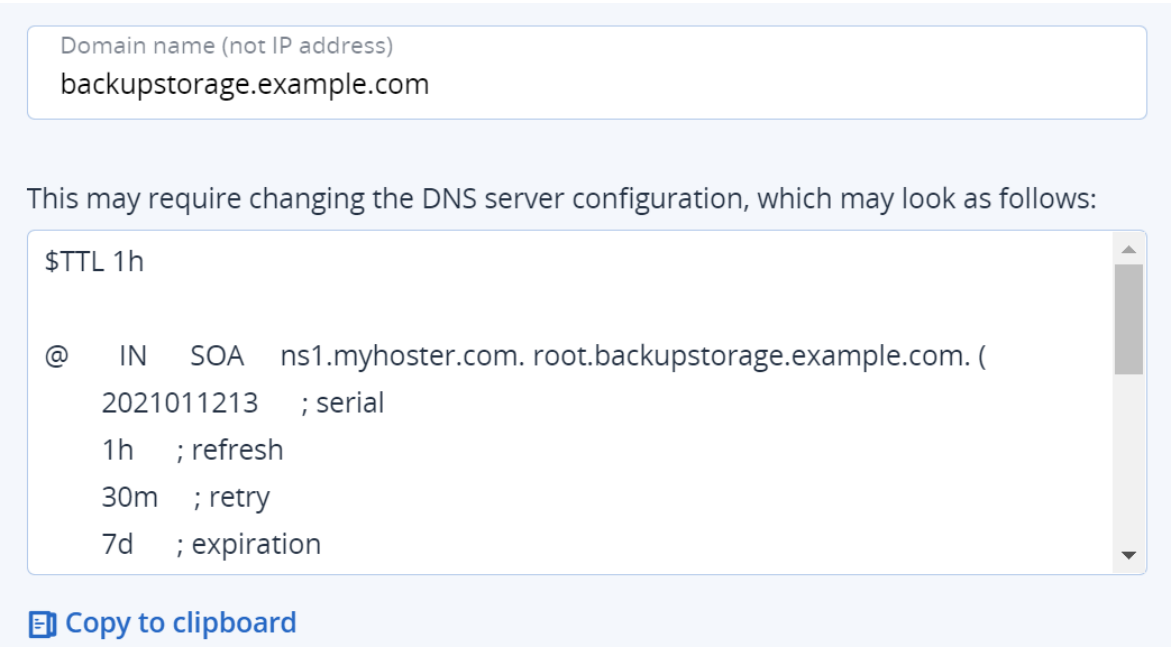
6. На шаге **Политика хранения** выберите нужный уровень, область отказов и режим избыточности данных. Затем нажмите кнопку **Далее**.



7. На шаге **DNS** укажите внешнее доменное имя для хранилища резервных копий, например **backupstorage.example.com**. Агенты резервного копирования будут использовать это доменное имя и TCP-порт 44445 для передачи данных в хранилище. Затем нажмите кнопку **Далее**.

Внимание

- Настройте свой DNS-сервер в соответствии с примером, приведенным на панели администратора.
- При каждом изменении сетевой конфигурации серверов в кластере хранилища резервных копий корректируйте записи DNS соответствующим образом.



Примечание

В сложных средах можно использовать HAProxy для создания масштабируемой избыточной платформы балансировки нагрузки, которую можно легко перемещать или переносить, независимо от продукта Кибер Инфраструктура. Дополнительные сведения см. в статье Как запустить хранилище за HAProxy.

8. На шаге **Учетная запись Киберпротект** укажите следующую информацию для вашего продукта Киберпротект:
   - URL-адрес портала управления облаком или имя хоста/IP-адрес и порт локального сервера управления (например, http://192.168.1.2:9877)
   - Данные партнерской учетной записи в облаке или учетные данные администратора организации на локальном сервере управления.
9. На шаге **Сводка** просмотрите конфигурацию и нажмите **Создать**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service backup cluster create --nodes <nodes> --domain <domain>
                                     --reg-account <reg-account>
                                     --reg-server <reg-server>
                                     --tier {0,1,2,3} --encoding <M>+<N>
                                     --failure-domain {0,1,2,3,4}
                                     --storage-type {s3,swift,azure,google}
                                     [--s3-flavor <flavor>]
                                     [--s3-region <region>]
                                     [--s3-bucket <bucket>]
                                     [--s3-endpoint <endpoint>]
                                     [--s3-access-key-id <access-key-id>]
                                     [--s3-secret-key-id <secret-key-id>]
                                     [--s3-cert-verify <cert-verify>]
                                     [--swift-auth-url <auth-url>]
                                     [--swift-auth-version <auth-version>]
                                     [--swift-user-name <user-name>]
                                     [--swift-api-key <api-key>]
                                     [--swift-domain <domain>]
                                     [--swift-domain-id <domain-id>]
                                     [--swift-tenant <tenant>]
                                     [--swift-tenant-id <tenant-id>]
                                     [--swift-tenant-domain <tenant-domain>]
                                     [--swift-tenant-domain-id <tenant-domain-id>]
                                     [--swift-trust-id <trust-id>]
                                     [--swift-region <region>]
                                     [--swift-internal <internal>]
                                     [--swift-container <container>]
                                     [--swift-cert-verify <cert-verify>]
                                     [--azure-endpoint <endpoint>]
                                     [--azure-container <container>]
                                     [--azure-account-name <account-name>]
```

```
                [--azure-account-key <account-key>]
                [--google-bucket <bucket>]
                [--google-credentials <credentials>] [--stdin]
```

--nodes <nodes>

Список имен хостов или идентификаторов серверов через запятую

--domain <domain>

Имя домена для кластера хранилища резервных копий

--reg-account <reg-account>

Партнерская учетная запись в облаке или учетная запись администратора организации на локальном сервере управления

--reg-server <reg-server>

URL-адрес портала управления облаком или имя хоста/IP-адрес и порт локального сервера управления

--tier {0,1,2,3}

Уровень хранилища

--encoding <M>+<N>

Схема помехоустойчивого кодирования хранилища в формате:

- M: число блоков данных
- N: число паритетных блоков

--failure-domain {0,1,2,3,4}

Область отказа хранилища

--storage-type {s3,swift,azure,google}

Тип хранилища

--stdin

Используется для настройки пароля регистрации из stdin.

Параметры хранилища типа s3:

--s3-flavor <flavor> (необязательно)

Имя типа ВМ

--s3-region <region> (необязательно)

Задайте регион для Amazon S3.

--s3-bucket <bucket>

Имя корзины

--s3-endpoint <endpoint>

URL-адрес оконечной точки

--s3-access-key-id <access-key-id>

Идентификатор ключа доступа

--s3-secret-key-id <secret-key-id>

Идентификатор секретного ключа

--s3-cert-verify <cert-verify> (необязательно)

Разрешить самозаверяющий сертификат оконечной точки S3

Параметры хранилища типа swift:

--swift-auth-url <auth-url>

URL аутентификации (Keystone)

--swift-auth-version <auth-version> (необязательно)

Версия протокола проверки подлинности

--swift-user-name <user-name>

Имя пользователя

--swift-api-key <api-key>

Ключ API (пароль)

--swift-domain <domain> (необязательно)

Имя домена

--swift-domain-id <domain-id> (необязательно)

Идентификатор домена

--swift-tenant <tenant> (необязательно)

Имя тенанта

--swift-tenant-id <tenant-id> (необязательно)

Идентификатор тенанта

--swift-tenant-domain <tenant-domain> (необязательно)

Имя домена тенанта

--swift-tenant-domain-id <tenant-domain-id> (необязательно)

Идентификатор домена тенанта

--swift-trust-id <trust-id> (необязательно)

Идентификатор Trust

--swift-region <region> (необязательно)

Имя региона

--swift-container <container> (необязательно)

Имя контейнера

--swift-cert-verify <cert-verify> (необязательно)

Разрешить самозаверяющий сертификат оконечной точки Swift (true или false)

Параметры хранилища типа azure:

--azure-endpoint <endpoint>

URL-адрес оконечной точки

--azure-container <container>

Имя контейнера

--azure-account-name <account-name>

Имя учетной записи

--azure-account-key <account-key>

Ключ учетной записи

Параметры хранилища типа google:

--google-bucket <bucket>

Имя корзины Google

--google-credentials <credentials>

Путь к файлу с учетными данными Google

Например, чтобы создать кластер хранилища резервного копирования, который будет состоять из трех серверов и использовать хранилище типа S3, выполните:

```
# vinfra service backup cluster create --nodes node001,node002,node003
--storage-type s3 --domain dns.example.com \
--tier 0 --encoding 1+2 --failure-domain host --s3-bucket mybucket --s3-endpoint s3.amazonaws.com
\
--s3-access-key-id e302a06df8adbe9fAIF1 --s3-secret-key-id
x1gXquRHQXuyiUJQoQMoAohA2TkYHer20o8tfPX7 \
--s3-cert-verify true --reg-account account@example.com --reg-server https://cloud.example.com/ --
stdin
```

Эта команда также задает доменное имя, уровень хранилища, область отказа, регистрационную учетную запись, URL-адрес портала и необходимые параметры S3.

Просмотреть подробную информацию о кластере хранилища резервных копий можно в выводе команды vinfra service backup cluster show:

```
# vinfra service backup cluster show
+----------------+-------------------------------------------------------+
| Field          | Value                                                 |
+----------------+-------------------------------------------------------+
| abgw_address   | dns.example.com                                       |
| account_server | https://cloud.example.com                             |
| dc_uid         | 44893a40296ecd9ae64567297a5b2b07-1577203369           |
| migration      | dns: null                                             |
|                | ips: []                                               |
|                | running: false                                        |
|                | time_left: 0.0                                        |
```

```
| reg_type      | abc                                                          |
| storage_params | access_key_id: e302a06df8adbe9fAIF1                  |
|               | bucket: mybucket                                             |
|               | cert_verify: true                                            |
|               | endpoint: s3.amazonaws.com                                   |
|               | flavour: null                                                |
|               | region: null                                                 |
|               | secret_key_id: x1gXquRHQXuyiUJQoQMoAohA2TkYHer20o8tfPX7 |
| storage_type   | s3                                                          |
+---------------+--------------------------------------------------------------+
```

6.8.3 Создание хранилища резервных копий на внешнем томе NFS

Ограничения

- Кибер Инфраструктура не обеспечивает избыточность данных поверх томов NFS. В зависимости от реализации тома NFS могут обеспечивать собственную аппаратную или программную избыточность.
- Только один сервер кластера может хранить резервные копии на томе NFS.
- Каждый экспорт NFS используется только одним шлюзом. В частности, не следует подключать два экземпляра продукта Кибер Инфраструктура к одному экспорту NFS для хранения резервных копий.
- Несколько полных резервных копий, хранящихся на томе NFS, могут потреблять дополнительное дисковое пространство из-за задержки автоматического уплотнения, которое выполняется для каждой резервной копии по очереди.

Предварительные требования

- В целевом хранилище достаточно места как для существующих, так и для новых резервных копий.
- Убедитесь, что на каждом сервере, который будет присоединен к кластеру хранилища резервных копий, открыт TCP-порт 44445 для исходящих подключений к Интернету, а также для входящих подключений от продукта Кибер Бэкап.
- Убедитесь, что у сервера, который будет присоединен к хранилищу резервных копий, есть доступ к внешнему NFS-хранилищу.

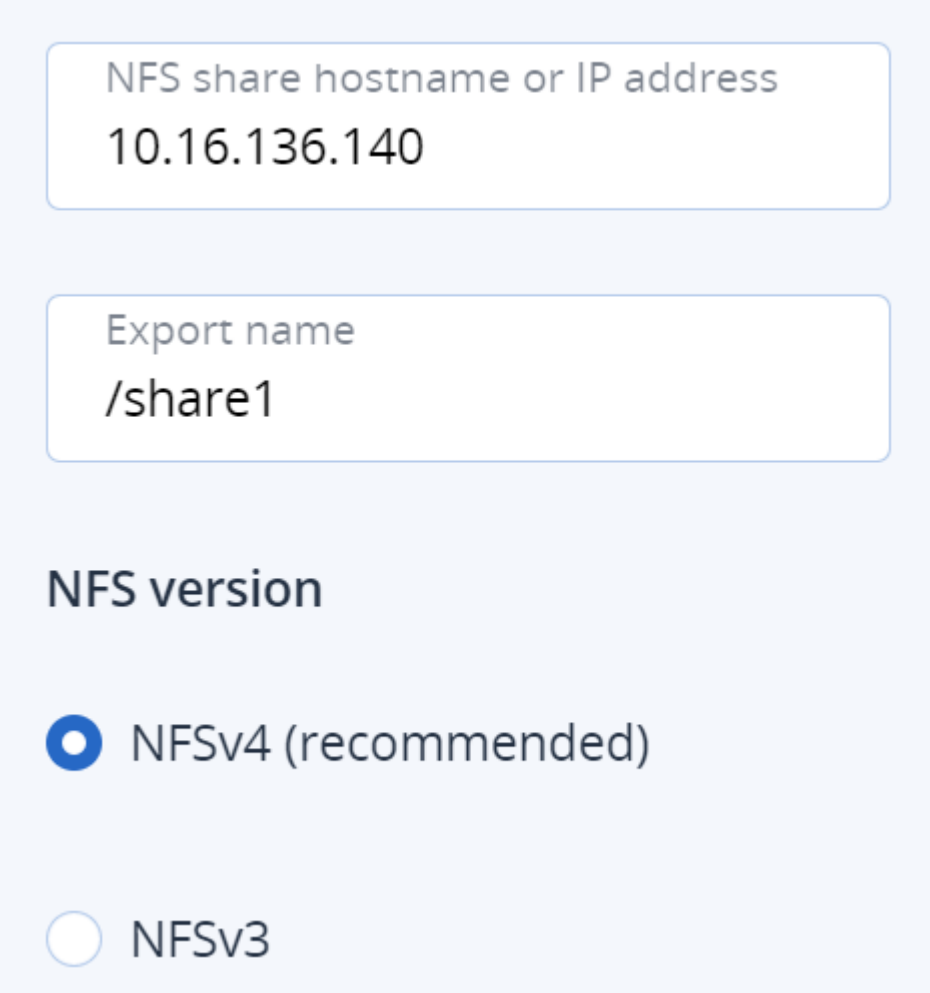
Как выбрать внешний том NFS в качестве места назначения резервных копий

Панель администратора

1. На экране **Инфраструктура** > **Сети** убедитесь, что в сети, которые вы собираетесь использовать, добавлены типы трафика **Резервное копирование (ABGW) внутр.** и **Резервное копирование (ABGW) внешн.**
2. Откройте экран **Сервисы хранилища** > **Резервные копии** и нажмите **Создать хранилище резервных копий**.
3. На шаге **Место назначения резервной копии** выберите **Том Network File System (NFS)**.

4. На шаге **Серверы** выберите один сервер для добавления в кластер хранилища резервных копий и нажмите кнопку **Далее**.
5. На шаге **Том NFS** укажите имя хоста или IP-адрес тома NFS, имя экспорта и версию NFS. Затем нажмите кнопку **Далее**.

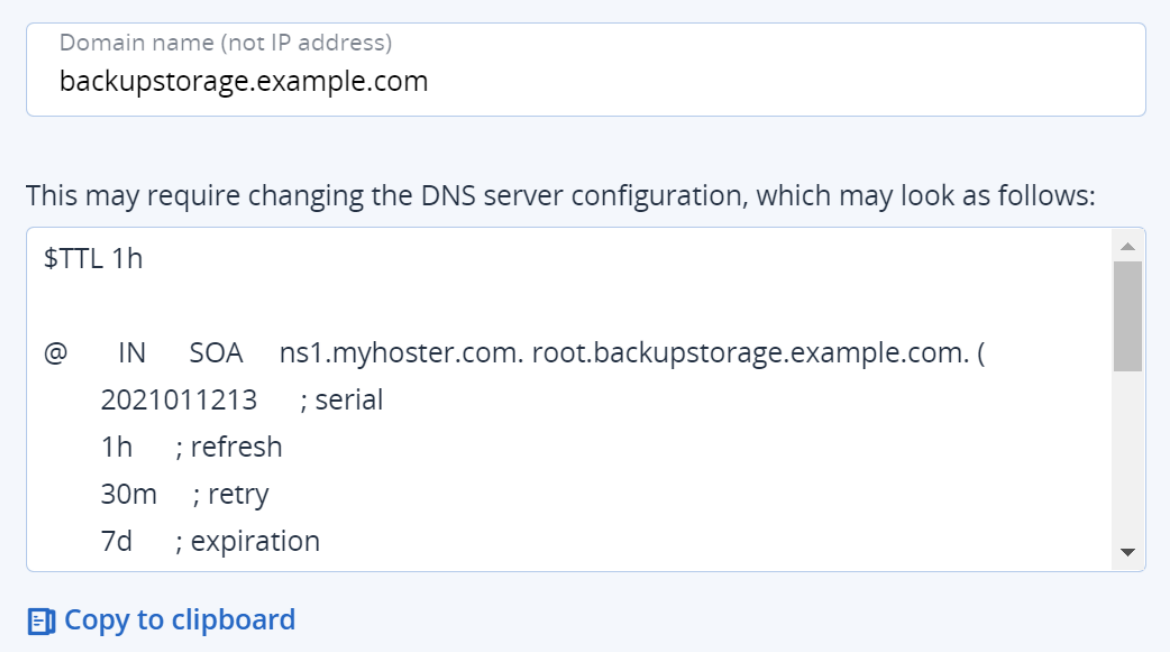
Примечание
Рекомендуется использовать NFS версии 4, поскольку она обеспечивает лучшую масштабируемость и производительность по сравнению с версией 3, которая имеет ограничения в протоколе.



6. На шаге **DNS** укажите внешнее доменное имя для хранилища резервных копий, например **backupstorage.example.com**. Агенты резервного копирования будут использовать это доменное имя и TCP-порт 44445 для передачи данных в хранилище. Затем нажмите кнопку **Далее**.

Внимание

- Настройте свой DNS-сервер в соответствии с примером, приведенным на панели администратора.
- При каждом изменении сетевой конфигурации серверов в кластере хранилища резервных копий корректируйте записи DNS соответствующим образом.



7. На шаге **Учетная запись Киберпротект** укажите следующую информацию для вашего продукта Киберпротект:
   - URL-адрес портала управления облаком или имя хоста/IP-адрес и порт локального сервера управления (например, http://192.168.1.2:9877)
   - Данные партнерской учетной записи в облаке или учетные данные администратора организации на локальном сервере управления.
8. На шаге **Сводка** просмотрите конфигурацию и нажмите **Создать**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service backup cluster create --nodes <nodes> --domain <domain>
                                     --reg-account <reg-account>
                                     --reg-server <reg-server>
                                     --tier {0,1,2,3} --encoding <M>+<N>
                                     --failure-domain {0,1,2,3,4}
                                     --storage-type nfs
                                     --nfs-host <host>
                                     --nfs-export <export>
                                     --nfs-version <version> [--stdin]
```

--nodes <nodes>

Список имен хостов или идентификаторов серверов через запятую

--domain <domain>

Имя домена для кластера хранилища резервных копий

--reg-account <reg-account>

Партнерская учетная запись в облаке или учетная запись администратора организации на локальном сервере управления

--reg-server <reg-server>

URL-адрес портала управления облаком или имя хоста/IP-адрес и порт локального сервера управления

--tier {0,1,2,3}

Уровень хранилища

--encoding <M>+<N>

Схема помехоустойчивого кодирования хранилища в формате:

- M: число блоков данных
- N: число паритетных блоков

--failure-domain {0,1,2,3,4}

Область отказа хранилища

--storage-type

Тип хранилища. Укажите значение nfs.

--stdin

Используется для настройки пароля регистрации из stdin.

Параметры хранилища типа nfs:

--nfs-host <host>

Имя хоста или IP-адрес NFS

--nfs-export <export>

Полный путь к экспорту NFS

--nfs-version <version>

Версия NFS (3 или 4)

Например, чтобы создать кластер хранилища резервных копий, состоящий из сервера node001 и использующий хранилище типа NFS, выполните:

```
# vinfra service backup cluster create --nodes node001 --storage-type nfs --domain
dns.example.com \
--tier 0 --encoding 1+2 --failure-domain host --nfs-host 10.136.18.149 --nfs-version 4 \
```

```
--nfs-export /share1/export1 --reg-account account@example.com --reg-server
https://cloud.example.com/ --stdin
```

Эта команда также задает доменное имя, уровень хранилища, область отказа, регистрационную учетную запись, URL-адрес портала и необходимые параметры NFS.

Просмотреть подробную информацию о кластере хранилища резервных копий можно в выводе команды vinfra service backup cluster show:

```
# vinfra service backup cluster show
+----------------+-------------------------------------+
| Field          | Value                               |
+----------------+-------------------------------------+
| abgw_address   | dns.example.com                     |
| account_server | https://cloud.example.com           |
| dc_uid         | 8f8fa1c5-cbfd-4b22-ba69-07c20e8f2bac |
| deployment_mode | standalone                         |
| hosts          | - node001.vstoragedomain           |
| migration      | dns: null                          |
|                | ips: []                            |
|                | running: false                     |
|                | time_left: 0.0                     |
| reg_type       | abc                                |
| storage_params | export: share1/export1             |
|                | host: 10.136.18.149                |
|                | version: 4                         |
| storage_type   | nfs                                |
| upstreams      | []                                 |
+----------------+-------------------------------------+
```

6.8.4 Добавление хранилищ резервных копий в Кибер Бэкап и Кибер Бэкап Облачный

Предварительные требования

- Хранилище резервных копий создается в соответствии с указаниями из раздела "Создание хранилища резервных копий в локальном кластере" на странице 151, "Создание хранилища резервных копий на внешнем томе NFS" на странице 163 или "Создание хранилища резервных копий в публичном облаке" на странице 154.

Как создать нового клиента и задать новое место назначения резервных копий в Кибер Бэкап Облачный

1. Выполните вход в консоль управления Кибер Бэкап Облачный.
2. Перейдите в раздел **Настройки** > **Хранилища**. Убедитесь, что было автоматически создано новое место назначения резервных копий с именем, соответствующим доменному имени.
3. Настройте агенты резервного копирования.

4. Создайте новую учетную запись клиента.
   a. Нажмите **Создать** в правом верхнем углу и выберите **Клиент**.
   b. Введите общие сведения о клиенте: имя, режим и язык. Затем укажите адрес электронной почты, язык, имя и фамилию для учетной записи администратора.
   c. Выберите сервисы, которые вы хотите предоставлять новому клиенту.
   d. Укажите устройства и рабочие нагрузки клиента, такие как серверы и рабочие станции.
   e. В разделе **Хранилище** щелкните по имени текущего расположения, чтобы отобразить все доступные варианты. Выберите нужное хранилище.
   f. Нажмите **Готово**, чтобы завершить процесс.
5. Чтобы подтвердить учетную запись, проверьте свою электронную почту и следуйте инструкциям в запросе на активацию.

Как настроить хранилище резервных копий в Кибер Бэкап Облачный или Кибер Бэкап

1. Выполните вход в Кибер Бэкап Облачный в качестве администратора.
2. Откройте экран **Клиенты**. Щелкните по имени созданного клиента и нажмите **Управление сервисом** на экране **Сводка**. Откроется клиентская консоль управления резервным копированием.
3. На экране **Устройства** нажмите **Добавить** на панели инструментов. Выберите устройство, которое нужно добавить. Будет загружен установщик агента резервного копирования.
4. В программе установки агента:
   a. Нажмите **Установить**.
   b. На экране **Почти готово...** нажмите **Зарегистрировать машину**.
   c. Введите регистрационные данные устройства и подтвердите их.
   d. Убедитесь, что используется созданная учетная запись клиента: проверьте имя пользователя в правом верхнем углу.

После завершения регистрации добавленное устройство будет отображаться на экране **Устройства** > **Все устройства** в клиентской консоли управления резервным копированием.

6.9 Подготовка вычислительных ресурсов к работе

Мультитенантные вычислительные ресурсы, такие как виртуальные ЦП, ОЗУ, хранилища, плавающие IP-адреса, балансировщики нагрузки и кластеры Kubernetes, можно подготавливать к работе для конечных пользователей на панели самообслуживания. Кроме того, можно установить сервис учета и биллинга, чтобы собирать данные об использовании вычислительных ресурсов в различных проектах.

Ограничения

- Пространство хранилища для вычислительных ресурсов не полностью реализует экономное распределение. После удаления пользовательских данных неиспользуемое пространство хранилища не высвобождается и о нем сообщается как о фактически используемом

пространстве, за которое взимается оплата в соответствии с вашей моделью лицензирования. Более подробные сведения см. в разделе "Диаграмма «Логическое пространство»" на странице 732.

Предварительные требования

- Четкое понимание понятий, связанных с вычислительным кластером, который описывается в разделе "О вычислительном кластере" на странице 22.
- Оборудование, соответствующее требованиям, приведенным в разделе "Требования для вычислительного кластера" на странице 54.
- Сети инфраструктуры должны быть настроены, как описано в разделе "Настройка сетей в вычислительном кластере" на странице 113.
- Кластер хранилища должен быть создан в соответствии с указаниями из раздела "Развертывание кластера хранилища данных" на странице 141.

Обзор подготовки к работе

1. Создайте вычислительный кластер. После создания кластера можно управлять вычислительными объектами с панели администрирования (см. раздел "Управление вычислительным кластером" на странице 427).
2. Настройте вычислительные узлы так, чтобы для виртуальных машин использовалась одна и та же модель ЦП.
3. Задайте DNS-имя для API вычислений.
4. Защитите трафик API OpenStack с помощью SSL.
5. Создайте домены, проекты и пользователей.
6. Предоставьте доступ к панели самообслуживания. После настройки панели можно выполнить вход на нее от имени пользователя самообслуживания и приступить к управлению вычислительными объектами (см. руководство по самообслуживанию).
7. Если необходимо подготовить к работе балансировщик нагрузки как услугу, установите сервис балансировщика нагрузки.
8. Если необходимо подготовить к работе Kubernetes как услугу, установите сервис Kubernetes.
9. Если необходимо подготовить к работе учет и биллинг, установите сервис учета и биллинга.

6.9.1 Создание вычислительного кластера

Ограничения

- В вычислительном кластере должно быть как минимум три сервера, чтобы пользователи в режиме самообслуживания могли включить высокую доступность для мастер-серверов Kubernetes.
- Поверх сети инфраструктуры можно создать только одну нетегированную сеть.

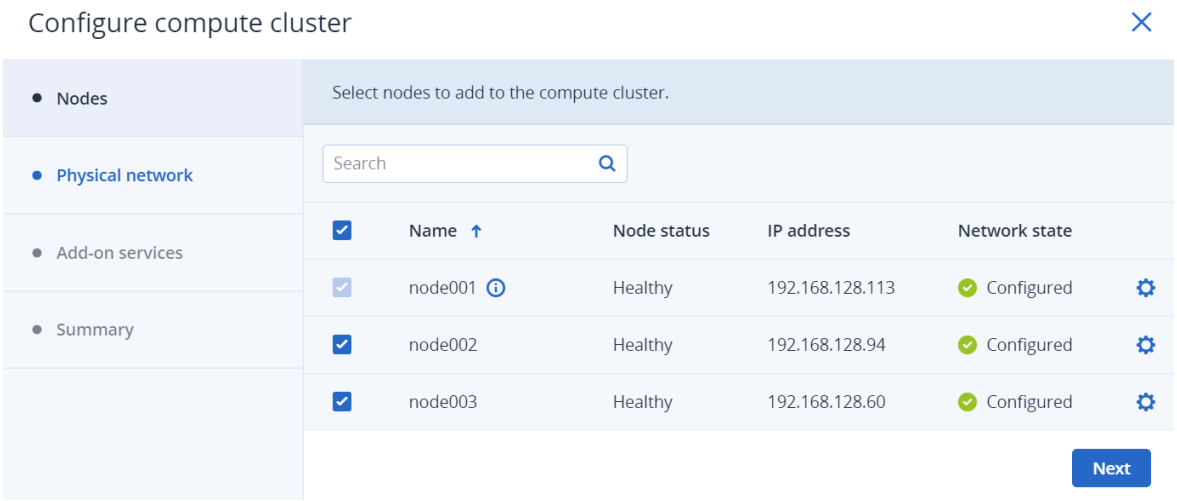
Предварительные требования

- В кластере хранилища данных есть один или более дисков с ролью **Хранилище**.

Чтобы создать вычислительный кластер

Панель администратора

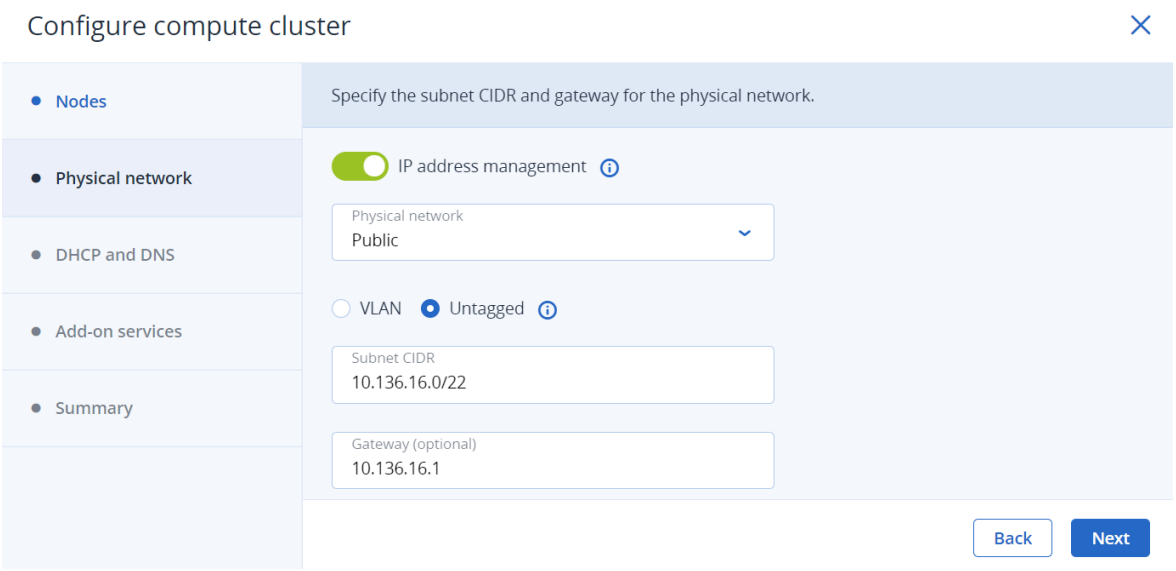
1. Откройте экран **Вычисления** и нажмите **Создать вычислительный кластер**.
2. На шаге **Серверы** добавьте серверы в вычислительный кластер:
   a. Выберите серверы для добавления в вычислительный кластер. Можно выбрать только серверы с состоянием сети **Настроено**. Серверы в кластере высокой доступности сервера управления автоматически выбираются для присоединения к вычислительному кластеру.
   b. Если сетевые интерфейсы серверов не настроены, щелкните по значку шестерни, выберите необходимые сети и нажмите **Применить**.
   c. Нажмите кнопку **Далее**.



3. На шаге **Физическая сеть** выполните следующие действия:
   a. Включите или отключите управление IP-адресами:
      - Если управление IP-адресами включено, встроенный DHCP-сервер автоматически назначит ВМ, подключенным к сети, IP-адреса из пулов IP-адресов, а также задаст для ВМ настраиваемые DNS-серверы. Кроме того, по умолчанию для всех сетевых портов ВМ будет включена защита от спуфинга. Каждый сетевой интерфейс ВМ сможет принимать и отправлять IP-пакеты, только если ему назначены IP- и MAC-адреса. При необходимости защиту от спуфинга для интерфейса ВМ можно отключить вручную.
      - Если управление IP-адресами отключено, то ВМ, подключенные к сети, получат IP-адреса от DHCP-серверов в этой сети (при их наличии). Кроме того, защита от спуфинга будет отключена для всех сетевых портов ВМ, и ее нельзя будет включить вручную. Это означает, что каждый сетевой интерфейс ВМ с назначенными IP- и MAC-адресами или без них сможет принимать и отправлять IP-пакеты.

      В любом случае можно будет вручную назначить статические IP-адреса изнутри виртуальных машин.

b. Укажите необходимые сведения для физической сети:
   i. Выберите сеть инфраструктуры, к которой будет подключена физическая сеть.
   ii. Выберите тип физической сети: выберите **VLAN** и укажите идентификатор VLAN для создания сети на базе VLAN либо выберите **Untagged** (Без тега) для создания плоской физической сети.
   iii. Если вы включили управление IP-адресами, диапазон IP-адресов подсети в формате CIDR будет заполнен автоматически. При необходимости можно указать шлюз. Если оставить поле **Шлюз** пустым, то шлюз будет исключен из сетевых параметров.
c. Нажмите кнопку **Далее**.

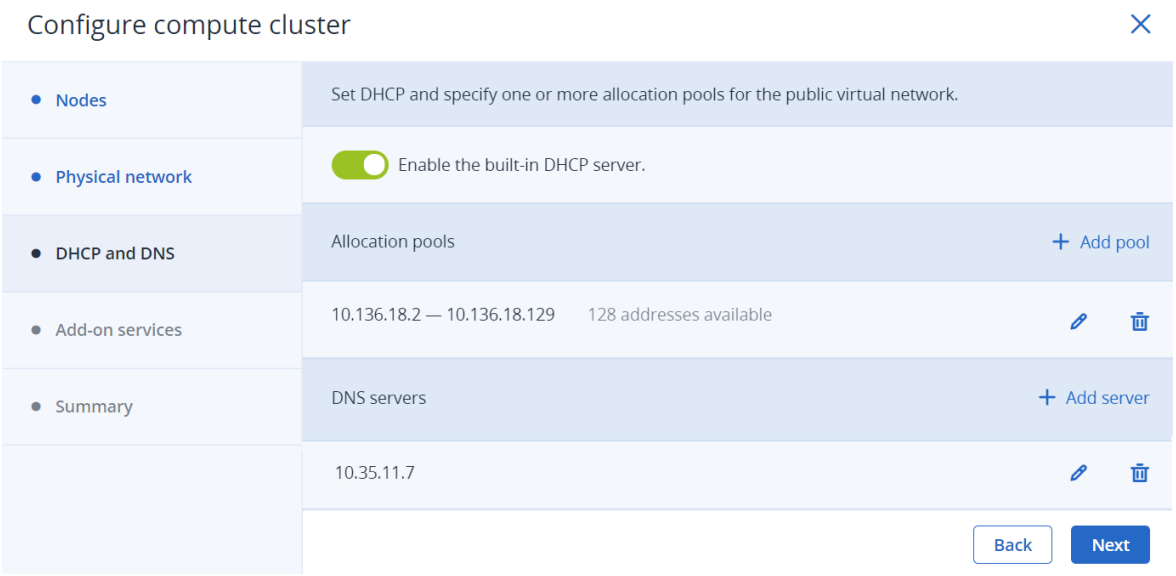


Выбранная физическая сеть появится в списке вычислительных сетей на вкладке **Сеть** вычислительного кластера. По умолчанию она будет совместно использоваться всеми будущими проектами. Доступ к сети можно позже отключить на правой панели сети.

4. Если вы включили управление IP-адресами, вы будете перенаправлены на шаг **DHCP и DNS**, где можно настроить сетевые параметры для управления IP-адресами.
   a. Включите или отключите встроенный DHCP-сервер:
      - Если DHCP-сервер включен, сетевым интерфейсам ВМ будут автоматически назначены IP-адреса: либо из пулов IP-адресов, либо при отсутствии пулов из всего диапазона IP-адресов сети. DHCP-сервер получит первые два IP-адреса из пула IP-адресов. Например:
        - В подсети 192.168.128.0/24 без шлюза DHCP-серверу будут назначены IP-адреса 192.168.128.1 и 192.168.128.2.
        - В подсети 192.168.128.0/24, в которой шлюзу назначен IP-адрес 192.168.128.1, DHCP-серверу будут назначены IP-адреса 192.168.128.2 и 192.168.128.3.
      - Если DHCP-сервер отключен, сетевые интерфейсы ВМ все равно получат IP-адреса, но их нужно будет назначить вручную внутри виртуальных машин.

      Виртуальный DHCP-сервер будет работать только внутри текущей сети и не будет виден из других сетей.

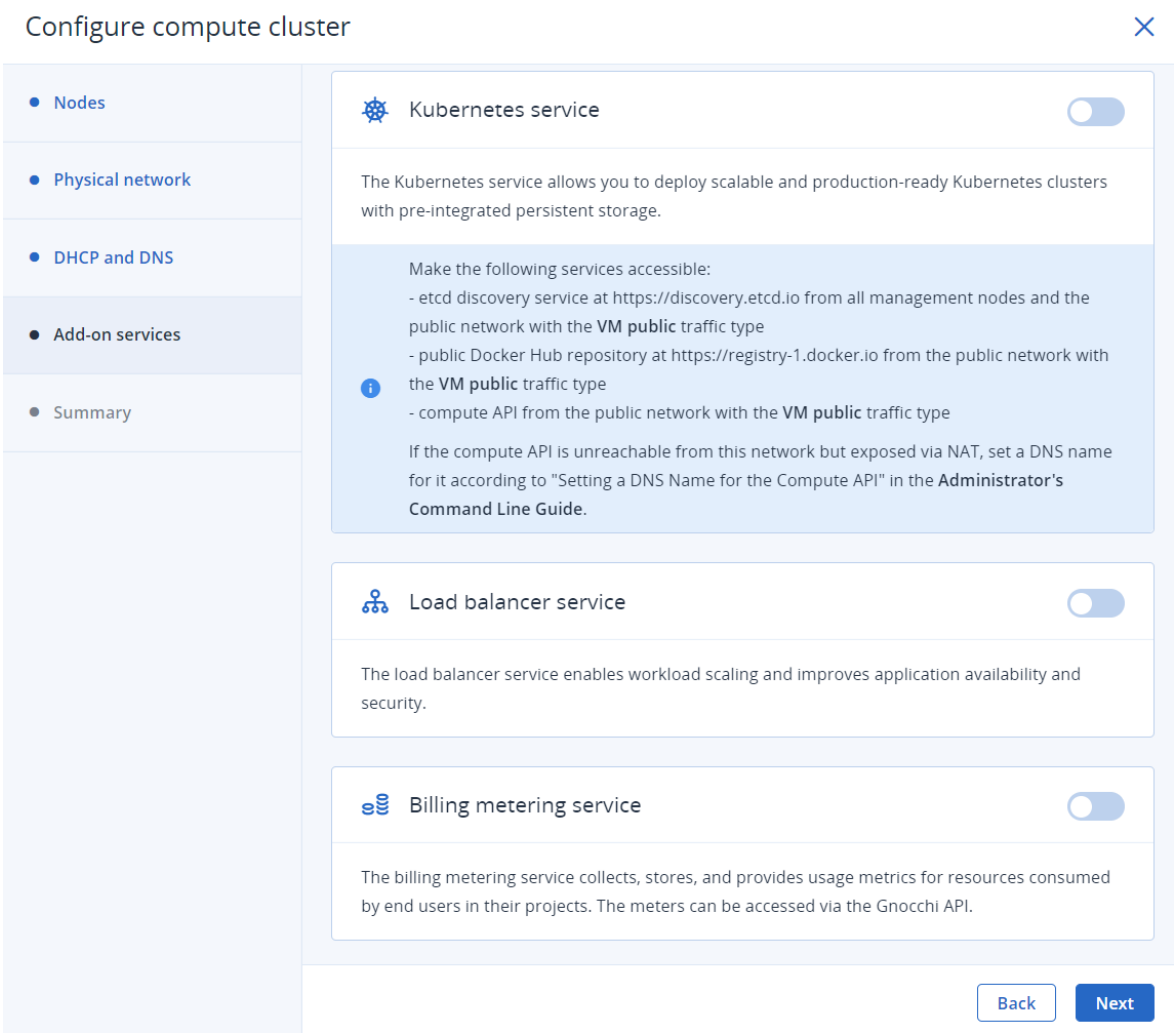
b. Укажите один или несколько пулов IP-адресов (диапазоны IP-адресов, которые будут автоматически назначаться виртуальным машинам).
c. Укажите DNS-серверы, которые будут использоваться виртуальными машинами. Эти серверы могут предоставляться виртуальным машинам посредством встроенного DHCP-сервера либо с помощью сетевой конфигурации cloud-init (если пакет cloud-init установлен в ВМ).
d. Нажмите **Добавить**.



5. На шаге **Дополнительные сервисы** включите сервисы, которые будут установлены во время развертывания вычислительного кластера. Эти сервисы также можно установить позже. Затем нажмите кнопку **Далее**.

Примечание

- При установке Kubernetes также автоматически устанавливается сервис балансировщика нагрузки.
- Для автономной установки Kubernetes и сервиса балансировщика нагрузки в среде без доступа к Интернету (в закрытом контуре) необходимо заранее установить на узлы пакеты hci-k8saas-files и amphora-x64-haproxy.qcow2.



6. На шаге **Сводка** просмотрите конфигурацию и нажмите **Создать кластер**.

Отслеживать развертывание вычислительного кластера можно на экране **Вычисления**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute create [--public-network <network>] [--subnet cidr=CIDR[,key=value,…]]
                              [--force] [--enable-k8saas] [--enable-lbaas] [--enable-metering] [--notification-
forwarding <transport-url>]
                              [--disable-notification-forwarding] [--vlan-id <vlan-id>] --nodes <nodes>
```

--public-network <network>

Инфраструктурная сеть для подключения к ней физической вычислительной сети. Должна включать тип трафика «BM внешн.».

--subnet cidr=CIDR[,key=value,…]

Подсеть для управления IP-адресами в физической вычислительной сети (требуется параметр --public-network):

- cidr: маска подсети в нотации CIDR;
- разделенные запятыми пары key=value с ключами (необязательно):
  - gateway: IP-адрес шлюза.
  - dhcp: включение/отключение виртуального DHCP-сервера.
  - allocation-pool: пул IP-адресов из CIDR в формате ip1-ip2, где ip1 и ip2 — начальный и конечный IP-адреса. Укажите ключ несколько раз, чтобы создать несколько пулов IP-адресов.
  - dns-server: IP-адрес сервера DNS; укажите несколько раз, чтобы задать несколько DNS-серверов.

Пример: --subnet cidr=192.168.5.0/24,dhcp=enable

--force

Пропустить проверку минимальных требований к оборудованию.

--enable-k8saas

Включение сервиса «Kubernetes как услуга».

--enable-lbaas

Включение сервиса «Балансировка нагрузки как услуга».

--enable-metering

Включение сервисов учета.

--notification-forwarding <transport-url>

Включение перенаправления уведомлений через указанный транспортный URL в формате driver://[user:pass@]host:port[,[userN:passN@]hostN:portN]?query, где:

- driver — поддерживаемый транспортный драйвер (kafka);
- user:pass — имя пользователя и пароль, используемые для аутентификации в брокере сообщений;
- host:port указывает имя хоста или IP-адрес и номер порта брокера сообщений;
- query — параметры, которые переопределяют указанные в файле конфигурации брокера:
  - topic указывает имя топика;
  - driver — драйвер сообщений: messaging, messagingv2, routing, log, test, noop.

Пример: kafka://10.10.10.10:9092?topic=notifications

--disable-notification-forwarding

Отключение перенаправления уведомлений

--vlan-id <vlan-id>

Создание физической сети на базе VLAN по указанному идентификатору VLAN.

--nodes <nodes>

Список имен хостов или идентификаторов серверов через запятую.

Например, чтобы создать состоящий из пяти серверов вычислительный кластер, который будет использовать инфраструктурную сеть Public и пул IP-адресов 10.94.129.64-10.94.129.79 для назначения виртуальным машинам IP-адресов, выполните:

```
# vinfra service compute create --nodes node001,node002,node003,node004,node005 \
--public-network Public --subnet cidr=10.94.0.0/16,dhcp=enable,gateway=10.94.0.1,\
allocation-pool=10.94.129.64-10.94.129.79,dns-server=10.30.0.27
```

Просмотреть сведения о вычислительном кластере можно в выводе команды vinfra service compute show:

```
# vinfra service compute show
+--------------+-------------------------------------------------------------------------------------------------------------------------+
| Field        | Value                                                                                                                   |
+--------------+-------------------------------------------------------------------------------------------------------------------------+
| capabilities | cpu_models:                                                                                                             |
|              | - EPYC-IBPB                                                                                                             |
|              | - Nehalem                                                                                                               |
|              | - Nehalem-IBRS                                                                                                          |
|              | - SandyBridge                                                                                                           |
|              | - SandyBridge-IBRS                                                                                                      |
|              | - IvyBridge                                                                                                             |
|              | - IvyBridge-IBRS                                                                                                        |
|              | - Haswell                                                                                                               |
|              | - Haswell-IBRS                                                                                                          |
|              | - Haswell-noTSX                                                                                                         |
|              | - Haswell-noTSX-IBRS                                                                                                    |
|              | - Broadwell                                                                                                             |
|              | - Broadwell-IBRS                                                                                                        |
|              | - Broadwell-noTSX                                                                                                       |
|              | - Broadwell-noTSX-IBRS                                                                                                  |
|              | - Skylake-Client                                                                                                        |
|              | - Skylake-Client-IBRS                                                                                                   |
|              | - Skylake-Server                                                                                                        |
|              | - Skylake-Server-IBRS                                                                                                   |
|              | - HostPassthrough                                                                                                       |
|              | k8saas_capabilities:                                                                                                    |
|              |   v1.18.6:                                                                                                              |
|              |     features:                                                                                                           |
|              |     - nodegroups                                                                                                        |
|              |     release: v1.18                                                                                                      |
|              |     upgrade:                                                                                                            |
|              |     - v1.19.9                                                                                                           |
|              |   v1.19.9:                                                                                                              |
|              |     features:                                                                                                           |
|              |     - nodegroups                                                                                                        |
|              |     links:                                                                                                              |
|              |       deprecation: https://v1-19.docs.kubernetes.io/docs/setup/release/notes/#deprecation                               |
              |
```

```
|           |    release: v1.19                                                    |
|           |    upgrade:                                                        |
|           |    - v1.20.7                                                       |
|           |  v1.20.7:                                                          |
|           |    features:                                                       |
|           |    - nodegroups                                                      |
|           |    links:                                                        |
|           |      deprecation: https://v1-20.docs.kubernetes.io/docs/setup/release/notes/#deprecation
            |
|           |    release: v1.20                                                    |
|           |    upgrade:                                                        |
|           |    - v1.21.3                                                       |
|           |  v1.21.3:                                                          |
|           |    features:                                                       |
|           |    - nodegroups                                                      |
|           |    links:                                                        |
|           |      deprecation:
https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-
1.21.md#deprecation |
|           |    release: v1.21                                                    |
|           |    upgrade: []                                                     |
|           |  v1.22.2:                                                          |
|           |    features:                                                       |
|           |    - nodegroups                                                      |
|           |    links:                                                        |
|           |      deprecation:
https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-
1.22.md#deprecation |
|           |    release: v1.22                                                    |
|           |    upgrade: []                                                     |
|           | k8saas_versions:                                                         |
|           | - v1.22.2                                                          |
|           | - v1.21.3                                                          |
|           | - v1.20.7                                                          |
|           | os_distributions:                                                        |
|           | - id: linux                                                      |
|           |   os_type: linux                                                     |
|           |   title: Generic Linux                                                 |
|           | - id: rockylinux8                                                      |
|           |   os_type: linux                                                     |
|           |   title: Rocky Linux 8                                                   |
|           | - id: almalinux8                                                       |
|           |   os_type: linux                                                     |
|           |   title: Alma Linux 8                                                  |
|           | - id: centos8                                                        |
|           |   os_type: linux                                                     |
|           |   title: CentOS 8                                                    |
|           | - id: centos7                                                        |
|           |   os_type: linux                                                     |
|           |   title: CentOS 7                                                    |
|           | - id: centos6                                                        |
|           |   os_type: linux                                                     |
```

```
|         |  title: CentOS 6                                    |
|         | - id: rhel8                                         |
|         |  os_type: linux                                     |
|         |  title: Red Hat Enterprise Linux 8                  |
|         | - id: rhel7                                         |
|         |  os_type: linux                                     |
|         |  title: Red Hat Enterprise Linux 7                  |
|         | - id: ubuntu20.04                                   |
|         |  os_type: linux                                     |
|         |  title: Ubuntu 20.04                                |
|         | - id: ubuntu18.04                                   |
|         |  os_type: linux                                     |
|         |  title: Ubuntu 18.04                                |
|         | - id: ubuntu16.04                                   |
|         |  os_type: linux                                     |
|         |  title: Ubuntu 16.04                                |
|         | - id: debian10                                      |
|         |  os_type: linux                                     |
|         |  title: Debian 10                                   |
|         | - id: debian9                                       |
|         |  os_type: linux                                     |
|         |  title: Debian 9                                    |
|         | - id: windows                                       |
|         |  os_type: windows                                   |
|         |  title: Generic Windows                             |
|         | - id: win2k22                                       |
|         |  os_type: windows                                   |
|         |  title: Windows Server 2022                         |
|         | - id: win2k19                                       |
|         |  os_type: windows                                   |
|         |  title: Windows Server 2019                         |
|         | - id: win2k16                                       |
|         |  os_type: windows                                   |
|         |  title: Windows Server 2016                         |
|         | - id: win2k12r2                                     |
|         |  os_type: windows                                   |
|         |  title: Windows Server 2012 R2                      |
|         | - id: win2k12                                       |
|         |  os_type: windows                                   |
|         |  title: Windows Server 2012                         |
|         | - id: win2k8r2                                      |
|         |  os_type: windows                                   |
|         |  title: Windows Server 2008 R2                      |
|         | - id: win2k8                                        |
|         |  os_type: windows                                   |
|         |  title: Windows Server 2008                         |
|         | - id: win10                                         |
|         |  os_type: windows                                   |
|         |  title: Windows 10                                  |
|         | - id: win8.1                                        |
|         |  os_type: windows                                   |
|         |  title: Windows 8.1                                 |
```

```
|          | - id: win7                                   |
|          |  os_type: windows                                |
|          |  title: Windows 7                               |
| features    | []                                     |
| options     | cpu_model: ''                               |
|          | custom_params: []                              |
|          | notification_forwarding: disabled                       |
| status      | active                                   |
+--------------+----------------------------------------------------------------------------------------------------------------+
```

6.9.2 Настройка модели ЦП виртуальных машин

По умолчанию виртуальные машины создаются с моделью ЦП хоста. Если серверы в вычислительном кластере имеют разные ЦП, может не работать динамическая миграция ВМ либо могут неправильно работать приложения внутри ВМ, зависящие от конкретных ЦП. Во избежание этого можно определить, какая модель ЦП обеспечивает совместимость по всем серверам в вычислительном кластере, и вручную установить ее для кластера по умолчанию. Однако в этом случае модель ЦП вычислительного кластера будет наименее продвинутая и вычислительные серверы потеряют возможности более производительного процессора.

Чтобы вывести список поддерживаемых моделей ЦП, выполните команду vinfra service compute show.

Ограничения

- Изменение модели ЦП влияет только на новые ВМ (то есть созданные после изменения).

Предварительные условия

- Должен быть создан вычислительный кластер, как описано в разделе "Создание вычислительного кластера" на странице 169.

Чтобы задать модель ЦП для вычислительного кластера

Выполните следующие действия:

1. Выполните команду virsh capabilities на всех вычислительных узлах, чтобы распечатать документ XML с данными о ЦП узла.
2. На одном из узлов создайте файл XML, например cpu-compare.xml. Добавьте разделы <cpu> изо всех узлов в этот файл, например:

```
<cpu>
 <arch>x86_64</arch>
 <model>SandyBridge-IBRS</model>
 <vendor>Intel</vendor>
 <counter name='tsc' frequency='2099999000' scaling='yes'/>
 <topology sockets='1' cores='16' threads='2'/>
 <feature policy='require' name='vme'/>
 <feature policy='require' name='ds'/>
 <feature policy='require' name='acpi'/>
```



```
  <feature policy='require' name='ss'/>
  <feature policy='require' name='ht'/>
  <feature policy='require' name='tm'/>
  <feature policy='require' name='pbe'/>
  <feature policy='require' name='dtes64'/>
  <feature policy='require' name='monitor'/>
  <feature policy='require' name='ds_cpl'/>
  <feature policy='require' name='vmx'/>
  <feature policy='require' name='smx'/>
  <feature policy='require' name='est'/>
  <feature policy='require' name='tm2'/>
  <feature policy='require' name='xtpr'/>
  <feature policy='require' name='pdcm'/>
  <feature policy='require' name='pcid'/>
  <feature policy='require' name='dca'/>
  <feature policy='require' name='arat'/>
  <feature policy='require' name='md-clear'/>
  <feature policy='require' name='stibp'/>
  <feature policy='require' name='ssbd'/>
  <feature policy='require' name='xsaveopt'/>
  <feature policy='require' name='pdpe1gb'/>
  <feature policy='require' name='invtsc'/>
</cpu>
<cpu>
  <arch>x86_64</arch>
  <model>Skylake-Server</model>
  <vendor>Intel</vendor>
  <counter name='tsc' frequency='2099999000' scaling='yes'/>
  <topology sockets='1' cores='16' threads='2'/>
  <feature name='ds'/>
  <feature name='acpi'/>
  <feature name='ss'/>
  <feature name='ht'/>
  <feature name='tm'/>
  <feature name='pbe'/>
  <feature name='dtes64'/>
  <feature name='monitor'/>
  <feature name='ds_cpl'/>
  <feature name='vmx'/>
  <feature name='smx'/>
  <feature name='est'/>
  <feature name='tm2'/>
  <feature name='xtpr'/>
  <feature name='pdcm'/>
  <feature name='dca'/>
  <feature name='tsc_adjust'/>
  <feature name='cmt'/>
  <feature name='intel-pt'/>
  <feature name='pku'/>
  <feature name='md-clear'/>
  <feature name='stibp'/>
```

```
  <feature name='arch-capabilities'/>
  <feature name='xsaves'/>
  <feature name='invtsc'/>
  <feature name='rdctl-no'/>
  <feature name='ibrs-all'/>
  <feature name='skip-l1dfl-vmentry'/>
  <feature name='mds-no'/>
  <pages unit='KiB' size='4'/>
  <pages unit='KiB' size='2048'/>
  <pages unit='KiB' size='1048576'/>
</cpu>
```

3. Сравните характеристики ЦП с помощью команды virsh cpu-baseline, например:

```
# virsh cpu-baseline cpu-compare.xml | grep model
<model fallback='allow'>SandyBridge</model>
```

   Команда выведет наиболее совместимую модель ЦП для всех серверов. В рассмотренном примере это SandyBridge.

4. Установите эту модель ЦП для вычислительного кластера, например:

```
# vinfra service compute set --cpu-model SandyBridge
```

6.9.3 Установка доменного имени для API вычислений

С помощью типа трафика **API вычислений** Кибер Инфраструктура открывает внешнюю оконечную точку, которая прослушивает запросы API OpenStack. По умолчанию она указывает на IP-адрес сервера управления (или его виртуальный IP-адрес, если включена высокая доступность).

В некоторых случаях необходимо изменить все внешние оконечные точки так, чтобы использовалось доменное имя, преобразуемое в IP-адрес сервера управления (или его виртуальный IP-адрес), например, чтобы защитить трафик API OpenStack с помощью SSL-сертификата без поля subjectAltName или чтобы сервис Kubernetes обращался к API вычислений через доменное имя.

Чтобы изменить все внешние оконечные точки так, чтобы использовалось доменное имя

Выполните следующую команду:

```
vinfra service compute set [--endpoint-hostname <hostname>]
```

--endpoint-hostname <hostname>

Использовать указанное доменное имя для внешней оконечной точки. Укажите пустое значение в кавычках, чтобы использовать IP-адрес.

Например, чтобы использовать для внешних оконечных точек dns-name.example, выполните следующую команду:

```
# vinfra service compute set --endpoint-hostname dns-name.example
+---------+--------------------------------------+
| Field   | Value                                |
+---------+--------------------------------------+
| task_id | 534391a2-946a-4406-8dc0-756f161cd595 |
+---------+--------------------------------------+
```

Дождитесь выполнения задания.

```
# vinfra task show 534391a2-946a-4406-8dc0-756f161cd595
+---------+-----------------------------------------------------------------+
| Field   | Value                                                           |
+---------+-----------------------------------------------------------------+
| details |                                                                 |
| name    | backend.presentation.compute.tasks.ReconfigureComputeClusterTask |
| result  |                                                                 |
| state   | success                                                         |
| task_id | 534391a2-946a-4406-8dc0-756f161cd595                            |
+---------+-----------------------------------------------------------------+
```

Чтобы проверить, что вместо IP-адреса сервера управления используется указанное доменное имя, выполните следующие действия.

1. Создайте или пересоздайте скрипт администратора OpenRC.

   ```
   # kolla-ansible post-deploy
   ```

2. Запустите скрипт.

   ```
   # source /etc/kolla/admin-openrc.sh
   ```

3. Выведите список внешних оконечных точек.

   ```
   # openstack --insecure endpoint list | grep public
   | 5a845b4b<...> | <...> | https://dns-name.example:8780                |
   | 7d901686<...> | <...> | https://dns-name.example:8776/v2/%(tenant_id)s   |
   | 44aa0f53<...> | <...> | https://dns-name.example:8774/v2.1/%(tenant_id)s |
   | 0e6d3a39<...> | <...> | https://dns-name.example:9292                |
   | 0b906e51<...> | <...> | https://dns-name.example:9696                |
   | 1b68ac7c<...> | <...> | https://dns-name.example:8776/v3/%(tenant_id)s   |
   | d80af756<...> | <...> | https://dns-name.example:8004/v1/%(tenant_id)s   |
   | d0e8c7da<...> | <...> | https://dns-name.example:5000/v3             |
   ```

6.9.4 Защита трафика API OpenStack с помощью SSL

Входящий и исходящий трафик внешней оконечной точки, прослушивающей запросы API OpenStack, можно защитить с помощью сертификата SSL. Но поскольку доменные имена не используются по умолчанию, сертификат должен будет содержать поле subjectAltName с IP-адресом вышеупомянутого сервера управления. Если такого поля нет, потребуется изменить

внешнюю оконечную точку так, чтобы использовалось доменное имя, для которого у вас есть сертификат.

Ограничения

- Для панели администрирования и API OpenStack можно добавить и применить только один SSL-сертификат.

Чтобы защитить трафик API OpenStack с помощью SSL

Выполните следующие действия:

1. На панели администрирования отправьте SSL-сертификат и закрытый ключ на экране **Настройки** > **Сервер управления** > **Доступ по SSL**.
2. На стороне клиента поместите файл сертификата ЦС в доверенную цепочку операционной системы.

   ```
   # cp ca.pem /etc/pki/ca-trust/source/anchors/
   # update-ca-trust extract
   ```

   Как вариант, можно добавить параметр --os-cacert ca.pem к каждому вызову клиента OpenStack.
3. Если в сертификате нет поля subjectAltName, измените все внешние оконечные точки так, чтобы использовалось доменное имя, для которого у вас есть сертификат, как описано в разделе "Установка доменного имени для API вычислений" на странице 180. Это доменное имя должно разрешаться в IP-адрес сервера управления (или его виртуальный IP-адрес, если включена высокая доступность).
4. В скрипте OpenRC измените OS_AUTH_URL на то же доменное имя и удалите все параметры, связанные с незащищенным доступом, например:

   ```
   export OS_PROJECT_DOMAIN_NAME=Default
   export OS_USER_DOMAIN_NAME=Default
   export OS_PROJECT_NAME=admin
   export OS_USERNAME=admin
   export OS_PASSWORD=<ADMIN_PASSWORD>
   export OS_AUTH_URL=https://<DOMAIN_NAME>:5000/v3
   export OS_IDENTITY_API_VERSION=3
   ```

Теперь можно выполнять команды OpenStack без параметра --insecure.

6.9.5 Настройка мультитенантности

Чтобы настроить мультитенантность для вычислительного кластера, необходимо создать домены и проекты, назначить им пользователей и определить квоты проектов.

Ограничения

- Квоты проектов можно задать только после развертывания вычислительного кластера.

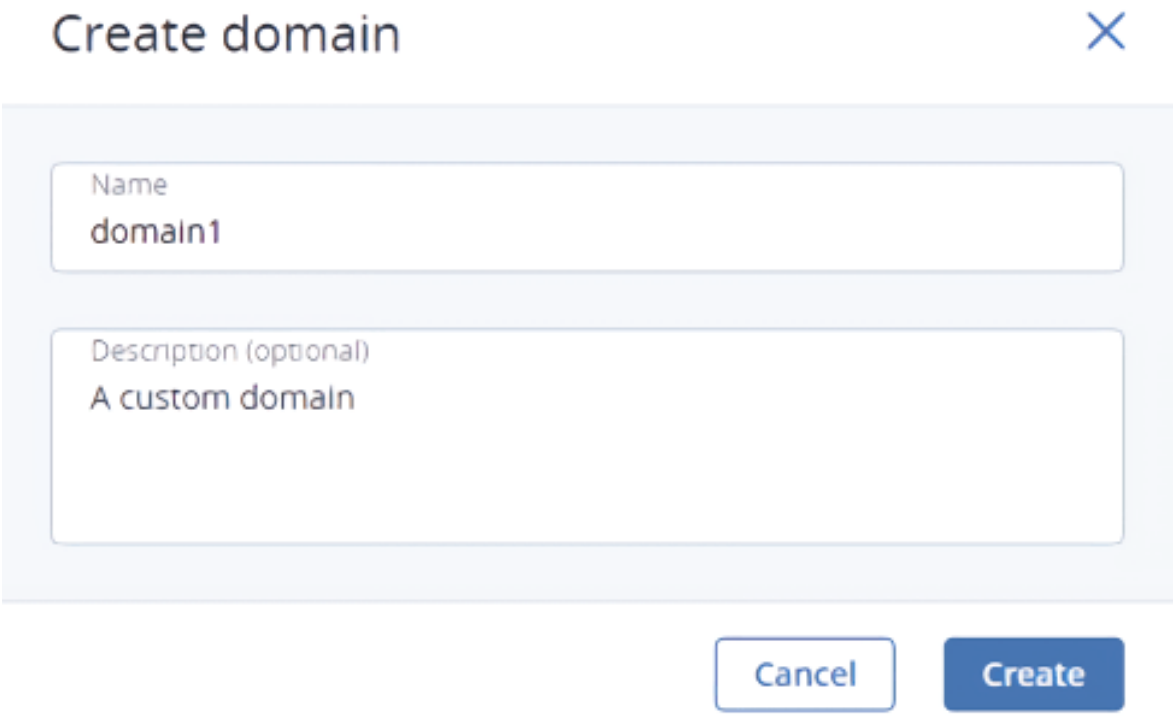
Предварительные требования

- Четкое понимание концепции "Мультитенантность" на странице 40.
- Поскольку квоты могут превышать существующие виртуальные ресурсы, а виртуальные ресурсы не резервируются для каждого из проектов по отдельности, в вычислительном кластере должно быть достаточно виртуальных ресурсов для всех проектов во всех доменах.

Чтобы создать домен

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** нажмите **Создать домен**.
2. В окне **Создать домен** укажите имя домена и при необходимости его описание.



3. Нажмите кнопку **Создать**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain create [--description <description>] [--enable | --disable] <name>
```

--description <description>
: Описание домена

--enable
: Включение домена

--disable
: Отключение домена

<name>

Имя домена

Например, чтобы создать домен mydomain, выполните:

```
# vinfra domain create mydomain
```

Созданный домен появится в выводе команды vinfra domain list:

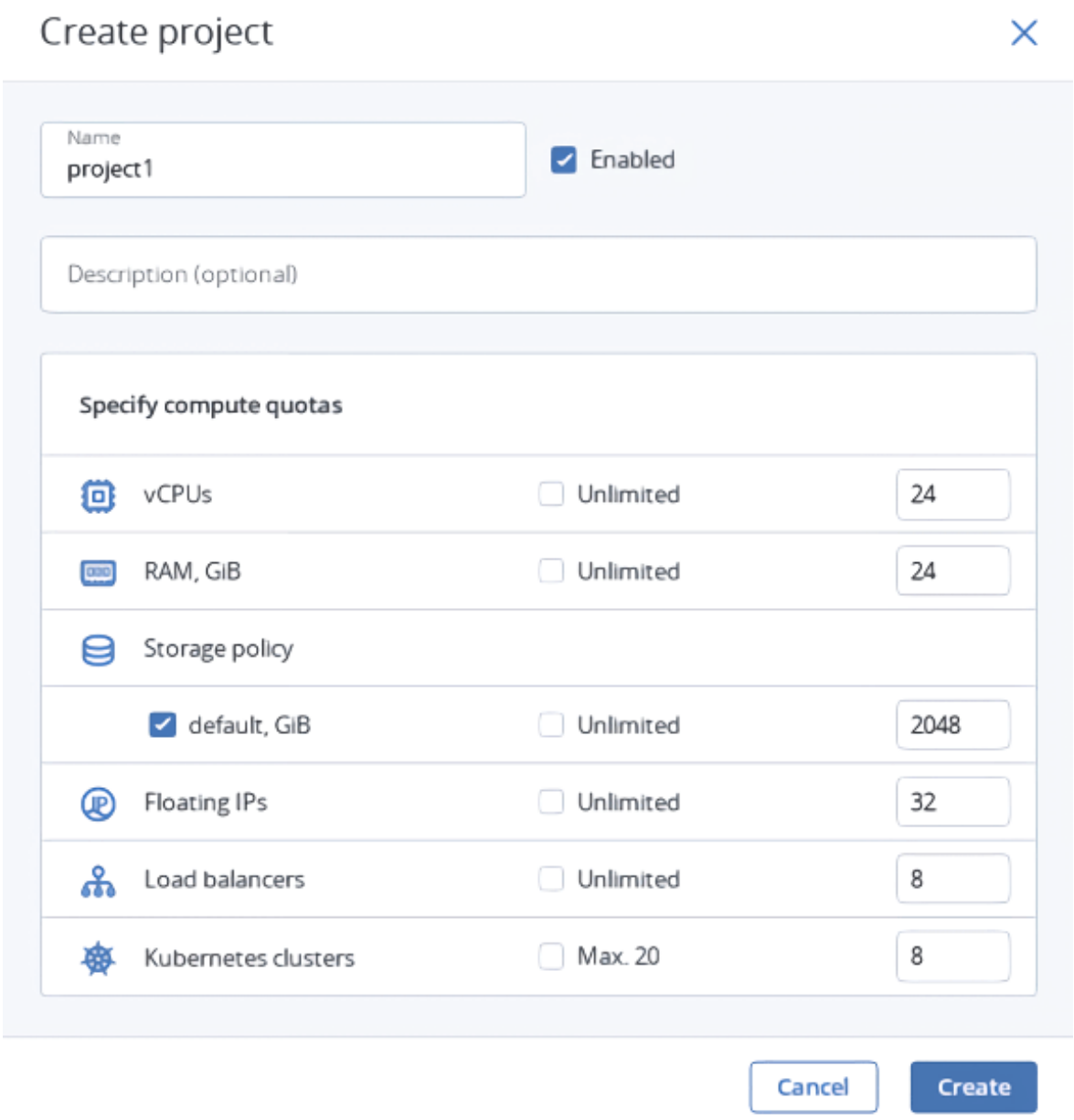
```
# vinfra domain list
+--------------+----------+---------+--------------------+
| id           | name     | enabled | description        |
+--------------+----------+---------+--------------------+
| default      | Default  | True    | The default domain |
| 24986479e<...> | mydomain | True    |                    |
+--------------+----------+---------+--------------------+
```

Чтобы создать проект

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** щелкните по домену, внутри которого будет создан проект.
2. На вкладке **Проекты** нажмите **Создать проект**.
3. В окне **Создать проект** укажите имя проекта и при необходимости описание. Имя проекта должно быть уникальным в пределах домена.
4. [Необязательно] Снимите флажок **Включен**, чтобы отключить созданный проект.
5. Определите квоты для виртуальных ресурсов, которые будут доступны внутри проекта. Чтобы указать определенное значение для ресурса, сначала снимите рядом с ним флажок **Без ограничений**.

   Примечание
   Политика хранилища по умолчанию должна быть доступна проектам, которые будут использовать функцию «Kubernetes как услуга».



6. Нажмите кнопку **Создать**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain project create [--description <description>] [--enable | --disable]
                             --domain <domain> <name>
```

--description <description>

Описание проекта

--enable

Включение проекта

--disable

Выключение проекта

--domain <domain>

Имя или идентификатор домена

<name>

Имя проекта

Например, чтобы создать проект myproject в домене mydomain и задать описание для проекта, выполните:

```
# vinfra domain project create myproject --domain mydomain --description "A custom project"
```

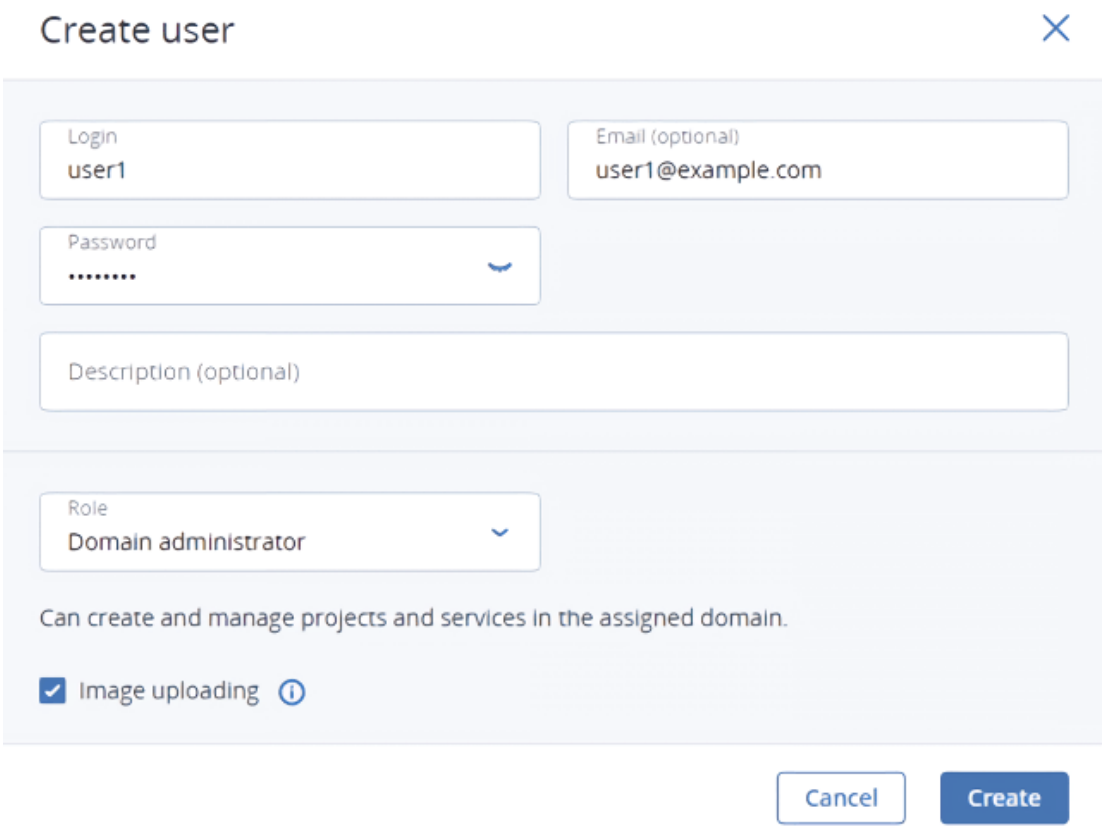
Созданный проект появится в выводе команды vinfra domain project list:

```
# vinfra domain project list --domain mydomain
+-------------+-----------+---------+-----------------+--------------+
| id          | name      | enabled | description     | domain_id    |
+-------------+-----------+---------+-----------------+--------------+
| 79830e3c<…> | myproject | True    | A custom project | 24986479e<…> |
+-------------+-----------+---------+-----------------+--------------+
```

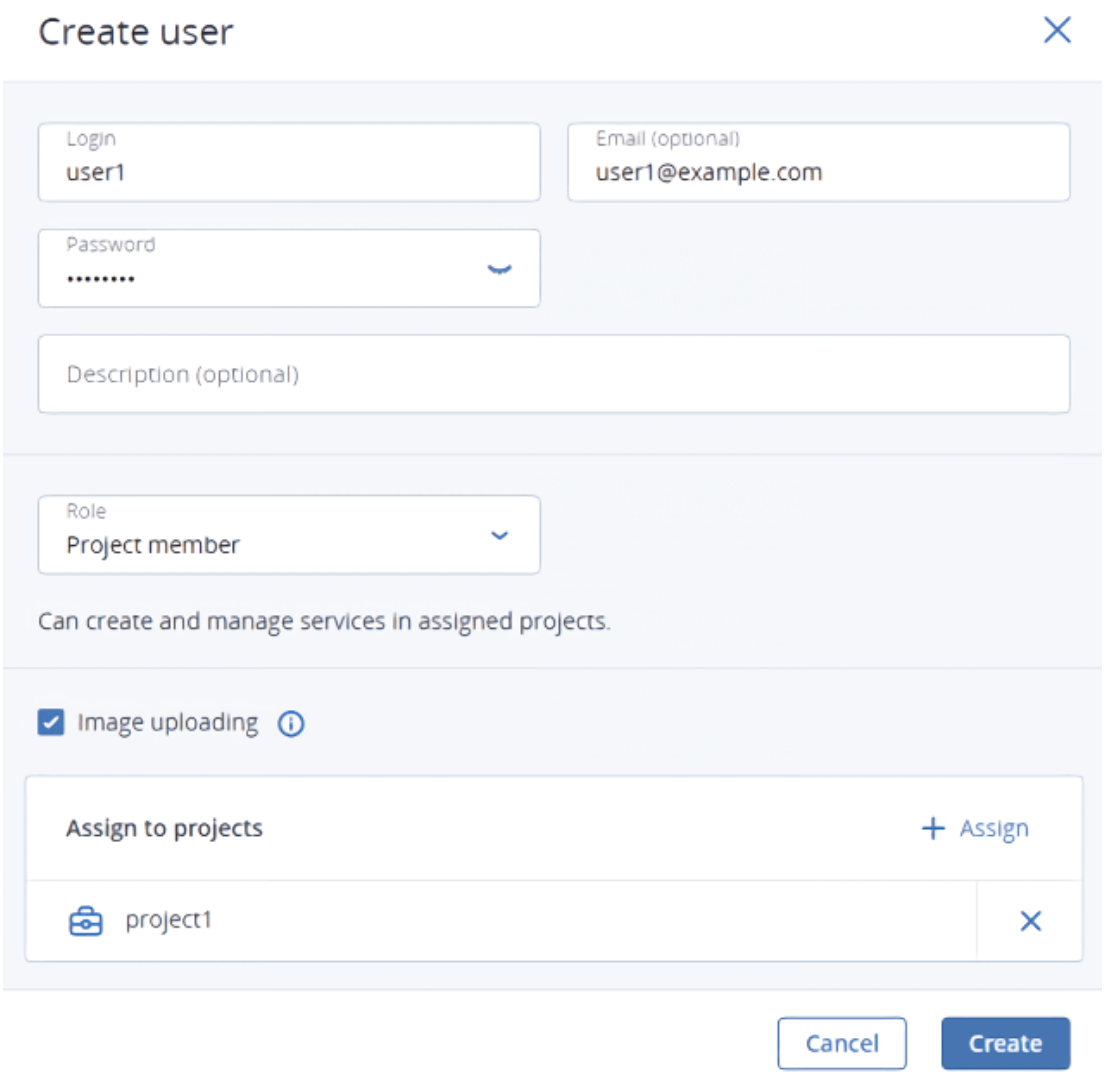
Чтобы создать пользователя самообслуживания

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** щелкните по домену, внутри которого будет создан пользователь.
2. Перейдите на вкладку **Пользователи домена** и нажмите **Создать пользователя**.
3. В окне **Создать пользователя** укажите имя пользователя, пароль и при необходимости адрес электронной почты и описание. Имя пользователя должно быть уникальным в пределах домена.
4. Выберите роль пользователя:
   - Чтобы создать администратора домена
     a. Выберите **Администратор домена**.
     b. [Необязательно] Установите флажок **Отправка образов**. Состояние этого разрешения будут наследовать пользователи, созданные этим администратором домена.



- Чтобы создать администратора проекта
  a. Выберите **Участник проекта**.
  b. Установите флажок **Отправка образов**. Если этот параметр отключен, данный пользователь не сможет отправлять образы.
  c. [Необязательно] Нажмите **Назначить** и выберите проект, на который будет назначен этот пользователь.



5. Нажмите кнопку **Создать**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain user create [--email <email>] [--description <description>]
                          [--assign <project> <role>] [--assign-domain <domain> <roles>]
                          [--domain-permissions <domain_permissions>]
                          [--enable | --disable] --domain <domain> <name>
```

--email <email>

Адрес электронной почты пользователя

--description <description>

Описание пользователя

--assign <project> <role>

Назначение пользователя проекту с одним или несколькими наборами разрешений. Укажите этот параметр несколько раз, чтобы назначить пользователя сразу нескольким проектам.

- <project>: идентификатор или имя проекта
- <role>: роль пользователя в проекте (project_admin — администратор проекта)

--assign-domain <domain> <roles>

Назначение пользователя в домен с одним или несколькими наборами разрешений. Укажите этот параметр несколько раз, чтобы назначить пользователя сразу в несколько доменов. Этот параметр допустим только для служебных учетных записей.

- <domain> — идентификатор или имя домена
- <roles> — список ролей служебной учетной записи через запятую (compute — вычисления)

--domain-permissions <domain_permissions>

Разделенный запятыми список разрешений домена. Чтобы просмотреть список доступных разрешений домена, используйте команду vinfra domain user list-available-roles | grep domain.

--system-permissions <system_permissions>

Разделенный запятыми список системных разрешений. Чтобы просмотреть список доступных системных разрешений, используйте команду vinfra domain user list-available-roles | grep system.

--enable

Включение пользователя

--disable

Отключение пользователя

--domain <domain>

Имя или идентификатор домена

<name>

Имя пользователя

Пример 1. Чтобы создать администратора домена myadmin для домена mydomain, выполните:

```
# vinfra domain user create myadmin --domain mydomain --domain-permissions domain_admin
```

Укажите пароль пользователя.

Пример 2. Чтобы создать участника проекта myuser для проекта myproject домена mydomain и разрешить этому пользователю загрузку образов, выполните:

```
# vinfra domain user create myuser --domain mydomain --assign myproject project_admin --domain-permissions image_upload
```

Укажите пароль пользователя.

Созданные пользователи появятся в выводе команды vinfra domain user list:

```
# vinfra domain user list --domain mydomain
+-------------+---------+-------+---------+-------------+-------------------+--------------------------+
| id          | name    | email | enabled | description | domain_permissions | assigned_projects        |
+-------------+---------+-------+---------+-------------+-------------------+--------------------------+
| 28aa0207<…> | myadmin |       | True    |             | - domain_admin    | []                       |
| fb9fa0b2<…> | myuser  |       | True    |             | - image_upload    | - project_id: 79830e3c<…> |
|             |         |       |         |             |                   | role: project_admin      |
+-------------+---------+-------+---------+-------------+-------------------+--------------------------+
```

6.9.6 Обеспечение доступа к панели самообслуживания

Панель самообслуживания представляет собой веб-панель управления, которая позволяет конечным пользователям управлять виртуальными объектами, такими как виртуальные машины, тома, виртуальные сети и т. д., в изолированных административных средах.

Ограничения

- Администратор системы по умолчанию не может выполнить вход на портал самообслуживания.

Предварительные требования

- Должен быть создан вычислительный кластер, как описано в разделе "Создание вычислительного кластера" на странице 169.
- Должны быть созданы проекты и пользователи самообслуживания, как описано в разделе "Настройка мультитенантности" на странице 182.
- Необходимые образы вычислений должны использоваться совместно во всех проектах, или пользователям самообслуживания должно быть предоставлено разрешение на передачу образов.
- Вычислительный кластер должен содержать как минимум одну физическую сеть.

Чтобы можно было получить доступ к панели самообслуживания

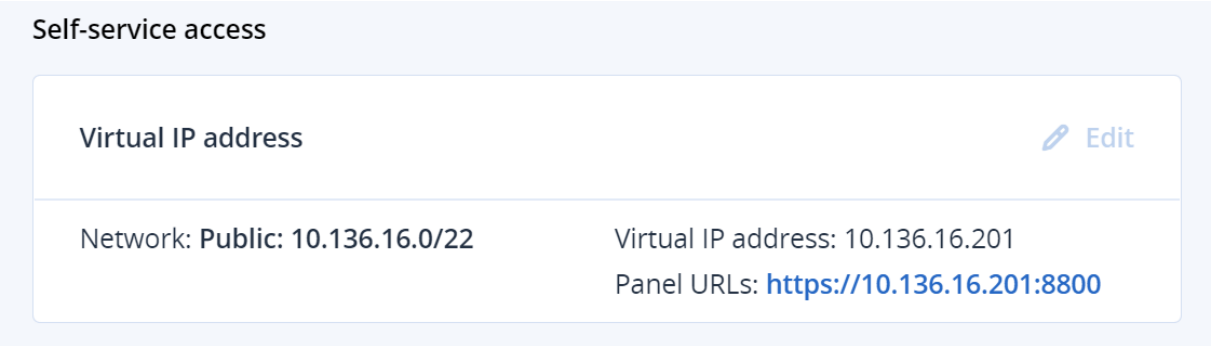
Панель администратора

Откройте TCP-порт 8800 на сервере управления следующим образом:

1. На экране **Инфраструктура** > **Сети** нажмите **Изменить**.
2. Добавьте тип трафика **Панель самообслуживания** к внешней сети, установив соответствующий флажок.
3. Нажмите кнопку **Сохранить**, чтобы применить изменения.

Теперь можно получить доступ к панели самообслуживания по адресу http://<admin_panel_IP_address>:8800. Используйте доменное имя и учетные данные пользователя для входа. Если для узла управления включена высокая доступность, выполните вход на панель самообслуживания с помощью виртуального адреса панели администрирования: http://<admin_panel_virtual_IP_

address>:8800. Также можно воспользоваться ссылкой в поле **URL-адреса панели** с экрана **Настройки** > **Настройки системы** > **Самообслуживание**.



Интерфейс командной строки

Откройте TCP-порт 8800 на сервере управления посредством добавления типа трафика **Панель самообслуживания** к внешней сети. Например:

```
# vinfra cluster network set Public --add-traffic-types "Self-service panel"
```

Теперь можно получить доступ к панели самообслуживания по адресу http://<admin_panel_IP_address>:8800. Используйте доменное имя и учетные данные пользователя для входа. Если для узла управления включена высокая доступность, выполните вход на панель самообслуживания с помощью виртуального адреса панели администрирования: http://<admin_panel_virtual_IP_address>:8800.

6.9.7 Подготовка к работе балансировщиков нагрузки

Кибер Инфраструктура предлагает балансировку нагрузки как сервис для вычислительной инфраструктуры. Балансировка нагрузки обеспечивает отказоустойчивость и повышает производительность веб-приложений путем распределения входящего сетевого трафика по виртуальным машинам из пула балансировки. Балансировщик нагрузки получает и перенаправляет входящие запросы на подходящую ВМ в зависимости от настроенного алгоритма балансировки и состояния ВМ.

Балансировщики нагрузки создаются и управляются пользователями самообслуживания, как описано в разделе «Управление балансировщиками нагрузки» в руководстве по самообслуживанию. Однако чтобы предоставить эту возможность пользователям самообслуживания, нужно установить сервис балансировщика нагрузки на панели администрирования.

Ограничения

- В текущей версии продукта Кибер Инфраструктура установленный сервис нельзя удалить.
- Чтобы пользователи панели самообслуживания могли создавать балансировщики нагрузки высокой доступности, в вычислительном кластере должно быть не менее двух узлов.

- Если установить этот сервис после создания проекта, то балансировщики нагрузки не будут автоматически включаться в квотах проекта.

Предварительные требования

- Должен быть создан вычислительный кластер, как описано в разделе "Создание вычислительного кластера" на странице 169.

Чтобы установить сервис балансировщика нагрузки

Панель администратора

1. Перейдите на экран **Настройки** > **Дополнительные сервисы**.
2. В разделе **Сервис балансировщика нагрузки** нажмите **Установить**.

Примечание
Для автономной установки сервиса балансировщика нагрузки в среде без доступа к Интернету (в закрытом контуре) необходимо заранее установить на узлы пакет amphora-x64-haproxy.qcow2.

Интерфейс командной строки

Выполните следующую команду:

```
# vinfra service compute cluster set --enable-lbaas
```

6.9.8 Подготовка к работе кластеров Kubernetes

Сервис Kubernetes позволяет развертывать масштабируемые, готовые к производственной эксплуатации кластеры Kubernetes с преинтегрированным постоянным хранилищем.

Кластер Kubernetes включает следующие компоненты:

Компонент	Название и версия
Базовая ОС	Fedora 34 CoreOS
Среда выполнения контейнеров	Docker 20.10.6
Подключаемый сетевой модуль	Flannel с VXLAN

Кластеры Kubernetes создаются и управляются пользователями самообслуживания. Однако чтобы предоставить эту возможность пользователям самообслуживания, нужно установить сервис Kubernetes на панели администрирования.

Ограничения

- В текущей версии продукта Кибер Инфраструктура установленный сервис нельзя удалить.
- Если установить этот сервис после создания проекта, то кластеры Kubernetes не будут автоматически включаться в квотах проекта.

Предварительные требования

- В соответствии с требованиями, приведенными в разделе "Требования к сети для компонента «Kubernetes как услуга»" на странице 75
  - Сервис обнаружения etcd должен быть доступен по адресу https://discovery.etcd.io со всех узлов управления и из внешней сети с типом трафика **ВМ внешн.**
  - Публичный репозиторий Docker Hub должен быть доступен по адресу https://registry-1.docker.io из внешней сети с типом трафика **ВМ внешн.**
  - API вычислений должен быть доступен из внешней сети с типом трафика **ВМ внешн.**
  - API Kubernetes должен быть доступен по публичному или плавающему IP-адресу ВМ балансировщика нагрузки или главной (master) ВМ Kubernetes через порт 6443 со всех узлов управления.

  Если тип трафика **API вычислений** добавляется к частной сети, которая недоступна напрямую из сети с типом трафика **ВМ внешн.**, но имеет доступ к внешним сетям через NAT и публично доступна по своему доменному имени, необходимо задать доменное имя для API вычислений, как описано в разделе "Установка доменного имени для API вычислений" на странице 180.
- Должен быть создан вычислительный кластер, как описано в разделе "Создание вычислительного кластера" на странице 169.

Чтобы установить сервис Kubernetes

Панель администратора

1. Перейдите на экран **Настройки** > **Дополнительные сервисы**.
2. В разделе **Сервис Kubernetes** нажмите **Установить**.

Примечание

- При установке Kubernetes также автоматически устанавливается сервис балансировщика нагрузки.
- Для автономной установки Kubernetes и сервиса балансировщика нагрузки в среде без доступа к Интернету (в закрытом контуре) необходимо заранее установить на узлы пакеты hci-k8saas-files и amphora-x64-haproxy.qcow2.

Интерфейс командной строки

Выполните следующую команду:

```
# vinfra service compute cluster set --enable-k8saas
```

6.9.9 Подготовка к работе учета и биллинга

Сервис учета и биллинга собирает, сохраняет и предоставляет метрики использования для ресурсов, потребляемых конечными пользователями в своих проектах. Этот вычислительный сервис открывает порт 8041 и включает два сервиса Gnocchi: HTTP-сервер gnocchi-api и демон метрик gnocchi-metricd.

Ограничения

- Сервис будет учитывать только вычислительные объекты, созданные после его включения.
- В текущей версии продукта Кибер Инфраструктура установленный сервис нельзя удалить.

Предварительные требования

- Должен быть создан вычислительный кластер, как описано в разделе "Создание вычислительного кластера" на странице 169.

Чтобы установить сервис учета и биллинга

Панель администратора

1. Перейдите на экран **Настройки** > **Дополнительные сервисы**.
2. В разделе **Сервис учета ресурсов для биллинга** нажмите **Установить**.

Интерфейс командной строки

Выполните следующую команду:

```
# vinfra service compute cluster set --enable-metering
```

6.9.10 Настройка быстрой сети DPDK для виртуальных машин

DPDK (Data Plane Development Kit) – это технология, которая позволяет уменьшить задержки при обработке сетевых пакетов и увеличить скорость передачи данных между приложением и сетью. При использовании DPDK приложение взаимодействует с сетевым устройством напрямую, то есть в обход ядра и его сетевого стека.

Кибер Инфраструктура поддерживает DPDK для физических вычислительных сетей и подключенных к ним виртуальных машин.

Ограничения

- Горячая миграция виртуальных машин не поддерживается.

Предварительные требования

- Используется рекомендуемая сетевая конфигурация, описанная в разделе "Требования к сети для вычислительного кластера" на странице 74.
- Создан вычислительный кластер, как описано в разделе "Создание вычислительного кластера" на странице 169.
- У серверов вычислительного кластера есть сетевые интерфейсы с поддержкой DPDK. Подробнее см. в разделе "Рекомендации по сети" на странице 76.
- Для DPDK создана отдельная сеть инфраструктуры. Сети назначен только один тип трафика – **ВМ внешн.** Подробнее см. в разделах "Управление сетями" на странице 254 и "Управление обычными типами трафика" на странице 249.
- Сетевым интерфейсам или объединениям сетевых интерфейсов, поддерживающим DPDK, назначена сеть инфраструктуры, предназначенная для DPDK. Подробнее см. в разделе

"Изменение параметров сетевого интерфейса" на странице 230.

- Объединениям сетевых интерфейсов, используемым для подключения серверов к предназначенной для DPDK инфраструктурной сети, установлен режим **active-backup**. Подробнее см. в разделе "Создание объединений сетевых интерфейсов" на странице 127.
- На основе сети инфраструктуры, предназначенной для DPDK, создана физическая вычислительная сеть. Всем проектам предоставлен полный доступ к этой сети. Подробнее см. в разделе "Создание физических вычислительных сетей" на странице 532.
- Сетевым мостам, добавленным при создании физической вычислительной сети для DPDK, установлен метод назначения IP-адресов **Вручную** и не назначено никаких IP-адресов (то есть список назначенных IP-адресов должен быть пустым).

Настройка сети с поддержкой DPDK

1. Проверьте, что вычислительные серверы подготовлены для поддержки быстрой сети DPDK для виртуальных машин. Для этого перейдите на экран **Инфраструктура** > **Серверы** и убедитесь, что серверы помечены тегом **DPDK готов**.

   Проверить готовность сервера также можно с помощью команды /usr/libexec/configure-dpdk.sh -r. Например:

   ```
   # /usr/libexec/configure-dpdk.sh -r
   <...>
   Check cmdline [OK]
   <...>
   ```

   Если сервер еще не подготовлен, выполните следующие действия:

   a. Проверьте совместимость сетевых интерфейсов с DPDK, выполнив команду /usr/libexec/configure-dpdk.sh -c -i <bridge_name>, где <bridge_name> – имя сетевого моста, который был добавлен при создании физической вычислительной сети для DPDK. Например:

      ```
      # /usr/libexec/configure-dpdk.sh -c -i br-oqoa66a
      enp129s0f1 DPDK compatibility [OK]
      enp129s0f1 NUMA support [OK]
      Load vfio-pci module [OK]
      ```

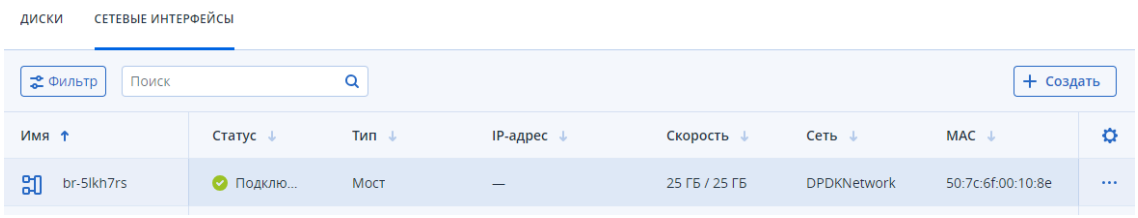
      Проверить совместимость всех сетевых интерфейсов сервера можно с помощью команды /usr/libexec/configure-dpdk.sh -n.

   b. Выполните команду /usr/libexec/configure-dpdk.sh -u -g и перезагрузите сервер.

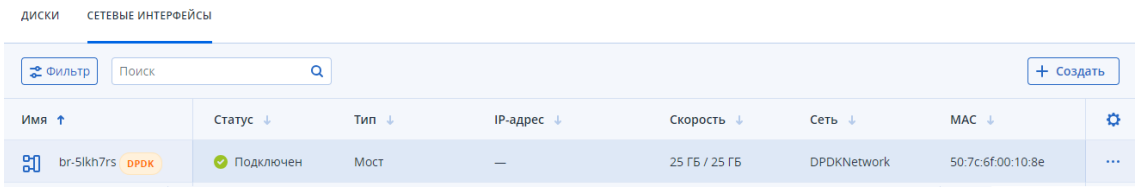
2. Активируйте поддержку DPDK для сетевых интерфейсов или объединений сетевых интерфейсов, которым назначена сеть инфраструктуры, предназначенная для DPDK:

   a. На экране **Инфраструктура** > **Сети** щелкните по имени сервера с тегом **DPDK готов** и перейдите на вкладку **Сетевые интерфейсы**.

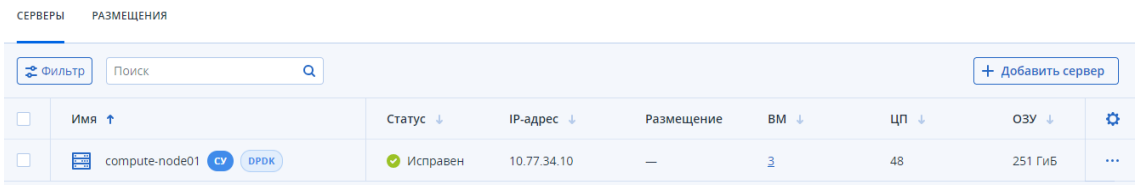
   b. Щелкните по имени сетевого моста, который был создан для сетевого интерфейса или объединения сетевых интерфейсов при создании физической вычислительной сети.



c. На правой панели нажмите **Актировать DPDK**. После активации сетевой мост будет помечен тегом **DPDK**.



Также тегом **DPDK** будет помечен вычислительный сервер, у которого есть хотя бы одно сетевое устройство с активированной поддержкой DPDK.



Для активации также можно использовать команду /usr/libexec/configure-dpdk.sh -e -a -i <bridge_name>, где <bridge_name> – имя сетевого моста.

3. Укажите, какое количество больших страниц (hugepages) можно будет использовать на вычислительных серверах для виртуальных машин с поддержкой DPDK:
   a. На экране **Вычисления** > **Серверы** щелкните по имени вычислительного сервера, помеченного тегом **DPDK**.
   b. На правой панели нажмите **Выделить большие страницы**.
   c. Укажите количество больших страниц, приняв во внимание следующее:
      - Размер большой страницы составляет 1 ГБ.
      - Минимально допустимое количество определяется динамически и равно количеству уже выделенных виртуальным машинам больших страниц.
      - Максимально допустимое количество определяется динамически и равно количеству больших страниц, которые можно разместить в свободном объеме ОЗУ.
      - Фрагментация памяти может привести к понижению максимального значения, так как для размещения большой страницы требуется непрерывная область памяти.
   d. Нажмите **Выделить**.
4. Создайте типы ВМ, в которых включена поддержка больших страниц. Подробные сведения см. в разделе "Создание пользовательских типов виртуальных машин" на странице 453.

После завершения настройки можно создавать ВМ и подключать их сетевые интерфейсы к физической вычислительной сети, которая была настроена для DPDK. ВМ необходимо создавать на основе типов ВМ, в которых включена поддержка больших страниц.

Подключение существующей ВМ к быстрой сети DPDK

Чтобы подключить виртуальную машину к быстрой сети DPDK, которая была настроена после создания этой ВМ, выполните следующие действия:

1. Остановите виртуальную машину.
2. Назначьте ей тип ВМ, в котором включена поддержка больших страниц.
3. Пересоздайте сетевой интерфейс ВМ, указав требуемую физическую вычислительную сеть с поддержкой DPDK.
4. Запустите виртуальную машину.

6.10 Подготовка пространства для блочного хранилища к работе

Пространство для блочного хранилища подготавливается к работе с помощью томов хранения, подсоединяемых к группе целевых устройств.

Ограничения

- Каждый узел в группе целевых устройств может размещать одно целевое устройство из этой группы.
- Подготовка к работе пространства блочного хранилища не реализует полностью экономное распределение. После удаления пользовательских данных неиспользуемое пространство хранилища не высвобождается и о нем сообщается как о фактически используемом пространстве, за которое взимается оплата в соответствии с вашей моделью лицензирования. Более подробные сведения см. в разделе "Диаграмма «Логическое пространство»" на странице 732.

Предварительные требования

- Четкое понимание понятий блочного хранилища, которое описывается в разделе "О хранилище блочных данных" на странице 17.
- Оборудование, соответствующее требованиям, приведенным в разделе "Требования к серверу" на странице 46.
- Сети инфраструктуры должны быть настроены, как описано в разделе "Настройка сетей для блочного хранилища" на странице 111.
- Кластер хранилища должен быть создан в соответствии с указаниями из раздела "Развертывание кластера хранилища данных" на странице 141.

Обзор подготовки к работе

1. Назначьте сеть с типом трафика **iSCSI** сетевому интерфейсу на каждом сервере, который будет добавлен в группу целевых устройств. См. раздел "Изменение сетевых интерфейсов" на странице 117.
2. Создайте группу целевых устройств на выбранных серверах, указав сведения о WWN-именах и порталах целевых устройств. Целевые устройства будут созданы автоматически и добавлены

в группу. Порталы целевых устройств будут созданы на указанных сетевых интерфейсах и портах. См. раздел "Создание групп целевых устройств" на следующей странице.

3. Создайте тома и присоедините их к группе целевых устройств. См. разделы "Создание томов" на странице 204 и "Присоединение томов к группам целевых устройств" на странице 205.
4. При необходимости включите авторизацию CHAP для группы целевых устройств: создайте учетные записи CHAP и назначьте их группе целевых устройств. См. раздел "Управление пользователями CHAP" на странице 386.
5. При необходимости включите авторизацию ACL для группы целевых устройств: создайте список инициаторов, которым будет разрешен доступ только к определенным LUN. Инициаторы, не включенные в список, будут иметь доступ ко всем LUN в группе целевых устройств. См. раздел "Управление списками управления доступом" на странице 383.
6. Подключите инициаторы к целевым устройствам с помощью стандартных средств операционной системы или используемого продукта. Например, на серверах с ОС Linux можно использовать утилиту iscsiadm. См. раздел «Осуществление доступа к целевым устройствам iSCSI» в руководстве пользователя хранилища.

   Чтобы просмотреть имена IQN целевых устройств, щелкните по имени группы целевых устройств.

   Используйте команду vstorage-target session-list для просмотра активных сеансов iSCSI на сервере в группе целевых устройств.

Примечание

Для корректной работы multipath в Linux необходимо указать дополнительные параметры в файле конфигурации /etc/multipath.conf:

```
device {
   vendor "VSTORAGE"
   product "VSTOR-DISK"
   path_grouping_policy "group_by_prio"
   path_checker "tur"
   features "1 queue_if_no_path"
   hardware_handler "1 alua"
   prio "alua"
   failback immediate
   no_path_retry 4
}
```

Если используется oVirt версии 4.3 и ниже, необходимо добавить # VDSM PRIVATE в начале файла конфигурации.

После этого следует перезапустить сервис:

```
systemctl restart multipathd
```

6.10.1 Настройка инструмента командной строки для управления блочным хранилищем

Если планируется использовать инструмент командной строки vstorage-target для управления блочным хранилищем, настройте его, как описано ниже. Выполните эти шаги на каждом сервере, где будут работать целевые устройства iSCSI.

1. Создайте файл конфигурации /etc/vstorage/iscsi/config.json, содержащий как минимум эти обязательные параметры:

   ```
   {
    "ClusterName": "cluster1",
    "VolumesRoot": "vols/iscsi/vols",
   }
   ```

   где ClusterName – имя кластера хранилища, а VolumesRoot – путь к каталогу для томов iSCSI.

   Также можно задать эти дополнительные параметры:

   - "PcsLogLevel" – уровень ведения журнала, в диапазоне от 1 (записываются только ошибки) до 7 (все сведения, включая сообщения отладки).
   - "LogPath" – путь к файлам журнала, по умолчанию /var/log/vstorage (журнал будет сохраняться в файл vstorage-target.log).
   - "GetTimeout" – время ожидания команды инициатора для чтения статуса группы портов целевых устройств, по умолчанию 3000 мс.
2. Включите сервис мониторинга целевых устройств.

   ```
   # systemctl start vstorage-target-monitor.service
   # systemctl enable vstorage-target-monitor.service
   ```

3. Создайте каталог томов iSCSI, если его не существует.

   ```
   # mkdir -p /mnt/vstorage/vols/iscsi/
   ```

Примечание

Для применения изменений, внесенных в файл конфигурации /etc/vstorage/iscsi/config.json запущенного сервиса мониторинга TCM, необходимо перезапустить сервис с помощью команды systemctl restart vstorage-target-monitor.service.

6.10.2 Создание групп целевых устройств

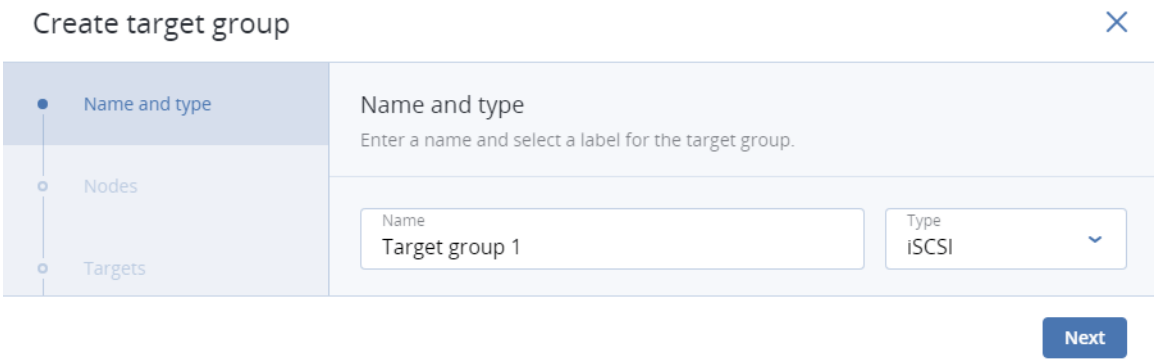
Предварительные требования

- В кластере хранилища данных есть один или более дисков с ролью **Хранилище**.

Чтобы создать группу целевых устройств

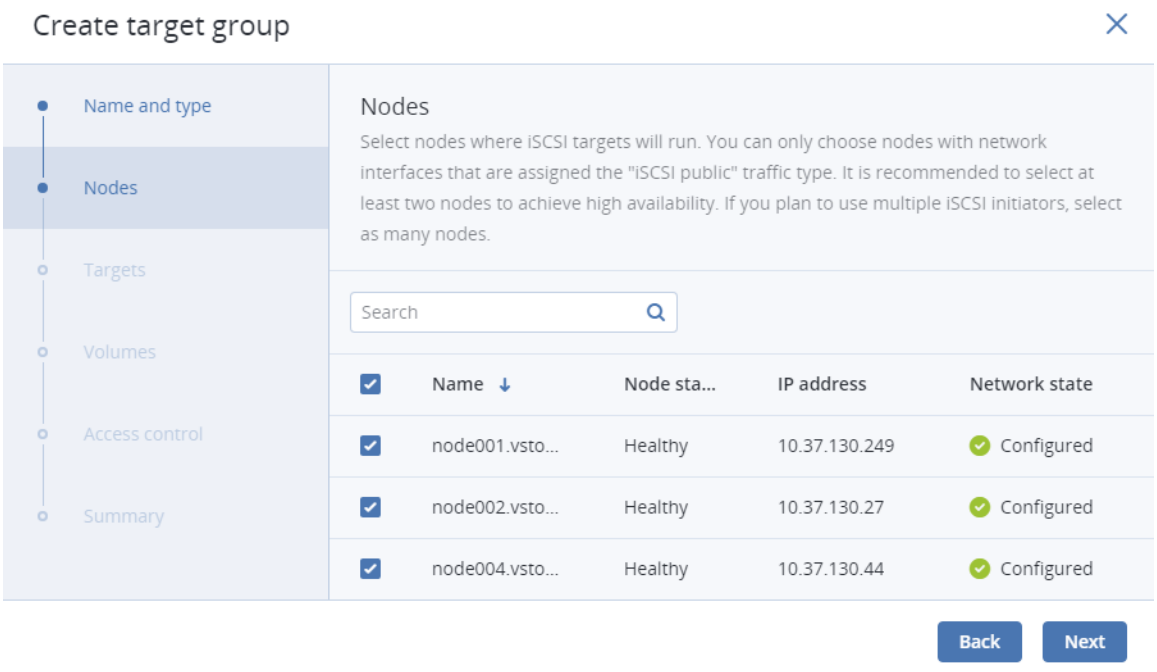
Панель администратора

1. Откройте **Сервисы хранилища** > **Блочное хранилище** > **Группы целей** и нажмите **Создать группу целей**. Откроется мастер **Создать группу целей**.
2. В поле **Имя** введите имя группы целевых устройств iSCSI.



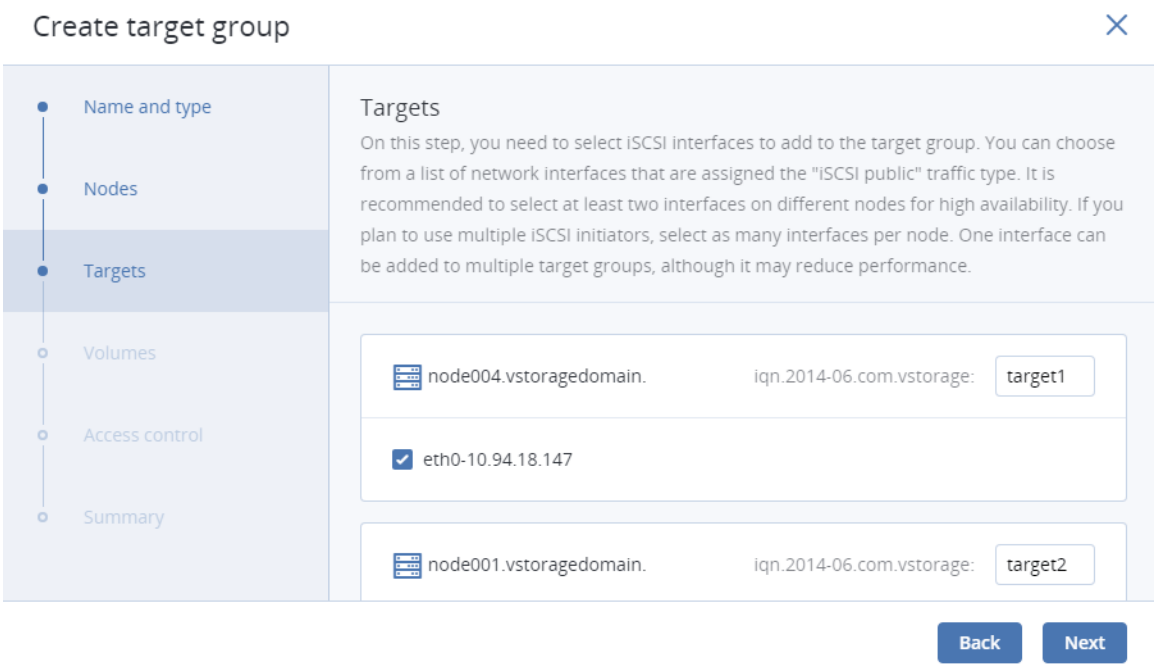
3. На экране **Серверы** выберите серверы для добавления в группу целевых устройств. На этих серверах будут запускаться целевые устройства iSCSI. Можно выбирать только серверы с сетевыми интерфейсами, которым назначен тип трафика **iSCSI**. Рекомендуется добавить в группу целевых устройств как минимум два сервера для обеспечения высокой доступности. Если планируется использовать несколько инициаторов iSCSI, следует добавить столько же серверов в целевую группу. Оптимальный вариант – создать по одному целевому устройству на сервер.

   Если сетевые интерфейсы серверов не настроены, щелкните по значку шестерни, выберите необходимые сети и нажмите **Применить**.

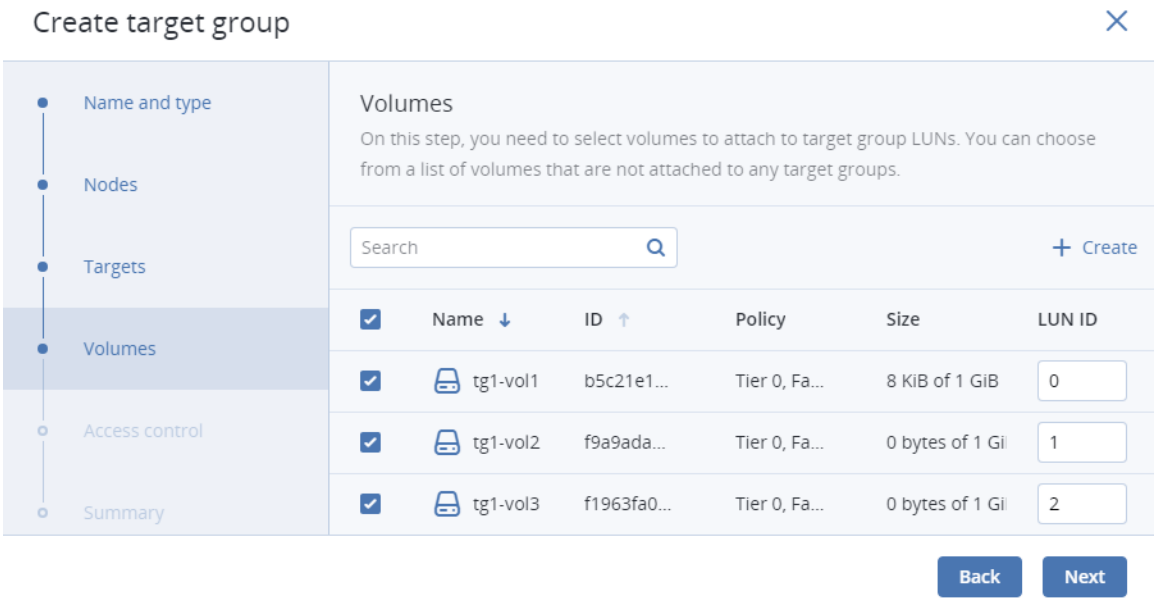


4. На экране **Цели** выберите интерфейсы iSCSI для добавления в группу целевых устройств. Возможен выбор из списка сетевых интерфейсов, которым назначен тип трафика **iSCSI**. Если планируется использовать несколько инициаторов iSCSI, следует выбрать по такому же

количеству интерфейсов на каждый сервер. Один интерфейс можно добавить в несколько групп целевых устройств, хотя это может снизить производительность.

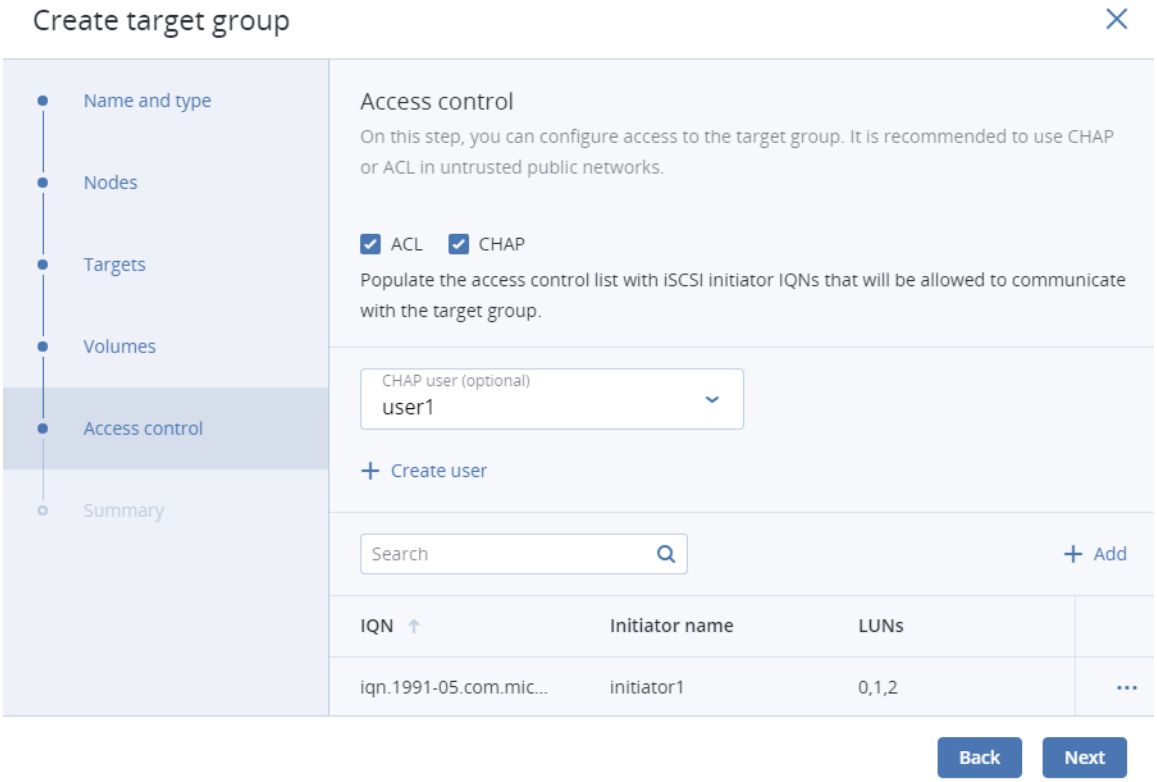


5. На экране **Тома** выберите тома для присоединения к LUN группы целевых устройств. Их можно выбрать из списка томов, которые не присоединены к группам целевых устройств. Если доступных томов нет, их можно создать на данном этапе, чтобы они были присоединены к группе целевых устройств автоматически, либо присоединить их позже вручную. Дополнительные сведения см. в разделе "Управление томами" на странице 379.



6. На экране **Контроль доступа** настройте доступ к группе целевых устройств. В недоверенных внешних сетях рекомендуется использовать протокол CHAP или списки ACL. Без управления доступом будут разрешены любые подключения к группе целевых устройств. Дополнительные

сведения см. в разделе "Ограничение доступа к группам целевых устройств" на странице 383.



7. На экране **Сводка** просмотрите сведения о группе целевых устройств. При необходимости можно вернуться назад и изменить их. Нажмите кнопку **Создать**.

Созданная группа целевых устройств появится на вкладке **Группы целей**. Ее целевые устройства запустятся автоматически.

Интерфейс командной строки

Перед созданием каких-либо групп целевых устройств назначьте сеть с типом трафика **iSCSI** сетевому интерфейсу на каждом сервере, который будет добавлен в группу целевых устройств.

Для создания группы целевых устройств потребуется файл конфигурации со списком всех серверов для добавления в группу, а также WWN-имен и порталов целевых устройств, например:

```
[
 {
  "NodeId": "01baeabee73e4a0d",
  "WWN": "iqn.2013-10.com.vstorage:test1",
  "Portals": [
   {
    "Addr": "192.168.10.11",
    "Port": 3025
   }
  ]
 },
 {
```

```
    "NodeId": "0d90158e9d2444e1",
    "WWN": "iqn.2013-10.com.vstorage:test2",
    "Portals": [
     {
      "Addr": "192.168.10.12",
      "Port": 3025
     }
    ]
   },
   {
    "NodeId": "a9eca47661a64031",
    "WWN": "iqn.2013-10.com.vstorage:test3",
    "Portals": [
     {
      "Addr": "192.168.10.13",
      "Port": 3025
     }
    ]
   }
]
```

В этом файле конфигурации:

- NodeId – идентификатор сервера, который можно получить из файла /etc/vstorage/host_id на сервере.
- WWN – целевое WWN-имя, IQN, например **iqn.2013-10.com.vstorage:test1** (можно изменить только последнюю часть после двоеточия)
- Portals – один или несколько порталов целевых устройств (комбинации IP-адреса и порта, через которые будет доступно целевое устройство). IP-адрес Addr принадлежит интерфейсу внешней сети на сервере, который обрабатывает тип трафика iSCSI. Порт Port указывать необязательно, по умолчанию используется 3260.

После создания файла конфигурации, например tg1.json, можно создать группу целевых устройств с помощью команды vstorage-target tg-create. Например, чтобы создать группу целевых устройств iSCSI, выполните следующую команду:

```
# vstorage-target tg-create -name tg1 -targets tg1.json -type ISCSI
{
 "Id": "3d8364f5-b830-4211-85af-3a19d30ebac4"
}
```

В результате выполнения команды целевые устройства будут созданы на серверах, указанных в файле конфигурации, и присоединены к группе целевых устройств. Также будут созданы порталы целевых устройств на указанных сетевых интерфейсах и портах.

При создании группы ее целевые устройства изначально остановлены. Их можно запустить с помощью команды vstorage-target tg-start, например:

```
# vstorage-target tg-start -id 3d8364f5-b830-4211-85af-3a19d30ebac4
```

Эта команда запускает все целевые устройства в группе с идентификатором 3d8364f5-b830-4211-85af-3a19d30ebac4.

6.10.3 Создание томов

Хотя нужные тома удобно создавать во время создания группы целевых устройств, это можно также сделать в любое время впоследствии.

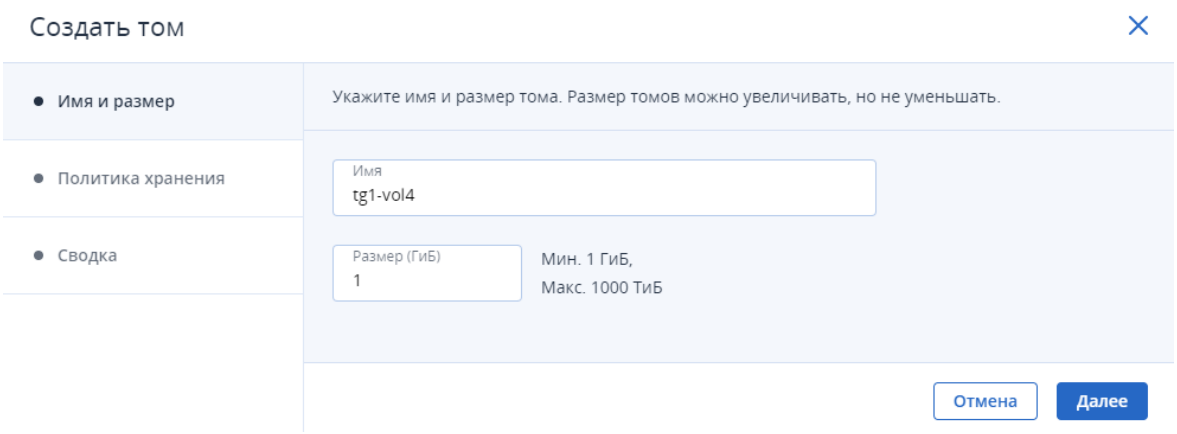
Предварительные требования

- Четкое понимание концепций из раздела "Политики хранения" на странице 37.
- Создана группа целевых устройств, как описано в разделе "Создание групп целевых устройств" на странице 199.

Как создать том

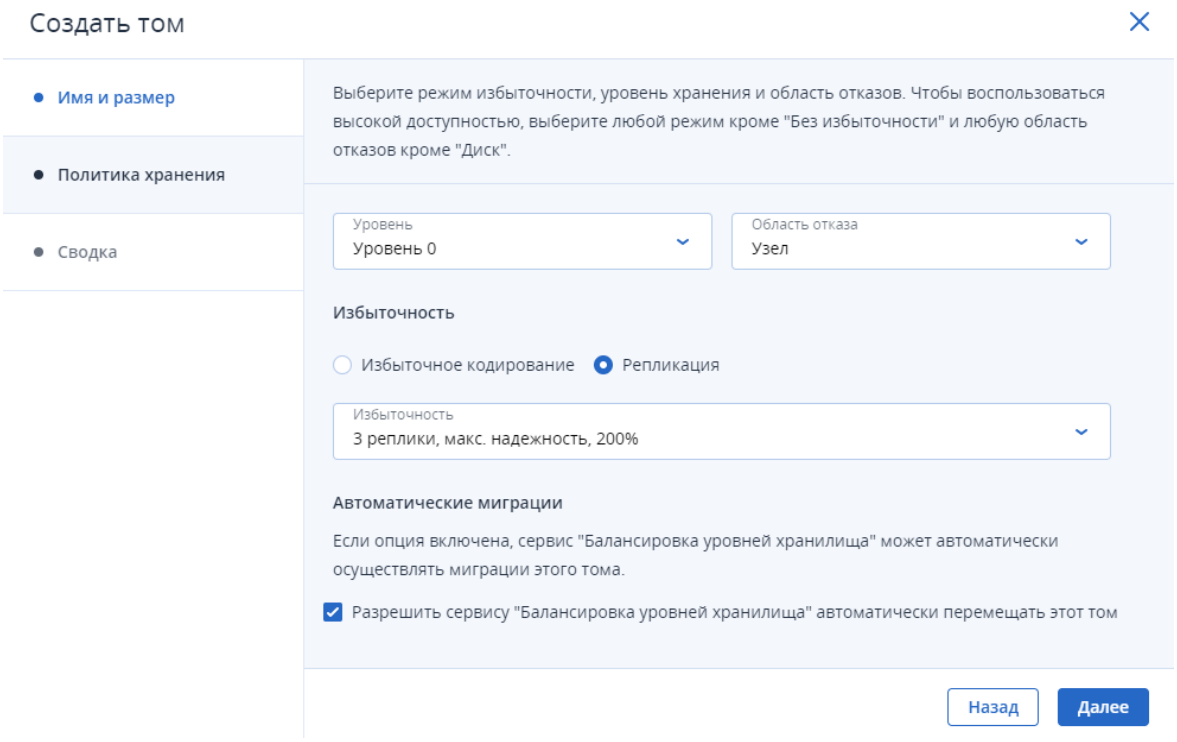
Панель администратора

1. Откройте **Сервисы хранилища** > **Блочное хранилище** > **Тома** и нажмите **Создать том**. Откроется мастер.
2. На экране **Имя и размер** введите имя тома и укажите размер в гигабайтах. Обратите внимание, что тома можно в дальнейшем увеличивать, но не уменьшать.



3. На экране **Политика хранения** выберите режим избыточности, уровень хранилища данных и область отказа. Чтобы воспользоваться преимуществами высокой доступности, выберите режим, отличный от **Без избыточности**, и область отказа, отличную от **Диск**.

   При необходимости снимите флажок **Разрешить сервису "Балансировка уровней хранилища" автоматически перемещать этот том**, который установлен по умолчанию.



4. На экране **Сводка** просмотрите сведения о томе. При необходимости можно будет вернуться и изменить их. Нажмите кнопку **Создать**.

Интерфейс командной строки

Чтобы создать том, используйте команду vstorage-target vol-create, например:

```
# vstorage-target vol-create -name vol1 -size 1G \
-vstorage-attr "replicas=3:2 failure-domain=host tier=0"
{
  "Id": "3277153b-5296-49c5-9b66-4c200ddb343d"
}
```

Эта команда создает том размером 1 ГБ с именем vol1 и задает ему уровень хранилища 0, режим репликации 3:2 и область отказа host.

6.10.4 Присоединение томов к группам целевых устройств

Предварительные требования

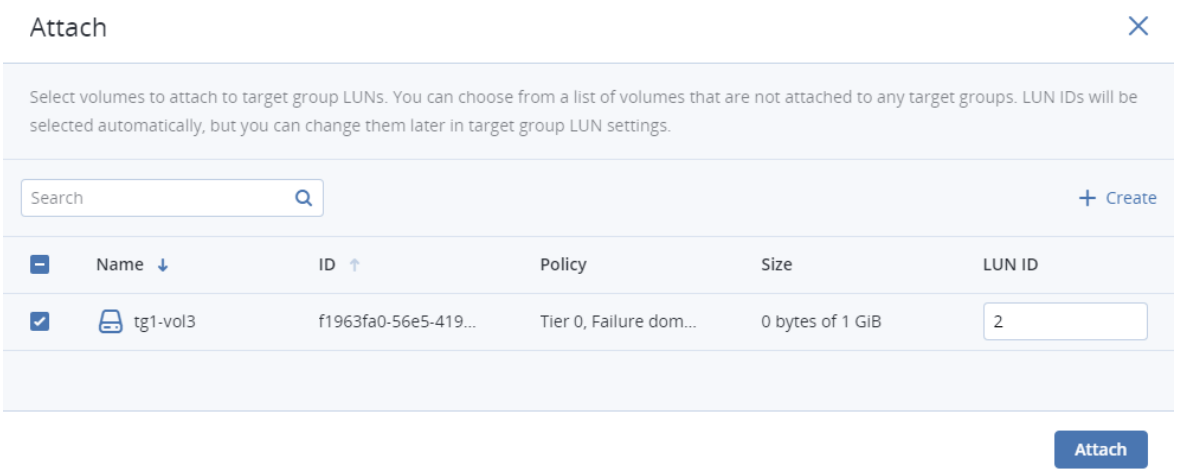
- Тома должны быть созданы, как описано в разделе "Создание томов" на предыдущей странице.

Чтобы добавить том в качестве LUN в группу целевых устройств

Панель администратора

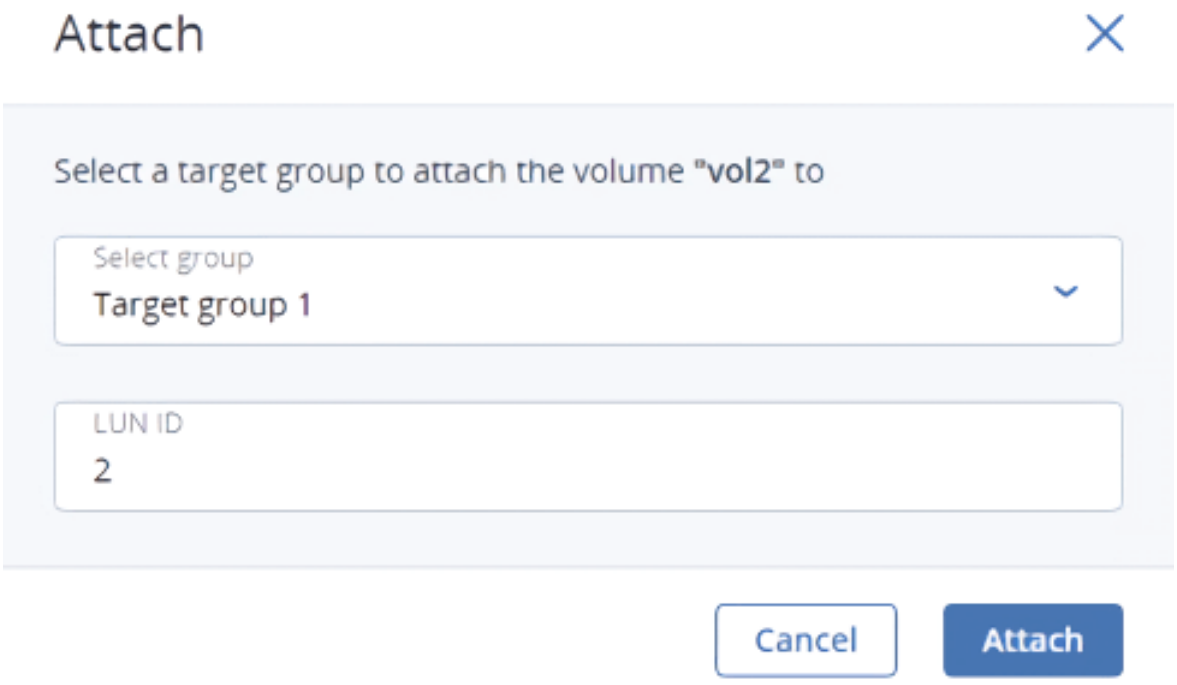
1. Откройте **Сервисы хранилища** > **Блочное хранилище** > **Группы целей**, щелкните по значку с многоточием возле нужной группы целевых устройств и нажмите **Добавить LUN**.

2. В окне **Присоединить** выберите тома для присоединения к группе целевых устройств (при необходимости создайте их) и нажмите **Присоединить**.



То же самое можно сделать и на вкладке **Тома**.

1. Щелкните по значку многоточия для нужного тома, затем нажмите **Присоединить**.
2. В окне **Присоединить** выберите группу целевых устройств и нажмите **Присоединить**.



Интерфейс командной строки

Чтобы присоединить том к группе целевых устройств, используйте команду vstorage-target tg-attach. Том нельзя присоединить к нескольким группам целевых устройств одновременно.

```
# vstorage-target tg-attach -id 3d8364f5-b830-4211-85af-3a19d30ebac4 \
-volume 3277153b-5296-49c5-9b66-4c200ddb343d -lun 0 -node bbfd0e7a26b1406d
```

Эта команда присоединяет том с идентификатором 3277153b-5296-49c5-9b66-4c200ddb343d к группе целевых устройств с идентификатором 3d8364f5-b830-4211-85af-3a19d30ebac4 как LUN 0. Нумерация идентификаторов LUN должна начинаться с 0. Эта же команда задает бит PREFERRED для сервера с идентификатором bbfd0e7a26b1406d. Активный/оптимизированный путь по умолчанию будет идти через этот сервер.

6.11 Подготовка пространства для хранилища объектов

Пространство для хранилища объектов подготавливается к работе с помощью корзин S3, создаваемых в кластере S3.

Ограничения

- Поверх кластера хранилища можно создать только один кластер S3.
- Все компоненты кластера S3 должны запускаться на нескольких узлах для обеспечения высокой доступности. Компоненты сервера имен и сервера объектов в кластере S3 автоматически балансируются и переносятся между узлами S3. Шлюзы S3 автоматически не переносятся; их высокая доступность основана на записях DNS. При добавлении или удалении шлюзов S3 необходимо поддерживать актуальность записей DNS вручную.

Предварительные требования

- Четкое понимание понятий, связанных с хранилищем объектов, которое описывается в разделе "О хранилище объектов" на странице 19.
- Оборудование, соответствующее требованиям, приведенным в разделе "Требования для хранилища объектов" на странице 56.
- Сети инфраструктуры должны быть настроены, как описано в разделе "Настройка сетей для хранилища объектов" на странице 112.
- Кластер хранилища должен быть создан в соответствии с указаниями из раздела "Развертывание кластера хранилища данных" на странице 141.
- Узлы, на которых будут выполняться службы S3, должны быть доступны в Кибер Инфраструктура.

Обзор подготовки к работе

1. Создайте кластер S3.
2. Добавьте пользователей S3.
3. Получайте доступ к корзинам S3 через панель пользователя Кибер Инфраструктура или сторонние приложения для работы с S3, такие как Cyberduck, Mountain Duck и т. д. (см. раздел «Получение доступа к корзинам S3» в руководстве пользователя хранилища).

6.11.1 Создание кластера S3

Ограничения

- После развертывания кластера S3 можно изменить только схему избыточности репликации. Изменение схемы избыточности кодирования не поддерживается, так как оно может снизить производительность кластера. Для перекодирования необходим большой объем ресурсов кластера в течение длительного времени. Если вы все же намерены изменить схему избыточности кодирования, обратитесь в службу технической поддержки.

Предварительные требования

- Четкое понимание концепции "Политики хранения" на странице 37.
- В кластере хранилища данных есть один или более дисков с ролью **Хранилище**.

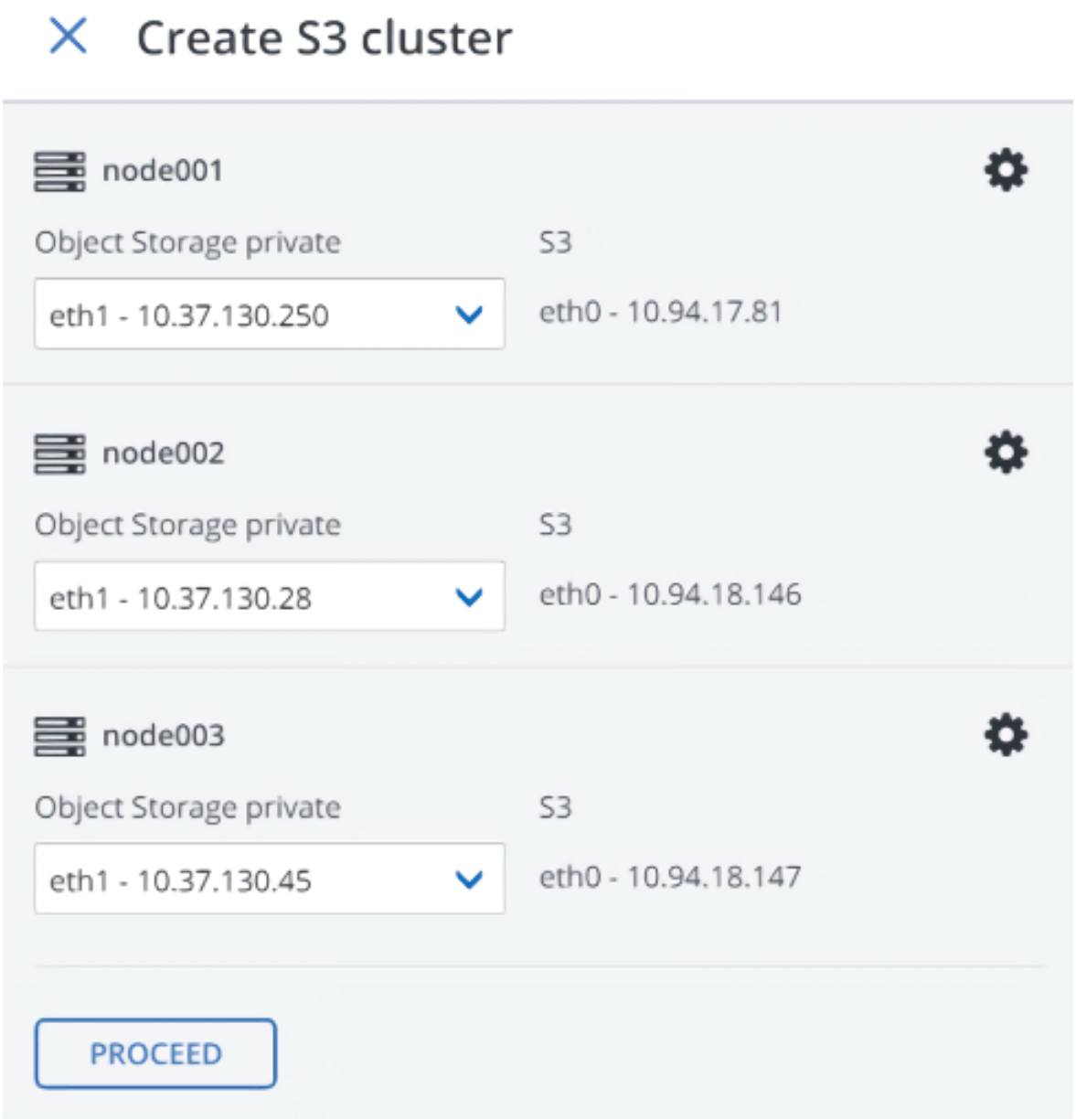
Чтобы настроить сервисы хранилища объектов на узлах кластера

Панель администратора

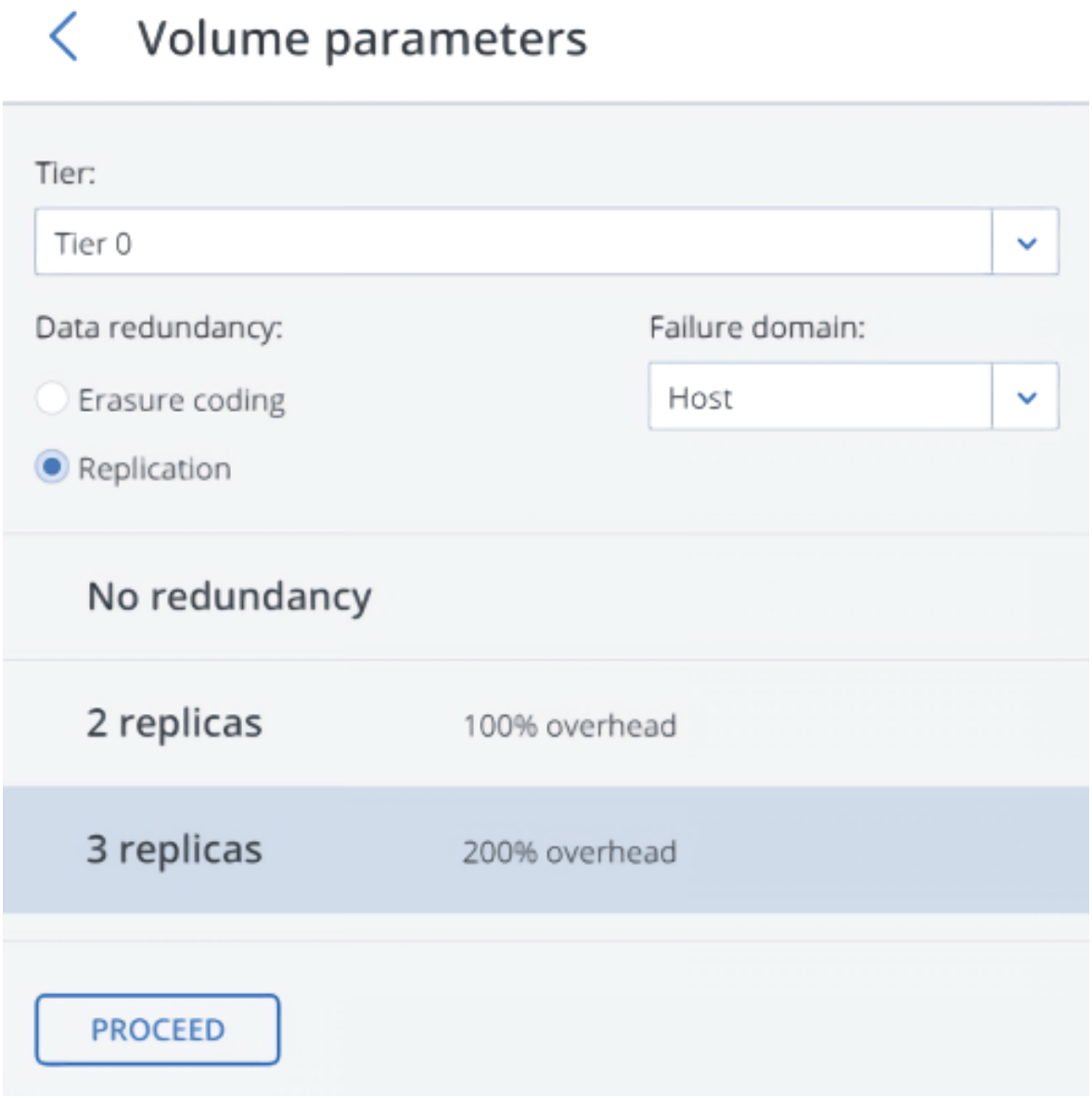
1. В меню слева нажмите **Сервисы хранилища** > **S3**.
2. Выберите один или несколько узлов, затем нажмите **Создать кластер S3** на правой панели. Чтобы создать кластер S3 с высокой доступностью, выберите не менее трех узлов.

   Примечание
   Серверы отображаются с небольшими значками, представляющими их роли внутри кластера. Дополнительные сведения о значках см. в статье Кибер Инфраструктура и Хранилище: роли иконок узлов.

3. Если сетевые интерфейсы серверов не настроены, щелкните по значку шестерни, выберите необходимые сети и нажмите **Применить**.



4. На панели **Параметры тома** выберите нужный уровень, область отказов и режим избыточности данных. Нажмите кнопку **Продолжить**.

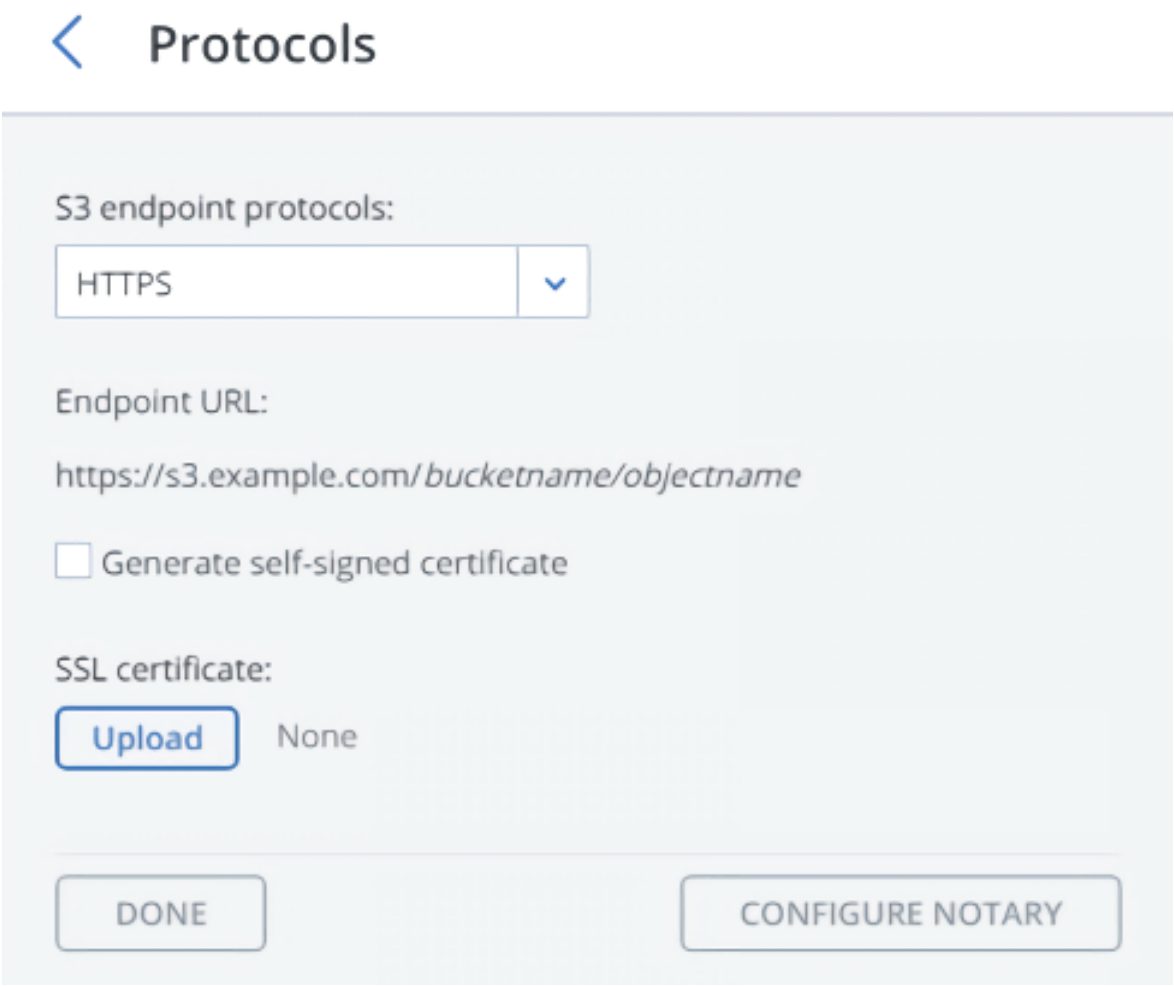


5. Укажите внешнее (публично разрешимое) доменное имя для оконечной точки S3, которая будет использоваться конечными пользователями для доступа к хранилищу объектных данных, например **s3.example.com**. Нажмите кнопку **Продолжить**.

Внимание
Настройте свой DNS-сервер в соответствии с примером, приведенным на панели администратора.

Примечание
В сложных средах можно использовать HAProxy для создания масштабируемой избыточной платформы балансировки нагрузки, которую можно легко перемещать или переносить, независимо от продукта Кибер Инфраструктура. Дополнительные сведения см. в статье Как запустить хранилище за HAProxy.

6. Из раскрывающегося списка выберите протокол оконечной точки S3: HTTP, HTTPS или оба.



Для производственного развертывания рекомендуется использовать только HTTPS.

После выбора протокола HTTPS

- Установите флажок **Сгенерировать самоподписанный сертификат**, чтобы получить самоподписанный сертификат для целей оценки HTTPS.

  Примечание
  - Для георепликации S3 требуется сертификат от доверенного центра. Она не работает с самоподписанными сертификатами.
  - Для доступа к данным в кластере S3 с помощью браузера добавьте самозаверяющий сертификат в исключения браузера.

- Получите ключ и доверенный подстановочный шаблон SSL-сертификата для домена нижнего уровня конечной точки. Например, конечной точке **s3.storage.example.com** потребуется подстановочный сертификат для ***.s3.storage.example.com** с альтернативным именем субъекта **s3.storage.example.com**.

  Если вы получили SSL-сертификат от промежуточного центра сертификации (ЦС), у вас должен быть сертификат конечного пользователя наряду с пакетом ЦС, содержащим

корневой и промежуточные сертификаты. Чтобы можно было использовать эти сертификаты, сначала необходимо объединить их в цепочку. Цепочка сертификатов включает в себя сертификат конечного пользователя, сертификаты промежуточных ЦС и сертификат доверенного корневого ЦС. В данном случае SSL-сертификат может быть доверенным только в том случае, если каждый сертификат в цепочке надлежащим образом выпущен и действителен.

Например, если у вас имеется сертификат конечного пользователя, два сертификата промежуточных ЦС и сертификат корневого ЦС, создайте новый файл сертификата и добавьте в него все сертификаты в следующем порядке:

```
# End-user certificate issued by the intermediate CA 1
-----BEGIN CERTIFICATE-----
MIICiDCCAg2gAwIBAgIQNfwmXNmET8k9Jj1X<...>
-----END CERTIFICATE-----
# Intermediate CA 1 certificate issued by the intermediate CA 2
-----BEGIN CERTIFICATE-----
MIIEIDCCAwigAwIBAgIQNE7VVyDV7exJ9ON9<...>
-----END CERTIFICATE-----
# Intermediate CA 2 certificate issued by the root CA
-----BEGIN CERTIFICATE-----
MIIC8jCCAdqgAwIBAgICZngwDQYJKoZIhvcN<...>
-----END CERTIFICATE-----
# Root CA certificate
-----BEGIN CERTIFICATE-----
MIIDODCCAiCgAwIBAgIGIAYFFnACMA0GCSqG<...>
-----END CERTIFICATE-----
```

Передайте подготовленный сертификат и, в зависимости от его типа, выполните одно из следующих действий:

- укажите парольную фразу (файлы PKCS#12);
- передайте ключ SSL.

Нажмите кнопку **Продолжить**.

Настройки протокола можно изменить позже. Для этого на экране **S3** > **Серверы** нажмите **Протокол** на панели справа.

7. Нажмите кнопку **Готово**, чтобы создать кластер S3.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service s3 cluster create [--tier {0,1,2,3}] [--failure-domain {0,1,2,3,4}]
                                 [--replicas <norm> | --encoding <M>+<N>]
                                 [--self-signed | --no-ssl | --cert-file <cert_file>]
                                 [--insecure] [--key-file <key_file>] [--password]
                                 --nodes <nodes> --s3gw-domain <domain>
```

--tier {0,1,2,3}

Уровень хранилища

--failure-domain {0,1,2,3,4}

Область отказа хранилища

--replicas <norm>

Схема репликации хранилища в формате:

- norm: количество сохраняемых реплик

--encoding <M>+<N>

Схема помехоустойчивого кодирования хранилища в формате:

- M: число блоков данных
- N: число паритетных блоков

--self-signed

Сгенерировать самоподписанный сертификат (используется по умолчанию)

--no-ssl

Не генерировать самоподписанный сертификат

--cert-file <cert_file>

Путь к файлу сертификата

--insecure

Разрешить незащищенные соединения наряду с защищенными (может использоваться только с параметрами --cert-file и --self-signed)

--key-file <key_file>

Путь к файлу закрытого ключа сертификата (может использоваться только с параметром --cert-file)

--password

Считать пароль сертификата из стандартного ввода (может использоваться только с параметром --cert-file)

--nodes <nodes>

Список имен хостов или идентификаторов серверов через запятую

--s3gw-domain <domain>

DNS-имя конечной точки кластера S3

Например, чтобы создать кластер S3, который будет состоять из узлов node001 и node002 и использовать самоподписанный сертификат, выполните:

```
# vinfra service s3 cluster create --nodes node001,node002 --tier 0 --failure-domain 1 \
--encoding 1+2 --self-signed --s3gw-domain dns.example.com
```

Эта команда также указывает уровень хранения данных, режим избыточности, область отказа и DNS-имя.

Посмотреть конфигурацию хранилища S3 можно в выводе команды vinfra service s3 show:

```
# vinfra service s3 show
+---------------+-------------------------------------------+
| Field         | Value                                     |
+---------------+-------------------------------------------+
| failure_domain | 1                                        |
| id            | 0100000000000002                          |
| name          | cluster1                                  |
| nodes         | - id: ca334b1d-20a1-1241-96a5-eb9acadb8ecd |
|               | - id: ab36b523-91dc-e78d-53a7-88baed44541e |
| np            |                                           |
| nusers        | 0                                         |
| protocol      | scheme: https                             |
| redundancy    | m: 1                                      |
|               | n: 2                                      |
|               | type: raid6                               |
| s3gw_domain   | dns.example.com                           |
| tier          | 0                                         |
+---------------+-------------------------------------------+
```

Чтобы проверить, успешно ли развернут кластер S3 и имеют ли к нему доступ пользователи, откройте в браузере адрес https://<S3_DNS_name> или http://<S3_DNS_name>. Должен отобразиться следующий ответ XML:

```
<Error>
<Code>AccessDenied</Code>
<Message/>
</Error>
```

Чтобы начать пользоваться хранилищем S3, также потребуется создать как минимум одного пользователя S3.

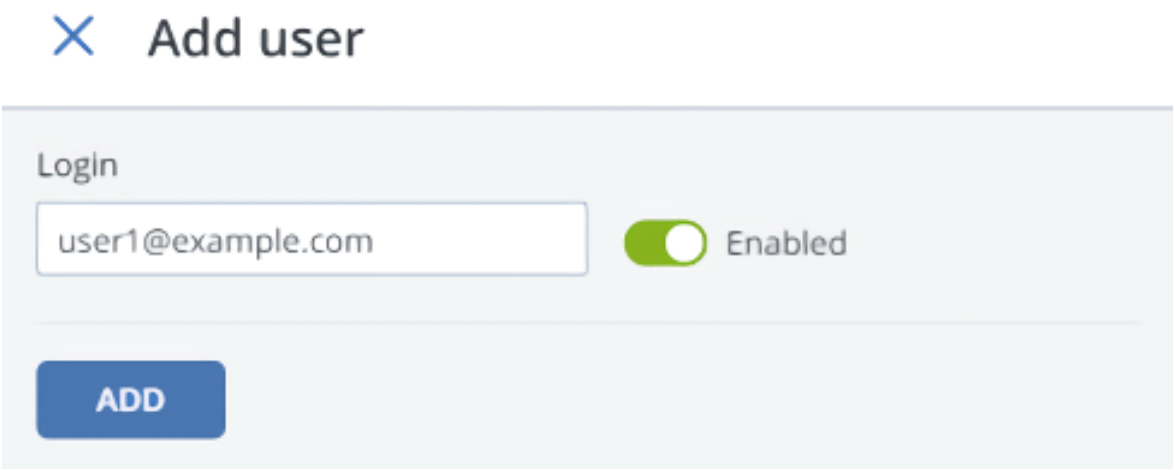
6.11.2 Добавление пользователей S3

Предварительные требования

- Кластер S3 должен быть создан в соответствии с указаниями из раздела "Создание кластера S3" на странице 208.

Чтобы добавить пользователя S3

1. На экране **Сервисы хранилища** > **S3** > **Пользователи** нажмите **Добавить пользователя**.
2. Укажите действительный адрес электронной почты в качестве имени входа для пользователя и нажмите **Добавить**.



6.11.3 Масштабирование хранилища объектов

При масштабировании хранилища объектов примите во внимание следующее:

- Пропускная способность каждого шлюза S3 ограничена 1100–1300 МБ/с при достаточной производительности основного хранилища и достаточной скорости сети.
- Для максимального использования производительности основного хранилища необходимо включить в кластер S3 все доступные серверы.
- Перед созданием кластера S3 необходимо назначить тип трафика **S3 public** всем доступным сетям для внешнего трафика S3. Увеличение количества используемых сетевых интерфейсов на сервере под тип трафика **S3 public** кратно увеличивает пропускную способность сервера.
- Для масштабирования совокупной производительности кластера S3 необходимо развернуть балансировщик нагрузки перед всеми шлюзами S3 этого кластера. В конфигурацию балансировщика нагрузки нужно включить IP-адреса всех сетевых интерфейсов с типом трафика **S3 public**. Например, чтобы развернуть балансировщик нагрузки на основе HAProxy, см. Как запустить хранилище за HAProxy.
- Можно развернуть несколько внутренних шлюзов S3 на сервере, использовав отдельный сетевой порт для каждого шлюза S3. Подробности описаны в разделе "Увеличение количества шлюзов S3 на серверах кластера S3" ниже.

6.11.4 Увеличение количества шлюзов S3 на серверах кластера S3

Для улучшения производительности кластера S3 можно установить большее количество шлюзов S3 на серверах кластера, чем устанавливается по умолчанию. Чтобы увеличить количество шлюзов S3, используйте приведенные ниже инструкции в зависимости от текущей конфигурации инфраструктуры.

Если кластер S3 еще не создан, выполните следующие шаги на каждом сервере, который будет добавлен в кластер:

1. В файле /opt/rh/rh-python36/root/lib/python3.6/site-packages/backend/config.py в параметре OSTOR_DEFAULT_NGW_PER_IFACE укажите необходимое количество шлюзов S3.

   Примечание
   В этом файле также можно задать следующие параметры при необходимости: OSTOR_DEFAULT_NNS_PER_NODE – количество служб имен S3 на сервере кластера по умолчанию; OSTOR_MAX_NNS – максимальное количество служб имен S3 в кластере; OSTOR_DEFAULT_NOS_PER_NODE – количество служб объектов S3 на сервере кластера по умолчанию; OSTOR_MAX_NOS – максимальное количество служб объектов S3 в кластере.

2. Перезапустите службу vstorage-ui-backend:

   ```
   systemctl restart vstorage-ui-backend
   ```

После создания кластера S3 на его серверах будет установлено указанное количество шлюзов S3.

Если кластер S3 уже создан, выполните следующие шаги на серверах кластера с внешними IP-адресами:

1. Получите идентификатор тома, который используется кластером S3 для хранения данных, запустив команду ostor-ctl get-config. Например:

   ```
   # ostor-ctl get-config
   ...
   VOL_ID          TYPE    STATE
   0100000000000002  OBJ    READY
   ...
   ```

2. Создайте дополнительные шлюзы S3, использовав следующую команду:

   ```
   ostor-ctl add-s3gw -a <internal_IP_address>:<port> -V <volume_ID>
   ```

   -a <internal_IP_address>:<port>

   Внутренний IP-адрес сервера и незанятый порт, которые будут использованы шлюзом S3. У каждого экземпляра шлюза S3 должен быть отдельный порт на сервере.

   -V <volume_ID>

   Идентификатор тома, используемого кластером S3.

   Рекомендуется создавать 4 шлюза S3 на одном сервере.

   Например:

   ```
   # ostor-ctl add-s3gw -a 127.0.0.1:9003 -V 0100000000000002
   ```

3. Укажите созданный шлюз S3 в конфигурационном файле /etc/nginx/conf.d/s3-gateway-<volume_ID>.conf в секции upstream s3. Например:

```
upstream s3 {
...
   server 127.0.0.1:9003;
}
...
```

4. Перезапустите службу nginx:

```
systemctl reload nginx
```

После выполнения данных шагов на серверах кластера S3 будут созданы дополнительные шлюзы S3.

6.12 Подготовка пространства для файлового хранилища

Пространство для файлового хранилища подготавливается к работе с помощью экспортов NFS, создаваемых в кластере NFS.

Предварительные требования

- Четкое понимание понятий, связанных с файловым хранилищем, которое описывается в разделе "О файловом хранилище" на странице 21.
- Оборудование, соответствующее требованиям, приведенным в разделе "Требования к серверу" на странице 46.
- Сети инфраструктуры должны быть настроены, как описано в разделе "Настройка сетей для файлового хранилища" на странице 113.
- Кластер хранилища должен быть создан в соответствии с указаниями из раздела "Развертывание кластера хранилища данных" на странице 141.

Обзор подготовки к работе

1. Создайте кластер NFS.
2. Создайте тома NFS.
3. Создайте экспорты NFS.
4. Получите доступ к томам NFS, подключив пользовательские экспорты (см. раздел «Доступ к томам NFS» в руководстве пользователя хранилища).

6.12.1 Создание кластера NFS

Предварительные требования

- В кластере хранилища данных есть один или более дисков с ролью **Хранилище**.

Чтобы создать кластер NFS

Панель администратора

1. Перейдите на экран **Сервисы хранилища** > **NFS** > **Серверы**.
2. Выберите один или несколько узлов и нажмите **Создать кластер NFS** на панели справа.

   Примечание
   Серверы отображаются с небольшими значками, представляющими их роли внутри кластера. Дополнительные сведения о значках см. в статье Кибер Инфраструктура и Хранилище: роли иконок узлов.

3. Убедитесь, что в раскрывающемся списке выбран правильный сетевой интерфейс.
   При необходимости нажмите значок шестерни и настройте сетевые интерфейсы узла в окне **Настройка сети**.
4. Нажмите кнопку **Создать**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service nfs cluster create --nodes <node>[:<ip_address>]
```

--nodes <node>[:<ip_address>]
: Разделенный запятыми список хостовых имен или идентификаторов узлов (IP-адреса указываются при необходимости)

Например, чтобы создать кластер NFS, состоящий из одного узла node001, выполните:

```
# vinfra service nfs cluster create --nodes node001
```

После создания кластера NFS можно перейти к созданию томов NFS.

6.12.2 Создание томов NFS

Ограничения

- После создания тома NFS можно изменять его режим избыточности только тогда, когда избыточность обеспечивается с помощью репликации. Возможность изменить режим избыточности отключена для остальных случаев, так как это может снизить производительность кластера. Причина в том, что перекодировка данных требует большого количества ресурсов кластера на долгое время. Если вы все же хотите изменить режим избыточности, свяжитесь со службой технической поддержки.

Предварительные требования

- Четкое понимание концепций, описанных в разделе "Политики хранения" на странице 37.
- Кластер NFS должен быть создан в соответствии с указаниями из раздела "Создание кластера NFS" на странице 217.

Чтобы создать том NFS

Панель администратора

1. На экране **Сервисы хранилища** > **NFS** > **Тома** нажмите **Добавить том NFS**.
2. На панели **Добавить том NFS** укажите уникальное имя и IP-адрес, который должен быть неиспользуемым и, если включена аутентификация, разрешимым в домене. Кроме того, этот IP-адрес должен находиться в диапазоне подсети интерфейса узла. Нажмите **Продолжить**.
3. В поле **Размер тома** укажите размер тома в гигабайтах. Для пользователей, обращающихся к экспортам, это значение будет размером файловой системы.
4. Выберите нужный уровень хранения, область отказа и тип избыточности данных.
5. Нажмите кнопку **Готово**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service nfs share create --node <node> --ip-address <ip_address> --size <size> --tier {0,1,2,3}
                (--replicas <norm> | --encoding <M>+<N>) --failure-domain {0,1,2,3,4} <name>
```

--node <node>

Идентификатор узла

--ip-address <ip_address>

IP-адрес тома NFS

--size <size>

Размер тома NFS в байтах. Также можно использовать следующие единицы измерения: KiB для кибибайтов, MiB для мебибайтов, GiB для гибибайтов, TiB для тебибайтов и PiB для пебибайтов.

--tier {0,1,2,3}

Уровень хранилища

--replicas <norm>

Схема репликации хранилища в формате:

- norm: количество сохраняемых реплик

--encoding <M>+<N>

Схема помехоустойчивого кодирования хранилища в формате:

- M: число блоков данных
- N: число паритетных блоков

--failure-domain {0,1,2,3,4}

Область отказа хранилища

<name>

Имя тома NFS

Например, чтобы создать том share1 с IP-адресом 10.136.18.149 на узле с идентификатором 923926da-a879-5f56-1b24-1462917ed335, выполните:

```
# vinfra service nfs share create share1 --node 923926da-a879-5f56-1b24-1462917ed335 \
--ip-address 10.136.18.149 --size 107374182400 --tier 0 --encoding 1+2 --failure-domain 1
```

Созданный том NFS появится в выводе команды vinfra service nfs share list output:

```
# vinfra service nfs share list
+--------+--------------+-----------------------------------------+
| name   | ip_address   | node                                    |
+--------+--------------+-----------------------------------------+
| share1 | 10.136.18.149 | cfgd_id: 1                             |
|        |              | has_configd: true                       |
|        |              | id: 923926da-a879-5f56-1b24-1462917ed335 |
|        |              | ip_address: node001.vstoragedomain      |
+--------+--------------+-----------------------------------------+
```

После того как том будет создан, можно перейти к созданию экспортов NFS.

6.12.3 Создание экспортов NFS

Предварительные требования

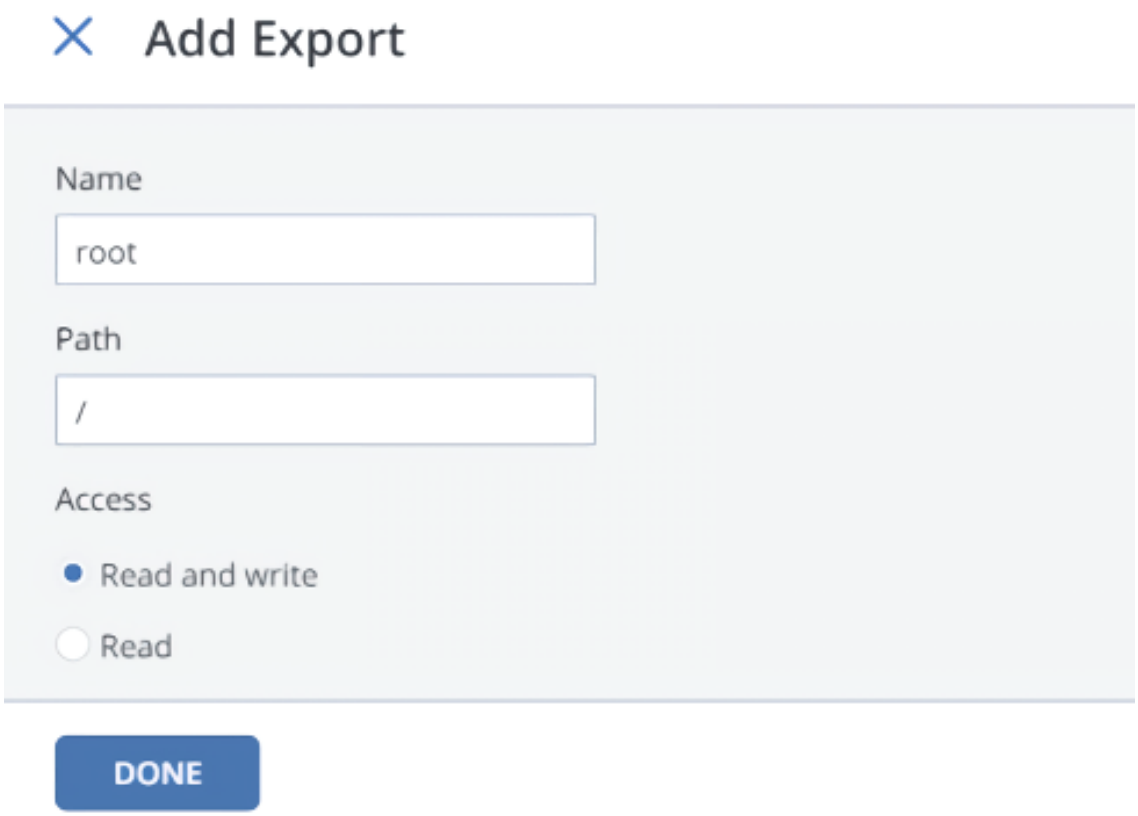
- Должны быть созданы тома NFS, как описано в разделе "Создание томов NFS" на странице 218.

Чтобы создать экспорты NFS

Панель администратора

1. Создайте корневой экспорт.
   a. На экране **Сервисы хранилища** > **NFS** > **Тома** щелкните по номеру в столбце **Экспорты** в строке нужного тома. Откроется экран тома.
   b. На экране тома нажмите **Добавить экспорт**, укажите **root** в качестве имени экспорта и **/** в качестве пути, а также выберите режим доступа **Чтение и запись**.

   Внимание
   Не используйте другие имена или пути для корневого экспорта.



Будет создан каталог с путем по умолчанию, который указывает на расположение экспорта внутри тома. Этот путь автоматически создается на основе имени тома и используется (наряду с IP-адресом тома) для подключения экспорта.

Внимание
Не предоставляйте пользователям доступ к корневому экспорту.

Корневой экспорт будет отображаться в списке экспортов.

2. Подключите корневой экспорт, как описано в руководстве пользователя хранилища.

Предупреждение
Не подключайте тома NFS на серверах кластера. Это может привести к зависанию серверов.

3. Создайте пользовательские экспорты в подключенном корневом экспорте.
   a. В подключенном корневом экспорте создайте подкаталог для пользовательского экспорта, например **export1**.
   b. На экране тома нажмите **Добавить экспорт**, введите имя пользовательского экспорта, укажите **/export1** в качестве пути и выберите режим доступа.
   c. Нажмите кнопку **Готово**.

Пользовательский экспорт появится в списке экспортов.

Интерфейс командной строки

1. Создайте корневой экспорт. Например, для тома share1 выполните:

```
# vinfra service nfs export create share1 root --path / --access-type rw --security-types none
```

2. Подключите корневой экспорт, как описано в руководстве пользователя хранилища.

Предупреждение
Не подключайте тома NFS на серверах кластера. Это может привести к зависанию серверов.

3. Создайте пользовательские экспорты в подключенном корневом экспорте, используя следующую команду:

```
vinfra service nfs export create --path <path> --access-type <access-type> --security-types
<security-types>
                    [--client <address=ip_addresses:access=access_type:security=security_
types>]
                    [--squash <squash>] [--anonymous-gid <anonymous-gid>] [--anonymous-uid
<anonymous-uid>]
                    <share-name> <export-name>
```

--path <path>
: Путь экспорта NFS

--access-type <access-type>
: Режим доступа экспорта NFS (none, rw или ro)

--security-types <security-types>
: Режим безопасности экспорта NFS (none, sys, krb5, krb5i или krb5p)

--client <address=ip_addresses:access=access_type:security=security_types>
: Список клиентского доступа экспорта NFS

--squash <squash>
: Режим отображения пользователей клиентов NFS в пользователей сервера NFS (root_squash, root_id_squash, all_squash или none)

--anonymous-gid <anonymous-gid>
: Идентификатор группы для анонимного доступа к экспорту NFS

--anonymous-uid <anonymous-uid>
: Идентификатор пользователя для анонимного доступа к экспорту NFS

<share-name>
: Имя тома NFS

<export-name>
: Имя экспорта NFS

Например, чтобы создать пользовательский экспорт export1 с путем /export1, выполните:

```
# vinfra service nfs export create share1 export1 --path /export1 --access-type rw --security-types
none
```

Созданный экспорт NFS появится в выводе команды vinfra service nfs export list:

```
# vinfra service nfs export list --share-name share1
+---------+-----------------+-------------+
| name    | path            | access_type |
+---------+-----------------+-------------+
| export1 | /share1/export1 | rw          |
| root    | /share1         | rw          |
+---------+-----------------+-------------+
```

6.12.4 Масштабирование файлового хранилища

Пропускная способность первого тома NFS составляет примерно 800–900 МБ/с при достаточной производительности основного хранилища и достаточной скорости сети. При добавлении от двух и более томов NFS пропускная способность каждого тома будет составлять примерно 500–600 МБ/с.

Для использования всей производительности основного хранилища необходимо создать по одному тому NFS на каждом сервере кластера NFS.

Чтобы совокупная производительность всех томов NFS масштабировалась линейно, тома необходимо создавать на разных серверах кластера NFS. Если при создании через панель управления два тома NFS оказались на одном и том же сервере, один из томов необходимо перенести на свободный сервер.

Чтобы перенести том NFS, выполните следующие шаги:

1. Определите, на каком сервере расположен том NFS, просмотрев сведения о томе на экране **Сервисы хранилища** > **NFS** > **Тома**.
2. На исходном сервере остановите том NFS и отмените его регистрацию, выполнив следующие команды:

   ```
   vstorage-nfs stop -n <name>
   vstorage-nfs unregister -n <name>
   ```

   <name>

   Имя тома NFS

3. На целевом сервере зарегистрируйте и запустите том NFS, выполнив следующие команды:

   ```
   vstorage-nfs register -n <name>
   vstorage-nfs start -n <name>
   ```

   <name>

   Имя тома NFS

После переноса дождитесь появления нового местоположения тома NFS на панели управления.

6.13 Настройка пользовательских режимов избыточности данных

На панели администрирования Кибер Инфраструктура доступны лишь предопределенные режимы избыточности данных. Чтобы настроить пользовательские режимы избыточности данных, используйте интерфейс командной строки. В таблице ниже приведены команды для каждого типа сервиса.

Сервис	Команды
Хранилище резервных копий	vinfra service backup volume-params change (см. раздел "Изменение схемы избыточности для хранилища резервных копий" на странице 354)
Хранилище блочных данных	vstorage-target vol-create (см. раздел "Создание томов" на странице 204) vstorage-target vol-attr set (см. раздел "Управление томами" на странице 379)
Хранилище объектов	ostor-ctl set-storage-class (см. раздел "Определение классов хранения объектов" на странице 407) ostor-ctl cfg-storage (см. раздел "Определение классов хранения объектов" на странице 407)
Файловое хранилище	vinfra service nfs share create (см. раздел "Создание томов NFS" на странице 218) vinfra service nfs share set (см. раздел "Управление томами NFS" на странице 422)
Вычислительный кластер	vinfra service compute storage-policy create (см. раздел "Управление политиками хранения" на странице 619) vinfra service compute storage-policy set (см. раздел "Управление политиками хранения" на странице 619)

7 Управление

Настроив инфраструктуру, вы сможете управлять серверами, сетями, пользователями, самообслуживанием и безопасностью, а также устанавливать лицензии и настраивать уведомления по электронной почте. Кроме того, вы сможете подготавливать ресурсы для резервного копирования, вычислений, а также хранилищ блоков, объектов и файлов и управлять ими на панели администрирования.

7.1 Управление инфраструктурой

В этом разделе описаны общие задачи администрирования инфраструктуры: лицензирование, управление сетями, серверами, безопасностью и самообслуживанием.

7.1.1 Управление серверами инфраструктуры

В этом разделе описывается, как разместить серверы в определенном расположении, изменить настройки сетевых интерфейсов и подключить устройства iSCSI.

7.1.1.1 Управление расположением серверов

Расположение сервера можно выбрать во время развертывания кластера хранилища или позже. По умолчанию серверы добавляются в стойку **Default rack** в ряду **Default row** в комнате **Default room**.

Расположения предназначены для использования в качестве областей отказа. Можно создавать новые расположения, переименовывать и удалять их, а также переносить серверы из одного расположения в другое.

Ограничения

- Расположение можно изменить только для неназначенных серверов. Если сервер является частью кластера, сначала освободите его. После перемещения сервер снова можно будет присоединить к кластеру.
- Удалять можно только пустые расположения. Если расположение содержит серверы, сначала нужно их переместить. Также нельзя удалить расположение по умолчанию. Однако его можно переименовать в соответствии с вашей инфраструктурой.

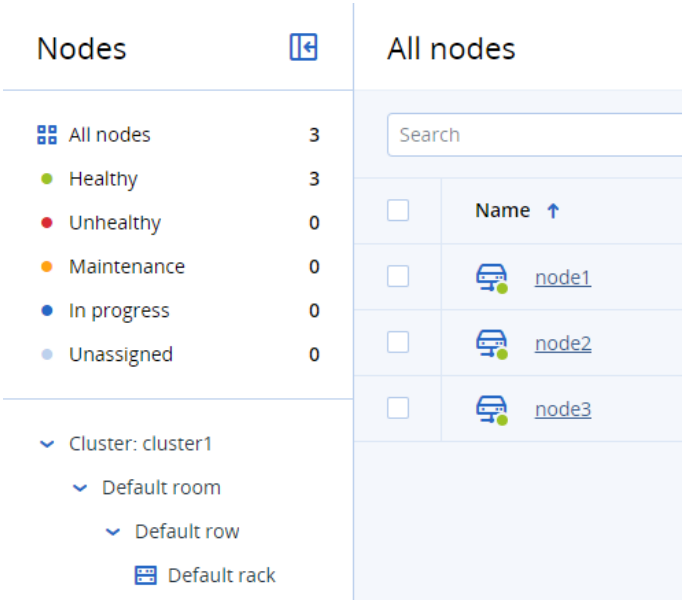
Предварительные требования

- Четкое понимание концепций, описанных в разделе "Области отказа" на странице 35.

Создание расположений

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по значку , чтобы показать расположение и фильтры серверов (если они скрыты).
2. На боковой панели расположения щелкните по верхней строке дерева с именем кластера.



3. Нажмите кнопку **Создать комнату** на панели инструментов и введите имя комнаты.
4. Чтобы добавить новый ряд, щелкните по созданной комнате. Нажмите кнопку **Создать ряд** и введите для него имя.
5. Чтобы добавить новую стойку, щелкните по созданному ряду. Нажмите кнопку **Создать стойку** и введите для нее имя. Теперь можно перемещать серверы в эту стойку.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra location create --fd <fd> --name <location-name> [--parent-id <parent-id>]
```

--fd <fd>

Идентификатор области отказа (0 – диск, 1 – хост, 2 – стойка, 3 – ряд стоек, 4 – комната). Список областей отказа можно получить с помощью команды vinfra failure domain list.

--name <location-name>

Имя создаваемого расположения.

--parent-id <parent-id>

Идентификатор родительского расположения, в котором должно быть создано дочернее расположение.

Например, чтобы создать расположение row2, выполните:

```
# vinfra location create --fd 3 --name row2 --parent-id 0
+----------+-------+
```

```
| Field    | Value |
+----------+-------+
| children | []    |
| id       | 1     |
| name     | row2  |
| parent   | 0     |
+----------+-------+
```

Примечание

Чтобы создать расположение 4-го уровня (комната), не используйте аргумент --parent-id.

Созданное расположение появится в выводе команды vinfra location list:

```
# vinfra location list --fd 3
+----+-------------+--------+----------+
| id | name        | parent | children |
+----+-------------+--------+----------+
| 0  | Default row | 0      | - 0      |
| 1  | row2        | 0      | []       |
+----+-------------+--------+----------+
```

Переименование расположений

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по значку  , чтобы показать расположение и фильтры серверов (если они скрыты).
2. На боковой панели щелкните по родительскому элементу для расположения, которое необходимо переименовать. Например, щелкните по ряду, если требуется переименовать стойку в этом ряду.
3. Выберите нужное расположение в списке. На правой панели нажмите **Переименовать** и введите новое имя.

Расположение будет переименовано.

Примечание

Можно переименовать расположения **room**, **row** и **rack**. Например, можно переименовать **rack** в **chassis** для соответствия фактическому расположению сервера. Дополнительные сведения см. в описании команды vinfra location rename.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra location rename --fd <fd> --id <location-id> --name <location-name>
```

--fd <fd>

Идентификатор области отказа (0 – диск, 1 – хост, 2 – стойка, 3 – ряд стоек, 4 – комната). Список областей отказа можно получить с помощью команды vinfra failure domain list.

--id <location-id>

Идентификатор расположения, которое следует переименовать.

--name <location-name>

Новое имя расположения.

Например, чтобы изменить имя расположения с идентификатором 1 на row_renamed, выполните:

```
# vinfra location rename --fd 3 --id 1 --name row_renamed
```

Можно также изменять имена областей отказа уровней 2, 3 и 4 с помощью следующей команды:

```
vinfra failure domain rename {2,3,4} <singular-name> <plural-name>
```

{2,3,4}

Идентификатор области отказа (0 – диск, 1 – хост, 2 – стойка, 3 – ряд стоек, 4 – комната). Список областей отказа можно получить с помощью команды vinfra failure domain list.

<singular-name>

Имя указанной области отказа в единственном числе.

<plural-name>

Имя указанной области отказа во множественном числе.

Например, чтобы изменить имя области отказа уровня 2 на chassis, выполните:

```
# vinfra failure domain rename 2 chassis chassis
```

Примечание

Если вы используете имя, отличное от zone, enclosure, chassis, blade server, на панели администрирования оно будет заменено **местоположением**.

Перемещение серверов в новое расположение

1. На экране **Инфраструктура** > **Серверы** существует два способа переместить сервер в новое расположение. Можно выбрать из дерева расположений стойку, в которую следует переместить сервер, и нажать **Переместить серверы**. Либо можно щелкнуть по строке с сервером, который следует переместить, и нажать **Переместить сервер** на правой панели.
2. В окне **Переместить серверы** выберите нужный сервер/расположение и нажмите **Переместить**.
3. Теперь можно присоединить этот сервер к кластеру. Для этого щелкните по строке с сервером и нажмите **Присоединить к кластеру** на правой панели. В открывшемся окне нажмите **Присоединить**.

Сервер будет перемещен в указанное расположение.

Перемещение расположений

Используйте следующую команду:

```
vinfra location move --children <children> [<children> ...]
                     --parent-fd <parent-fd> --parent-id <parent-id>
```

--children <children> [<children> ...]

Идентификаторы расположений, перемещаемых в родительское расположение.

--parent-fd <parent-fd>

Область отказа родительского расположения.

--parent-id <parent-id>

Идентификатор родительского расположения.

Например, чтобы переместить расположение с идентификатором 2 (ряд стоек) в расположение с идентификатором 1 (комната), выполните:

```
# vinfra location move --children 2 --parent-fd 4 --parent-id 1
Operation successful.
```

Просмотр сведений о расположениях

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по значку  , чтобы показать расположение и фильтры серверов (если они скрыты).
2. Для просмотра сведений о расположении щелкните по его родительскому элементу на боковой панели. Например, щелкните по комнате, если требуется просмотреть сведения об одном из рядов этой комнаты.
3. Щелкните по нужному расположению в списке. На правой панели будут отображены сведения об этом расположении.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra location show --fd <fd> --id <location-id>
```

--fd <fd>

Идентификатор области отказа.

--id <location-id>

Идентификатор расположения, которое следует отобразить.

Например, чтобы вывести сведения о расположении с идентификатором 2, выполните:

```
# vinfra location show --fd 3 --id 2
+----------+-------------+
| Field    | Value       |
+----------+-------------+
| children | []          |
| id       | 2           |
| name     | row_renamed |
| parent   | 1           |
+----------+-------------+
```

Удаление расположений

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по значку  , чтобы показать расположение и фильтры серверов (если они скрыты).
2. На боковой панели щелкните по родительскому элементу для расположения, которое необходимо удалить. Например, щелкните по ряду, если требуется удалить из него стойку.
3. Выберите нужное расположение в списке. На правой панели нажмите **Удалить**.

Расположение будет удалено.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra location delete --fd <fd> --id <location-id>
```

--fd <fd>

Идентификатор области отказа (0 – диск, 1 – хост, 2 – стойка, 3 – ряд стоек, 4 – комната). Список областей отказа можно получить с помощью команды vinfra failure domain list.

--id <location-id>

Идентификатор удаляемого расположения.

Например, чтобы удалить расположение с идентификатором 1, выполните:

```
# vinfra location delete --fd 3 --id 1
```

7.1.1.2 Изменение параметров сетевого интерфейса

Изменение конфигурации сетевого интерфейса после развертывания хранилища или вычислительных сервисов включает миграцию сети этого интерфейса.

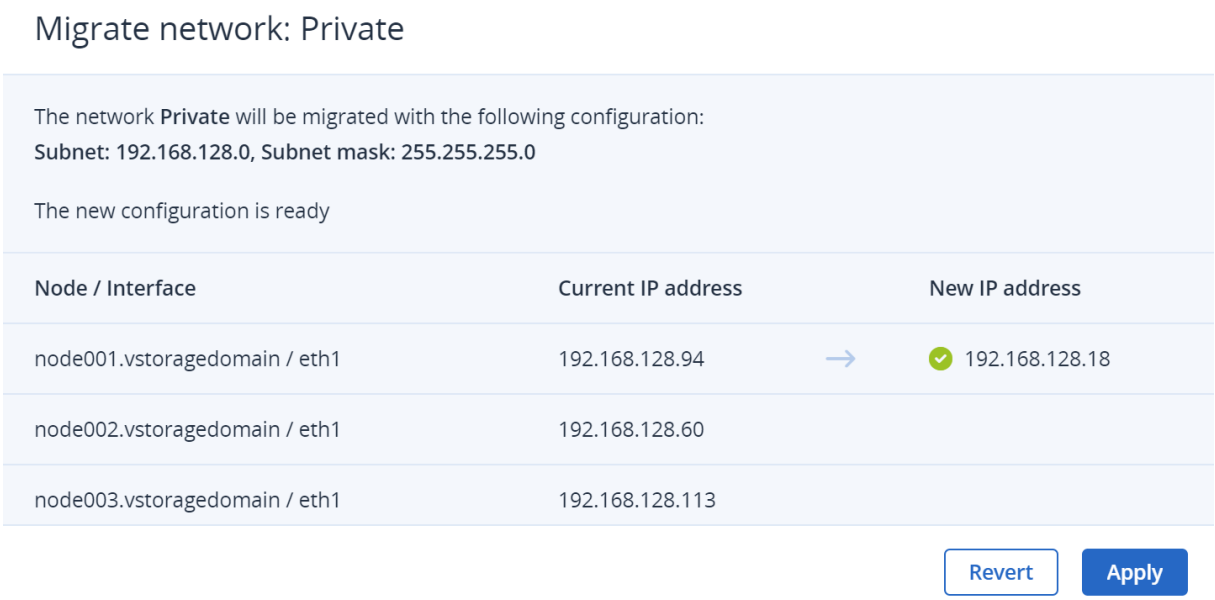
Предварительные требования

- Сетевой интерфейс настроен, как описано в разделе "Настройка сетевых интерфейсов серверов" на странице 117.

Изменение параметров сетевого интерфейса

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по имени узла, перейдите на вкладку **Сетевые интерфейсы** и выберите сетевой интерфейс.
2. На правой панели интерфейса нажмите **Изменить**.
3. В окне **Изменить сетевой интерфейс** внесите изменения в соответствующие сетевые параметры, например IP-адрес.
4. Нажмите кнопку **Сохранить**, чтобы применить изменения.
5. Если развертывание сервисов хранилища или вычислительных сервисов уже выполнено, откроется мастер миграции. Дождитесь создания новой конфигурации и нажмите **Применить**.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra node iface set [--ipv4 <ipv4>] [--ipv6 <ipv6>] [--gw4 <gw4>] [--gw6 <gw6>]
                      [--mtu <mtu>] [--dhcp4 | --no-dhcp4] [--dhcp6 | --no-dhcp6]
                      [--auto-routes-v4 | --ignore-auto-routes-v4]
                      [--auto-routes-v6 | --ignore-auto-routes-v6]
                      [--network <network> | --no-network] [--connected-mode | --datagram-mode]
                      [--ifaces <ifaces>] [--bond-type <bond-type>] [--node <node>] <iface>
```

--ipv4 <ipv4>

Разделенный запятыми список адресов IPv4

--ipv6 <ipv6>

Разделенный запятыми список адресов IPv6

--gw4 <gw4>

Адрес шлюза IPv4

--gw6 <gw6>

Адрес шлюза IPv6

--mtu <mtu>

Значение MTU (максимального размера передаваемого пакета) для интерфейса

--dhcp4

Включение DHCPv4

--no-dhcp4

Отключение DHCPv4

--dhcp6

Включение DHCPv6

--no-dhcp6

Отключение DHCPv6

--auto-routes-v4

Включить автоматические маршруты IPv4

--ignore-auto-routes-v4

Игнорировать автоматические маршруты IPv4

--auto-routes-v6

Включить автоматические маршруты IPv6

--ignore-auto-routes-v6

Игнорировать автоматические маршруты IPv6

--network <network>

Идентификатор или имя сети

--no-network

Удаление сети из интерфейса

--connected-mode

Включение подключенного режима (только для интерфейсов InfiniBand)

--datagram-mode

Включение режима дейтаграмм (только для интерфейсов InfiniBand)

--ifaces <ifaces>

Разделенный запятыми список имен сетевых интерфейсов, например: iface1,iface2...ifaceN

--bond-type <bond-type>

Тип объединения (balance-rr, balance-xor, broadcast, 802.3ad, balance-tlb, balance-alb)

Тип объединения для интерфейса OVS (balance-tcp, active-backup)

--node <node>

Идентификатор или имя хоста сервера (по умолчанию node001.vstoragedomain)

<iface>

Имя сетевого интерфейса

Например, чтобы изменить IP-адрес сетевого интерфейса eth1 сервера node002 на 192.168.128.91/24, выполните:

```
# vinfra node iface set eth1 --node node002 --ipv4 192.168.128.91/24
+---------------------------+-------------------------------------------------------------------------+
| Field                     | Value                                                                   |
+---------------------------+-------------------------------------------------------------------------+
| configuration             | network_id: f50605a3-64f4-4f0c-b50e-9481ec221c72                        |
| link                      | href: /api/v2/network/migration/ba7854ed-167e-4d6b-ab19-7244371a1b27/ |
|                           | method: GET                                                             |
|                           | rel: network-migration-details                                          |
| operation                 | network-migration                                                       |
| progress                  | 0.0                                                                     |
| single_interface_migration | True                                                                    |
| state                     | preparing                                                               |
| task_id                   | ba7854ed-167e-4d6b-ab19-7244371a1b27                                    |
| transitions               | 0                                                                       |
+---------------------------+-------------------------------------------------------------------------+
```

Если вы уже развернули сервис хранилища или сервис вычислений, вы увидите вывод, приведенный выше. Подождите, пока новая конфигурация сети проверяется, а затем примените ее:

```
# vinfra cluster network migration show | state
| state                     | test-passed                                                             |
# vinfra cluster network migration apply
```

7.1.1.3 Управление сетевыми интерфейсами

После настройки сетевых интерфейсов сервера можно их включать и выключать, а также удалять логические сетевые интерфейсы (сетевые объединения и VLAN-интерфейсы).

Предварительные требования

- Сетевой интерфейс настроен, как описано в разделе "Настройка сетевых интерфейсов серверов" на странице 117.

Ограничения

- Можно удалять только сетевые объединения и VLAN-интерфейсы.

Чтобы включить сетевой интерфейс

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по имени узла, перейдите на вкладку **Сетевые интерфейсы** и выберите сетевой интерфейс в состоянии **Отключен**.
2. На правой панели интерфейса нажмите **Включить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node iface up [--node <node>] <iface>
```

--node <node>

Идентификатор или имя хоста сервера

<iface>

Имя сетевого интерфейса

Например, чтобы включить сетевой интерфейс eth2 сервера node003, выполните:

```
# vinfra node iface up eth2 --node node003
```

Чтобы выключить сетевой интерфейс

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по имени узла, перейдите на вкладку **Сетевые интерфейсы** и выберите сетевой интерфейс в состоянии **Подключен**.
2. На правой панели интерфейса нажмите **Выключить**.
3. Нажмите **Выключить** в окне подтверждения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node iface down [--node <node>] <iface>
```

--node <node>

Идентификатор или имя хоста сервера

<iface>

Имя сетевого интерфейса

Например, чтобы выключить сетевой интерфейс eth2 сервера node003, выполните:

```
# vinfra node iface down eth2 --node node003
```

Чтобы удалить сетевой интерфейс

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по имени узла, перейдите на вкладку **Сетевые интерфейсы** и выберите логический сетевой интерфейс, который вы хотите удалить.
2. На правой панели интерфейса нажмите **Удалить**.
3. Нажмите **Удалить** в окне подтверждения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node iface delete [--node <node>] <iface>
```

--node <node>

Идентификатор или имя хоста сервера

<iface>

Имя сетевого интерфейса

Например, чтобы удалить сетевой интерфейс eth2.100 сервера node003, выполните:

```
# vinfra node iface delete eth2.100 --node node003
```

7.1.1.4 Подключение удаленных устройств iSCSI к серверам кластера

Кибер Инфраструктура позволяет подключать удаленные устройства iSCSI к серверам и воспринимает их LUN как диски хранилища. Устройства iSCSI можно подключать к серверам в любой момент.

После подключения устройства iSCSI назначьте роль дисков **Хранилище** всем его LUN. Несмотря на то, что можно назначать устройствам iSCSI роли **Метаданные** или **Кэш**, это рекомендуется делать только для установок, состоящих из одного узла, предназначенных для шлюза резервного копирования, где избыточность обеспечивается на стороне SAN.

Примечание
Для обеспечения отказоустойчивости при подключении внешней СХД по iSCSI необходимо разделить ее дисковое пространство на минимум три LUN и подключить их к разным узлам продукта Кибер Инфраструктура. Также необходимо иметь диск с метаданными на каждом узле. Минимально возможные режимы избыточности данных – избыточное кодирование 1+2 или две реплики. Не рекомендуется назначать роль **Метаданные** или **Кэш** подключенным по iSCSI дискам.

Примечание
Конфигурация из одного узла продукта Кибер Инфраструктура не является надежной для подключения внешней СХД по iSCSI, так как при потере этого узла хранимые данные на СХД будут безвозвратно утрачены.

Ограничения

- Целевые устройства iSCSI могут использоваться для хранилища, только если на них включена синхронная запись.
- Удаленные устройства iSCSI нельзя присоединить к хостам, которые входят в группы целевых устройств iSCSI.

- Можно использовать только одно имя IQN для каждого сервера. Вы можете подключить несколько целевых устройств iSCSI с помощью других серверов кластера.
- Имя IQN устройства iSCSI может содержать буквы нижнего регистра, цифры, точки, двоеточия и тире. См. список разрешенных символов для имен iSCSI в разделе Профиль строки для имен iSCSI.

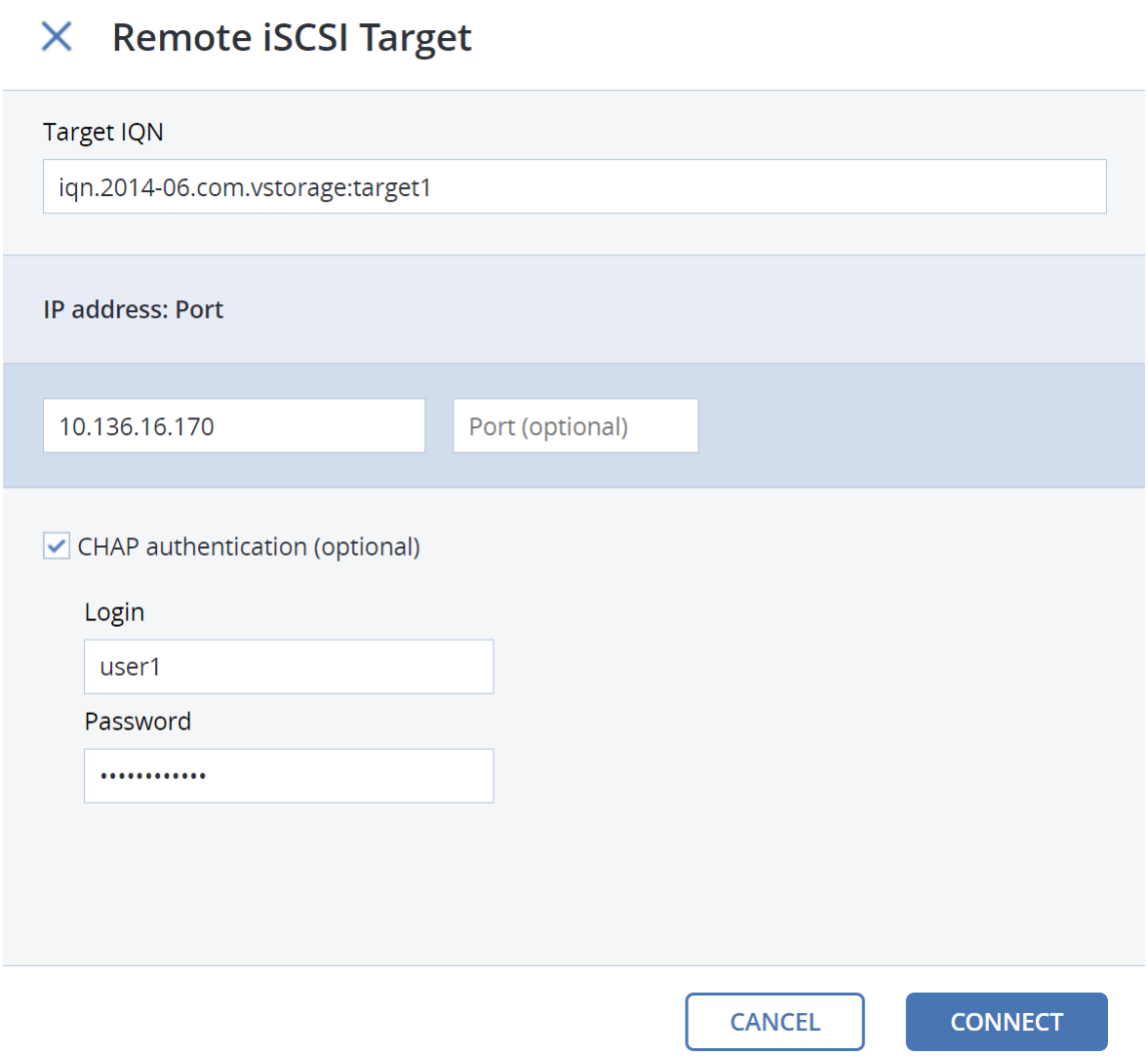
Предварительные требования

- Если для исходящего трафика в кластере настроены ограничения, следует вручную добавить правило, чтобы разрешить исходящий трафик через определенный порт, как описано в разделе "Настройка правил брандмауэра для исходящих подключений" на странице 263.

Чтобы подключить удаленное устройство iSCSI к серверу

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по имени нужного сервера. На вкладке **Диски** нажмите **Добавить цель iSCSI**.
2. В окне **Добавить удаленную цель iSCSI** выполните следующие действия:
   a. Укажите IQN целевого устройства.
   b. Укажите IP-адрес и номер порта (необязательно) целевого устройства.
   c. [Необязательно] Чтобы включить для целевого устройства проверку подлинности CHAP, установите флажок **Авторизация CHAP** и укажите учетные данные.
   d. Нажмите **Подключить**.



Целевое устройство будет подключено, а все его LUN будут инициированы. Устройства типа **iSCSI** появятся в списке **Диски** сервера.

Примечание

Если вы добавляете LUN к подключенному целевому устройству, выполните повторное сканирование с помощью команды iscsiadm -m node -R в консоли хоста.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node iscsi target add [--auth-username <auth-username>] [--auth-password <auth-password>]
                             --portal <portal> --node <node> <target-name>
```

--auth-username <auth-username>

Имя пользователя

--auth-password <auth-password>

Пароль пользователя

--portal <portal>

IP-адрес портала в формате IP-адрес:порт (этот параметр можно указывать несколько раз)

--node <node>

Идентификатор сервера или имя хоста

<target-name>

Имя целевого устройства

Например, чтобы подключить целевое устройство iqn.2014-06.com.vstorage:target1 с IP-адресом 172.16.24.244 и портом 3260 к серверу node003, выполните:

```
# vinfra node iscsi target add iqn.2014-06.com.vstorage:target1 --portal 172.16.24.244:3260 --node node003
```

Чтобы назначить роли дисков удаленным устройствам iSCSI LUN

Панель администратора

1. Выберите диск с типом **iSCSI** и нажмите **Назначить**.
2. В окне **Выбрать роль** выберите **Хранилище** и нажмите кнопку **Готово**.
3. Повторите указанные выше шаги для каждого диска с типом **iSCSI**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node disk assign --disk <disk>:<role>[:<key=value,...>] [--node <node>]
```

--disk <disk>:<role>[:<key=value,...>]

Конфигурация диска в формате:

- <disk>: идентификатор или имя дискового устройства
- <role>: роль диска (cs, mds, journal, mds-journal, mds-system, cs-system, system)
- разделенные запятыми пары key=value с ключами (необязательно):
  - tier: уровень диска (0, 1, 2 или 3)
  - journal-tier: уровень диска журнала (кэша) (0, 1, 2 или 3)
  - journal-type: тип диска журнала (кэша) (no_cache – без кэша, inner_cache – внутренний кэш или external_cache – внешний кэш)
  - journal-disk: идентификатор или имя устройства диска журнала (кэша)
  - bind-address: IP-адрес привязки для сервиса метаданных

Например: sda:cs:tier=0,journal-type=inner_cache.
Этот параметр можно указывать несколько раз.

--node <node>

Идентификатор или имя хоста сервера (по умолчанию node001.vstoragedomain)

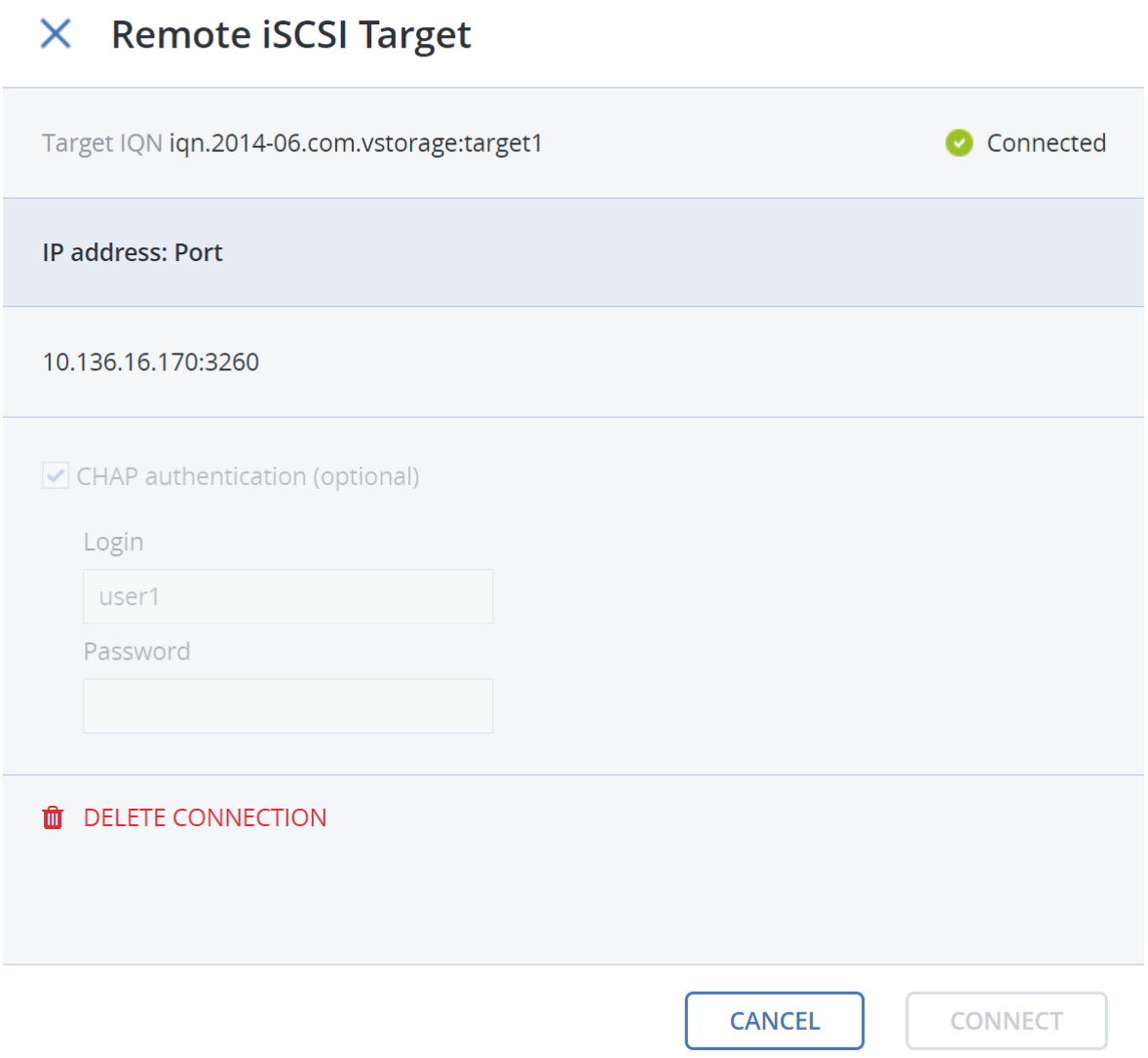
Например, чтобы назначить iSCSI-диску sde роль **Хранилище**, выполните:

```
# vinfra node disk assign --disk sde:cs:tier=0 --node node003
```

Чтобы удалить целевое устройство iSCSI

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по имени нужного сервера. На вкладке **Диски** нажмите **Цель iSCSI**.
2. В окне **Удаленная цель iSCSI** нажмите **Удалить соединение**, а затем **Удалить**.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra node iscsi target delete --node <node> <target-name>
```

--node <node>

Идентификатор сервера или имя хоста

<target-name>

Имя целевого устройства

Например, чтобы отсоединить целевое устройство iqn.2014-06.com.vstorage:target1 от сервера node003, выполните:

```
# vinfra node iscsi target delete iqn.2014-06.com.vstorage:target1 --node node003
```

7.1.2 Масштабирование кластера хранилища

После развертывания кластера хранилища можно в любое время расширить его емкость хранения, добавив больше дисков хранилища (вертикальное масштабирование) или увеличив количество узлов хранилища (горизонтальное масштабирование). Также можно заменить диски хранилища на диски большего размера, следуя инструкциям в "Замена дисков серверов" на странице 817.

Чтобы понять разницу между вертикальным и горизонтальным масштабированием, рассмотрим следующие сценарии:

- Вертикальное масштабирование. Кластер состоит из пяти узлов с 12 слотами для жестких дисков в каждом. Один диск используется для системы и метаданных, а 9 дисков используются для хранения на уровне 0. Хранилище резервных копий развертывается поверх кластера хранилища с режимом кодирования 3+2. Емкость хранилища резервных копий можно расширить, добавив еще два диска на каждый узел. В результате емкость хранилища увеличится на 2/9.
- Горизонтальное масштабирование. Кластер состоит из пяти узлов с 12 слотами для жестких дисков в каждом. Один диск используется для системы и метаданных, а 11 дисков используются для хранения на уровне 0. Хранилище резервных копий развертывается поверх кластера хранилища с режимом кодирования 3+2. Емкость и пропускную способность хранилища резервных копий можно расширить, добавив еще два узла того же размера (то есть с 12 дисками). В результате емкость хранилища увеличится на 2/5. Кроме того, чтобы максимизировать эффективность хранения, можно обновить режим кодирования до 5+2, как описано в "Изменение схемы избыточности для хранилища резервных копий" на странице 354.

Перед добавлением новых дисков и узлов обратите внимание на следующие рекомендации по выбору их размера:

- Для уровня хранения рекомендуется иметь одинаковое количество дисков на узел. Тогда данные будут распределяться между узлами более равномерно.
- Наличие дисков одинакового размера помогает более равномерно распределить нагрузку. Внутри кластера использование диска пропорционально размеру диска. Например, если у вас

есть диск на 10 ТБ и диск на 2 ТБ, при 50% загрузке кластера будет использоваться 5 ТБ и 1 ТБ соответственно.

Ограничения

- Диску можно назначить роль, только если его размер превышает 1 ГиБ.
- Системному диску можно назначить дополнительную роль, только если его размер не меньше 100 ГиБ.
- Жесткие диски с черепичной магнитной записью (SMR) можно использовать только с ролью **Хранилище** и только в случае, если на сервере есть твердотельный диск с ролью **Кэш**.
- Нельзя использовать на одном уровне хранилища стандартные и SMR-диски.
- Нельзя одновременно назначить роли системным и несистемным дискам.

Предварительные требования

- Кластер хранилища создается согласно описанию в разделе "Развертывание кластера хранилища данных" на странице 141.

Для добавления дисков в кластер хранилища

Панель администратора

1. На экране **Инфраструктура** > **Узлы** выберите имя узла.
2. На вкладке **Диски** выберите новый диск без роли.
3. На правой панели диска щелкните **Назначить роль**.
4. В окне **Назначить роль** выберите роль диска, в соответствии с которой вы хотите использовать диск:
   - [Только для твердотельных накопителей] Как хранить кэш записи
     a. Выберите роль **Кэш**.
     b. Выберите уровень хранилища, который следует кэшировать.

     Примечание
     Для того чтобы диски использовали кэш, роль **Кэш** необходимо назначить до назначения роли **Хранилище**.

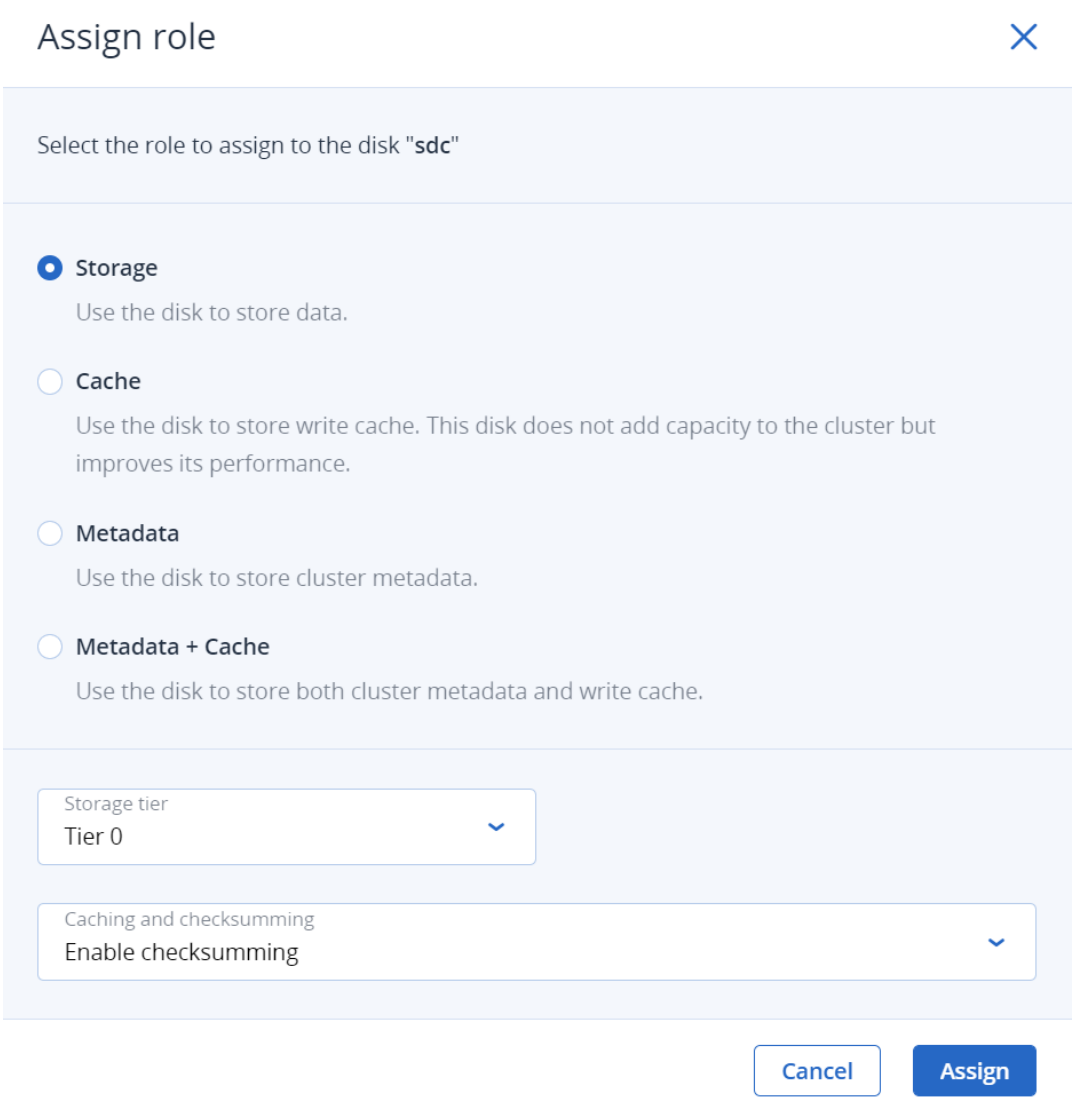
   - Как организовать хранение данных
     a. Выберите роль **Хранилище**.
     b. Выберите уровень хранилища для размещения данных. Чтобы повысить эффективность избыточности данных, не назначайте все диски сервера на один и тот же уровень. Вместо этого убедитесь, что каждый из уровней равномерно распределен по кластеру и на каждом сервере ему назначено по одному диску.
     c. Включите кэширование данных и проверку контрольных сумм:
        - **Использовать диск SSD для кэширования и проверки контрольных сумм**. Доступно и рекомендуется только для серверов с твердотельными накопителями.

- **Включить проверку контрольных сумм** (по умолчанию). Рекомендуется для серверов с жесткими дисками, так как обеспечивает повышенную надежность.
- **Отключить проверку контрольных сумм**. Не рекомендуется для производственной среды. В среде оценки или тестирования можно отключить проверку контрольных сумм для серверов с жесткими дисками для повышения производительности.

- Как хранить метаданные кластера
  Выберите роль **Метаданные**.

  Примечание
  Рекомендуется не больше одного сервиса метаданных на сервер и не больше пяти сервисов метаданных для кластера.

- [Только для твердотельных накопителей] Как хранить метаданные и кэш записи
  a. Выберите роль **Метаданные+Кэш**.
  b. Выберите уровень хранилища, который следует кэшировать.



5. Нажмите **Назначить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node disk assign --disk <disk>:<role>[:<key=value,...>]
                        [--node <node>]
```

--disk <disk>:<role>[:<key=value,...>]

Конфигурация диска в формате:

- <disk>: идентификатор или имя дискового устройства
- <role>: роль диска (cs, mds, journal, mds-journal, mds-system, cs-system, system)
- разделенные запятыми пары key=value с ключами (необязательно):
  - tier: уровень диска (0, 1, 2 или 3)
  - journal-tier: уровень диска журнала (кэша) (0, 1, 2 или 3)
  - journal-type: тип диска журнала (кэша) (no_cache – без кэша, inner_cache – внутренний кэш или external_cache – внешний кэш)
  - journal-disk: идентификатор или имя устройства диска журнала (кэша)
  - bind-address: IP-адрес привязки для сервиса метаданных

Например: sda:cs:tier=0,journal-type=inner_cache.

Этот параметр можно указывать несколько раз.

--node <node>

Идентификатор узла или имя хоста (по умолчанию: node001.vstoragedomain)

Например, чтобы назначить роль cs для диска sdc на узле node003, запустите команду:

```
# vinfra node disk assign --disk sdc:cs --node node003
```

Вы можете просмотреть конфигурацию диска узла в выводе vinfra node disk list:

```
# vinfra node disk list --node node003
+--------------------------------------+--------+------+------------+-------------+---------+----------+---------------+-----
-------+---------------+
| id                                   | device | type | role       | disk_status | used    | size     | physical_size | service_id |
service_status |
+--------------------------------------+--------+------+------------+-------------+---------+----------+---------------+-----
-------+---------------+
| 2A006CA5-732F-4E17-8FB0-B82CE0F28DB2 | sdc    | hdd  | cs         | ok          | 11.2GiB | 125.8GiB |
128.0GiB     | 1026       | active         |
| 642A7162-B66C-4550-9FB2-F06866FB7EA1 | sdb    | hdd  | cs         | ok          | 8.7GiB  | 125.8GiB |
128.0GiB     | 1025       | active         |
| 45D38CD2-3B94-4F0F-8864-9D51F716D3B1 | sda    | hdd  | mds-system | ok          | 21.0GiB |
125.9GiB | 128.0GiB     | 1          | avail          |
```

```
+-------------------------------------+--------+------+------------+-------------+---------+----------+---------------+-----
-------+---------------+
```

Для добавления узлов в кластер хранилища

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по неназначенному серверу.
2. На правой панели сервера нажмите **Присоединить к кластеру**.
3. Нажмите **Присоединить**, чтобы автоматически назначить роли дискам и добавить сервер в текущее расположение. Вместо этого можно нажать значок шестерни, чтобы вручную настроить роли дисков или расположение сервера.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node join [--disk <disk>:<role>[:<key=value,...>]] <node>
```

--disk <disk>:<role>[:<key=value,...>]

Конфигурация диска в формате:

- <disk>: идентификатор или имя дискового устройства
- <role>: роль диска (cs, mds, journal, mds-journal, mds-system, cs-system, system)
- разделенные запятыми пары key=value с ключами (необязательно):
  - tier: уровень диска (0, 1, 2 или 3)
  - journal-tier: уровень диска журнала (кэша) (0, 1, 2 или 3)
  - journal-type: тип диска журнала (кэша) (no_cache – без кэша, inner_cache – внутренний кэш или external_cache – внешний кэш)
  - journal-disk: идентификатор или имя устройства диска журнала (кэша)
  - bind-address: IP-адрес привязки для сервиса метаданных

Например: sda:cs:tier=0,journal-type=inner_cache.
Этот параметр можно указывать несколько раз.

<node>

Идентификатор узла или имя хоста

Например, чтобы добавить узел node002 в кластер хранилища и назначить роли дискам: mds-system на sda, cs на sdb и sdc, запустите команду:

```
# vinfra node join f59dabdb-bd1c-4944-8af2-26b8fe9ff8d4 --disk sda:mds-system \
--disk sdb:cs --disk sdc:cs
```

Добавленный узел появится в выводе vinfra node list:

```
# vinfra node list
+--------------+--------------+------------+-----------+-------------+----------+
| id           | host         | is_primary | is_online | is_assigned | is_in_ha |
+--------------+--------------+------------+-----------+-------------+----------+
| 09bb6b8<...> | node001<...> | True       | True      | True        | False    |
| 187edb1<...> | node002<...> | False      | True      | True        | False    |
+--------------+--------------+------------+-----------+-------------+----------+
```

7.1.3 Управление сетями инфраструктуры

В Кибер Инфраструктура можно управлять сетями инфраструктуры и назначать отдельным сетям разные типы трафика. Кроме того, можно менять IP-адреса и настройки сети, если нужно перенести кластер в другое расположение или изменить топологию сети.

Предварительные требования

- Сети инфраструктуры должны быть настроены, как описано в разделе "Настройка сетей" на странице 110.

7.1.3.1 Управление типами трафика

Можно управлять тремя группами типов трафика: двумя группами по умолчанию (эксклюзивные и обычные типы трафика, созданные в инфраструктуре) и группой пользовательских трафиков.

Предварительные требования

- Четкое понимание концепции "Типы трафика" на странице 42.

Управление эксклюзивными типами трафика

Эксклюзивные типы трафика можно только переназначать из одной сети в другую и только по одному за раз. Переназначение можно выполнять, даже если связанные сервисы уже развернуты. Это может пригодиться, например, в том случае, если изначальная сетевая конфигурация неправильная, но кластер хранилища уже заполнен данными и в нем работают критически важные сервисы, либо после добавления сетевой карты, для чего требуется изменить сетевые параметры, добавить новую сеть и назначить ей типы трафика.

Ограничения

- Эксклюзивные типы трафика нельзя изменить или удалить.
- Нельзя управлять правилами доступа для эксклюзивных типов трафика.

Предварительные требования

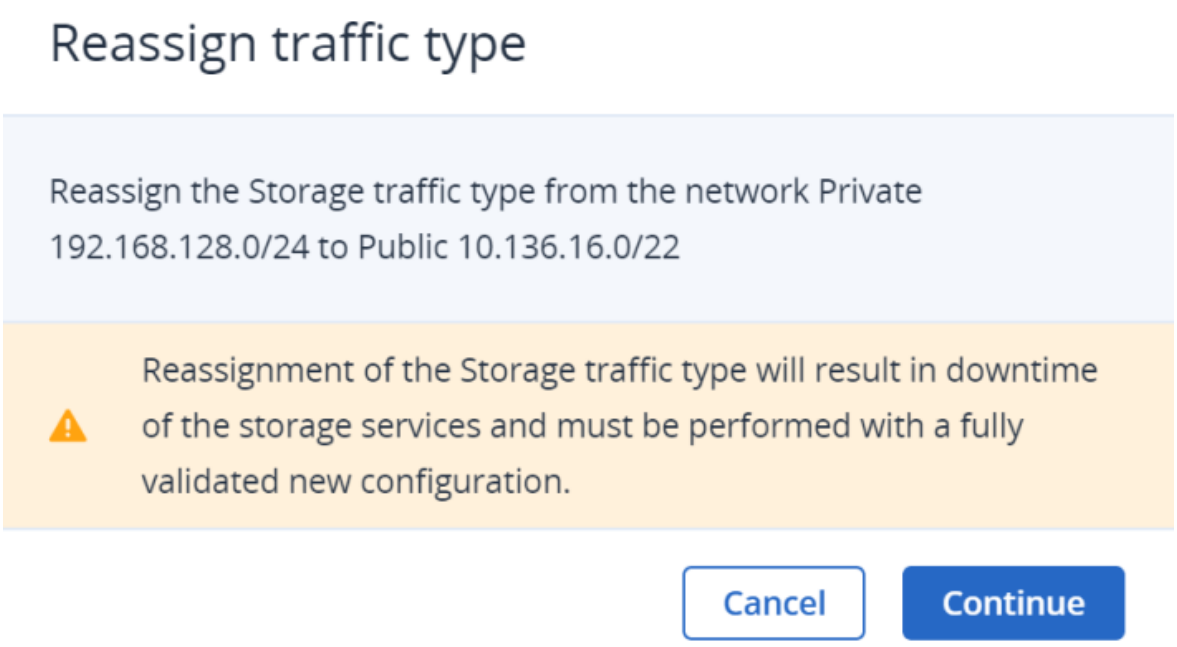
- Все подключенные интерфейсы серверов имеют статус «в сети».
- У каждого сетевого интерфейса только один IP-адрес.

- На серверах, подключенных к исходной и целевой сетям, имеется одинаковое количество интерфейсов. Серверы без назначения также учитываются.
- Развернутые связанные сервисы находятся в рабочем состоянии.
- Если для исходящего трафика в кластере настроены ограничения, следует вручную добавить правило, чтобы разрешить исходящий трафик через порты TCP и UDP 60000-60100, как описано в разделе "Настройка правил брандмауэра для исходящих подключений" на странице 263.

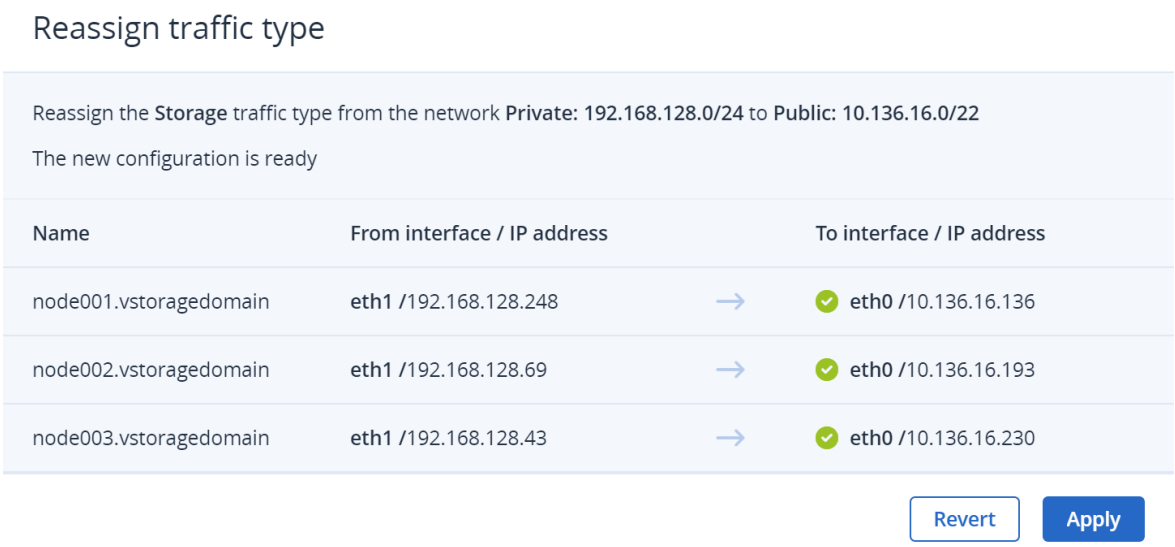
Чтобы переназначить эксклюзивный тип трафика

Панель администратора

1. На экране **Инфраструктура** > **Сети** щелкните **Назначить сети** рядом с разделом **Эксклюзивные типы трафика** и выберите тип трафика, который нужно переназначить.
2. Переназначьте тип трафика другой сети, выбрав соответствующий переключатель, а затем нажмите **Сохранить**.
3. В окне **Переназначить тип трафика** просмотрите сведения об исходной и целевой сетях, ознакомьтесь с информацией о потенциальных рисках и нажмите **Продолжить**, чтобы начать переназначение типа трафика.



4. Если связанные сервисы уже развернуты, дождитесь завершения проверки подключенных интерфейсов и создания новой конфигурации. Затем нажмите **Применить**.



Примечание

Пока идет переназначение типа трафика, пользователи не могут выполнять другие задачи на панели администрирования. Кроме того, у пользователей панели самообслуживания может не быть доступа к порталу, и им необходимо будет дождаться завершения переназначения.

5. Если проверка подключения выдает ошибку, можно вернуться к старой сетевой конфигурации, нажав **Вернуть**. После этого необходимо исправить обнаруженные проблемы и повторить попытку.
6. Дождитесь завершения переназначения на всех подключенных интерфейсах и нажмите кнопку **Готово**.
7. После переназначения типа трафика **Управление системными сервисами** или **ВМ внутр.** перезапустите вручную все работающие виртуальные машины, чтобы иметь доступ к ним через консоль VNC.

Интерфейс командной строки

1. Начните переназначение типа трафика с помощью следующей команды:

```
vinfra cluster traffic-type assignment start --traffic-type <traffic-type>
                                             --target-network <target-network>
```

--traffic-type <traffic-type>

Имя типа трафика

--target-network <target-network>

Идентификатор или имя целевой сети

Например:

```
# vinfra cluster traffic-type assignment start --traffic-type Storage --target-network Public
+--------------+-----------------------------------------------------------+
| Field        | Value                                                     |
+--------------+-----------------------------------------------------------+
| configuration | target_network: 69ad1db5-512f-4994-ab08-7d643fdb7b39        |
|              | traffic_type: Storage                                      |
| link         | href: /api/v2/network/traffic-type-assignment/285be91b-<...>/ |
|              | method: GET                                                |
|              | rel: traffic-type-assignment-details                       |
| operation    | traffic-type-assignment                                    |
| progress     | 0.0                                                        |
| state        | preparing                                                  |
| task_id      | 285be91b-77ee-4f8f-a118-8410ab792148                       |
| transitions  | 0                                                          |
+--------------+-----------------------------------------------------------+
```

2. Просмотрите сведения о переназначении типа трафика:

```
# vinfra cluster traffic-type assignment show
+-------------+-----------------------------------------------------------+
| Field       | Value                                                     |
+-------------+-----------------------------------------------------------+
| link        | href: /api/v2/network/traffic-type-assignment/285be91b-<...>/ |
|             | method: GET                                                |
|             | rel: traffic-type-assignment-details                       |
| operation   | traffic-type-assignment                                    |
| progress    | 1.0                                                        |
| state       | test-passed                                                |
| task_id     | 285be91b-77ee-4f8f-a118-8410ab792148                       |
| transitions | 3                                                          |
+-------------+-----------------------------------------------------------+
```

Вывод команды показывает, что новая конфигурация сети проверена и может быть применена.

3. Продолжите переназначение типа трафика и примените новую конфигурацию сети. Например:

```
# vinfra cluster traffic-type assignment apply
```

4. После переназначения типа трафика **Управление системными сервисами** или **ВМ внутр.** перезапустите вручную все работающие виртуальные машины, чтобы иметь доступ к ним через консоль VNC.

Если проверки подключения выдают ошибку, необходимо найти и исправить проблему, а затем повторить переназначение:

```
# vinfra cluster traffic-type assignment apply
```

Как вариант, можно вернуться к старой конфигурации сети с помощью команды vinfra cluster traffic-type assignment revert, исправить обнаруженную проблему и повторить переназначение.

В случае возникновения ошибки переназначения

Панель администратора

1. Подключитесь к кластеру через SSH.
2. Просмотрите файл /var/log/vstorage-ui-backend/celery.log для выяснения причины.
3. Исправьте проблему.
4. Вернитесь на экран мастера и нажмите **Повторить**.

Интерфейс командной строки

1. Подключитесь к кластеру через SSH.
2. Просмотрите файл /var/log/vstorage-ui-backend/celery.log для выяснения причины.
3. Исправьте проблему.
4. Выполните команду vinfra cluster traffic-type assignment retry, например:

```
# vinfra cluster traffic-type assignment retry
+-------------+-----------------------------------------------------------+
| Field       | Value                                                     |
+-------------+-----------------------------------------------------------+
| link        | href: /api/v2/network/traffic-type-assignment/f633af90-<...>/ |
|             | method: GET                                               |
|             | rel: traffic-type-assignment-details                      |
| operation   | traffic-type-assignment                                   |
| progress    | 0.444444444444                                            |
| state       | test-failed                                               |
| task_id     | f633af90-302e-4299-8055-d3e400dc0ea7                      |
| transitions | 3                                                         |
+-------------+-----------------------------------------------------------+
```

Управление обычными типами трафика

Обычные типы трафика можно добавить в несколько сетей или удалить из любой из них.

Ограничения

- Обычные типы трафика нельзя изменить или удалить.
- Назначение типа трафика можно отменить, только если не развернуты связанные сервисы. Например, нельзя отменить назначение типа трафика **ВМ внешн.**, если создан вычислительный кластер.
- Для типа трафика **ВМ внешн.** нельзя управлять правилами доступа.

Чтобы выполнить назначение, переназначение или снятие назначения для обычного типа трафика

Панель администратора

1. На экране **Инфраструктура** > **Сети** щелкните **Назначить сетям** рядом с разделом **Обычные типы трафика**.

2. Добавьте нужный тип трафика или удалите его из сетей, установив соответствующие флажки.
3. Нажмите кнопку **Сохранить**, чтобы применить изменения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster network set [--traffic-types <traffic-types> | --add-traffic-types <traffic-types> |
                            --del-traffic-types <traffic-types>] <network>
```

--traffic-types <traffic-types>

Разделенный запятыми список имен типов трафика (указанные типы трафика заменяют собой текущие типы трафика в сети)

--add-traffic-types <traffic-types>

Разделенный запятыми список имен типов трафика (указанные типы трафика добавляются к сети)

--del-traffic-types <traffic-types>

Разделенный запятыми список имен типов трафика (указанные типы трафика удаляются из сети)

<network>

Идентификатор или имя сети

Например, чтобы добавить тип трафика SNMP к сети Public, выполните:

```
# vinfra cluster network set Public --add-traffic-types "SNMP"
```

Управление пользовательскими типами трафика

Вы можете создавать пользовательские типы трафика, которые можно добавлять в несколько сетей, изменять и удалять.

Ограничения

- Если вы создадите правила разрешения, но оставите список запретов пустым, весь входящий трафик по-прежнему будет разрешен.
- Нельзя изменить имя типа трафика, если он назначен сети.

Чтобы создать пользовательский тип трафика

Панель администратора

1. На экране **Инфраструктура** > **Сети** нажмите **Создать тип трафика**.
2. В окне **Создать тип трафика** укажите имя для типа трафика и порт, который следует открыть. Имена типов трафика должны состоять из 3-32 буквенно-цифровых символов.
3. [Необязательно] В окне **Правила доступа** выполните следующие действия.

- Чтобы блокировать трафик с определенных IP-адресов, диапазонов IP-адресов или подсетей, укажите их в разделе **Запрещенный список**.
- Чтобы разрешить трафик с определенных IP-адресов, диапазонов IP-адресов или подсетей, укажите их в разделе **Разрешенный список**. Дополнительно укажите 0.0.0.0/0 в разделе **Запрещенный список**, чтобы блокировать весь остальной трафик.

4. Нажмите кнопку **Создать**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster traffic-type create --port <port> [--inbound-allow-list <addresses>]
                                   [--inbound-deny-list <addresses>] <traffic-type-name>
```

--port <port>

Порт для типа трафика

--inbound-allow-list <addresses>

Разделенный запятыми список IP-адресов

--inbound-deny-list <addresses>

Разделенный запятыми список IP-адресов

<traffic-type-name>

Имя типа трафика

Например, чтобы создать пользовательский тип трафика MyTrafficType для порта 6900, выполните:

```
# vinfra cluster traffic-type create "MyTrafficType" --port 6900
+--------------------+---------------+
```

```
| Field            | Value        |
+------------------+--------------+
| exclusive        | False        |
| hidden           | False        |
| inbound_allow_list | []         |
| inbound_deny_list  | []         |
| name             | MyTrafficType |
| port             | 6900         |
| type             | custom       |
+------------------+--------------+
```

Созданный тип трафика появится в выводе команды vinfra cluster traffic-type list:

```
# vinfra cluster traffic-type list -c name -c type -c exclusive -c port
+----------------------+------------+-----------+------+
| name                 | type       | exclusive | port |
+----------------------+------------+-----------+------+
| Storage              | predefined | True      |      |
| Internal management  | predefined | True      |      |
| OSTOR private        | predefined | True      |      |
| S3 public            | predefined | False     |      |
| iSCSI                | predefined | False     |      |
| NFS                  | predefined | False     |      |
| Backup (ABGW) private | predefined | True     |      |
| Backup (ABGW) public | predefined | False     |      |
| Admin panel          | predefined | False     |      |
| SSH                  | predefined | False     |      |
| VM public            | predefined | False     |      |
| VM private           | predefined | True      |      |
| Compute API          | predefined | True      |      |
| MyTrafficType        | custom     | False     | 6900 |
+----------------------+------------+-----------+------+
```

Чтобы выполнить назначение, переназначение или снятие назначения для пользовательского типа трафика

Панель администратора

1. На экране **Инфраструктура** > **Сети** щелкните **Назначить сетям** рядом с разделом **Пользовательские типы трафика**.
2. Добавьте нужный тип трафика или удалите его из сетей, установив соответствующие флажки.
3. Нажмите кнопку **Сохранить**, чтобы применить изменения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster network set [--traffic-types <traffic-types> | --add-traffic-types <traffic-types> |
                    --del-traffic-types <traffic-types>] <network>
```

--traffic-types <traffic-types>

Разделенный запятыми список имен типов трафика (указанные типы трафика заменяют собой текущие типы трафика в сети)

--add-traffic-types <traffic-types>

Разделенный запятыми список имен типов трафика (указанные типы трафика добавляются к сети)

--del-traffic-types <traffic-types>

Разделенный запятыми список имен типов трафика (указанные типы трафика удаляются из сети)

<network>

Идентификатор или имя сети

Например, чтобы добавить тип трафика MyTrafficType к сети MyNet, выполните:

```
# vinfra cluster network set MyNet --add-traffic-types "MyTrafficType"
```

Чтобы изменить пользовательский тип трафика

Панель администратора

1. На экране **Инфраструктура** > **Сети** щелкните по значку с многоточием рядом с нужным типом трафика и выберите **Изменить**.
2. В окне **Изменить тип трафика** измените имя, порт или правила для типа трафика и нажмите **Сохранить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster traffic-type set [--name <name>] [--port <port>] <traffic-type>
```

--name <name>

Новое имя для типа трафика

--port <port>

Новый порт для типа трафика

<traffic-type>

Имя типа трафика

Например, чтобы переименовать тип трафика MyTrafficType в MyOtherTrafficType и изменить его порт на 6901, выполните:

```
# vinfra cluster traffic-type set "MyTrafficType" --name "MyOtherTrafficType" --port 6901
```

Чтобы удалить пользовательский тип трафика

Панель администратора

1. Убедитесь, что он исключен из всех сетей.
2. На экране **Инфраструктура** > **Сети** щелкните по значку с многоточием рядом с нужным типом трафика и выберите **Удалить**.
3. В окне **Удалить тип трафика** подтвердите действие, нажав кнопку **Удалить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster traffic-type delete <traffic-type>
```

<traffic-type>
    Имя типа трафика

Например, чтобы удалить пользовательский тип трафика MyOtherTrafficType, выполните:

```
# vinfra cluster traffic-type delete "MyOtherTrafficType"
```

7.1.3.2 Управление сетями

Вы можете создавать, изменять и удалять сети, а также просматривать сведения о них.

Ограничения

- Если вы создадите правила разрешения, но оставите список запретов пустым, весь входящий трафик по-прежнему будет разрешен.
- Сеть инфраструктуры нельзя изменить, если она используется виртуальной вычислительной сетью.
- Удалять можно только сети, не назначенные сетевым адаптерам.

Чтобы создать сеть

Панель администратора

1. На экране **Инфраструктура** > **Сети** нажмите **Создать сеть**.
2. В окне **Новая сеть** укажите имя сети. Имена сетей должны быть длиной от 3 до 32 символов и содержать только буквы латинского алфавита, цифры и символы подчеркивания.
3. В окне **Правила доступа** выполните следующие действия.
    - Чтобы блокировать трафик с определенных IP-адресов, диапазонов IP-адресов или подсетей, укажите их в разделе **Запрещенный список**.
    - Чтобы разрешить трафик с определенных IP-адресов, диапазонов IP-адресов или подсетей, укажите их в разделе **Разрешенный список**. Дополнительно укажите 0.0.0.0/0 в разделе **Запрещенный список**, чтобы блокировать весь остальной трафик.

4. Нажмите кнопку **Создать**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster network create [--traffic-types <traffic-types>] [--inbound-allow-list <addresses>]
                              [--inbound-deny-list <addresses>] [--outbound-allow-list <rules>]
                              <network-name>
```

--traffic-types <traffic-types>

Разделенный запятыми список идентификаторов или имен типов трафика

--inbound-allow-list <addresses>

Разделенный запятыми список IP-адресов

--inbound-deny-list <addresses>

Разделенный запятыми список IP-адресов

--outbound-allow-list <rules>

Разделенный запятыми список правил разрешенного списка в формате <address>:<protocol>:<port>:<description>

<network-name>

Имя сети

Например, чтобы создать сеть MyNet и назначить ей тип трафика SSH, выполните:

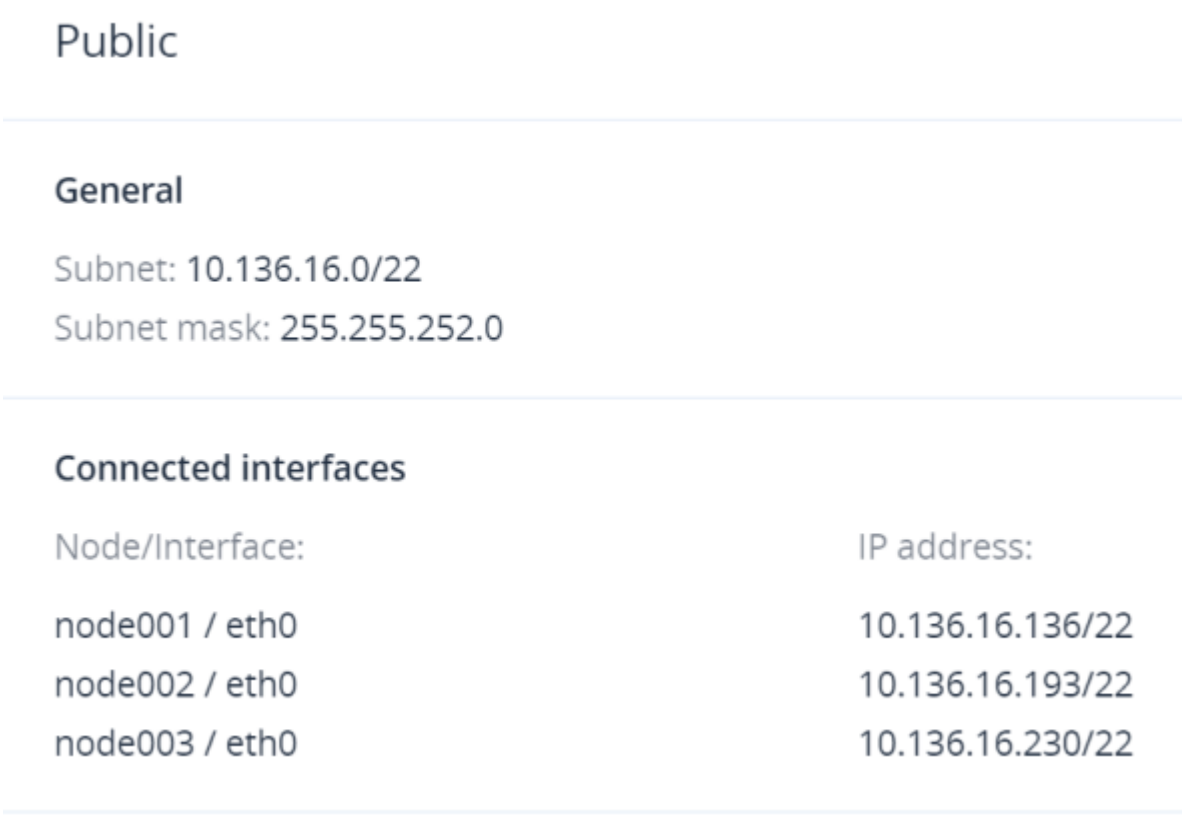
```
# vinfra cluster network create MyNet --traffic-types ssh
+--------------------+------------------------------------------+
| Field              | Value                                    |
```

```
+--------------------+----------------------------------------+
| id                 | b451c5ed-a553-4214-96c4-d926daa6110e   |
| inbound_allow_list | []                                     |
| inbound_deny_list  | []                                     |
| name               | MyNet                                  |
| outbound_allow_list | - 0.0.0.0:tcp:8888:Internal management |
|                    | - 0.0.0.0:tcp:80:HTTP                  |
|                    | - 0.0.0.0:tcp:443:HTTPS                |
|                    | - 0.0.0.0:udp:53:DNS                   |
|                    | - 0.0.0.0:tcp:53:DNS                   |
|                    | - 0.0.0.0:udp:123:NTP                  |
|                    | - 0.0.0.0:tcp:8443:ABGW registration   |
|                    | - 0.0.0.0:tcp:44445:ABGW Geo-replication |
|                    | - 0.0.0.0:tcp:9877:Acronis Cyber Protect |
|                    | - 0.0.0.0:any:0:Allow all              |
| name               | MyNet                                  |
| traffic_types      | SSH                                    |
| vlan               |                                        |
+--------------------+----------------------------------------+
```

Чтобы просмотреть сведения о сети

Щелкните по значку шестерни рядом с именем сети. В окне информации о сети доступны следующие сведения:

- В разделе **Общие сведения** указаны CIDR и маска подсети.
- В разделе **Подключенные интерфейсы** указаны сетевые интерфейсы серверов с IP-адресами.



Чтобы переименовать сеть

Панель администратора

1. На экране **Инфраструктура** > **Сети** щелкните по значку шестерни рядом с именем сети.
2. В окне информации о сети нажмите **Изменить**.
3. В окне **Изменить** введите новое имя и нажмите **Сохранить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster network set [--name <network-name>] <network>
```

--name <network-name>

Новое имя сети

<network>

Идентификатор или имя сети

Например, чтобы переименовать сеть MyNet в MyOtherNet, выполните:

```
# vinfra cluster network set MyNet --name MyOtherNet
```

Чтобы удалить сеть

Панель администратора

1. На экране **Инфраструктура** > **Сети** щелкните по значку шестерни рядом с именем сети.
2. В окне сводки сети нажмите **Удалить**.
3. В окне **Удалить сеть** подтвердите действие, нажав кнопку **Удалить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster network delete <network>
```

<network>

Идентификатор или имя сети

Например, чтобы удалить сеть MyOtherNet, выполните:

```
# vinfra cluster network delete MyOtherNet
```

7.1.3.3 Настройка правил брандмауэра для входящих подключений

Для предотвращения доступа к кластеру из непроверенных источников вы можете настроить на серверах правила брандмауэра для входящих подключений. Чтобы включить фильтрацию трафика, необходимо настроить разрешенный и запрещенный списки для сети или типа трафика. По умолчанию эти списки пусты и разрешен весь входящий трафик. Можно создать в них правила доступа для фильтрации входящего трафика. Правила доступа в разрешенном списке имеют более высокий приоритет, чем правила в запрещенном списке. Если у вас также имеются правила доступа для сетей, то списки доступа, настроенные для типов трафика, будут иметь более высокий приоритет.

Ограничения

- Если вы создадите правила разрешения, но оставите список запретов пустым, весь входящий трафик по-прежнему будет разрешен.

Чтобы включить фильтрацию сетевого трафика для сети

Панель администратора

1. На экране **Инфраструктура** > **Сети** щелкните по значку шестерни рядом с именем сети.
2. В окне информации о сети нажмите **Изменить**.
3. В окне **Изменить сеть** выполните следующие действия:
   - Чтобы блокировать трафик с определенных IP-адресов, диапазонов IP-адресов или подсетей, укажите их в разделе **Запрещенный список**.
   - Чтобы разрешить трафик с определенных IP-адресов, диапазонов IP-адресов или подсетей, укажите их в разделе **Разрешенный список**. Дополнительно укажите 0.0.0.0/0 в разделе **Запрещенный список**, чтобы блокировать весь остальной трафик.

4. Нажмите кнопку **Сохранить**, чтобы применить изменения.

Измененные правила доступа будут применены ко всем серверам, подключенным к этой сети.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster network set [--inbound-allow-list <addresses> | --add-inbound-allow-list <addresses> |
                            --del-inbound-allow-list <addresses> | --clear-inbound-allow-list]
                            [--inbound-deny-list <addresses> | --add-inbound-deny-list <addresses> |
                            --del-inbound-deny-list <addresses> | --clear-inbound-deny-list] <network>
```

--inbound-allow-list <addresses>

Разделенный запятыми список IP-адресов (перезаписывает текущие правила в списке разрешенных входящих подключений)

--add-inbound-allow-list <addresses>

Разделенный запятыми список IP-адресов (добавляет указанные правила в список разрешенных входящих подключений)

--del-inbound-allow-list <addresses>

Разделенный запятыми список IP-адресов (удаляет указанные правила из списка разрешенных входящих подключений)

--clear-inbound-allow-list

Удаляет все правила из списка разрешенных входящих подключений

--inbound-deny-list <addresses>

Разделенный запятыми список IP-адресов (перезаписывает текущие правила в списке запрещенных входящих подключений)

--add-inbound-deny-list <addresses>

Разделенный запятыми список IP-адресов (добавляет указанные правила в список запрещенных входящих подключений)

--del-inbound-deny-list <addresses>

Разделенный запятыми список IP-адресов (удаляет указанные правила из списка запрещенных входящих подключений)

--clear-inbound-deny-list <addresses>

Удаляет все правила из списка запрещенных входящих подключений

<network>

Имя или идентификатор сети

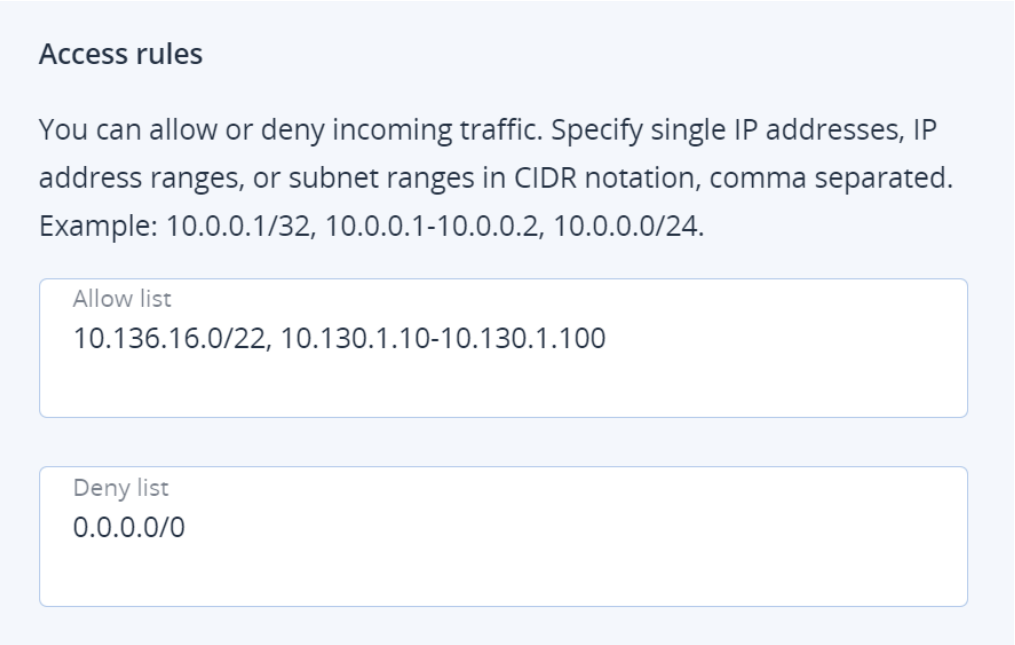
Например, чтобы разрешить входящие подключения из подсети 10.136.100.0/24 к сети MyNet, выполните:

```
# vinfra cluster network set MyNet --add-inbound-allow-list 10.136.100.0/24 --add-inbound-deny-list 0.0.0.0/0
```

Чтобы включить фильтрацию сетевого трафика для обычного или пользовательского типа трафика

Панель администратора

1. На экране **Инфраструктура** > **Сети** щелкните по значку карандаша рядом с именем типа трафика.
2. В появившемся окне выполните следующие действия:
   - Чтобы блокировать трафик с определенных IP-адресов, диапазонов IP-адресов или подсетей, укажите их в разделе **Запрещенный список**.
   - Чтобы разрешить трафик с определенных IP-адресов, диапазонов IP-адресов или подсетей, укажите их в разделе **Разрешенный список**. Дополнительно укажите 0.0.0.0/0 в разделе **Запрещенный список**, чтобы блокировать весь остальной трафик.



3. Нажмите кнопку **Сохранить**, чтобы применить изменения.

После изменения разрешенного и запрещенного списков обновленные правила доступа будут применены ко всем серверам, подключенным к сетям с этим типом трафика.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster traffic-type set [--inbound-allow-list <addresses> | --add-inbound-allow-list
<addresses> |
                    --del-inbound-allow-list <addresses> | --clear-inbound-allow-list]
                    [--inbound-deny-list <addresses> | --add-inbound-deny-list <addresses> |
                    --del-inbound-deny-list <addresses> | --clear-inbound-deny-list] <traffic-type>
```

--inbound-allow-list <addresses>

Разделенный запятыми список IP-адресов (перезаписывает текущие правила в списке разрешенных входящих подключений)

--add-inbound-allow-list <addresses>

Разделенный запятыми список IP-адресов (добавляет указанные правила в список разрешенных входящих подключений)

--del-inbound-allow-list <addresses>

Разделенный запятыми список IP-адресов (удаляет указанные правила из списка разрешенных входящих подключений)

--clear-inbound-allow-list

Удаляет все правила из списка разрешенных входящих подключений

--inbound-deny-list <addresses>

Разделенный запятыми список IP-адресов (перезаписывает текущие правила в списке запрещенных входящих подключений)

--add-inbound-deny-list <addresses>

Разделенный запятыми список IP-адресов (добавляет указанные правила в список запрещенных входящих подключений)

--del-inbound-deny-list <addresses>

Разделенный запятыми список IP-адресов (удаляет указанные правила из списка запрещенных входящих подключений)

--clear-inbound-deny-list <addresses>

Удаляет все правила из списка запрещенных входящих подключений

<traffic-type>

Имя типа трафика

Например, чтобы разрешить входящие подключения из подсети 10.136.100.0/24 для типа трафика MyTrafficType, выполните:

```
# vinfra cluster traffic-type set MyTrafficType --add-inbound-allow-list 10.136.100.0/24 --add-inbound-deny-list 0.0.0.0/0
```

Чтобы просмотреть правила доступа для сети или типа трафика

Панель администратора

1. На экране **Инфраструктура** > **Сети** найдите сеть или тип трафика со значком щита рядом с именем.
2. Для просмотра правил, назначенных этой сети или этому типу трафика, наведите курсор на значок.

Интерфейс командной строки

- Для сети используйте команду vinfra cluster network show. Например:

```
# vinfra cluster network show MyNet
+--------------------+-----------------------------------------+
| Field              | Value                                   |
+--------------------+-----------------------------------------+
| id                 | db43aed5-82ec-4c60-8c5a-d60767203d89    |
| inbound_allow_list | - 10.136.100.0/24                       |
| inbound_deny_list  | - 0.0.0.0/0                             |
| name               | MyNet                                   |
| outbound_allow_list | - 0.0.0.0:tcp:8888:Admin panel         |
|                    | - 0.0.0.0:tcp:80:HTTP                   |
|                    | - 0.0.0.0:tcp:443:HTTPS                 |
|                    | - 0.0.0.0:udp:53:DNS                    |
|                    | - 0.0.0.0:tcp:53:DNS                    |
|                    | - 0.0.0.0:udp:123:NTP                   |
```

```
|                | - 0.0.0.0:tcp:8443:ABGW registration    |
|                | - 0.0.0.0:tcp:44445:ABGW Geo-replication |
|                | - 0.0.0.0:tcp:9877:Acronis Cyber Protect |
|                | - 0.0.0.0:tcp:5900-6079:VM VNC Legacy   |
|                | - 0.0.0.0:udp:4789:VXLAN                |
|                | - 0.0.0.0:tcp:15900-16900:VM VNC        |
|                | - 0.0.0.0:udp:2049:NFS                  |
|                | - 0.0.0.0:tcp:2049:NFS                  |
|                | - 0.0.0.0:tcp:111:NFS Rpcbind           |
|                | - 0.0.0.0:any:0:Allow all               |
| traffic_types  |                                         |
| vlan           |                                         |
+----------------+-----------------------------------------+
```

- Для типа трафика используйте команду vinfra cluster traffic-type show. Например:

```
# vinfra cluster traffic-type show MyTrafficType
+-------------------+-------------------+
| Field             | Value             |
+-------------------+-------------------+
| exclusive         | False             |
| hidden            | False             |
| inbound_allow_list | - 10.136.100.0/24 |
| inbound_deny_list  | - 0.0.0.0/0       |
| name              | MyTrafficType     |
| port              | 6900              |
| type              | custom            |
+-------------------+-------------------+
```

7.1.3.4 Настройка правил брандмауэра для исходящих подключений

Чтобы управлять исходящим трафиком узлов кластера, настройте правила брандмауэра для публичных сетей с помощью инструмента vinfra. По умолчанию порты, которые используют системные службы, открыты, чтобы обеспечить непрерывную работу кластера. Кроме того, исходящий трафик всегда разрешен в выделенной подсети для внутренней связи между узлами кластера. Поскольку частная сеть закрыта для доступа извне и не взаимодействует с внешними конечными точками, для нее не требуется ограничивать исходящий трафик. Сеть считается частной, если ей назначен один из следующих видов трафика:

- OSTOR внутр.
- Резервное копирование (ABGW) внутр.
- Управление системными сервисами
- Хранилище

Частной сети всегда назначено правило <private_subnet_cidr>:any:0, которое разрешает любой исходящий трафик в текущей подсети. Это правило нельзя просмотреть с помощью команд vinfra, оно существует только в iptables.

Чтобы блокировать весь исходящий трафик, за исключением необходимого для работы кластера, выполните следующие действия.

1. Создайте дополнительные правила брандмауэра, чтобы разрешить исходящие подключения для отдельных служб.
2. Удалите правило, которое разрешает любые исходящие подключения.
3. Проверьте сетевые параметры.

Стандартные правила брандмауэра для исходящих подключений

Для всех сетей кластера применяются стандартные правила для исходящих подключений в формате <address>:<protocol>:<port>:<description>. Эти правила перечислены ниже.

0.0.0.0:tcp:8888:Admin panel

Используется в API кластера

0.0.0.0:tcp:80:HTTP

Подключение к репозиторию обновлений и серверу S3, если настроено обслуживание запросов HTTP

0.0.0.0:tcp:443:HTTPS

Связь с Кибер Бэкап Облачный и службами S3

0.0.0.0:udp:53:DNS

Разрешение имен DNS

0.0.0.0:tcp:53:DNS

Разрешение имен DNS

0.0.0.0:udp:123:NTP

Синхронизация времени

0.0.0.0:tcp:8443:ABGW registration

Контроль данных агентов Кибер Бэкап и сервера управления

0.0.0.0:tcp:44445:ABGW Geo-replication

Репликация данных резервного копирования между кластерами

0.0.0.0:tcp:9877:Кибер Бэкап

Регистрация на сервере управления Кибер Бэкап в локальных развертываниях

0.0.0.0:tcp:5900-6079:VM VNC Legacy

Доступ с помощью консоли VNC ко всем виртуальным машинам в вычислительном кластере

0.0.0.0:udp:4789:VXLAN

Сетевой трафик между виртуальными машинами в частных виртуальных сетях

0.0.0.0:tcp:15900-16900:VM VNC

Доступ с помощью консоли VNC ко всем виртуальным машинам в вычислительном кластере

0.0.0.0:any:0:Allow all

Разрешает все исходящие подключения

Создание правил брандмауэра для исходящих подключений

Чтобы создать собственные правила брандмауэра для исходящих соединений

Используйте следующую команду:

```
vinfra cluster network set --add-outbound-allow-list <rules> <network>
```

--add-outbound-allow-list <rules>

Разделенный запятыми список правил разрешения для исходящих соединений в следующем формате: <address>:<protocol>:<port>:<description>, где:

- <address> – это отдельный IP-адрес (10.10.10.10), диапазон адресов (10.10.10.0-10.10.10.10) или CIDR подсети (10.10.10.0/32);
- <protocol> может иметь значение udp, tcp или any (любой);
- <port> – целое значение (22) или диапазон (20-22);
- <description> обычно содержит имя службы, которая использует определенный порт.

<network>

Идентификатор или имя сети

Дополнительные правила требуется создавать в следующих случаях.

- При подключении удаленного устройства iSCSI к узлу кластера необходимо вручную добавить правило, чтобы указать номер порта для подключения такого устройства, например:

  ```
  # vinfra cluster network set Public --add-outbound-allow-list "0.0.0.0:tcp:3260:Remote iSCSI"
  ```

- Если вы хотите изменить конфигурацию сети и IP-адреса, назначенные узлам кластера с помощью миграции сети, необходимо вручную добавить правило, чтобы указать порты для подключений TCP и UDP в диапазоне 60000-60100, например:

  ```
  # vinfra cluster network set Public --add-outbound-allow-list \
  "0.0.0.0:tcp:60000-60100:Network migration","0.0.0.0:udp:60000-60100:Network migration"
  ```

- Если вы хотите переназначить эксклюзивный тип трафика для одной сети другой, необходимо вручную добавить правила, чтобы указать порты для подключений TCP и UDP в диапазоне 60000-60100 для обеих сетей, например:

  ```
  # vinfra cluster network set Public --add-outbound-allow-list \
  "0.0.0.0:tcp:60000-60100:Network migration","0.0.0.0:udp:60000-60100:Network migration"
  # vinfra cluster network set MyNet --add-outbound-allow-list \
  "0.0.0.0:tcp:60000-60100:Network migration","0.0.0.0:udp:60000-60100:Network migration"
  ```

- Если вы использовали Kerberos V5 для аутентификации пользователей при доступе к тому NFS, необходимо вручную добавить правила, чтобы задать TCP-порты 88 и 749, UDP-порт 88 и IP-адрес сервера Kerberos. Например, если IP-адрес сервера Kerberos 10.128.168.20, выполните следующую команду:

```
# vinfra cluster network set Public --add-outbound-allow-list \
"10.128.168.20:tcp:88:Kerberos","10.128.168.20:tcp:749:Kerberos",\
"10.128.168.20:udp:88:Kerberos"
```

- Если вы настраиваете пользовательский порт для какой-либо службы, необходимо вручную добавить правило, чтобы указать номер используемого порта, например:

```
# vinfra cluster network set Public --add-outbound-allow-list "0.0.0.0:udp:161:Zabbix"
```

Удаление правил брандмауэра для исходящих подключений

Примечание
Если исходящий трафик ограничен, рекомендуется изменить стандартные правила для исходящих подключений, чтобы использовались избранные IP-адреса или подсети в соответствии с требованиями сетевой инфраструктуры или политиками безопасности.

Чтобы удалить правила брандмауэра для исходящих подключений

Используйте следующую команду:

```
vinfra cluster network set --del-outbound-allow-list <rules> <network>
```

--del-outbound-allow-list <rules>

Разделенный запятыми список правил разрешения для исходящих соединений в следующем формате: <address>:<protocol>:<port>:<description>, где:

- <address> – это отдельный IP-адрес (10.10.10.10), диапазон адресов (10.10.10.0-10.10.10.10) или CIDR подсети (10.10.10.0/32);
- <protocol> может иметь значение udp, tcp или any (любой);
- <port> – целое значение (22) или диапазон (20-22);
- <description> обычно содержит имя службы, которая использует определенный порт.

<network>

Идентификатор или имя сети

Например, чтобы удалить правило 0.0.0.0:any:0:Allow all, разрешающее любые исходящие подключения, запустите:

```
# vinfra cluster network set Public --del-outbound-allow-list "0.0.0.0:any:0:Allow all"
```

В этом случае все попытки установить подключение из кластера к внешним конечным точкам будут блокироваться.

Составление списка правил брандмауэра для исходящих подключений

Чтобы проверить, что все необходимые правила брандмауэра для исходящих соединений применяются к вашей сети

Используйте следующую команду:

```
vinfra cluster network show <network>
```

<network>

Идентификатор или имя сети

Например, чтобы отобразить список правил брандмауэра для исходящих соединений сети Public, выполните:

```
# vinfra cluster network show Public
+--------------------+--------------------------------------------+
| Field              | Value                                      |
+--------------------+--------------------------------------------+
| id                 | c2e799f5-c41d-4865-bcce-06b471affed6       |
| inbound_allow_list | []                                         |
| inbound_deny_list  | []                                         |
| name               | Public                                     |
| outbound_allow_list | - 0.0.0.0:tcp:8888:Internal management     |
|                    | - 0.0.0.0:tcp:80:HTTP                      |
|                    | - 0.0.0.0:tcp:443:HTTPS                    |
|                    | - 0.0.0.0:udp:53:DNS                       |
|                    | - 0.0.0.0:tcp:53:DNS                       |
|                    | - 0.0.0.0:udp:123:NTP                      |
|                    | - 0.0.0.0:tcp:8443:ABGW registration       |
|                    | - 0.0.0.0:tcp:44445:ABGW Geo-replication   |
|                    | - 0.0.0.0:tcp:9877:Acronis Cyber Protect   |
|                    | - 0.0.0.0:tcp:5900-6079:VM VNC Legacy      |
|                    | - 0.0.0.0:udp:4789:VXLAN                   |
|                    | - 0.0.0.0:tcp:15900-16900:VM VNC           |
| traffic_types      | Backup (ABGW) public,Compute API,iSCSI,NFS, |
|                    | S3 public,Self-service ...<truncated>      |
| vlan               | 0                                          |
+--------------------+--------------------------------------------+
```

Восстановление стандартных правил брандмауэра для исходящих подключений

Ограничения

- При сбросе настроек пользовательские правила брандмауэра для исходящих соединений будут удалены.

Чтобы восстановить стандартные правила брандмауэра для исходящих соединений

Используйте следующую команду:

```
vinfra cluster network set --restore-default-outbound-allow-list <network>
```

<network>

Идентификатор или имя сети

Например, чтобы восстановить стандартные правила брандмауэра для исходящих соединений сети Public, выполните:

```
vinfra cluster network set Public --restore-default-outbound-allow-list
```

7.1.3.5 Изменение конфигурации сети

Сетевую конфигурацию и назначение IP-адресов серверам кластера можно изменить с помощью миграции сетей.

Ограничения

- DHCP можно включить для исходной сети, но следует отключить для целевой сети. После миграции IP-адреса, полученные через DHCP, станут статическими.

Предварительные требования

- Все подключенные интерфейсы серверов имеют статус «в сети».
- У каждого сетевого интерфейса только один IP-адрес.
- Функция высокого уровня доступности отключена в соответствии с инструкциями в разделе "Управление конфигурацией высокой доступности" на странице 815. При необходимости ее можно включить позже.
- Если сеть является сетью шлюза по умолчанию, то все подключенные к ней серверы должны использовать один шлюз по умолчанию.
- Если для исходящего трафика в кластере настроены ограничения, следует вручную добавить правило, чтобы разрешить исходящий трафик через порты TCP и UDP 60000-60100, как описано в разделе "Настройка правил брандмауэра для исходящих подключений" на странице 263.

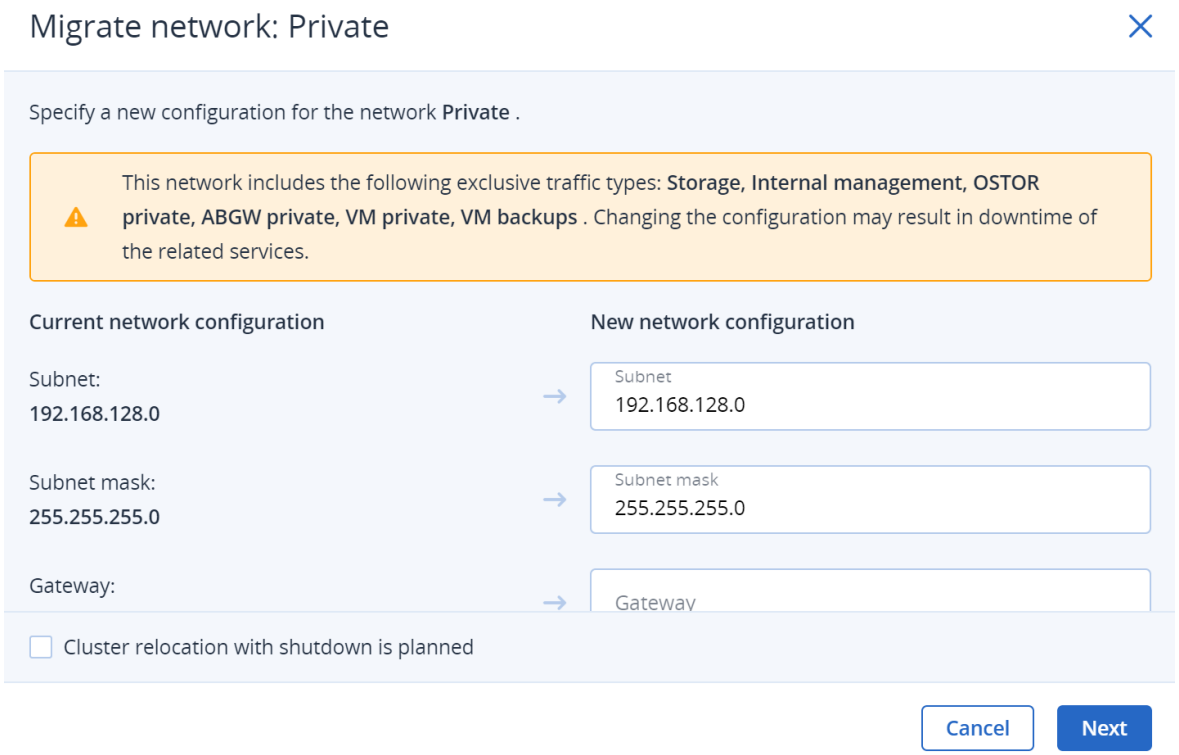
Для миграции сети из исходной конфигурации в целевую

Панель администратора

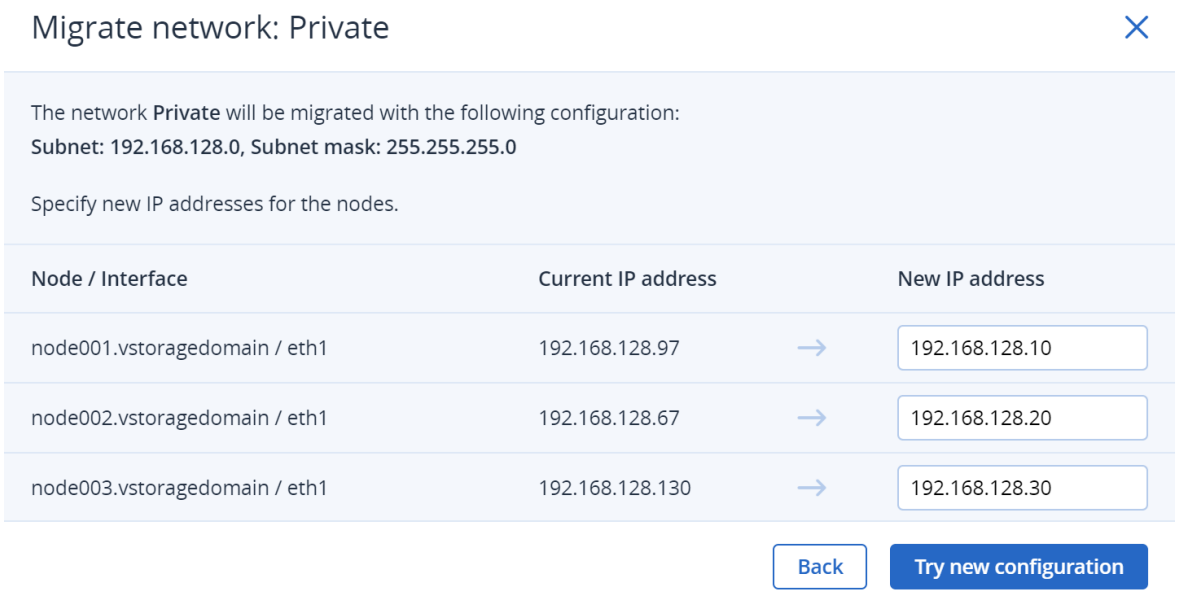
1. На экране **Инфраструктура** > **Сети** щелкните по значку шестерни рядом с именем сети.
2. В окне сводки сети нажмите **Мигрировать**.
3. В окне **Мигрировать сеть: <имя сети>** проверьте текущую сетевую конфигурацию, ознакомьтесь с информацией о потенциальных рисках и при необходимости измените новую сетевую конфигурацию.

   Если вы планируете перенести кластер в другое расположение, что предполагает отключение кластера вручную, выберите **Планируется перемещение кластера с отключением**.

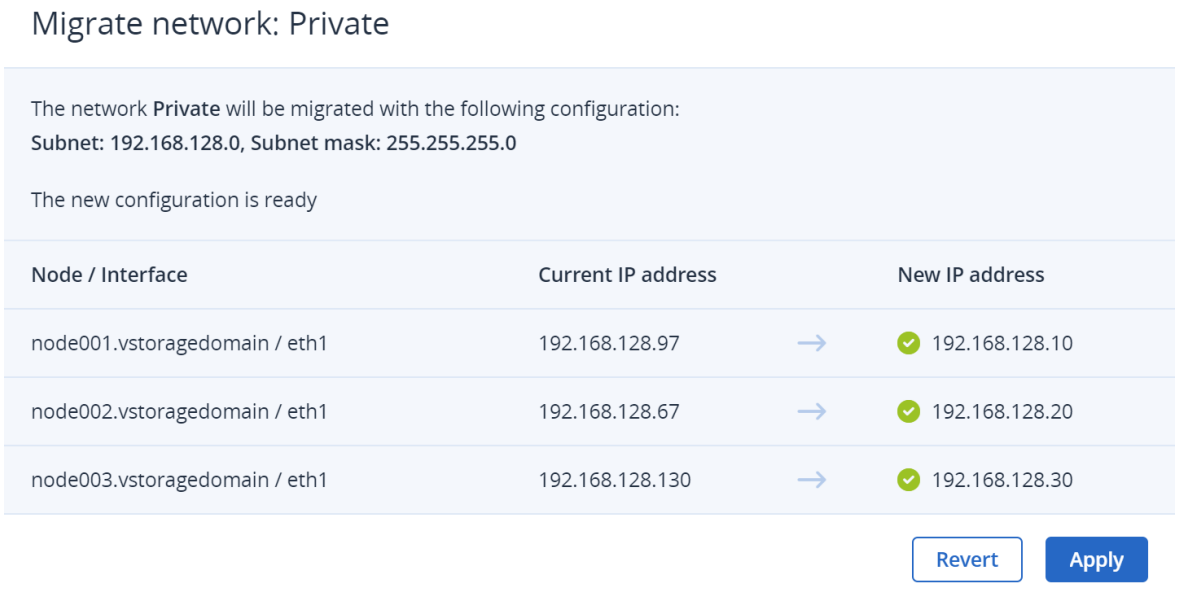
Затем нажмите кнопку **Далее**.



4. На следующем шаге укажите новые IP-адреса для серверов кластера и нажмите **Попробовать новую конфигурацию**. Затем подтвердите действие, нажав **Продолжить** в окне **Попробовать новую конфигурацию**.



5. Если планируется перемещение кластера, можно отключить серверы кластера, а затем включить их в новом ЦОД, как описано в разделе "Выключение и запуск кластера" на странице 823. После перемещения кластера нажмите **Возобновить работу**.
6. Дождитесь создания новой конфигурации и нажмите **Применить**.



Примечание

Пока идет миграция сетей, пользователи не могут выполнять другие задачи на панели администрирования. Кроме того, у пользователей панели самообслуживания может не быть доступа к порталу, и им необходимо будет дождаться завершения миграции.

7. Если проверка подключения выдает ошибку, необходимо исправить обнаруженные проблемы и повторить попытку. Если указанные новые IP-адреса недоступны или недопустимы, можно изменить их в мастере и нажать **Повторить**. В случае других проблем с сетью вернитесь к старой сетевой конфигурации, нажав **Вернуть**, исправьте проблему и повторите попытку.
8. Дождитесь завершения миграции на всех подключенных интерфейсах и нажмите кнопку **Готово**.
9. После миграции сети с типом трафика **Управление системными сервисами** или **ВМ внутр.** перезапустите вручную все работающие виртуальные машины, чтобы иметь доступ к ним через консоль VNC.

Интерфейс командной строки

1. Начните миграцию сети с помощью следующей команды:

```
vinfra cluster network migration start <network> [--subnet <subnet>]
                                    [--netmask <netmask>]
                                    [--gateway <gateway>] [--shutdown]
                                    [--node <node> <address>]
```

--network <network>

Идентификатор или имя сети

--subnet <subnet>

Новая подсеть

--netmask <netmask>

Новая маска сети

--gateway <gateway>

Новый сетевой шлюз

--shutdown

Подготовка кластера к завершению работы вручную для последующего перемещения

--node <node> <address>

Новый адрес сервера в формате:

- <node> – имя хоста или идентификатор сервера
- <address> – адрес IPv4

Этот параметр можно использовать несколько раз.

Например:

```
# vinfra cluster network migration start --network "Private" \
--subnet 192.168.128.0 --netmask 255.255.255.0 --node node001 192.168.128.11 \
--node node002 192.168.128.12 --node node003 192.168.128.13
+---------------------------+-------------------------------------------------+
| Field                     | Value                                           |
+---------------------------+-------------------------------------------------+
| configuration             | network_id: 3e3619b7-2c93-4e90-a187-135c6f8b9060 |
| link                      | href: /api/v2/network/migration/2d4ec3a9-<...>/  |
|                           | method: GET                                      |
|                           | rel: network-migration-details                   |
| operation                 | network-migration                                |
| progress                  | 0.0                                              |
| single_interface_migration | False                                           |
| state                     | preparing                                        |
| task_id                   | 2d4ec3a9-7714-479d-a03c-1efbe6ffecf5             |
| transitions               | 0                                                |
+---------------------------+-------------------------------------------------+
```

2. Просмотрите сведения о текущей операции миграции сети. Например:

```
# vinfra cluster network migration show
+---------------------------+-------------------------------------------------+
| Field                     | Value                                           |
+---------------------------+-------------------------------------------------+
| link                      | href: /api/v2/network/migration/2d4ec3a9-<...>/ |
|                           | method: GET                                      |
|                           | rel: network-migration-details                   |
| operation                 | network-migration                                |
| progress                  | 1.0                                              |
| single_interface_migration | False                                           |
| state                     | test-passed                                      |
| task_id                   | 2d4ec3a9-7714-479d-a03c-1efbe6ffecf5             |
```

```
| transitions              | 5                                                  |
+--------------------------+----------------------------------------------------+
```

В выводе команды отображается, что новая конфигурация сети была проверена и может быть применена.

3. Если планируется перемещение кластера, можно отключить серверы кластера, а затем включить их в новом ЦОД, как описано в разделе "Выключение и запуск кластера" на странице 823. После перемещения кластера выполните:

```
# vinfra cluster network migration resume
```

4. Продолжите миграцию сети и примените новую конфигурацию сети. Например:

```
# vinfra cluster network migration apply
```

5. После миграции сети с типом трафика **Управление системными сервисами** или **ВМ внутр.** перезапустите вручную все работающие виртуальные машины, чтобы иметь доступ к ним через консоль VNC.

Если проверка подключения выдает ошибку, необходимо исправить обнаруженные проблемы и повторить попытку. Если указанные новые IP-адреса недоступны или недопустимы, можно изменить их с помощью следующей команды:

```
vinfra cluster network migration retry [--subnet <subnet>]
                                       [--netmask <netmask>]
                                       [--node <node> <address>]
```

--subnet <subnet>

Новая подсеть

--netmask <netmask>

Новая маска сети

--node <node> <address>

Новый адрес сервера в формате:

- <node> – имя хоста или идентификатор сервера
- <address> – адрес IPv4

Этот параметр можно использовать несколько раз.

Например:

```
# vinfra cluster network migration retry --subnet 192.168.128.0 \
--netmask 255.255.255.0 --node node001 192.168.128.12 --node node002 192.168.128.13 \
--node node003 192.168.128.14
+--------------------------+----------------------------------------------------+
| Field                    | Value                                              |
```

```
+--------------------------+-------------------------------------------------+
| link                     | href: /api/v2/network/migration/2d4ec3a9-<...>/ |
|                          | method: GET                                     |
|                          | rel: network-migration-details                  |
| operation                | network-migration                               |
| progress                 | 0.9                                             |
| single_interface_migration | False                                         |
| state                    | failed-to-apply                                 |
| task_id                  | 2ce42f0e-6401-47c1-a52f-33e7c68d0df4            |
| transitions              | 5                                               |
+--------------------------+-------------------------------------------------+
```

В случае других проблем с сетью вернитесь к старой сетевой конфигурации, использовав команду vinfra cluster network migration revert, исправьте проблему и повторите попытку.

В случае возникновения ошибки при миграции

1. Подключитесь к кластеру через SSH.
2. Просмотрите файл /var/log/vstorage-ui-backend/celery.log для выяснения причины.
3. Исправьте проблему.
4. Вернитесь на экран мастера и нажмите **Повторить**.

7.1.4 Управление доменами, пользователями и проектами

В панели администратора можно управлять доменами и их настройками, администраторами и пользователями самообслуживания, проектами и квотами для них. Участники проекта также могут быть созданы и назначены для проектов в панели самообслуживания администраторами домена.

Предварительные требования

- Четкое понимание концепции "Мультитенантность" на странице 40.

7.1.4.1 Управление доменами

Количество доменов можно увеличить, как описано в разделе "Настройка мультитенантности" на странице 182. Кроме того, можно редактировать, включать/отключать и удалять существующие домены. Отключение и включение доменов запрещает или разрешает доступ к доменам в панели самообслуживания.

Ограничения

- Домен нельзя удалить, если в нем есть проекты.

Для изменения имени домена или его описания

Панель администратора

1. Перейдите на экран **Настройки** > **Проекты и пользователи**.
2. Щелкните значок с многоточием рядом с доменом, а затем выберите **Изменить**.
3. Внесите необходимые изменения и нажмите **Сохранить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain set [--description <description>] [--name <name>] <domain>
```

--description <description>

Описание домена

--name <name>

Имя домена

<domain>

Имя или ID домена

Например, чтобы добавить описание домена mydomain, запустите команду:

```
# vinfra domain set mydomain --description "Пользовательский домен"
```

Для включения или отключения домена

Панель администратора

1. Перейдите на экран **Настройки** > **Проекты и пользователи**.
2. Щелкните значок с многоточием рядом с доменом, а затем выберите **Включить** или **Отключить**.

Интерфейс командной строки

Используйте команду:

```
vinfra domain set [--enable | --disable] <domain>
```

--enable

Включить домен

--disable

Отключить домен

<domain>

Имя или ID домена

Например, чтобы отключить домен mydomain, запустите команду:

```
# vinfra domain set mydomain --disable
```

Для просмотра сведений о домене

Используйте следующую команду:

```
vinfra domain show <domain>
```

<domain>

Идентификатор или имя домена

Например, чтобы вывести сведения о домене mydomain, выполните:

```
# vinfra domain show mydomain
+---------------+----------------------------------+
| Field         | Value                            |
+---------------+----------------------------------+
| description   |                                  |
| enabled       | True                             |
| id            | 24986479ee3246048d3ef2a065ea99f5 |
| name          | mydomain                         |
| projects_count | 0                               |
+---------------+----------------------------------+
```

Для удаления домена

Панель администратора

1. Перейдите на экран **Настройки** > **Проекты и пользователи**.
2. Щелкните значок с многоточием рядом с доменом, а затем выберите **Удалить**.

Интерфейс командной строки

Используйте команду:

```
vinfra domain delete <domain>
```

<domain>

Имя или ID домена

Например, чтобы удалить домен mydomain, запустите команду:

```
# vinfra domain delete mydomain
```

7.1.4.2 Управление пользователями панели администратора

Во время развертывания основного узла создается уникальный домен по умолчанию **Default** вместе с учетной записью пользователя и проектом:

- Учетная запись администратора по умолчанию создается с уникальными правами доступа **суперпользователя**. Имя пользователя для этой учетной записи – **admin**, а пароль указывается во время развертывания основного узла. Данная учетная запись не может быть удалена или отключена, а ее разрешения не могут быть изменены. В остальном пользователь **admin** ничем

не отличается от пользователя, которому назначена роль **Системный администратор**.

- Проект администратора по умолчанию – это проект начальной загрузки для инициализации вычислительного облака. Имя этого проекта – **admin**. Его нельзя удалить или переименовать.

Домен **Default** с системными пользователями и проектами используется системой для различных сервисов. Системные объекты помечаются тегом **Системный** и не могут быть изменены или удалены.

В целях безопасности может потребоваться создать других системных администраторов с разрешениями для управления инфраструктурой. Например, вы можете создать системных администраторов, которые будут следить за производительностью и параметрами кластера, но не смогут изменять какие-либо настройки.

Другие пользователи, такие как администраторы домена и участники проекта, имеют доступ только к панели самообслуживания и обязаны выделять мультитенантные вычислительные ресурсы.

Ограничения

- Системных администраторов можно создавать только в домене **Default**.

Для создания системного администратора

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** выберите домен **Default**.
2. Перейдите на вкладку **Пользователи домена** и нажмите **Создать пользователя**.
3. В окне **Создать пользователя** укажите имя пользователя и пароль. При необходимости укажите адрес электронной почты и описание пользователя. Имя пользователя должно быть уникальным в пределах домена.
4. Выберите роль **Системный администратор** в раскрывающемся меню **Роль**.
5. Выберите разрешения для учетной записи пользователя в разделе **Набор системных ролей**:
   - **Все права**: администратор имеет все разрешения и может выполнять все операции по управлению, включая создание проектов и управление другими пользователями.
   - **Вычисления**: администратор может создавать вычислительный кластер и управлять им.
   - **ISCSI**: администратор может создавать цели iSCSI и LUN, пользователей CHAP и управлять ими.
   - **S3**: администратор может создавать кластер S3 и управлять им.
   - **ABGW**: администратор может создавать резервный шлюз и управлять им.
   - **NFS**: администратор может создавать и настраивать тома и экспорты NFS.
   - **Кластер**: администратор может создавать кластер хранения, присоединять к нему узлы и управлять дисками (назначать и освобождать).
   - **Сеть**: администратор может изменять сети и типы трафика.

- **Обновление**: администратор может устанавливать обновления.
- **SSH**: администратор может добавлять и удалять ключи SSH для доступа к узлам кластера.

Примечание
Разрешение на просмотр всегда активно.

6. [Необязательно] Активируйте **Набор разрешений домена**, чтобы управлять виртуальными объектами во всех проектах в домене **Default** и другими пользователями в панели самообслуживания.
7. Щелкните **Создать**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain user create [--email <email>] [--description <description>]
                          [--system-permissions <system_permissions>]
                          [--enable | --disable] --domain <domain> <name>
```

--email <email>

Электронная почта пользователя

--description <description>

Описание пользователя

--system-permissions <system_permissions>

Разделенный запятыми список разрешений системы. Просмотрите список доступных системных разрешений, используя команду vinfra domain user list-available-roles | grep system.

--enable

Включение пользователя

--disable

Отключение пользователя

--domain <domain>

Имя или ID домена

<name>

Имя или ID пользователя

Например, чтобы создать учетную запись системного администратора с именем mysysadmin в домене по умолчанию, чтобы управлять вычислительным кластером, запустите команду:

```
# vinfra domain user create mysysadmin --domain Default --system-permissions compute
```

При появлении запроса укажите пароль пользователя.

Созданный системный администратор появится в выводе команды vinfra domain user list:

```
# vinfra domain user list --domain Default
+----------------------------------+----------------------+-------+---------+-------------+--------------------+-------------
-----+
| id                               | name                 | email | enabled | description | domain_permissions | assigned_
projects |
+----------------------------------+----------------------+-------+---------+-------------+--------------------+-------------
-----+
| 1d207818a205433fabb85d68ff8bd45a | nova                 |       | True    |             | []                 | []
|
| 1eb4cd6272d84d0a824877a8afe16269 | heat                 |       | True    |             | []                 | []
|
| 4ae74e324e7241139e1357c9ce65f0b1 | backup-service-user  |       | False   |             | []                 | []
|
| 4e7db09ec1794aff92cbac0a70159478 | gnocchi              |       | True    |             | []                 | []
|
| 8d54115532ee421a8551ab32910998ad | octavia              |       | True    |             | []                 | []
|
| 8fd6757e10494c399cd8445dd8c83c87 | barbican             |       | True    |             | []                 | []
|
| 9e462afe59a742049970bdbb902569d1 | neutron              |       | True    |             | []                 | []
|
| a2c7eda0ea5a45749d0af7742ace85b0 | glance               |       | True    |             | []                 | []
|
| a91aa030575c474f9753abda3bf7afa0 | cinder               |       | True    |             | []                 | []
|
| c727a901a6444ee1a8ad31e3d5b53b3a | admin                |       | True    |             | []                 | []
|
| ca92d0b41f354a6882f24e0eb101b4ea | vstorage-service-user |       | True    |             | []                 | []
|
| e03bf89a89ef4a018dbf5aae107beed8 | mysysadmin           |       | True    |             | []                 | []
|
| ed4b3f0b6e61470ba0b79662671679f6 | ceilometer           |       | True    |             | []                 | []
|
| f62f123df20c4b388fefebf058fb185c | placement            |       | True    |             | []                 | []
|
+----------------------------------+----------------------+-------+---------+-------------+--------------------+-------------
-----+
```

Для смены пароля

Панель администратора

1. В правом верхнем углу панели администратора щелкните значок пользователя, а затем нажмите **Сменить пароль**.
2. В окне **Сменить пароль** введите текущий пароль и дважды введите новый пароль.
3. Нажмите **Сохранить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain user set [--password] --domain <domain> <user>
```

--password

Запросить пароль со стандартного ввода

--domain <domain>

Имя или ID домена

<user>

Имя или ID пользователя

Например, чтобы изменить пароль системного администратора mysysadmin, запустите команду:

```
# vinfra domain user set mysysadmin --domain Default --password
```

При появлении запроса введите новый пароль, который заменит старый.

Для просмотра сведений о пользователе

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** щелкните домен, который содержит необходимого пользователя.
2. Перейдите на вкладку **Пользователи домена** и щелкните пользователя. На правой панели будут отображены сведения об этом пользователе.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain user show --domain <domain> <user>
```

--domain <domain>

Идентификатор или имя домена

<user>

Идентификатор или имя пользователя

Например, чтобы вывести сведения о пользователе myuser из домена mydomain, выполните:

```
# vinfra domain user show myuser --domain mydomain
+-------------------+----------------------------------+
| Field             | Value                            |
+-------------------+----------------------------------+
| assigned_domains  | []                               |
| assigned_projects | []                               |
| description       |                                  |
| domain_id         | 2929ff42b1e64884a05dea3011862aed |
| domain_permissions | - domain_admin                  |
| email             |                                  |
| enabled           | True                             |
| id                | a9c67c6acf1f4df1818fdeeee0b4bd5e |
| name              | myuser                           |
| role              | domain_admin                     |
| system_permissions | []                              |
| tags              | []                               |
+-------------------+----------------------------------+
```

7.1.4.3 Управление пользователями самообслуживания

О добавлении администраторов домена и участников проекта написано в разделе "Настройка мультитенантности" на странице 182. Также доступно редактирование, назначение проектов,

включение/отключение и удаление существующих пользователей. Включение и отключение пользователей разрешает или запрещает вход пользователя в панель самообслуживания.

Для изменения учетных данных пользователя

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** выберите домен, в котором нужно изменить пользователя.
2. Перейдите на вкладку **Пользователи домена**, щелкните значок с многоточием рядом с пользователем, а затем нажмите **Изменить**.
3. Внесите необходимые изменения и выберите **Сохранить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain user set [--password] [--email <email>] [--name <name>]
                       --domain <domain> <user>
```

--password
: Запросить пароль со стандартного ввода

--email <email>
: Электронная почта пользователя

--name <name>
: Имя пользователя

--domain <domain>
: Имя или ID домена

<user>
: Имя или ID пользователя

Например, чтобы изменить адрес электронной почты пользователя myuser на user@example.com, запустите команду:

```
# vinfra domain user set myuser --domain mydomain --email user@example.com
```

Для включения или отключения пользователя

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** выберите домен, в котором хотите изменить пользователя.
2. Перейдите на вкладку **Пользователи домена**, щелкните значок с многоточием рядом с пользователем, а затем нажмите **Включить** или **Отключить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain user set [--enable | --disable] --domain <domain> <user>
```

--enable

Включить пользователя

--disable

Выключить пользователя

--domain <domain>

Имя или ID домена

<user>

Имя или ID пользователя

Например, чтобы отключить пользователя myuser в домене mydomain, запустите команду:

```
# vinfra domain user set myuser --domain mydomain --disable
```

Для назначения пользователя в проект

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** выберите домен, в котором хотите изменить пользователя.
2. Перейдите на вкладку **Пользователи домена**, щелкните значок с многоточием рядом с пользователем с ролью **Участник проекта**, а затем выберите **Настроить проекты**.
3. В окне **Настроить проекты** выберите проекты, которым нужно назначить пользователя, а затем нажмите **Сохранить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain user set [--assign <project> <role>] --domain <domain> <user>
```

--assign <project> <role>

Назначить пользователя в проект с одним или несколькими наборами разрешений. Укажите этот параметр несколько раз, чтобы назначить пользователя нескольким проектам.

- <project>: имя или ID проекта
- <role>: роль пользователя в проекте (project_admin)

--domain <domain>

Имя или ID домена

<user>

Имя или ID пользователя

Например, чтобы назначить пользователя myuser из домена mydomain в проект myproject в качестве администратора проекта, запустите команду:

```
# vinfra domain user set myuser --domain mydomain --assign myproject project_admin
```

Для просмотра сведений о пользователе

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** щелкните домен, который содержит необходимого пользователя.
2. Перейдите на вкладку **Пользователи домена** и щелкните пользователя. На правой панели будут отображены сведения об этом пользователе.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain user show --domain <domain> <user>
```

--domain <domain>

Идентификатор или имя домена

<user>

Идентификатор или имя пользователя

Например, чтобы вывести сведения о пользователе myuser из домена mydomain, выполните:

```
# vinfra domain user show myuser --domain mydomain
+--------------------+----------------------------------+
| Field              | Value                            |
+--------------------+----------------------------------+
| assigned_domains   | []                               |
| assigned_projects  | []                               |
| description        |                                  |
| domain_id          | 2929ff42b1e64884a05dea3011862aed |
| domain_permissions | - domain_admin                   |
| email              |                                  |
| enabled            | True                             |
| id                 | a9c67c6acf1f4df1818fdeeee0b4bd5e |
| name               | myuser                           |
| role               | domain_admin                     |
| system_permissions | []                               |
| tags               | []                               |
+--------------------+----------------------------------+
```

Для удаления пользователя

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** выберите домен, в котором вы хотите удалить пользователя.
2. Перейдите на вкладку **Пользователи домена**, щелкните значок с многоточием рядом с пользователем, а затем нажмите **Удалить**.
3. Выберите **Удалить** в окне подтверждения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain user delete --domain <domain> <user>
```

--domain <domain>

Имя или ID домена

<user>

Имя или ID пользователя

Например, чтобы удалить пользователя myuser из домена mydomain:

```
# vinfra domain user delete myuser --domain mydomain
```

7.1.4.4 Управление проектами

Подробнее о добавлении проектов написано в разделе "Настройка мультитенантности" на странице 182. Кроме того, здесь можно редактировать квоты проекта, назначать/отменять назначение пользователей, включать/отключать и удалять существующие проекты. Включение и отключение проектов разрешает или запрещает доступ к проектам в панели самообслуживания.

Ограничения

- Проект нельзя удалить, если в нем есть виртуальные объекты.

Для изменения названия или описания проекта

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** щелкните домен, в рамках которого хотите управлять проектами.
2. Перейдите на вкладку **Проекты**, щелкните значок с многоточием рядом с проектом, а затем нажмите **Изменить**.
3. Внесите необходимые изменения и выберите **Сохранить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain project set [--description <description>] [--name <name>] --domain <domain>
<project>
```

--description <description>

Описание проекта

--name <name>

Имя проекта

--domain <domain>

Имя или ID домена

<project>

Имя или ID проекта

Например, чтобы изменить имя проекта myproject в домене mydomain на newproject, запустите команду:

```
# vinfra domain project set myproject --domain mydomain --name newproject
```

Для назначения участников в проект

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** щелкните домен, в рамках которого хотите управлять проектами.
2. Перейдите на вкладку **Проекты**, щелкните значок с многоточием рядом с проектом, а затем нажмите **Назначить участников**.
3. В окне **Назначить участников** выберите пользователей, которых хотите добавить, и нажмите **Назначить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain user set [--assign <project> <role>] --domain <domain> <user>
```

--assign <project> <role>

Назначить пользователя в проект с одним или несколькими наборами разрешений. Укажите этот параметр несколько раз, чтобы назначить пользователя нескольким проектам.

- <project>: имя или ID проекта
- <role>: роль пользователя в проекте (project_admin)

--domain <domain>

Имя или ID домена

<user>

Имя или ID пользователя

Например, чтобы назначить пользователя myuser из домена mydomain в проект myproject в качестве администратора проекта, запустите команду:

```
# vinfra domain user set myuser --domain mydomain --assign myproject project_admin
```

Для просмотра списка участников проекта

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** щелкните домен, в рамках которого хотите управлять проектами.
2. Перейдите на вкладку **Проекты** и щелкните проект, список участников которого необходимо просмотреть.
3. На правой панели перейдите на вкладку **Участники**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain project user list [--long] --domain <domain> <project>
```

--long

Включение доступа и перечисления для всех полей объектов.

--domain <domain>

Имя или идентификатор домена.

<project>

Идентификатор или имя проекта.

Например, чтобы вывести список участников проекта myproject из домена mydomain, выполните:

```
# vinfra domain project user list myproject --domain mydomain
+----------------------------------+--------+-------------+---------------+
| id                               | name   | description | role          |
+----------------------------------+--------+-------------+---------------+
| eb0203e6b8a641d8be5b54b2f3fc9f47 | myuser |             | project_admin |
+----------------------------------+--------+-------------+---------------+
```

Для удаления участников из проекта

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** щелкните домен, в рамках которого хотите управлять проектами.
2. Перейдите на вкладку **Проекты**, щелкните значок с многоточием рядом с проектом, а затем нажмите **Удалить участников проекта**.
3. В окне **Удалить участников проекта** выберите пользователей, которых вы хотите удалить, и нажмите **Снять назначение**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain project user remove --user <user> --domain <domain> <project>
```

--user <user>

Имя или ID пользователя

--domain <domain>

Имя или ID домена

<project>

Имя или ID проекта

Например, чтобы удалить пользователя myuser из проекта myproject в домене mydomain, запустите команду:

```
# vinfra domain project user remove myproject --domain mydomain --user myuser
```

Для изменения квоты проекта

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** щелкните домен, в рамках которого хотите управлять проектами.
2. Перейдите на вкладку **Проекты**, щелкните значок с многоточием рядом с проектом, а затем нажмите **Изменить лимиты**.
3. Внесите необходимые изменения и выберите **Сохранить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute quotas update [--cores <cores>] [--ram-size <ram>] [--floatingip <floating-ip>]
                                     [--storage-policy <storage_policy>:<size>]
                                     [--k8saas-cluster <cluster>] [--lbaas-loadbalancer <load-balancer>]
                                     [--placement <placement>] <project-id>
```

--cores <cores>

Количество ядер

--ram-size <ram>

Количество оперативной памяти. Используйте следующие единицы измерения: M или MiB для мебибайтов, G или GiB для гибибайтов, T или TiB для тебибайтов, P или PiB для пебибайтов, и E или EiB для эксбибайтов.

--floatingip <floating-ip>

Количество плавающих IP-адресов

--storage-policy <storage_policy>:<size>

Разделенный запятыми список <storage_policy>:<size>. Чтобы указать размер, используйте следующие единицы измерения: M или MiB для мебибайтов, G или GiB для гибибайтов, T или TiB для тебибайтов, P или PiB для пебибайтов, и E или EiB для эксбибайтов.

--k8saas-cluster <cluster>

Количество кластеров Kubernetes

--lbaas-loadbalancer <load-balancer>

Новое значение предела квоты балансировщика нагрузки. Значение -1 означает "неограниченный".

--placement <placement>

Список через запятую <placement-id>:<size>

<project-id>

Идентификатор проекта

Например, чтобы обновить квоты для проекта с идентификатором 6ef6f48f01b640ccb8ff53117b830fa3 до 10 виртуальных ЦП, 20 ГБ ОЗУ и 512 ГБ дискового пространства для политики хранения default, запустите команду:

```
# vinfra service compute quotas update 6ef6f48f01b640ccb8ff53117b830fa3 --cores 10 --ram-size
10G --storage-policy default:512G
```

Обновленные квоты можно просмотреть в выводе вычислительных квот службы vinfra:

```
# vinfra service compute quotas show 79830e3c64c74ded9bac6bffde5d26e4
+---------------------------------------+----------+
| Field                                 | Value    |
+---------------------------------------+----------+
| compute.cores.limit                   | 10       |
| compute.ram.limit                     | 10.0GiB  |
| compute.ram_quota.limit               | 10.0GiB  |
| lbaas.loadbalancer.limit              | -1       |
| network.floatingip.limit              | -1       |
| storage.gigabytes.default.limit       | 512.0GiB |
| storage.storage_policies.default.limit | 512.0GiB |
+---------------------------------------+----------+
```

Для включения или отключения проекта

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** щелкните домен, в рамках которого хотите управлять проектами.
2. Перейдите на вкладку **Проекты**, щелкните значок с многоточием рядом с проектом, а затем нажмите **Включить** или **Отключить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain project set [--enable | --disable] --domain <domain> <project>
```

--enable

Включить проект

--disable

Отключить проект

--domain <domain>

Имя или ID домена

<project>

Имя или ID проекта

Например, чтобы отключить проект myproject в домене mydomain, запустите команду:

```
# vinfra domain project set myproject --domain mydomain --disable
```

Для просмотра сведений о проекте

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** щелкните домен, который содержит необходимый проект.
2. Перейдите на вкладку **Проекты** и щелкните проект. На правой панели будут отображены сведения об этом проекте.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain project show --domain <domain> <project>
```

--domain <domain>

Имя или идентификатор домена

<project>

Идентификатор или имя проекта

Например, чтобы вывести сведения о проекте myproject из домена mydomain, выполните:

```
# vinfra domain project show myproject --domain mydomain
+--------------+----------------------------------+
| Field        | Value                            |
+--------------+----------------------------------+
| description  | A custom project                 |
| domain_id    | 9f7e68938fe946a2a862e360bbe40d98 |
| enabled      | True                             |
| id           | d1c4d6198fb940e6b971cf306571ebbd |
| members_count | 0                               |
```

```
| name        | myproject                    |
| tags        | []                           |
+---------------+--------------------------------+
```

Для удаления проекта

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** щелкните домен, в рамках которого хотите управлять проектами.
2. Перейдите на вкладку **Проекты**, щелкните значок с многоточием рядом с проектом и нажмите **Удалить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain project delete --domain <domain> <project>
```

--domain <domain>

Имя или ID домена

<project>

Имя или ID проекта

Например, чтобы удалить проект myproject из домена mydomain, запустите команду:

```
# vinfra domain project delete myproject --domain mydomain
```

7.1.4.5 Управление группами домена

Группа домена — это группа пользователей с одинаковыми разрешениями в определенном домене. Пользователи, назначенные группе домена, наследуют разрешения роли, установленные для этой группы домена. Использование доменных групп позволяет настраивать разрешения нескольких пользователей без необходимости делать это индивидуально.

Вы можете создавать, редактировать и удалять существующие группы домена, а также управлять назначением пользователей и проектов в группы домена.

Создание доменных групп

Ограничения

- Вы можете создавать доменные группы с ролью **Системный администратор** только в домене **По умолчанию**. Подробнее см. в разделе "Управление пользователями панели администратора" на странице 275.

Предварительные требования

- Четкое понимание концепции "Мультитенантность" на странице 40.

Для создания группы домена

Панель администратора

1. В разделе **Настройки** > **Проекты и пользователи** выберите домен, в котором будет создана группа домена.
2. Перейдите на вкладку **Группы домена** и нажмите **Создать группу домена**.
3. В окне **Создать группу** укажите имя группы и, при необходимости, описание. Имя группы должно быть уникальным в пределах домена.
4. Выберите роль пользователя::
   - Чтобы создать группу администраторов домена
     a. Выберите **Администратор домена**.
     b. [Необязательно] Установите флажок **Загрузка образа**. Состояние этого разрешения будет унаследовано пользователями, созданными этим администратором домена.
   - Чтобы создать группу системных администраторов
     a. Выберите **Системный администратор**.
     b. Выберите разрешения, которые будут предоставлены учетной записи пользователя, в разделе **Набор разрешений системы**:
        - **Все права** (Системный администратор): имеет все разрешения и может выполнять все операции по управлению, включая создание проектов и управление другими пользователями.
        - **Вычисления**: может создавать вычислительный кластер и управлять им.
        - **ISCSI**: может создавать цели iSCSI и LUN, пользователей CHAP и управлять ими.
        - **S3**: может создавать кластер S3 и управлять им.
        - **ABGW**: может создавать резервный шлюз и управлять им.
        - **NFS**: может создавать и настраивать тома и экспорты NFS.
        - **Кластер**: может создавать кластер хранения, присоединять к нему узлы и управлять дисками (назначать и освобождать).
        - **Сеть**: может изменять сети и типы трафика.
        - **Обновление**: может устанавливать обновления.
        - **SSH**: может добавлять и удалять ключи SSH для доступа к узлам кластера.

        Примечание
        Разрешение на просмотр всегда включено.

     c. [Необязательно] Активируйте **Набор разрешений домена**, чтобы иметь возможность управлять виртуальными объектами во всех проектах в домене **по умолчанию** и другими пользователями в панели самообслуживания.
   - Чтобы создать группу администраторов проекта

a. Выберите **Участник проекта**.

b. Установите флажок **Загрузка образа**. Если эта опция отключена, пользователь не сможет загружать образы.

c. [Необязательно] Щелкните **Назначить** и выберите проекты, в которые будут назначены пользователи из этой группы.

5. Нажмите **Создать**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain group create [--description <description>] [--assign <project> <role>]
                           [--domain-permissions <domain_permissions>]
                           [--system-permissions <system_permissions>]
                           [--enable | --disable] --domain <domain> <name>
```

--description <description>

Описание группы

--assign <project> <role>

Назначить группу проекту с одним или несколькими наборами разрешений. Укажите этот параметр несколько раз, чтобы назначить группу нескольким проектам.

- <project>: имя или ID проекта
- <role>: роль группы в проекте (project_admin)

--domain-permissions <domain_permissions>

Разделенный запятыми список разрешений домена. Просмотрите список доступных разрешений домена, используя команду vinfra domain user list-available-roles | grep domain.

--system-permissions <system_permissions>

Разделенный запятыми список разрешений системы. Просмотрите список доступных системных разрешений, используя команду vinfra domain user list-available-roles | grep system.

--enable

Включить группу

--disable

Отключить группу

--domain <domain>

Имя или ID домена

<name>

Имя группы

Пример 1. Чтобы создать группу администраторов домена domain_admins в домене с именем mydomain, запустите команду:

```
# vinfra domain group create domain_admins --domain mydomain --domain-permissions domain_
admin
```

Пример 2. Чтобы создать группу системных администраторов с именем sys_admins в домене по умолчанию для управления вычислительным кластером, запустите команду:

```
# vinfra domain group create mysysadmin --domain Default --system-permissions compute
```

Пример 3. Чтобы в домене mydomain создать группу участников проекта, называемых пользователями проекта myproject, и предоставить этой группе пользователей разрешение на загрузку образов, запустите команду:

```
# vinfra domain group create myusers --domain mydomain --assign myproject project_admin --
domain-permissions image_upload
```

Созданная группа появится в выводе списка групп домена vinfra domain group list:

```
# vinfra domain group list --domain mydomain
+-------------+--------------+-------------+--------------------+--------------------------+
| id          | name         | description | domain_permissions | assigned_projects        |
+-------------+--------------+-------------+--------------------+--------------------------+
| 1670fbc6<…> | domain_admins |             | - domain_admin     | []                       |
| d2fb8a2d<…> | myusers       |             | - image_upload     | - project_id: db49fd71<…> |
|             |              |             |                    |   role: project_admin    |
+-------------+--------------+-------------+--------------------+--------------------------+
```

Управление назначением пользователей в группы домена

Создав группу домена, вы можете назначить в нее пользователей. Можно выбрать пользователей, добавленных в инфраструктуру вручную или автоматически от внешних поставщиков удостоверений. Пользователи, назначенные группе домена, наследуют роль, установленную для этой группы домена, независимо от их исходных ролей. Например, если вы назначаете пользователя с ролью **Участник проекта** в доменную группу с ролью **Администратор домена**, пользователь будет действовать как администратор домена в этом домене.

Предварительные требования

- Созданы группы домена, как описано в разделе "Создание доменных групп" на странице 289.
- Пользователи созданы локально, как описано в разделе "Настройка мультитенантности" на странице 182 или "Управление пользователями панели администратора" на странице 275, или добавлены из внешних поставщиков удостоверений, как описано в разделе "Добавление поставщиков удостоверений" на странице 297.

Управление пользователями доменной группы

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** выберите домен, в котором хотите изменить доменную группу.
2. Перейдите на вкладку **Группы домена**, щелкните значок с многоточием рядом с группой и выберите **Настроить пользователей**.
3. В окне **Настроить пользователей** выберите пользователей, которых нужно добавить в группу, или отмените их выбор, чтобы отменить назначение из группы, а затем нажмите **Сохранить**.

Интерфейс командной строки

- Чтобы добавить пользователя в группу домена, используйте следующую команду:

  ```
  vinfra domain group user add --domain <domain> <group> <user>
  ```

  --domain <domain>
  : Имя или ID домена

  <group>
  : Имя или ID группы

  <user>
  : Имя или ID пользователя

  Например, чтобы добавить пользователя myuser в доменную группу users в домене mydomain, запустите команду:

  ```
  # vinfra domain group user add --domain mydomain users myuser
  ```

- Чтобы удалить пользователя из группы домена, используйте следующую команду:

  ```
  vinfra domain group user remove --domain <domain> <group> <user>
  ```

  --domain <domain>
  : Имя или ID домена

  <group>
  : Имя или ID группы

  <user>
  : Имя или ID пользователя

  Например, чтобы удалить пользователя myuser из доменной группы users в домене mydomain, запустите команду:

  ```
  # vinfra domain group user remove --domain mydomain users myuser
  ```

Управление назначением проекта в группы домена

Создав доменную группу с ролью **Участник проекта**, вы можете назначать ей проекты. Проекты, которые вы назначаете группе домена, будут автоматически назначены всем пользователям

группы домена.

Предварительные требования

- Созданы группы домена, как описано в разделе "Создание доменных групп" на странице 289.
- Созданы проекты, как описано в разделе "Настройка мультитенантности" на странице 182.

Для управления проектами доменной группы

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** выберите домен, в котором хотите изменить доменную группу.
2. Перейдите на вкладку **Группы домена**, щелкните значок с многоточием рядом с группой, которой назначена роль **Участник проекта**, а затем нажмите **Настроить проекты**.
3. В окне **Настроить проекты** выберите проекты для назначения или отмените назначение проектов, а затем нажмите **Сохранить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain group set [--assign <project> <role>] [--unassign <project>] --domain <domain>
<group>
```

--assign <project> <role>

Назначить проект с одним или несколькими наборами разрешений. Укажите этот параметр несколько раз, чтобы назначить несколько проектов.

- <project>: имя или ID проекта
- <role>: роль пользователя в проекте (project_admin)

--unassign <project>

Отменить назначение проекта. Укажите этот параметр несколько раз, чтобы отменить назначение нескольких проектов.

- <project>: имя или ID проекта

--domain <domain>

Имя или ID домена

<group>

Имя или ID группы

Например, чтобы назначить группе mygroup из домена mydomain проект myproject с ролью пользователей project_admin, запустите команду:

```
# vinfra domain group set mygroup --domain mydomain --assign myproject project_admin
```

Редактирование и удаление доменных групп

Редактировать можно следующие параметры доменной группы: ее имя, описание, роль пользователя, системные и доменные разрешения. При удалении группы домена все назначенные пользователи автоматически выходят из панели управления.

Предварительные требования

- Созданы группы домена, как описано в разделе "Создание доменных групп" на странице 289.

Для редактирования доменной группы

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** выберите домен, в котором хотите изменить группу.
2. Перейдите на вкладку **Группы домена**, щелкните значок с многоточием рядом с группой и выберите **Изменить**.
3. Внесите необходимые изменения и нажмите **Сохранить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain group set [--name <name>] [--description <description>]
                        [--domain-permissions <domain_permissions>]
                        [--system-permissions <system_permissions>]
                        [--enable | --disable] --domain <domain> <group>
```

--name <name>

Новое имя группы

--description <description>

Описание группы

--domain-permissions <domain_permissions>

Разделенный запятыми список разрешений домена. Просмотрите список доступных разрешений домена, используя команду vinfra domain user list-available-roles | grep domain.

--system-permissions <system_permissions>

Разделенный запятыми список разрешений системы. Просмотрите список доступных системных разрешений, используя команду vinfra domain user list-available-roles | grep system.

--enable

Включить группу

--disable

Отключить группу

--domain <domain>

Имя или ID домена

<group>

Имя или ID группы

Например, чтобы изменить имя доменной группы с users на myusers, запустите команду:

```
# vinfra domain group set users --domain mydomain --name myusers
```

Для удаления доменной группы

Панель администратора

1. На экране **Настройки** > **Проекты и пользователи** выберите домен, в котором хотите удалить доменную группу.
2. Перейдите на вкладку **Группы домена**, щелкните значок с многоточием рядом с группой домена и выберите **Удалить**.
3. Нажмите **Удалить** в окне подтверждения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain group delete --domain <domain> <group>
```

--domain <domain>

Имя или ID домена

<group>

Имя или ID группы

Например, чтобы удалить группу users из домена mydomain, выполните:

```
# vinfra domain group delete users --domain mydomain
```

7.1.4.6 Управление поставщиками удостоверений

Помимо создания локальных пользователей вручную, можно добавлять пользователей от внешних поставщиков удостоверений и автоматически сопоставлять их с локальными доменными группами. Аутентификация пользователя основана на неявном потоке протокола OpenID Connect (OIDC) protocol.

Пользователи, импортированные из поставщиков удостоверений, называются **федеративными**, то есть общими для разных систем управления удостоверениями. В отличие от локальных пользователей, у федеративных пользователей нет учетных данных, установленных в Кибер инфраструктура. Они входят в панель администратора или панели самообслуживания, используя соответствующие учетные данные из основной системы управления идентификацией. Набор

действий, доступных федеративным пользователям, определяется ролями, назначаемыми их локальным группам домена.

Ограничения

- Поддерживаются только поставщики удостоверений Microsoft Active Directory Federation Services (AD FS).
- Когда федеративные пользователи удаляются их поставщиком удостоверений, они не удаляются автоматически из инфраструктуры.

Добавление поставщиков удостоверений

Прежде чем подключаться к поставщику удостоверений и импортировать его пользователей, необходимо создать доменные группы для этих пользователей и назначить этим группам соответствующие роли.

Предварительные требования

- Локальные группы домена создаются, как описано в разделе "Создание доменных групп" на странице 289.
- URL-адрес перенаправления (redirect_uri) для кластера должен быть https://<url>:8800/api/v2/login/idp/.

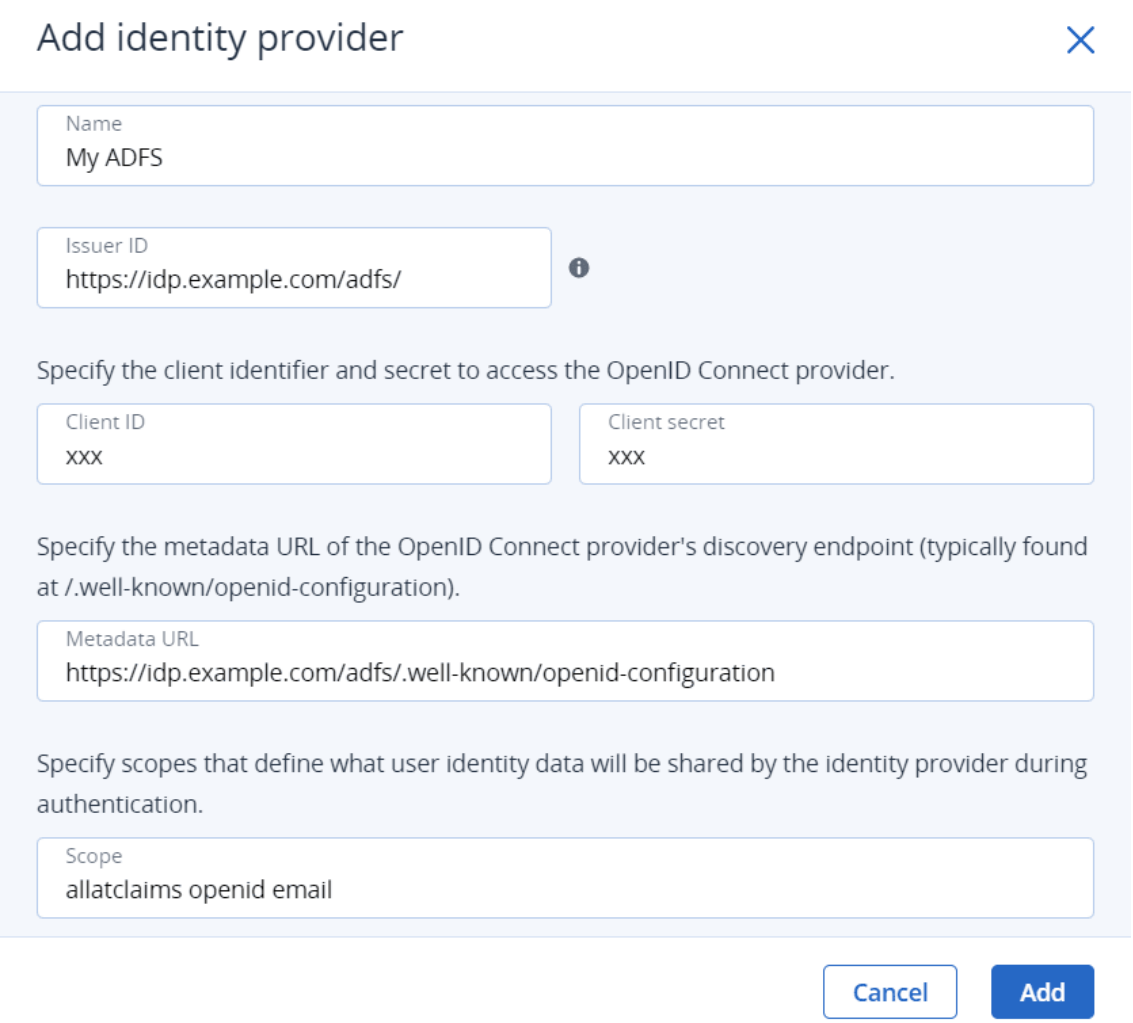
Для добавления поставщика удостоверений

Панель администратора

1. На экране **Проекты и пользователи** выберите нужный домен.
2. Перейдите в раздел **Настройки** > **Поставщик удостоверений** и нажмите **Добавить**.
3. В окне **Добавить поставщика удостоверений** укажите следующие параметры:
   a. Пользовательское имя поставщика удостоверений, которое будет отображаться на экране входа в систему.
   b. Уникальный идентификатор эмитента, предоставленный поставщиком OIDC. Обычно отображается как URN.
   c. Идентификатор клиента и секрет для доступа к поставщику OIDC.
   d. URL-адрес метаданных конечной точки обнаружения поставщика OIDC. URL-адрес метаданных обычно представляет собой конечную точку издателя, соединенную с путем /.well-known/openid-configuration. Например, если идентификатор эмитента **https://idp.example.com/adfs/**, URL-адрес метаданных будет **https://idp.example.com/adfs/.well-known/openid-configuration**.
   e. Области, определяющие, какие данные удостоверения пользователя будут совместно использоваться поставщиком OIDC во время проверки подлинности.

   Внимание

Области **allatclaims** и **openid** являются обязательными для поставщиков Microsoft AD FS.



4. В разделе **Сопоставление** можно создавать правила сопоставления вручную или автоматически из файла сопоставления:
   - Ручное создание правил сопоставления
     a. Выберите **Создать правила сопоставления**, а затем нажмите **Добавить**.
     b. В окне **Добавить правило** создайте **Условия сопоставления**, нажав кнопку **Добавить** и указав необходимые параметры:
        - Укажите атрибут пользователя **Атрибут**, который вы получаете от поставщика удостоверений во время аутентификации.
        - В поле **Условие** укажите условие, которое будет применяться к атрибуту. При условии **Существует** будут сопоставлены все пользователи с этим атрибутом. Условие **Содержит** отображает пользователей, если этот атрибут содержит любое из указанных значений. Условие **Не содержит** сопоставляет пользователей, если этот атрибут не содержит ни одного из указанных значений.
        - В поле **Значение** укажите желаемое значение атрибута в виде строки, списка, разделенного запятыми, или регулярного выражения.

c. Выберите существующую группу домена для назначения федеративных пользователей.

d. Если у вас есть правило сопоставления с условием **Существует**, выберите атрибуты, из которых будет состоять имя локального пользователя. Например, с атрибутом сопоставления **email** и условием сопоставления **Существует**, имена локальных пользователей могут состоять из их адресов электронной почты.

- Автоматическое создание правил сопоставления

a. Выберите **Загрузить файл сопоставления** в формате JSON с уже настроенными правилами сопоставления.

b. Напишите правила сопоставления в формате JSON в поле **Данные сопоставления**. Либо щелкните **Загрузить**, а затем просмотрите файл JSON на локальном сервере, чтобы загрузить данные сопоставления.

Файл сопоставления может выглядеть следующим образом:

```
# cat mapping.json
[
  {
    "local": [
      {
        "user": {
          "name": "{0}"
        },
        "group": {
          "name":"users"
        }
      }
    ],
    "remote": [{"type": "email"}]
  }
]
```

В этом примере все пользователи с атрибутом email будут сопоставлены группе users домена default. Для получения подробных сведений о создании файла сопоставления см. документацию OpenStack.

5. Нажмите **Добавить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain idp create --domain <domain> --issuer <issuer> --scope <scope>
                         [--metadata-url <metadata-url>] [--client-id <client-id>]
                         [--client-secret <client-secret>] [--mapping <path>]
                         [--enable] [--disable] <name>
```

--domain <domain>

Имя или ID домена

--issuer <issuer>

Эмитент поставщика удостоверений

--scope <scope>

Область, определяющая, какие данные удостоверения пользователя будут совместно использоваться поставщиком удостоверений во время проверки подлинности.

Внимание

Области **allatclaims** и **openid** являются обязательными для поставщиков Microsoft AD FS.

--metadata-url <metadata-url>

URL-адрес метаданных конечной точки обнаружения поставщика удостоверений

--client-id <client-id>

Идентификатор клиента для доступа к поставщику удостоверений

--client-secret <client-secret>

Секрет клиента для доступа к поставщику удостоверений

--mapping <path>

Путь к файлу конфигурации сопоставления

Файл сопоставления может выглядеть следующим образом:

```
# cat mapping.json
[
  {
    "local": [
      {
        "user": {
          "name": "{0}"
        },
        "group": {
          "name":"users"
        }
      }
    ],
    "remote": [{"type": "email"}]
  }
]
```

В этом примере все пользователи с атрибутом email будут сопоставлены группе users домена default. Для получения подробных сведений о создании файла сопоставления см. документацию OpenStack.

--enable

Включить поставщика удостоверений

--disable

Отключить поставщика удостоверений

<name>

Имя поставщика удостоверений

Например, чтобы добавить поставщика удостоверений с именем My ADFS в домене mydomain, запустите команду:

```
# vinfra domain idp create --domain mydomain --issuer https://idp.example.com/adfs/ \
--scope "allatclaims openid email" --client-id xxx --client-secret xxx --mapping mapping.json "My
ADFS"
```

Добавленный поставщик удостоверений появится в выводе команды vinfra domain idp list:

```
# vinfra domain idp list --domain mydomain
+-------------+---------+-----------------------------+-------------------------+-----------+
| id          | name    | issuer                      | scope                   | domain_id |
+-------------+---------+-----------------------------+-------------------------+-----------+
| df5a54ce<…> | My ADFS | https://idp.example.com/adfs/ | allatclaims openid email | 36f454<…> |
+-------------+---------+-----------------------------+-------------------------+-----------+
```

Вход через поставщиков удостоверений

После подключения к поставщику удостоверений вы можете получить прямую ссылку на страницу входа в систему самообслуживания и поделиться ею с федеративными пользователями. На этой странице входа федеративные пользователи должны выбрать **Войти с помощью <поставщика удостоверений>**, чтобы быть перенаправленными к своему поставщику удостоверений для аутентификации. После успешной аутентификации федеративные пользователи перенаправляются обратно на панель самообслуживания.

Внимание
Конечная точка авторизации AD FS должна поддерживать ответ Form Post Response Mode.

Если федеративные пользователи добавляются в группу домена **по умолчанию** с разрешениями **системного администратора**, они также смогут входить в панель администратора через своего поставщика удостоверений.

Предварительные требования

- Поставщики удостоверений добавляются в панель администратора, как описано в разделе "Добавление поставщиков удостоверений" на странице 297.

Чтобы поделиться URL-адресом панели самообслуживания с федеративными пользователями

1. На экране **Проекты и пользователи** выберите нужный домен.
2. Перейдите в раздел **Настройки** > **Поставщик удостоверений**, а затем щелкните значок стрелки рядом с поставщиком удостоверений, чтобы развернуть подробную информацию..
3. В **URL-адрес панели самообслуживания** скопируйте прямую ссылку на панель самообслуживания, а затем поделитесь ею с федеративными пользователями.

Изменение и удаление поставщиков удостоверений

Можно изменять конфигурацию поставщиков удостоверений, а также включать, отключать и удалять их. Включение или отключение поставщика удостоверений разрешает или запрещает вход в панели управления для его федеративных пользователей.

Предварительные требования

- Поставщики удостоверений добавляются в панель администратора, как описано в разделе "Добавление поставщиков удостоверений" на странице 297.

Для изменения поставщика удостоверений

Панель администратора

1. На экране **Проекты и пользователи** выберите нужный домен.
2. Перейдите в раздел **Настройки** > **Поставщик удостоверений**, щелкните значок с многоточием рядом с поставщиком удостоверений, а затем нажмите **Редактировать**.
3. Внесите необходимые изменения и нажмите **Сохранить**.

После изменения параметров поставщика удостоверений все его федеративные пользователи выйдут из панели управления.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain idp set [--issuer <issuer>] [--scope <issuer>] [--metadata-url <metadata-url>]
                      [--client-id <client-id>] [--client-secret <client-secret>]
                      [--mapping <path>] [--name <name>] --domain <domain> <idp>
```

--issuer <issuer>

Эмитент поставщика удостоверений

--scope <scope>

Область, определяющая, какие данные удостоверения пользователя будут совместно использоваться поставщиком удостоверений во время проверки подлинности.

--metadata-url <metadata-url>

URL-адрес метаданных конечной точки обнаружения поставщика удостоверений

--client-id <client-id>

Идентификатор клиента для доступа к поставщику удостоверений

--client-secret <client-secret>

Секрет клиента для доступа к поставщику удостоверений

--mapping <path>

Путь к файлу конфигурации сопоставления.

Файл сопоставления может выглядеть следующим образом:

```
# cat mapping.json
[
   {
      "local": [
         {
            "user": {
               "name": "{0}"
            },
            "group": {
               "name":"users"
            }
         }
      ],
      "remote": [{"type": "email"}]
   }
]
```

В этом примере все пользователи с атрибутом email будут сопоставлены группе users домена default. Для получения подробных сведений о создании файла сопоставления см. документацию OpenStack.

--name <name>

Новое имя поставщика удостоверений

--domain <domain>

Имя или ID домена

<idp>

Имя или ID поставщика удостоверений

Например, чтобы изменить правила сопоставления поставщика удостоверений My ADFS в домене mydomain с помощью файла сопоставления new_mapping.json, запустите команду:

```
# vinfra domain idp set "My ADFS" --domain mydomain --mapping new_mapping.json
```

После изменения параметров поставщика удостоверений все его федеративные пользователи выйдут из панели управления.

Для включения или отключения поставщика удостоверений

Панель администратора

1. На экране **Проекты и пользователи** выберите нужный домен.
2. Перейдите в раздел **Настройки** > **Поставщик удостоверений**, щелкните значок с многоточием рядом с поставщиком удостоверений, а затем нажмите **Включить** или **Выключить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain idp set [--enable] [--disable] --domain <domain> <idp>
```

--enable

Включить поставщика удостоверений

--disable

Отключить поставщика удостоверений

--domain <domain>

Имя или ID домена

<idp>

Имя или ID поставщика удостоверений

Например, чтобы отключить поставщика удостоверений My ADFS в домене mydomain, запустите команду:

```
# vinfra domain idp set "My ADFS" --domain mydomain --disable
```

Удаление поставщика удостоверений

Панель администратора

1. На экране **Проекты и пользователи** выберите нужный домен.
2. Перейдите в раздел **Настройки** > **Поставщик удостоверений**, щелкните значок с многоточием рядом с поставщиком удостоверений, а затем нажмите **Удалить**.
3. Нажмите **Удалить** в окне подтверждения.

После удаления поставщика удостоверений все его федеративные пользователи удаляются вместе с ним.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain idp delete --domain <domain> <idp>
```

--domain <domain>

Имя или ID домена

<idp>

Имя или ID поставщика удостоверений

Например, чтобы удалить поставщика удостоверений My ADFS в домене mydomain, запустите команду:

```
# vinfra domain idp delete "My ADFS" --domain mydomain
```

После удаления поставщика удостоверений все его федеративные пользователи удаляются вместе с ним.

7.1.4.7 Включение горячей замены ЦП и ОЗУ для каждого домена

Чтобы позволить пользователям самообслуживания добавлять дополнительные ресурсы ЦП и ОЗУ к виртуальным машинам во время выполнения, вы можете включить горячее подключение ЦП и ОЗУ для определенного домена. В доменах, в которых эта функция отключена, пользователям потребуется сначала остановить виртуальную машину, чтобы иметь возможность изменить ее вид. По умолчанию горячая замена ЦП и ОЗУ отключена для всех доменов.

Для включения горячего подключения ЦП и ОЗУ для домена

Панель администратора

1. На экране **Проекты и пользователи** выберите нужный домен.
2. Перейдите в раздел **Настройки** > **Горячее подключение ЦП и ОЗУ**, а затем включите **Горячее подключение ЦП и ОЗУ**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain properties create --key <key> --data <data> [--access <access>] <domain>
```

--key <key>

Имя свойства.

--data <data>

Значение свойства в формате JSON.

--access <access>

Тип доступа:

- pub: разрешить доступ для чтения всем пользователям (проверка подлинности не требуется).
- auth: разрешить доступ для чтения авторизованным пользователям.
- domain: разрешить доступ для чтения пользователям домена.

У суперадминистратора и администратора домена есть доступ для записи.

<domain>

Имя или идентификатор домена.

Например, чтобы создать свойство allow_live_resize, которое разрешает горячее подключение ЦП и ОЗУ для виртуальных машин в домене mydomain, запустите команду:

```
# vinfra domain properties create --key allow_live_resize mydomain --data '{"enabled":true}'
```

Созданное свойство появится в выводе vinfra domain properties keys list:

```
# vinfra domain properties keys list
+----------+--------------------+
| domain   | keys               |
+----------+--------------------+
| mydomain | - allow_live_resize |
| Default  | - allow_live_resize |
+----------+--------------------+
```

Для отключения горячего подключения ЦП и ОЗУ для домена

Панель администратора

1. На экране **Проекты и пользователи** выберите нужный домен.
2. Перейдите в раздел **Настройки** > **Горячее подключение ЦП и ОЗУ**, а затем отключите **Горячее подключение ЦП и ОЗУ**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra domain properties update --key <key> --data <data> [--access <access>] <domain>
```

--key <key>

Имя свойства.

--data <data>

Значение свойства в формате JSON.

--access <access>

Тип доступа:

- pub: разрешить доступ для чтения всем пользователям (проверка подлинности не требуется).
- auth: разрешить доступ для чтения авторизованным пользователям.
- domain: разрешить доступ для чтения пользователям домена.

У суперадминистратора и администратора домена есть доступ для записи.

<domain>

Имя или ID домена.

Например, чтобы изменить свойство allow_live_resize и отключить горячее подключение ЦП и ОЗУ для виртуальных машин в домене mydomain, запустите команду:

```
# vinfra domain properties update --key allow_live_resize mydomain \
--data '{"enabled": false}'
```

7.1.4.8 Разрешение администраторам домена управлять проектами

Вы можете разрешить администраторам домена управлять проектами в назначенном домене. С этим разрешением администраторы домена могут выполнять следующие дополнительные задачи с помощью инструмента командной строки OpenStack:

- Создание, обновление и удаление проектов
- Установка и обновление квот проекта
- Создание сетевых политик QoS и управление ими

Создание и назначение роли менеджера квот

Предварительные требования

- Для авторизации выполнения приведенных ниже команд настроен клиент командной строки OpenStack, как описано в разделе "Подключение к интерфейсу командной строки OpenStack" на странице 427.

Чтобы создать администратора домена, который может управлять проектами

1. Создайте роль quota_manager:

```
# openstack --insecure role create 'quota_manager'
```

2. Создайте домен и администратора домена с помощью инструмента vinfra. Например:

```
# vinfra domain create test
# vinfra domain user create --domain test --domain-permissions domain_admin testuser
```

3. Назначьте новому пользователю роль quota_manager. Например:

```
# openstack --insecure role add --user-domain test --user testuser --domain test quota_manager
# openstack --insecure role add --user-domain test --user testuser --domain test quota_manager --inherited
```

4. Подготовьте файл переменных среды для нового пользователя. Например:

```
# vi domain-admin.sh
export OS_PROJECT_DOMAIN_NAME=test
export OS_USER_DOMAIN_NAME=test
export OS_DOMAIN_NAME=test
export OS_USERNAME=testuser
export OS_PASSWORD=1q2w3e
export OS_AUTH_URL=https://127.0.0.1:5000/v3
export OS_IDENTITY_API_VERSION=3
export OS_AUTH_TYPE=password
export OS_INSECURE=true
export PYTHONWARNINGS="ignore:Unverified HTTPS request is being made"
```

```
export NOVACLIENT_INSECURE=true
export NEUTRONCLIENT_INSECURE=true
export CINDERCLIENT_INSECURE=true
export OS_PLACEMENT_API_VERSION=1.22
```

Управление проектами в качестве администратора домена

Предварительные требования

- Файл переменных среды для администратора домена, который будет управлять проектами, создан, как описано в разделе "Создание и назначение роли менеджера квот" на предыдущей странице.

Управление проектом в качестве администратора домена

1. Используйте файл переменных среды для администратора домена, чтобы авторизовать выполнение дальнейших команд OpenStack:

   ```
   # unset OS_PROJECT_NAME; unset OS_DOMAIN_NAME; source domain-admin.sh
   ```

2. Получите список всех доступных доменов, чтобы получить идентификатор необходимого домена:

   ```
   # openstack --insecure federation domain list
   +----------------------------------+---------+------+-------------+
   | ID                               | Enabled | Name | Description |
   +----------------------------------+---------+------+-------------+
   | b41c5bd8ca1e43f19f9720390c2869d5 | True    | test |             |
   +----------------------------------+---------+------+-------------+
   ```

3. Создайте проект. Например:

   ```
   # openstack --insecure project create --domain b41c5bd8ca1e43f19f9720390c2869d5
   testproject
   ```

4. Чтобы установить и обновить квоты проекта, авторизуйтесь в новом проекте. Например:

   ```
   # export OS_PROJECT_NAME=testproject
   ```

5. Установите квоту для проекта с помощью команды openstack quota set:
   - Чтобы ограничить количество виртуальных процессоров, используйте параметр --cores. Например, чтобы ограничить количество виртуальных ЦП до 128, запустите команду:

     ```
     # openstack --insecure quota set --cores 128 testproject
     ```

   - Чтобы ограничить объем оперативной памяти, используйте параметр --ram. Например, чтобы ограничить объем оперативной памяти до 100 ГБ, запустите команду:

     ```
     # openstack --insecure quota set --ram 102400 testproject
     ```

- Чтобы ограничить размер дискового пространства, укажите политику с параметром --volume-type и необходимое пространство с параметром --gigabytes. Например, чтобы ограничить размер дискового пространства для политики хранения default до 1 ТиБ, запустите команду:

  ```
  # openstack --insecure quota set --volume-type default --gigabytes 1024 testproject
  ```

- Чтобы ограничить количество плавающих IP-адресов, используйте параметр --floating-ips. Например, чтобы ограничить количество плавающих IP-адресов до 128, запустите команду:

  ```
  # openstack --insecure quota set --floating-ips 128 testproject
  ```

- Чтобы ограничить количество кластеров Kubernetes, сначала получите идентификатор проекта, а затем используйте команду coe quotas create с параметрами --resource и --hard-limit. Например, чтобы ограничить количество кластеров Kubernetes до 10, запустите команды:

  ```
  # openstack --insecure federation project list
  +----------------------------------+-----------+---------+-------------+
  | ID                               | Domain ID | Enabled | Name        |
  +----------------------------------+-----------+---------+-------------+
  | d746acd8b2e847c4925685b8ad95b828 | b41c<...> | True    | testproject |
  +----------------------------------+-----------+---------+-------------+
  # openstack --insecure coe quotas create --project-id d746acd8b2e847c4925685b8ad95b828
  \
  --resource Cluster --hard-limit 10
  ```

- Чтобы ограничить количество балансировщиков нагрузки, используйте команду loadbalancer quota set с параметром --loadbalancer. Например, чтобы ограничить количество балансировщиков нагрузки до 20, запустите команду:

  ```
  # openstack --insecure loadbalancer quota set testproject --loadbalancer 20
  ```

Проверьте примененные квоты проекта, запустив команду:

```
# openstack --insecure quota show
```

Изменения, вносимые в квоты проекта, также отражаются в панели администратора.

7.1.4.9 Назначение пользователей нескольким доменам

С помощью инструмента vinfra системные администраторы могут создавать пользователей специальных служб, которые могут использоваться сторонними приложениями для доступа к API вычислений с правами администратора. Эти пользователи не могут войти в административную панель или панель самообслуживания. Пользователи службы аналогичны системным администраторам с разрешением **Вычисления**: они существуют только в домене **По умолчанию** и могут просматривать и управлять всеми объектами в вычислительном кластере, включая вычислительные узлы. Вы можете назначать пользователей службы доменам, что дает им

возможность создавать вычислительные объекты в проектах этих назначенных доменов (например, создавать виртуальные машины из резервной копии).

Пользователи службы могут просматривать виртуальные машины во всех существующих проектах, указав параметр запроса all_tenants для запроса GET /servers (см. документацию OpenStack API).

Предварительные требования

- Для авторизации выполнения приведенных ниже команд настроен клиент командной строки OpenStack, как описано в разделе "Подключение к интерфейсу командной строки OpenStack" на странице 427.

Назначение пользователя службы домену

Используйте следующую команду:

```
vinfra domain user create --domain default --assign-domain <domain> compute <username>
```

--assign-domain <domain>

ID или имя домена, на который следует назначить пользователя сервиса

<username>

Имя пользователя службы

Например, чтобы создать пользователя службы my-service-user и назначить его доменам mydomain и mydomain2, запустите команду:

```
# vinfra domain user create my-service-user --domain default --assign-domain mydomain compute \
--assign-domain mydomain2 compute
```

Чтобы убедиться, что созданный пользователь службы успешно назначен двум доменам, используйте клиент OpenStack. Например, если IP-адрес узла управления – это 10.136.16.227, используйте команду:

```
# openstack --insecure --os-username my-service-user --os-user-domain-name \
Default --os-auth-url=https://10.136.16.227:5000/v3 federation domain list
Password:
+----------------------------------+---------+-----------+-------------+
| ID                               | Enabled | Name      | Description |
+----------------------------------+---------+-----------+-------------+
| 2929ff42b1e64884a05dea3011862aed | True    | mydomain  |             |
| 7e0d54797152424a9331ae904e220b88 | True    | mydomain2 |             |
+----------------------------------+---------+-----------+-------------+
```

Вы также можете просмотреть список всех проектов в назначенных доменах с помощью этой команды:

```
openstack --insecure --os-username <username> --os-user-domain-name Default --os-auth-
url=https://<MN_IP_address>:5000/v3 federation project list
```

Отмена назначения пользователя службы домену

Используйте параметр --unassign-domain <domain> для команды vinfra domain user set.

```
vinfra domain user set --domain default --unassign-domain <domain> <username>
```

--unassign-domain <domain>

ID или имя домена, для которого требуется отменить назначение пользователя службы

<username>

Имя пользователя службы

Например, чтобы отменить назначение пользователя службы my-service-user домену mydomain, запустите команду:

```
# vinfra domain user set my-service-user --domain default --unassign-domain mydomain
```

7.1.4.10 Управление свойствами домена

Создание списка свойств для домена

Используйте следующую команду:

```
vinfra domain properties create --key <key> --data <data>
                        [--access <access>] <domain>
```

--key <key>

Имя ключа.

--data <data>

Список свойств в виде объекта JSON.

--access <access>

Тип доступа:

- pub: разрешить доступ для чтения всем пользователям (проверка подлинности не требуется).
- auth: разрешить доступ для чтения авторизованным пользователям.
- domain: разрешить доступ для чтения пользователям домена.

У суперадминистратора и администратора домена есть доступ для записи.

<domain>

Имя или идентификатор домена.

Например, чтобы создать список свойств с ключом myproperty, доступный всем пользователям, выполните:

```
# vinfra domain properties create --key myproperty mydomain \
--data '{"key1": "value1", "key2": "value2"}' --access pub
Operation successful.
```

Созданный список свойств появится в выводе команды vinfra domain properties keys list:

```
# vinfra domain properties keys list
+----------+--------------------+
| domain   | keys               |
+----------+--------------------+
| mydomain | - allow_live_resize |
|          | - myproperty       |
| Default  | - allow_live_resize |
+----------+--------------------+
```

Отображение подробных данных о списке свойств домена

Используйте следующую команду:

```
vinfra domain properties show --key <key> <domain>
```

--key <key>

Имя ключа.

<domain>

Имя или идентификатор домена.

Например, чтобы вывести подробные сведения о списке свойств с ключом myproperty, выполните:

```
# vinfra domain properties show --key myproperty mydomain
+--------+--------------+
| Field  | Value        |
+--------+--------------+
| data   | key1: value1 |
|        | key2: value2 |
| domain | mydomain     |
| key    | myproperty   |
+--------+--------------+
```

Обновление прав доступа к списку свойств домена

Используйте следующую команду:

```
vinfra domain properties access set [--access <access>]
                                    [--key <key>] <domain>
```

--key <key>

Имя ключа.

--access <access>

Тип доступа:

- pub: разрешить доступ для чтения всем пользователям (проверка подлинности не требуется).
- auth: разрешить доступ для чтения авторизованным пользователям.
- domain: разрешить доступ для чтения пользователям домена.

У суперадминистратора и администратора домена есть доступ для записи.

<domain>

Имя или идентификатор домена.

Например, чтобы предоставить доступ для чтения к списку свойств с ключом myproperty только пользователями домена, выполните:

```
# vinfra domain properties access set --key myproperty mydomain --access domain
Operation successful.
```

Обновление списка свойств домена

Используйте следующую команду:

```
vinfra domain properties update --key <key> --data <data>
                                [--access <access>] <domain>
```

--key <key>

Имя ключа.

--data <data>

Список свойств в виде объекта JSON.

--access <access>

Тип доступа:

- pub: разрешить доступ для чтения всем пользователям (проверка подлинности не требуется).
- auth: разрешить доступ для чтения авторизованным пользователям.
- domain: разрешить доступ для чтения пользователям домена.

У суперадминистратора и администратора домена есть доступ для записи.

<domain>

Имя или идентификатор домена.

Например, чтобы обновить список свойств с ключом myproperty, выполните:

```
# vinfra domain properties update --key myproperty mydomain \
--data '{"key1": "value1", "key2": "value2"}'
Operation successful.
```

Удаление списка свойств домена

Используйте следующую команду:

```
vinfra domain properties delete --key <key> <domain>
```

--key <key>

Имя ключа.

<domain>

Имя или идентификатор домена.

Например, чтобы удалить список свойств с ключом myproperty, выполните:

```
# vinfra domain properties delete --key myproperty mydomain
Operation successful.
```

7.1.5 Настройка панели самообслуживания

После предоставления доступа к панели самообслуживания можно настроить ее виртуальный IP-адрес и тему фирменной символики.

Предварительные требования

- Порт для доступа к панели самообслуживания открыт в соответствии с инструкциями в разделе "Обеспечение доступа к панели самообслуживания" на странице 190.

7.1.5.1 Изменение IP-адреса панели самообслуживания

Если создана конфигурация высокого уровня доступности для сервера управления, виртуальный IP-адрес можно изменить на панели самообслуживания.

Ограничения

- Виртуальный IP-адрес нельзя изменить, если тип трафика **Панель самообслуживания** назначен наряду с типами трафика **API вычислений** или **Управление системными сервисами** одной и той же сети. В этом случае необходимо удалить конфигурацию высокого уровня доступности сервера управления и повторно создать ее с указанием нужного IP-адреса.

Предварительные требования

- Конфигурация высокой доступности создана в соответствии с инструкциями в разделе "Включение высокой доступности сервера управления" на странице 146.

Чтобы изменить виртуальный IP-адрес панели самообслуживания

1. На экране **Настройки** > **Системные настройки** > **Самообслуживание** щелкните **Изменить** рядом с полем **Виртуальный IP-адрес**.
2. В окне **Изменить виртуальный IP-адрес** введите нужный IP-адрес и нажмите кнопку **Сохранить**.

7.1.5.2 Настройка фирменной символики для панели самообслуживания

Для пользовательского интерфейса панели самообслуживания можно установить тему в собственном фирменном стиле. Тема фирменной символики включает наименование продукта, значок веб-сайта, логотипы и цветовую схему панели.

Доступны следующие темы фирменной символики:

- **Стандартная** – тема, которая по умолчанию настроена и применяется ко всем доменам. Чтобы изменить тему, перейдите на экран **Настройки** > **Системные настройки** > **Самообслуживание**. Чтобы отменить изменения, внесенные в стандартную тему, выполните сброс настроек.
- **Персональная** – пользовательская тема, которая настраивается отдельно для каждого домена. Чтобы внести изменения в тему, перейдите на экран **Настройки** > **Тема фирменной символики**. Чтобы применить к домену стандартный тему, сбросьте настройки персональной темы до настроек по умолчанию.

Чтобы настроить тему фирменной символики

- В разделе **Заголовок продукта** нажмите значок карандаша, чтобы изменить заголовок, отображаемый на вкладке портала самообслуживания в веб-браузере. В открывшемся окне укажите заголовок продукта и нажмите **Сохранить**.
- В разделе **Значок веб-сайта** нажмите **Загрузить** или отображаемое изображение, чтобы загрузить пиктограмму веб-сайта для панели самообслуживания, и выберите файл изображения в формате PNG или ICO. Изображение должно иметь размеры 32 × 32 пикселя.

- В разделе **Логотипы** загрузите две версии одного логотипа: с выравниванием по левому краю и по центру.
  1. В разделе **Логотип для заголовка** нажмите **Загрузить** или щелкните по изображению и укажите версию логотипа с выравниванием по левому краю. Это изображение будет использоваться в заголовке панели.
  2. В разделе **Логотип для экрана входа** нажмите **Загрузить** или изображение и укажите логотип с выравниванием по центру. Это изображение будет использоваться на экране входа.

  Изображения должны иметь размеры 256 × 64 пикселя и объем до 2 МБ. Поддерживаются следующие форматы изображений: PNG, JPG или SVG. При использовании формата PNG рекомендуется прозрачный фон.
- В разделе **Цветовая схема** нажмите **Изменить**, чтобы выбрать цветовую схему для панели самообслуживания. В открывшемся окне выберите нужную цветовую схему и нажмите кнопку **Применить**.

Чтобы сбросить настройки темы фирменной символики

Щелкните **Вернуть к исходному виду** рядом с полем **Тема фирменной символики** и щелкните **Сбросить** в окне подтверждения.

После сброса для стандартной темы фирменной символики будут использоваться стандартные настройки и персональная тема фирменной символики будет заменена на стандартную.

7.1.6 Управление безопасностью

В соответствии с требованиями безопасности можно настроить доступ SSL к панели администрирования и шифрование данных для разных уровней, а также защищенный административный доступ к серверам кластера с помощью SSH.

7.1.6.1 Доступ к панели администрирования через SSL

При настройке инфраструктуры и сервисов продукта Кибер Инфраструктура может потребоваться ввести конфиденциальную информацию, например: данные учетных записей пользователей и электронной почты, сервисов S3 и т. п. По умолчанию система использует предварительно созданный самозаверяющий сертификат, но вы можете загрузить вместо него сертификат, выданный доверенным центром сертификации.

Ограничения

- Можно загрузить SSL-сертификат перед созданием кластера высокой доступности. Однако если позже вы создадите кластер высокого уровня доступности, панель администрирования переместится на выбранный виртуальный IP-адрес. В случае если SSL-сертификат был выдан для текущего IP-адреса панели администрирования, потребуется получить новый сертификат, выданный для виртуального IP-адреса. Если сертификат был выдан для доменного имени, убедитесь, что это доменное имя разрешается в виртуальный IP-адрес.

- Если вы получили SSL-сертификат от промежуточного центра сертификации (ЦС), у вас должен быть сертификат конечного пользователя наряду с пакетом ЦС, содержащим корневой и промежуточные сертификаты. Чтобы можно было использовать эти сертификаты, сначала необходимо объединить их в цепочку. Цепочка сертификатов включает в себя сертификат конечного пользователя, сертификаты промежуточных ЦС и сертификат доверенного корневого ЦС. В данном случае SSL-сертификат может быть доверенным только в том случае, если каждый сертификат в цепочке надлежащим образом выпущен и действителен.

  Например, если у вас имеется сертификат конечного пользователя, два сертификата промежуточных ЦС и сертификат корневого ЦС, создайте новый файл сертификата и добавьте в него все сертификаты в следующем порядке:

```
# End-user certificate issued by the intermediate CA 1
-----BEGIN CERTIFICATE-----
MIICiDCCAg2gAwIBAgIQNfwmXNmET8k9Jj1X<...>
-----END CERTIFICATE-----
# Intermediate CA 1 certificate issued by the intermediate CA 2
-----BEGIN CERTIFICATE-----
MIIEIDCCAwigAwIBAgIQNE7VVyDV7exJ9ON9<...>
-----END CERTIFICATE-----
# Intermediate CA 2 certificate issued by the root CA
-----BEGIN CERTIFICATE-----
MIIC8jCCAdqgAwIBAgICZngwDQYJKoZIhvcN<...>
-----END CERTIFICATE-----
# Root CA certificate
-----BEGIN CERTIFICATE-----
MIIDODCCAiCgAwIBAgIGIAYFFnACMA0GCSqG<...>
-----END CERTIFICATE-----
```

Чтобы загрузить SSL-сертификат

Панель администратора

1. На вкладке **Настройки** > **Сервер управления** > **Доступ по SSL** нажмите **Загрузить**.
2. Загрузите SSL-сертификат, выданный для текущего IP-адреса панели администрирования.
3. Загрузите закрытый ключ. Эта опция отображается после загрузки действительного сертификата.
4. Нажмите **Сохранить**.

Загруженный сертификат будет добавлен в конфигурацию веб-сервера, на котором размещается панель администрирования, и вы сможете получить к нему доступ по протоколу HTTPS.

Также можно создать новый самозаверяющий сертификат вместо используемого по умолчанию. Однако он не будет доверенным, и вам потребуется вручную принять его в браузере.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster settings ssl set (--self-signed | --cert-file <cert_file>) [--key-file <key_file>] [--password]
```

--self-signed

Создать новый самозаверяющий сертификат

--cert-file <cert_file>

Путь к файлу с новым сертификатом

--key-file <key_file>

Путь к файлу с закрытым ключом (используется только с параметром --cert-file)

--password

Прочитать пароль сертификата из стандартного ввода (используется только с параметром --cert-file)

Например, чтобы загрузить SSL-сертификат из файлов cert.pem и key.pem, выполните:

```
# vinfra cluster settings ssl set --cert-file cert.pem --key-file key.pem
```

Просмотреть загруженный сертификат можно в выводе команды vinfra cluster settings ssl show:

```
# vinfra cluster settings ssl show
+-------------+-------+
| Field       | Value |
+-------------+-------+
| is_valid    | True  |
| self_signed | False |
| ssl         | True  |
+-------------+-------+
```

7.1.6.2 Обеспечение административного доступа к серверам кластера через SSH

В некоторых ситуациях вам или службе технической поддержки может потребоваться административный доступ (root) к серверам кластера через SSH. Рекомендуем использовать SSH-ключи, поскольку они в целом более безопасны, чем пароли. Можно создать пару ключей на клиенте, с которого вы будете подключаться к серверам через SSH. Закрытый ключ будет храниться на клиенте. Никому не передавайте закрытый ключ в целях безопасности. Открытый ключ необходимо будет загрузить в продукт Кибер Инфраструктура.

После загрузки ключа можно будет получать доступ к серверам кластера с помощью способа проверки подлинности на основе ключа SSH. При подключении через SSH следуйте этим правилам.

- Не используйте сторонние репозитории. Установка программного обеспечения должна осуществляться только из репозитория по умолчанию.
- Используйте только команды, разрешенные в документации продукта.

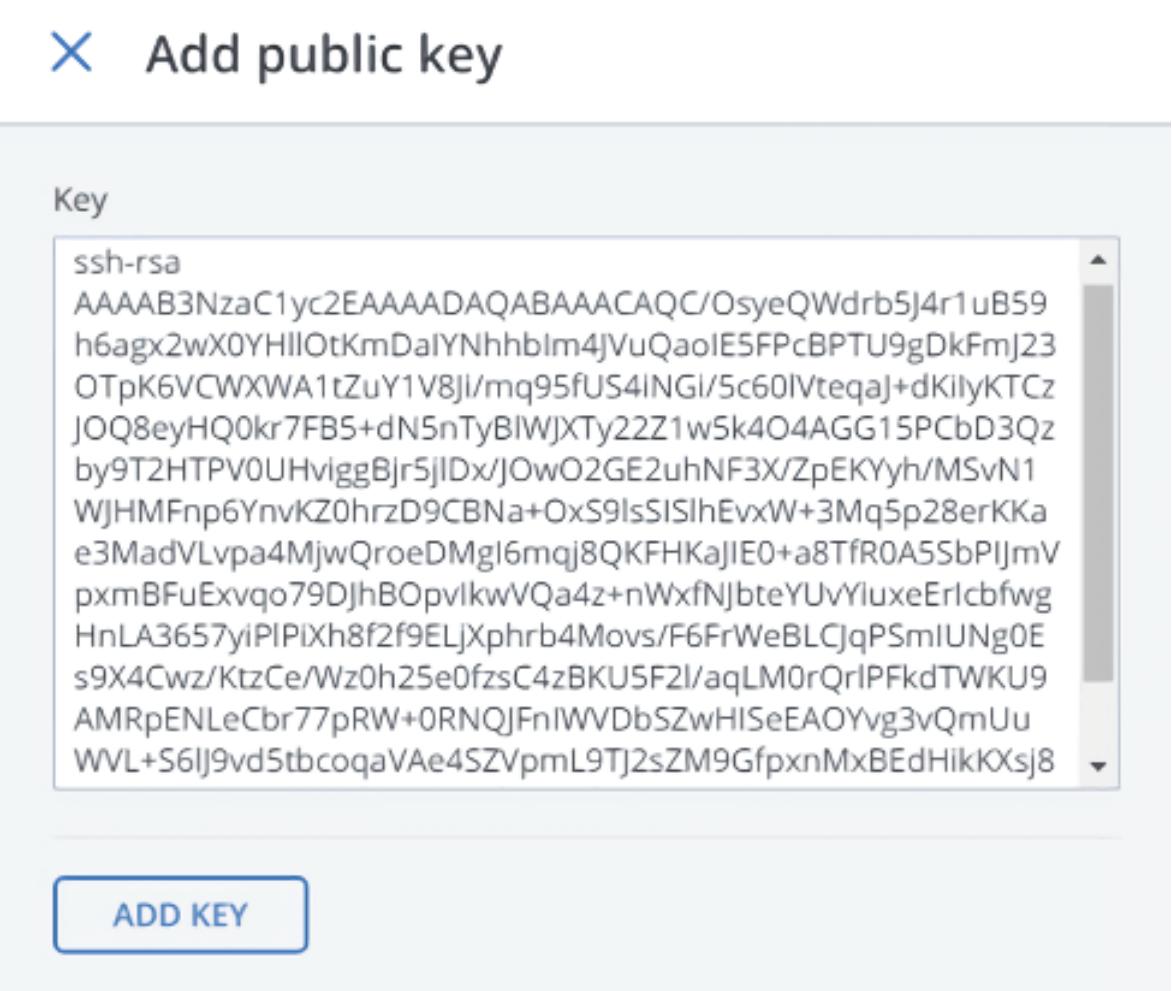
Чтобы создать и загрузить открытый ключ

Панель администратора

1. Получите открытый SSH-ключ от службы технической поддержки или создайте пару SSH-ключей на клиенте с помощью утилиты ssh-keygen.

   ```
   # ssh-keygen -t rsa
   ```

   По умолчанию созданный открытый ключ находится в /root/.ssh/id_rsa.pub.
2. Откройте экран **Настройки** > **Безопасность** > **SSH** и нажмите **Добавить**.
3. На панели **Добавить открытый ключ** вставьте скопированный ключ и нажмите **Добавить ключ**.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster sshkey add <file>
```

<file>

Файл открытого ключа SSH

Например, чтобы добавить открытый ключ SSH, содержащийся в файле mykey.pub, в список доверенных ключей, выполните:

```
# vinfra cluster sshkey add id_rsa.pub
```

Добавленный открытый ключ SSH появится в выводе команды vinfra cluster sshkey list:

```
# vinfra cluster sshkey list
+--------------------+---------------------------------+-----------------+
| id                 | key                             | label           |
+--------------------+---------------------------------+-----------------+
| 8ccf7f1b-6a53-<...> | ssh-rsa AAAAB3NzaC1yc2EAAAA<...> | user@example.com |
|                    | user@example.com                |                 |
+--------------------+---------------------------------+-----------------+
```

Чтобы удалить открытый ключ

Панель администратора

1. Откройте экран **Настройки** > **Безопасность** > **SSH**, выберите открытый ключ и нажмите **Удалить**.
2. Нажмите **Да** в окне подтверждения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster sshkey delete <sshkey>
```

<sshkey>
: Идентификатор открытого ключа

Например, чтобы удалить открытый ключ SSH с идентификатором 8ccf7f1b-6a53-4d74-99ce-c410d51a9921, выполните:

```
# vinfra cluster sshkey delete 8ccf7f1b-6a53-4d74-99ce-c410d51a9921
```

7.1.6.3 Включение шифрования данных

Кибер Инфраструктура может шифровать данные, хранящиеся на дисках, по стандарту AES-256, чтобы защитить их в случае потери или кражи диска. Кибер Инфраструктура хранит ключи шифрования дисков в метаданных кластера (MDS).

Шифрование можно включить или отключить только для новых создаваемых сервисов фрагментов данных (CS). После включения шифрования уровня можно выполнять дешифровку дисков (сервисов CS) путем высвобождения их вручную из шифрованных уровней. Соответственно, простое включение шифрования на уровне диска не шифрует его данные (CS). Чтобы зашифровать диск, его нужно назначить на шифрованный уровень.

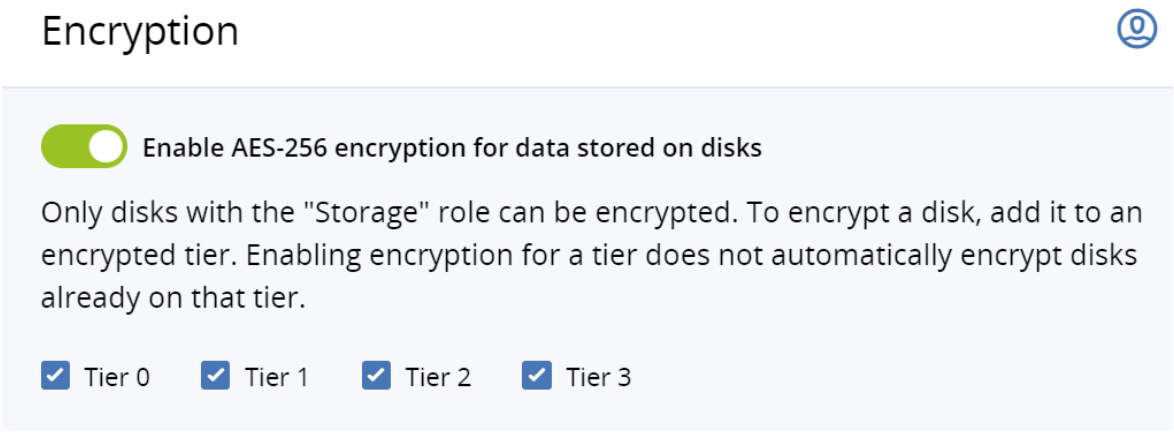
Ограничения

- Кибер Инфраструктура не шифрует данные, передаваемые по внутренней сети.
- Включенное шифрование слегка снижает производительность.

Чтобы включить шифрование уровней

Панель администратора

1. Перейдите в раздел **Настройки** > **Системные настройки** > **Шифрование**.
2. Установите флажок **Включить шифрование AES-256 для данных на диске**.
3. Выберите уровни, которые следует шифровать, и нажмите **Сохранить**.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster settings encryption set [--tier-enable {0,1,2,3}] [--tier-disable {0,1,2,3}]
```

--tier-enable {0,1,2,3}
: Включить шифрование для уровней хранения данных. Этот параметр можно указывать несколько раз.

--tier-disable {0,1,2,3}
: Выключить шифрование для уровней хранения данных. Этот параметр можно указывать несколько раз.

Например, чтобы включить шифрование для уровня хранения 2, выполните:

```
# vinfra cluster settings encryption set --tier-enable 2
```

Посмотреть статус шифрования для каждого уровня хранения можно в выводе команды vinfra cluster settings encryption show:

```
# vinfra cluster settings encryption show
+-------+-------+
| Field | Value |
```

```
+-------+-------+
| tier0 | False |
| tier1 | False |
| tier2 | True  |
| tier3 | False |
+-------+-------+
```

7.1.7 Управление лицензиями

Кибер Инфраструктура поставляется с пробной лицензией, позволяющей ознакомиться с возможностями продукта. У пробной лицензии нет даты окончания срока действия, но емкость хранилища ограничена до 1 ТБ.

Кибер Инфраструктура поддерживает следующие модели лицензирования для производственных сред:

- Лицензионный ключ. В зависимости от модели выделения ресурсов ключи действуют ограниченное время (подписка) или бессрочно и предоставляют определенную емкость хранилища. Если уже установлена коммерческая лицензия, ключ увеличивает срок действия или лимит хранилища.
- Лицензионное соглашение с поставщиком услуг (SPLA). Соглашение SPLA реализует модель оплаты по факту использования: оно предоставляет неограниченную емкость хранилища, а с клиентов взимается плата за фактическое использование этих ресурсов. С соглашением SPLA продукт Кибер Инфраструктура автоматически отправляет отчеты в Кибер Бэкап Облачный каждые четыре часа. Лицензия отображается со сроком действия в две недели, который отсчитывается от последнего отправленного отчета и продляется после каждого отчета. Если в течение двух недель не было получено ни одного отчета, действие лицензии заканчивается. Чтобы отчеты достигали места назначения, кластер должен иметь доступ к центру обработки данных, который использовался для включения SPLA. Убедитесь, что TCP-порт 443 открыт.

  Примечание
  Лицензия SPLA действительна для облачных партнеров. Если соглашение SPLA включено, шлюз Backup Gateway можно подключить только к Кибер Бэкап Облачный, но не к Кибер Бэкап. Для подключения Backup Gateway к этим продуктам потребуется использовать лицензионные ключи. Кроме того, использование Cyber Backup Gateway не учитывается в соглашении SPLA для продукта Кибер Инфраструктура. SPLA учитывает только универсальное использование, которое не связано с резервным копированием. Использование резервного копирования отображается в разделе Кибер Бэкап Облачный в Кибер Бэкап Облачный.

Модель лицензирования можно переключить в любой момент.

- Переключение режима лицензирования (например, с лицензионного ключа на SPLA или с подписки на бессрочную лицензию) прекращает действие ранее использовавшегося ключа, даже если его срок еще не истек. Ключи, действие которых прекращено, нельзя использовать повторно.

- Переключение с соглашения SPLA на лицензионный ключ изменяет модель лицензирования на подписку или бессрочную лицензию. После этого попросите поставщика услуг прекратить действие вашего соглашения SPLA, отключив приложение Кибер Инфраструктура для вашей учетной записи либо удалив учетную запись.

Внимание
Если срок действия лицензии истечет, все операции записи в кластер хранилища данных остановятся до тех пор, пока не будет установлена действующая лицензия.

Ограничения

- Выделение пространства для хранилища блочных данных, которое используется LUN iSCSI и вычислительными томами, осуществляется с частичным соблюдением принципов экономного распределения. После удаления данных неиспользуемое пространство не возвращается и помечается как используемое. Дополнительные сведения см. в разделе "Диаграмма «Логическое пространство»" на странице 732.

Предварительные требования

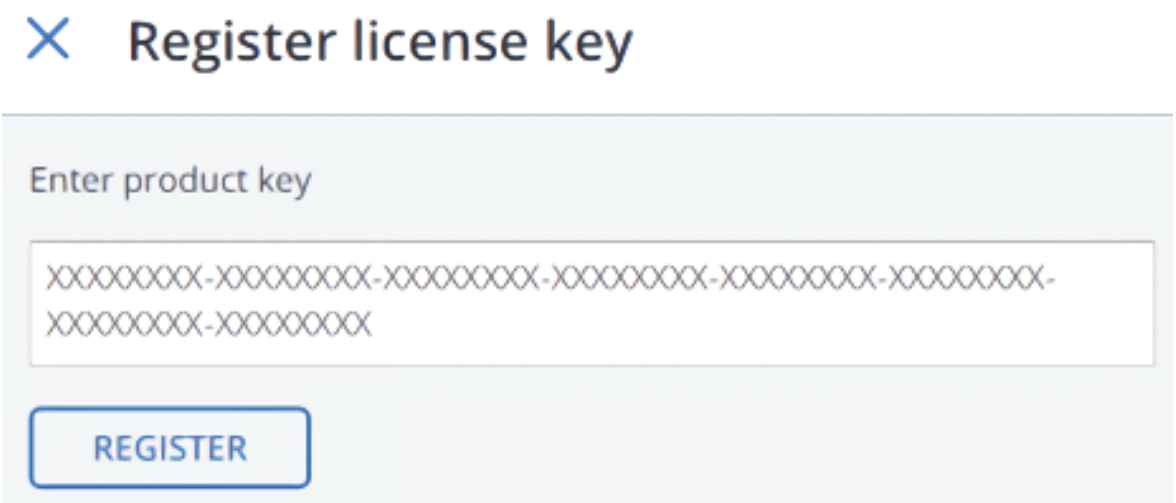
- Кластер хранилища должен быть создан в соответствии с указаниями из раздела "Развертывание кластера хранилища данных" на странице 141.

7.1.7.1 Установка лицензионных ключей

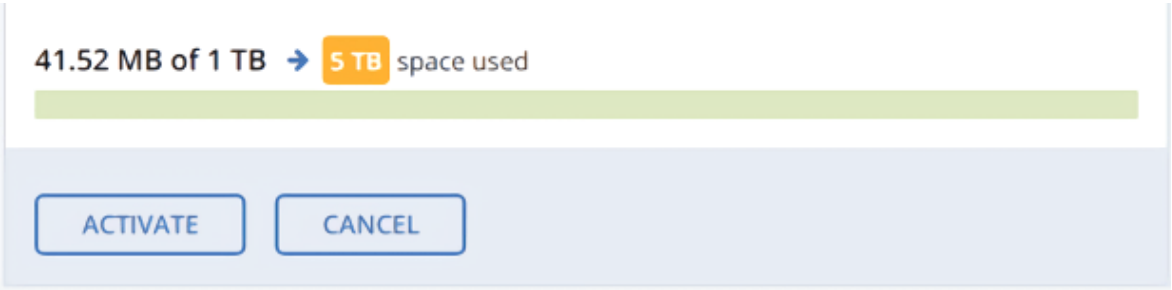
Чтобы установить лицензионный ключ

Панель администратора

1. В случае переключения с соглашения SPLA попросите поставщика услуг прекратить действие соглашения, отключив приложение Кибер Инфраструктура для вашей учетной записи либо удалив учетную запись.
2. На экране **Настройки** > **Лицензии** нажмите **Обновить**, а затем нажмите **Зарегистрировать ключ**.

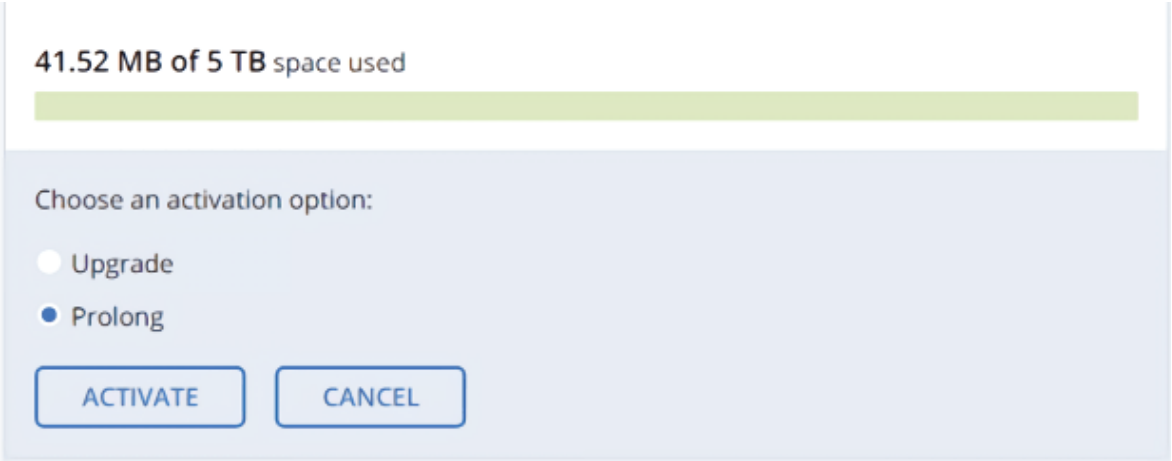


3. В окне **Зарегистрировать ключ лицензии** вставьте лицензионный ключ и нажмите **Зарегистрировать**.



4. Вернувшись на экран **Лицензии**, нажмите **Активировать**, если выполняется активация пробной версии, или выберите один из следующих вариантов:
   - **Обновить**, чтобы добавить емкость хранилища в активную лицензию.
   - **Продлить**, чтобы продлить лицензию с истекающим сроком действия.

   Затем нажмите **Активировать**.



Дата окончания срока действия или емкость хранилища изменится в соответствии с тем, что предоставляет ключ.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster license load --key <license-key> --type <license-type>
```

--key <license-key>

Регистрируемый лицензионный ключ. Введите этот параметр несколько раз, чтобы зарегистрировать сразу несколько ключей.

--type <license-type>

Тип лицензии (prolong – продление или upgrade – обновление)

Например, чтобы установить лицензию из ключа A38600-3P6W74-RZSK58-Y9ZH05-2X7J48, выполните:

```
# vinfra cluster license load --key A38600ML-3P6W746P-RZSK58BV-Y9ZH05Q5-2X7J48J6-KVRXRYPY-Z2FK7ZQ6-Y7FGZNYF \
--type upgrade
```

Получить подробные данные об установленной лицензии можно в выводе команды vinfra cluster license show:

```
# vinfra cluster license show
+------------+------------------------+
| Field      | Value                  |
+------------+------------------------+
| capacity   | 10995116277760         |
| expiration | 2021-01-10T12:42:00    |
| free_size  | 10973383165601         |
| spla       | registered: false      |
|            | registration_url: null |
| status     | active                 |
| total_size | 10995116277760         |
| used_size  | 21733112159            |
+------------+------------------------+
```

7.1.7.2 Установка лицензий SPLA

Предварительные требования

- Если включен контроль входа для веб-интерфейса Кибер Бэкап Облачный, убедитесь, что внешний IP-адрес кластера хранилища резервных копий добавлен в список разрешенных IP-адресов, как описано в Руководстве администратора партнера в разделе "Ограничение доступа к веб-интерфейсу".

Чтобы установить лицензию SPLA

1. На экране **Настройки** > **Лицензии** нажмите **Обновить**, а затем **Использовать SPLA**.
2. В окне **Использовать SPLA** выберите регион из раскрывающегося списка. Если вашего ЦОД нет в списке, просто введите его URL-адрес непосредственно в поле раскрывающегося списка. Затем нажмите **Активировать**. Вы будете перенаправлены на страницу входа Кибер Бэкап Облачный.

   Примечание
   Дополнительные сведения о центрах обработки данных см. в статье Список сервисов продукта Кибер Бэкап Облачный по каждому ЦОД.

3. Выполните вход в Кибер Бэкап Облачный.

4. В окне **Register cluster (Регистрация кластера)** примите лицензионное соглашение.
5. В окне подтверждения регистрации нажмите кнопку **Готово**.

   Зарегистрированный кластер отобразится в Кибер Бэкап Облачный. Вы сможете отслеживать использование его ресурсов и загружать отчеты.

7.1.8 Управление уведомлениями

В центре уведомлений хранятся и отображаются уведомления о последних заданиях текущего пользователя на панели управления. Уведомления отображаются только для заданий, выполненных во время текущего пользовательского сеанса, и очищаются после выхода пользователя.

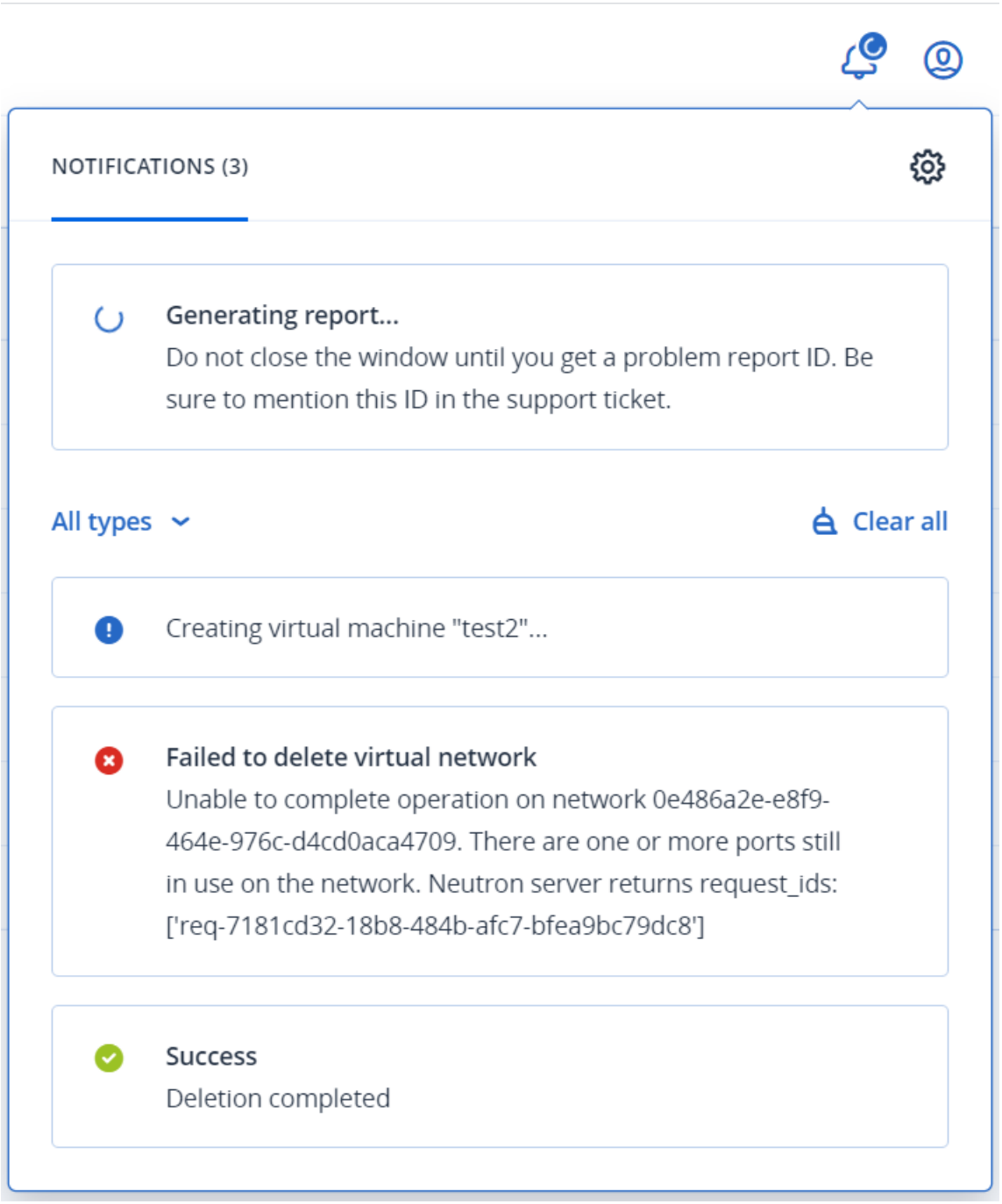
Пользователь информируется о каждом задании с помощью всплывающего уведомления в правом нижнем углу. Это же уведомление также отображается в центре уведомлений. После закрытия всплывающего окна уведомление будет доступно в центре уведомлений.

В следующей таблице описаны все поддерживаемые типы уведомлений.

Тип уведомления	Значок	Описание	Время отображения всплывающего окна	Срок хранения в центре уведомлений
Сведения		Уведомления о запуске заданий	3 секунд	10 минут
Успешно		Уведомления об успешно выполненных заданиях	3 секунд	10 минут
Error		Уведомления о заданиях, завершившихся ошибкой	10 секунд	50 минут
Выполняется		Длительные задания, такие как передача образа или создание отчета о проблеме	Время выполнения задания	Время выполнения задания

Как просмотреть уведомления

Нажмите значок колокольчика в правом верхнем углу.

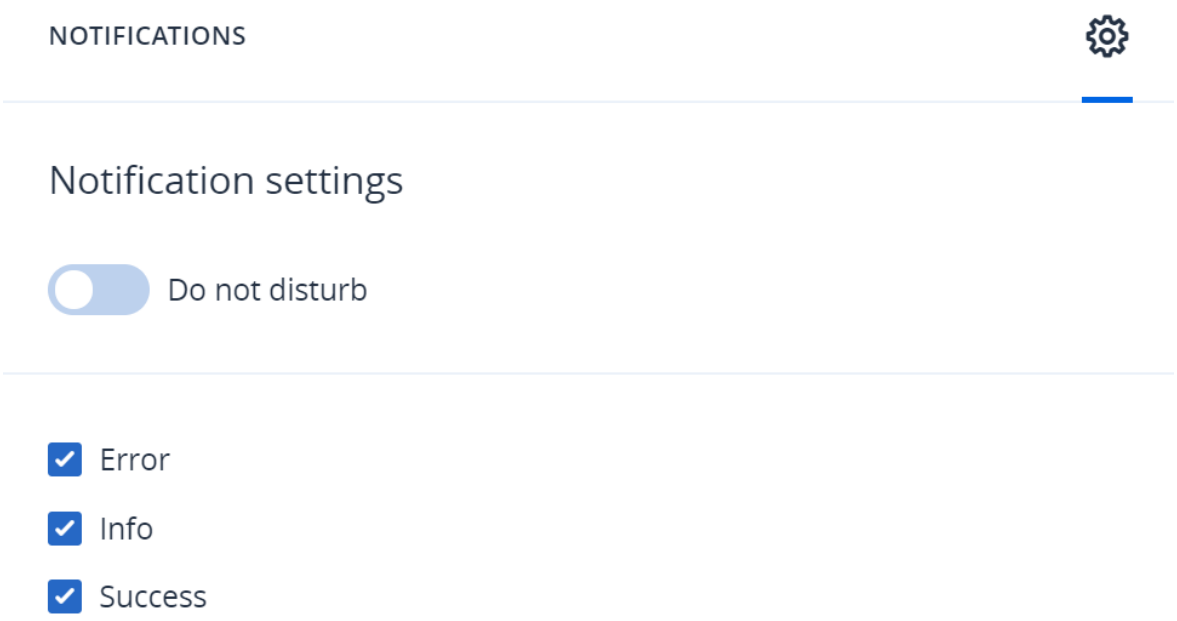


Рядом со значком колокольчика расположен счетчик уведомлений или значок загрузки, если в данный момент выполняется задание.

Как настроить уведомления

1. На любом экране щелкните по значку колокольчика в правом верхнем углу.
2. Щелкните по значку шестерни и выберите типы уведомлений, которые следует отображать в

центре уведомлений.



Как очистить уведомления

1. На любом экране щелкните по значку колокольчика в правом верхнем углу.
2. Чтобы удалить только одно уведомление, нажмите крестик рядом с ним.
3. Чтобы очистить все уведомления, нажмите **Очистить все** над списком уведомлений.

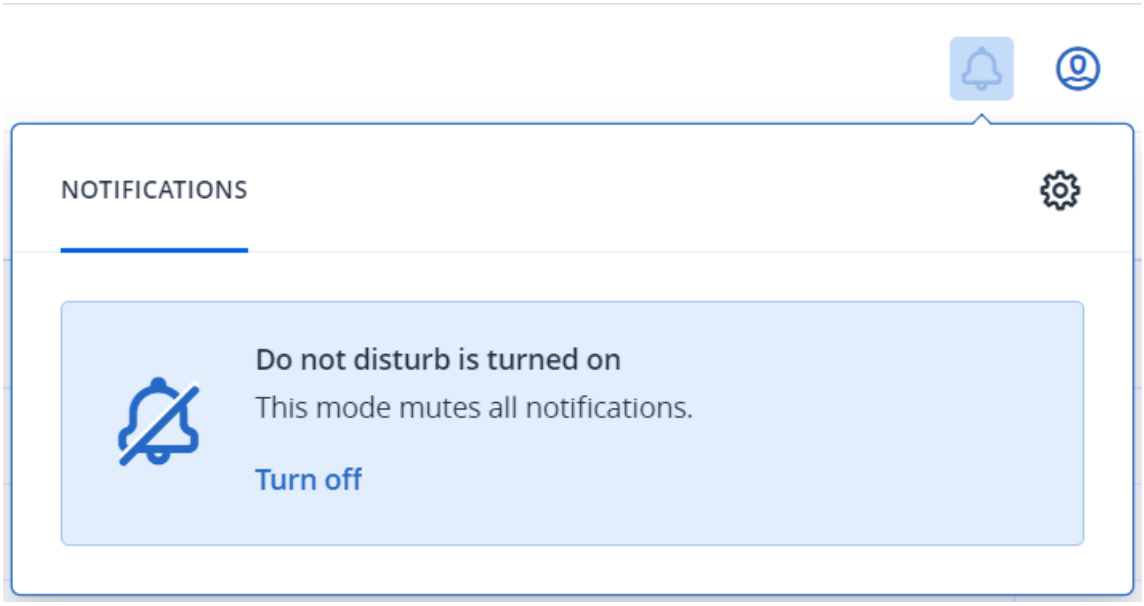
Как скрыть уведомления

1. На любом экране щелкните по значку колокольчика в правом верхнем углу.
2. Щелкните по значку шестерни и включите режим **Не беспокоить**.

Значок колокольчика станет серым, а счетчик уведомлений исчезнет. При этом последние уведомления по-прежнему будут доступны в центре уведомлений.

Как снова включить показ уведомлений

1. На любом экране щелкните по серому значку колокольчика в правом верхнем углу.
2. Нажмите **Отключить**, чтобы отключить режим **Не беспокоить**.



7.1.9 Отправка уведомлений по электронной почте

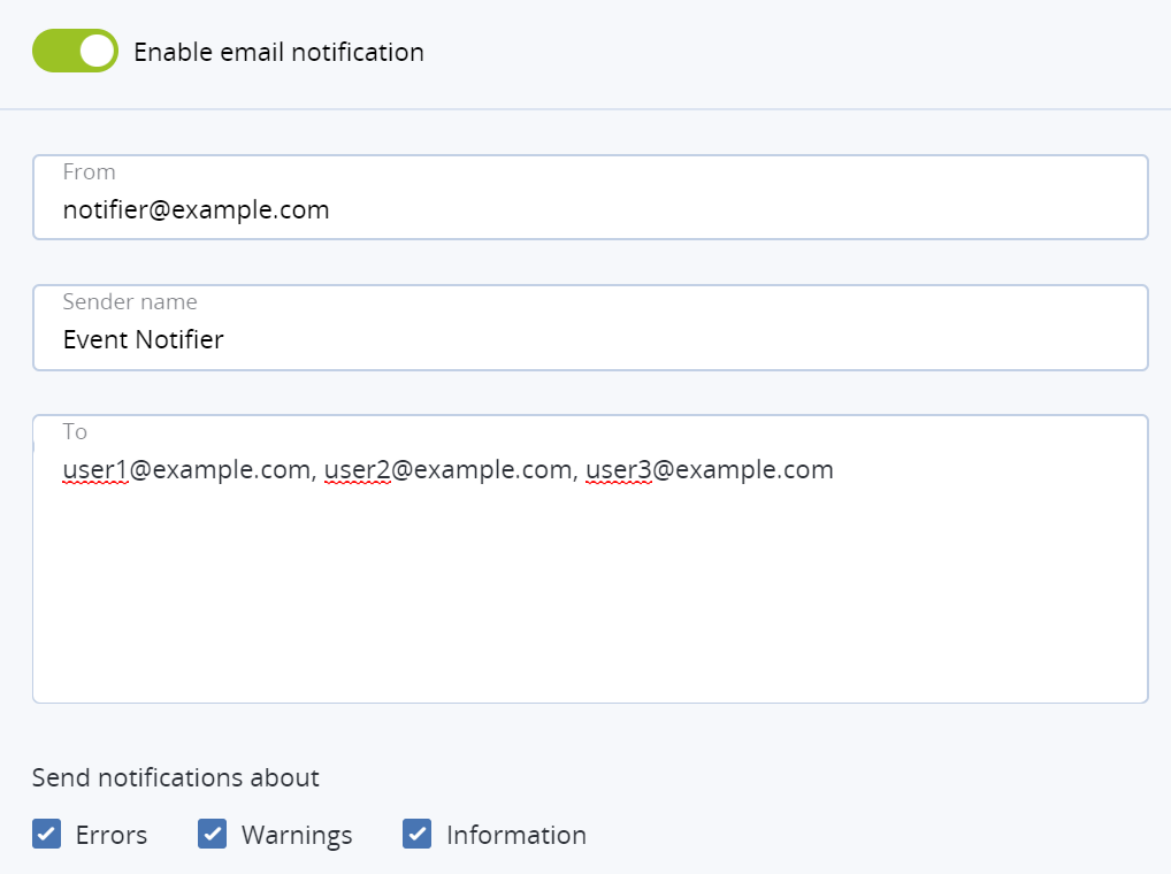
Кибер Инфраструктура может отправлять автоматические уведомления по электронной почте об ошибках, предупреждениях и оповещениях.

Ограничения

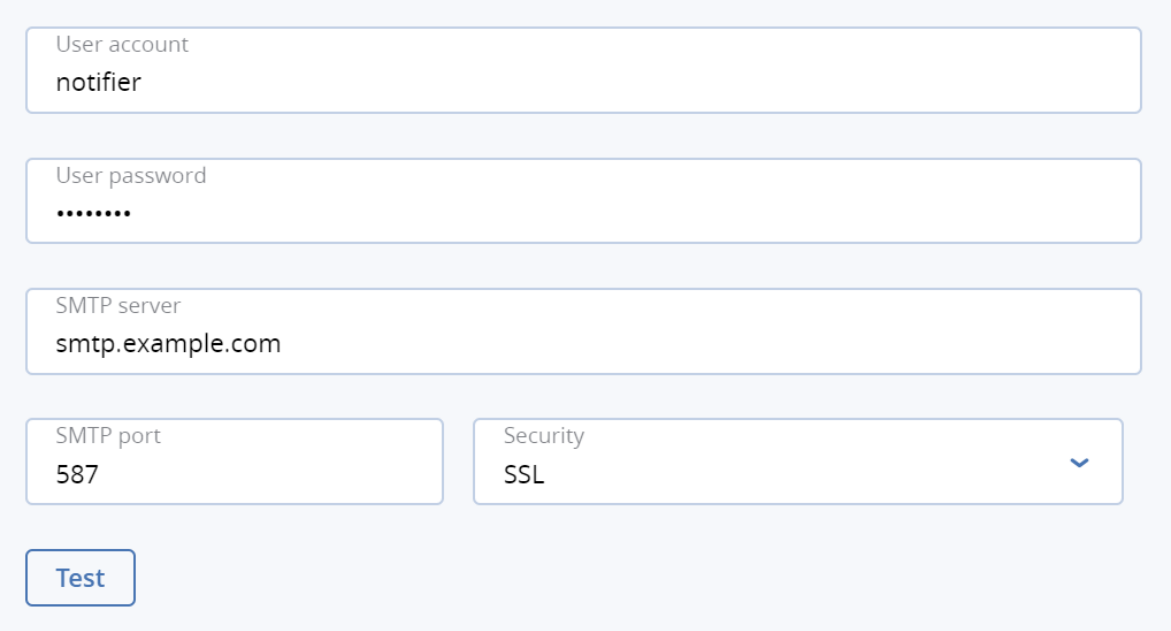
- Сервер управления должен иметь возможность доступа к SMTP-серверу.

Чтобы настроить уведомления по электронной почте

1. Перейдите в раздел **Настройки** > **Настройки системы** > **Уведомления** и установите переключатель **Включить уведомление по эл. почте**.
2. Укажите следующую информацию:
   a. В полях **От** и **Имя отправителя** введите адрес электронной почты и имя отправителя уведомления.
   b. В поле **Кому** введите один или несколько адресов электронной почты получателей через запятую.
3. Установите флажки для оповещений, о которых вы хотите получать уведомления.



4. Укажите сведения о сервере SMTP.
   a. В полях **Учетная запись пользователя** и **Пароль пользователя** учетные данные отправителя уведомления, зарегистрированного на SMTP-сервере.
   b. В поле **Сервер SMTP** введите доменное имя SMTP-сервера: публичное (например, **smtp.gmail.com**) либо внутреннее для вашей организации.
   c. При необходимости пользовательский **порт SMTP**, который используется сервером.
   d. В поле **Безопасность** протокол безопасности SMTP-сервера.



5. Чтобы отправить тестовое сообщение, нажмите **Проверка**.
6. Нажмите **Сохранить**.

7.1.10 Настройка параметров памяти для сервисов хранилища

Ограничения и гарантированные объемы памяти для сервисов хранилища можно настроить во время выполнения с помощью команд vinfra memory-policy vstorage-services. Это можно сделать для всего кластера или отдельного сервера.

Следующие параметры памяти можно настроить вручную:

- Гарантированный объем памяти
- Размер файла подкачки
- Кэш страниц, который, в свою очередь, задается с помощью множителя, минимального значения и максимального значения

Кэш страниц рассчитывается по следующей формуле:

```
$PAGE_CACHE = minimum <= ratio * $TOTAL_MEMORY <= maximum
```

Значения minimum и maximum – это «жесткие» ограничения, которые применяются, если значение ratio * $TOTAL_MEMORY выходит за эти пределы.

Чтобы лучше понять, как вычисляется размер кэша страниц, рассмотрите примеры в таблице.

Примеры кэша страниц

	Пример 1 (размер кэша в пределах ограничений)	Пример 2 (размер кэша равен минимальному)	Пример 3 (размер кэша равен максимальному)
Всего памяти	4 ГиБ	4 ГиБ	4 ГиБ
Множитель кэша	0,5	0,1	0,9
Минимальный кэш	1 ГиБ	2 ГиБ	1 ГиБ
Максимальный кэш	3 ГиБ	3 ГиБ	3 ГиБ
Размер кэша	2 ГиБ	2 ГиБ	3 ГиБ

Если параметры памяти заданы как для сервера, так и для кластера, применяются параметры для сервера. Если параметры памяти, настраиваемые вручную, отсутствуют, то управление памятью автоматически выполняется демоном vcmmd следующим образом:

- Каждый CS (например, диск хранилища) требует 512 МиБ ОЗУ для кэша страниц;
- Минимальный кэш страниц составляет 1 ГиБ;
- Если общий объем памяти меньше 48 ГиБ, то максимальный кэш страниц рассчитывается как две трети этого объема;
- Если общий объем памяти больше 48 ГиБ, то максимальный кэш страниц составляет 32 ГиБ.

Чтобы проверить текущие параметры памяти для сервисов хранилища, заданные демоном vcmmd, выполните следующую команду:

```
# vcmmdctl list
name                          type active guarantee    limit swap   cache
<...>
vstorage.slice/vstorage-services.sl... SRVC    yes   1310720 24522132    0 1048576
```

7.1.10.1 Настройка параметров памяти для кластера

Чтобы изменить параметры памяти сервисов хранилища для кластера

Выполните следующую команду:

```
vinfra memory-policy vstorage-services per-cluster change [--guarantee <guarantee>] [--swap
<swap>]
                                                          [--cache-ratio <cache-ratio> --cache-minimum <cache-minimum>
                                                          --cache-maximum <cache-maximum>]
```

Где:

--guarantee <guarantee>

Гарантированный объем в байтах

--swap <swap>

Размер файла подкачки в байтах или -1, если размер неограничен

--cache-ratio <cache-ratio>

Множитель кэша от 0 до 1 включительно

--cache-minimum <cache-minimum>

Минимальный размер кэша в байтах

--cache-maximum <cache-maximum>

Максимальный размер кэша в байтах

Например, чтобы задать параметры памяти сервисов хранилища для всех серверов в кластере, выполните следующую команду:

```
# vinfra memory-policy vstorage-services per-cluster change --guarantee 8796093022208 --swap
1099511627776 \
--cache-ratio 0.5 --cache-minimum 1099511627776 --cache-maximum 3298534883328
```

Эта команда задает параметры памяти сервисов хранилища для всех серверов в кластере следующим образом:

- Гарантируемый объем памяти – 8 ГБ;
- Размер файла подкачки – 1 ГБ;
- Ограничения кэша страниц: минимум – 1 ГБ, максимум – 3 ГБ, множитель кэша – 0,5.

Вы можете получить текущие значения параметров памяти сервисов хранилища для кластера в выходных данных команды vinfra memory-policy vstorage-services per-cluster show:

```
# vinfra memory-policy vstorage-services per-cluster show
+-----------+------------------------+
| Field     | Value                  |
+-----------+------------------------+
| cache     | maximum: 3298534883328 |
|           | minimum: 1099511627776 |
|           | ratio: 0.5             |
| guarantee | 8796093022208          |
| swap      | 1099511627776          |
+-----------+------------------------+
```

Чтобы сбросить параметры памяти сервисов хранилища до значений по умолчанию для кластера

Выполните следующую команду:

```
vinfra memory-policy vstorage-services per-cluster reset [--guarantee] [--swap] [--cache]
```

Где:

--guarantee

Сброс только гарантированного объема.

--swap

Сброс только размера файла подкачки.

--cache

Сброс только значений кэша.

Например, чтобы сбросить настроенные вручную ограничения кэша страниц до значений по умолчанию для всех серверов в кластере, выполните следующую команду:

```
# vinfra memory-policy vstorage-services per-cluster reset --cache
```

7.1.10.2 Настройка параметров памяти для сервера

Чтобы изменить параметры памяти сервисов хранилища для сервера

Выполните следующую команду:

```
vinfra memory-policy vstorage-services per-node change [--guarantee <guarantee>] [--swap
<swap>]
                                                       [--cache-ratio <cache-ratio> --cache-minimum <cache-minimum>
                                                       --cache-maximum <cache-maximum>] --node <node>
```

Где:

--guarantee <guarantee>

Гарантированный объем в байтах

--swap <swap>

Размер файла подкачки в байтах или -1, если размер неограничен

--cache-ratio <cache-ratio>

Множитель кэша от 0 до 1 включительно

--cache-minimum <cache-minimum>

Минимальный размер кэша в байтах

--cache-maximum <cache-maximum>

Максимальный размер кэша в байтах

--node <node>

Идентификатор сервера или имя хоста

Например, чтобы задать параметры памяти сервисов хранилища для сервера с именем хоста node001, выполните следующую команду:

```
# vinfra memory-policy vstorage-services per-node change --guarantee 8796093022208 --swap
1099511627776 --cache-ratio 0.5 \
--cache-minimum 1099511627776 --cache-maximum 3298534883328 --node node001
```

Эта команда задает параметры памяти сервисов хранилища для указанного сервера следующим образом:

- Гарантируемый объем памяти – 8 ГБ;
- Размер файла подкачки – 1 ГБ;
- Ограничения кэша страниц: минимум – 1 ГБ, максимум – 3 ГБ, множитель кэша – 0,5.

Вы можете получить текущие значения параметров памяти сервисов хранилища для сервера с именем хоста node001 в выходных данных команды vinfra memory-policy vstorage-services per-node show:

```
# vinfra memory-policy vstorage-services per-node show --node node001
+-----------+------------------------+
| Field     | Value                  |
+-----------+------------------------+
| cache     | maximum: 13194139533312 |
|           | minimum: 8796093022208  |
|           | ratio: 0.7              |
| guarantee | 8796093022208           |
| swap      | 1099511627776           |
+-----------+------------------------+
```

Чтобы сбросить параметры памяти сервисов хранилища до значений по умолчанию для сервера

Выполните следующую команду:

```
vinfra memory-policy vstorage-services per-node reset [--guarantee] [--swap] [--cache] --node
<node>
```

Где:

--guarantee
: Сброс только гарантированного объема.

--swap
: Сброс только размера файла подкачки.

--cache
: Сброс только значений кэша.

--node <node>
: Идентификатор сервера или имя хоста

Например, чтобы сбросить установленные вручную параметры памяти сервисов хранилища до значений по умолчанию для сервера с именем хоста node001, выполните следующую команду:

```
# vinfra memory-policy vstorage-services per-node reset --cache --node node001
```

7.1.11 Управление паролем кластера хранилища

Предварительные требования

- Создан кластер хранилища, как описано в разделе "Развертывание кластера хранилища данных" на странице 141.

Отображение пароля кластера хранилища

Используйте следующую команду:

```
vinfra cluster password show
```

Пример:

```
# vinfra cluster password show
+----------+----------+
| Field    | Value    |
+----------+----------+
| id       | 1        |
| name     | cluster1 |
| password | aR2oRG   |
+----------+----------+
```

Установка нового пароля кластера хранилища

Используйте следующую команду:

```
vinfra cluster password reset
```

Пример:

```
# vinfra cluster password reset
Password:
+----------+----------+
| Field    | Value    |
+----------+----------+
| id       | 1        |
| name     | cluster1 |
| password | 1q2w3e   |
+----------+----------+
```

7.1.12 Управление токенами

Токены используются для регистрации серверов в продукте Кибер Инфраструктура. В этом разделе описывается как создавать, просматривать и проверять токены.

Создание токена внутреннего хранилища

Панель администратора

1. На экране **Инфраструктура** > **Серверы** нажмите кнопку **Подключить сервер**.
2. В окне **Подключить сервер** нажмите **Сгенерировать новый токен**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node token create [--ttl <ttl>]
```

--ttl <ttl>

Время существования (TTL) токена в секундах

Например, чтобы создать токен со временем существования (TTL) 86 400 секунд, выполните:

```
# vinfra node token create --ttl 86400
+-------+---------------+
| Field | Value         |
+-------+---------------+
| host  | 10.37.130.101 |
| token | dc56d4d2      |
| ttl   | 86398         |
+-------+---------------+
```

Просмотр текущего токена внутреннего хранилища

Панель администратора

На экране **Инфраструктура** > **Серверы** нажмите кнопку **Подключить сервер**. В окне **Подключить сервер** будет отображен текущий токен внутреннего хранилища, а также дата и время окончания срока действия этого токена.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node token show
```

Например, чтобы вывести подробные данные о текущем токене, выполните:

```
# vinfra node token show
+-------+---------------+
```

```
| Field | Value        |
+-------+--------------+
| host  | 10.37.130.101 |
| token | dc56d4d2     |
| ttl   | 86398        |
+-------+--------------+
```

Проверка токена внутреннего хранилища

Используйте следующую команду:

```
vinfra node token validate <token>
```

<token>

Значение токена

Например, чтобы проверить токен dc56d4d2, выполните:

```
# vinfra node token validate dc56d4d2
+--------+-------+
| Field  | Value |
+--------+-------+
| status | valid |
+--------+-------+
```

7.1.13 Управление технологией Fast Path

Технология Fast Path ускоряет чтение данных из Хранилища. Она помогает, когда скорость ввода-вывода на серверах, использующих Хранилище, является узким местом. В предыдущих версиях Хранилища производительность могла быть ограничена тем, что ввод-вывод на серверах обрабатывался одним потоком в пространстве пользователя. В текущей версии Хранилища Fast Path используется по умолчанию, а ввод-вывод на серверах обрабатывается несколькими потоками в пространстве ядра. Это устраняет ненужные переключения контекста и улучшает производительность.

Если производительность ввода-вывода данных на сервере ограничена, эта технология в некоторых случаях может увеличить максимальную производительность чтения данных на сервере в три раза.

Примечание
Как правило, производительность ввода-вывода данных на серверах может представлять собой узкое место в кластерах с кэшем на твердотельных накопителях или в конфигурациях, состоящих только из твердотельных накопителей.

Для отключения технологии Fast Path выполните следующие шаги на каждом сервере:

Внимание
Настоятельно рекомендуется не выключать эту технологию в промышленных средах, за исключением случаев поиска и устранения проблем. Во всех остальных случаях эта технология должна быть включена.

1. Задайте параметру kdirect.enable значение 0 в конфигурационном файле /etc/vstorage/vstorage-mount.conf.
2. Переведите сервер в режим обслуживания и эвакуируйте все сервисы, расположенные на этом сервере, на другие серверы, как описано в разделе "Выполнение обслуживания сервера" на странице 805.
3. Остановите службу vstorage-ui-agent:

   ```
   # systemctl stop vstorage-ui-agent.service
   ```

4. Отсоедините Хранилище от сервера:

   ```
   # umount /vstorage/<cluster_name>
   ```

5. Снова запустите службу vstorage-ui-agent:

   ```
   # systemctl start vstorage-ui-agent.service
   ```

   Служба автоматически подключит Хранилище к серверу.
6. Верните сервер в рабочий режим.

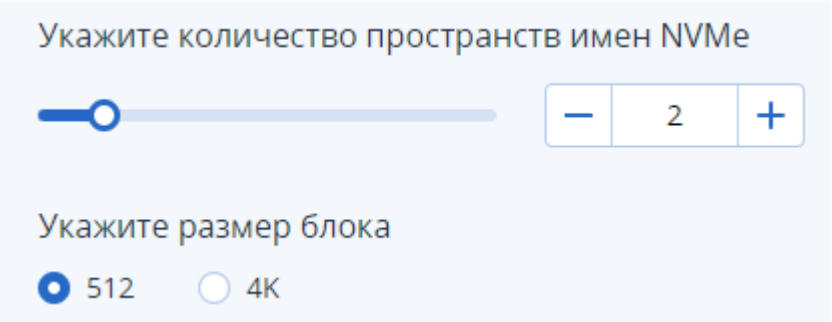
7.1.14 Настройка производительности дисков NVMe

Диски NVMe поддерживают функцию NVMe Namespaces (пространства имен), которая позволяет разделить один физический диск на несколько логических дисков меньшего размера. С помощью этой функции можно значительно увеличить производительность кластера хранилища данных, разделив диски NVMe на пространства имен и использовав получившиеся логические диски для хранения фрагментов данных. Прирост производительности обуславливается тем, что один и тот же физический диск используется несколькими службами фрагментов данных, хотя при этом кратно возрастает потребление ОЗУ, ядер ЦП и дискового пространства за счет большего количества служб фрагментов данных в расчете на один физический диск.

Предупреждение
Не создавайте больше одного пространства имен на дисках NVMe, если используется область отказа «Диск», так как отказ одного физического диска NVMe приведет к одновременному отказу всех его логических дисков.

Изменение параметров производительности дисков NVMe

1. На экране **Настройки** > **Системные настройки** перейдите в раздел **Производительность NVMe**. Будут отображены текущие значения параметров.



2. Укажите количество пространств имен NVMe и размер блока, а затем нажмите **Сохранить**. На каждом диске NVMe, логическим дискам которого не назначена роль в кластере хранилища, будет создано заданное количество логических дисков с указанным размером блока.

После изменения параметров логическим дискам NVMe можно назначить роль **Хранилище** и уровень хранения данных. При необходимости вы можете назначить логическим дискам NVMe роли, отличные от роли **Хранилище**.

Просмотр сведений о дисках NVMe

Выполнив команду nvme list на сервере с дисками NVMe, можно просмотреть сведения об этих дисках, такие как список пространств имен, их объемы и размеры блоков. Например:

```
# nvme list
Node             Generic          SN               Model                                    Namespace  Usage
Format         FW Rev
---------------- ---------------- ---------------- ---------------------------------------- ---------- ----------
-------- ---------------- --------
/dev/nvme1n3     ng1n3            S665NC0TA04280   SAMSUNG MZ1L2960HCJR-00A07
  0x3     314.15  GB / 314.15  GB    4 KiB +  0 B   GDC7302Q
/dev/nvme1n2     ng1n2            S665NC0TA04280   SAMSUNG MZ1L2960HCJR-00A07
  0x2     314.15  GB / 314.15  GB    4 KiB +  0 B   GDC7302Q
/dev/nvme1n1     ng1n1            S665NC0TA04280   SAMSUNG MZ1L2960HCJR-00A07
  0x1     314.15  GB / 314.15  GB    4 KiB +  0 B   GDC7302Q
/dev/nvme0n1     ng0n1            S665NC0TA04286   SAMSUNG MZ1L2960HCJR-00A07
  0x1     122.91  GB / 960.20  GB   512   B +  0 B   GDC7302Q
```

В этом примере /dev/nvme1n1, /dev/nvme1n2 и /dev/nvme1n3 – это пространства имен диска /dev/nvme1; в колонке Format показан размер блока для каждого из них.

Организация уровней хранения данных с разными конфигурациями производительности дисков NVMe

В некоторых случаях может понадобиться организовать несколько уровней хранения данных с разными конфигурациями производительности дисков NVMe (например, диски одних моделей могут работать с максимальной производительностью только при маленьких значениях размера блока, а диски других моделей – при больших значениях размера блока). Чтобы организовать уровни с разными конфигурациями, сделайте следующее:

1. Подготовьте необходимое количество дисков NVMe и убедитесь, что они не используются в кластере хранилища.

2. Задайте параметры производительности для одного уровня хранения, а затем сформируйте этот уровень хранения из части дисков.
3. Повторите шаг 2 для остальных уровней хранения.

7.1.15 Управление автоматической балансировкой нагрузки на уровни хранилища

Функция автоматической балансировки нагрузки на уровни хранилища позволяет обнаруживать чрезмерно или недостаточно нагруженные уровни и уравновешивать нагрузку путем перемещения томов с более нагруженных уровней на менее нагруженные. Эта функция снимает с администраторов хранилища необходимость выполнять вышеперечисленное вручную, а также позволяет повысить общую производительность хранилища за счет оптимального распределения нагрузки.

Примечание
После создания кластера хранилища балансировщику нагрузки необходимо до двух часов, чтобы собрать необходимую минимальную статистику для принятия решений и отображения ненулевых значений на странице мониторинга нагрузки на уровни.

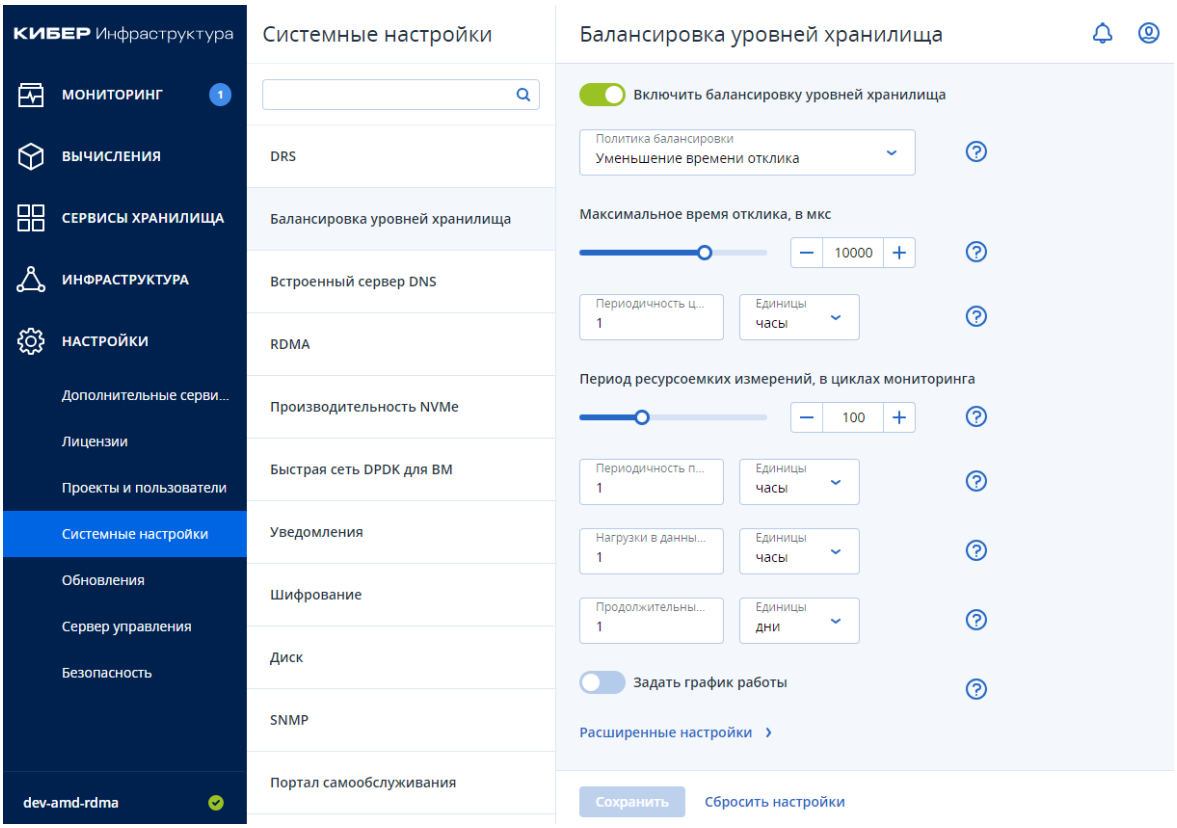
В выключенном состоянии балансировщик нагрузки не выполняет ресурсоемкие измерения, а в качестве максимально достижимых значений скорости выполнения операций ввода-вывода и скорости передачи данных использует максимальные значения, измеренные под пользовательской нагрузкой.

Ограничения

- Поддерживаются только тома виртуальных машин и блочного хранилища.

Включение автоматической балансировки нагрузки

1. На экране **Настройки** > **Системные настройки** > **Балансировка уровней хранилища** установите флажок **Включить балансировку уровней хранилища**.



2. Выберите одну из политик балансировки:
   - **Уменьшение времени отклика**. Политика направлена на обеспечение минимального времени отклика при работе с данными хранилища. Балансировка осуществляется таким образом, что часть наиболее используемых томов перемещается с уровней с большим временем отклика на уровни с меньшим временем отклика.
   - **Увеличение IOPS**. Политика направлена на обеспечение высокой производительности хранилища. Балансировка осуществляется таким образом, что часть наиболее используемых томов перемещается с уровней, запасы производительности которых исчерпаны, на уровни, где есть достаточные запасы производительности.
   - **Оптимизация использования пространства**. Политика направлена на максимальное использование дискового пространства хранилища. Балансировка осуществляется таким образом, что тома либо перемещаются с уровней с меньшим объемом свободного пространства на уровни с большим объемом свободного пространства, либо остаются на своих изначальных уровнях, но для освобождения места изменяются их режимы избыточности.
   - **Обеспечение минимальной избыточности**. Политика направлена на обеспечение минимальной избыточности данных томов. Балансировка осуществляется таким образом, что тома перемещаются с уровней, на которых нет достаточного числа работоспособных областей отказа, для того чтобы разместить необходимое количество реплик фрагментов данных, блоков данных и блоков четности, на уровни с достаточным числом работоспособных зон отказа.

Перемещение тома осуществляется посредством назначения ему новой политики хранения, в которой указан необходимый уровень.

3. Задайте параметры балансировки в зависимости от выбранной политики.

   Параметры политики **Уменьшение времени отклика**

   - **Максимальное время отклика**. Максимальное время отклика (latency) для каждого уровня хранилища. Если время отклика уровня превышает максимальное, то этот уровень считается перегруженным и часть томов будет перенесена с него на уровни с меньшими временами отклика.
   - **Периодичность циклов мониторинга**. Интервал времени между запусками мониторинга нагрузки на уровни хранилища. При мониторинге для каждого диска измеряются: текущая и максимальная скорости выполнения операций ввода-вывода, текущая и максимальная скорости передачи данных, объемы свободного и использованного дискового пространства, а также время отклика. По этим данным вычисляются совокупные характеристики для каждого уровня хранилища.
   - **Период ресурсоемких измерений, в циклах мониторинга**. Доля ресурсоемких измерений во всех измерениях, выполняемых при мониторинге нагрузки на уровни хранилища. К ресурсоемким относятся измерения максимальных скоростей выполнения операций ввода-вывода и передачи данных (используется утилита fio, которая создает дополнительную нагрузку). Например, если этому параметру задать значение 5, то на каждом пятом запуске мониторинга будут выполняться ресурсоемкие измерения.
   - **Периодичность принятия решений**. Интервал времени между запусками балансировки нагрузки. Во время каждого запуска обрабатываются измерения нагрузки на уровни хранилища и тома, принимаются решения о перемещениях томов, осуществляются запланированные перемещения томов. Чем больше значение этого параметра, тем реже будут происходить перемещения томов.
   - **Нагрузки в данный момент на том**. Длительность промежутка времени для вычисления средней нагрузки на том, которая будет интерпретироваться как текущая (мгновенная) нагрузка. Применяется для отбора наиболее подходящих для переноса томов. Тома, испытывающие высокую нагрузку в течении длительного промежутка времени, но при этом не испытывающие ее в данный момент, переносятся в первую очередь. Для вычислений используются соответствующие метрики томов, сохраненные в базе данных временных рядов Prometheus.
   - **Продолжительные нагрузки на том**. Длительность промежутка времени для вычисления средней нагрузки на том, которая будет интерпретироваться как общая (продолжительная) нагрузка. Применяется для отбора наиболее подходящих для переноса томов. Тома, испытывающие высокую нагрузку в течении длительного промежутка времени, но при этом не испытывающие ее в данный момент, переносятся в первую очередь. Для вычислений используются соответствующие метрики томов, сохраненные в базе данных временных рядов Prometheus.

   Параметры политики **Увеличение IOPS**

   - **Порог IOPS для операций чтения, %**. Пороговое значение скорости выполнения операций чтения в процентах от максимальной скорости выполнения операций чтения. Если пороговое

значение превышено, то уровень считается перегруженным и часть томов будет с него перенесена на менее нагруженные уровни.

- **Порог IOPS для операций записи, %**. Пороговое значение скорости выполнения операций записи в процентах от максимальной скорости выполнения операций записи. Если пороговое значение превышено, то уровень считается перегруженным и часть томов будет с него перенесена на менее нагруженные уровни.
- **Периодичность циклов мониторинга**. Интервал времени между запусками мониторинга нагрузки на уровни хранилища. При мониторинге для каждого диска измеряются: текущая и максимальная скорости выполнения операций ввода-вывода, текущая и максимальная скорости передачи данных, объемы свободного и использованного дискового пространства, а также время отклика. По этим данным вычисляются совокупные характеристики для каждого уровня хранилища.
- **Период ресурсоемких измерений, в циклах мониторинга**. Доля ресурсоемких измерений во всех измерениях, выполняемых при мониторинге нагрузки на уровни хранилища. К ресурсоемким относятся измерения максимальных скоростей выполнения операций ввода-вывода и передачи данных (используется утилита fio, которая создает дополнительную нагрузку). Например, если этому параметру задать значение 5, то на каждом пятом запуске мониторинга будут выполняться ресурсоемкие измерения.
- **Периодичность принятия решений**. Интервал времени между запусками балансировки нагрузки. Во время каждого запуска обрабатываются измерения нагрузки на уровни хранилища и тома, принимаются решения о перемещениях томов, осуществляются запланированные перемещения томов. Чем больше значение этого параметра, тем реже будут происходить перемещения томов.
- **Нагрузки в данный момент на том**. Длительность промежутка времени для вычисления средней нагрузки на том, которая будет интерпретироваться как текущая (мгновенная) нагрузка. Применяется для отбора наиболее подходящих для переноса томов. Тома, испытывающие высокую нагрузку в течении длительного промежутка времени, но при этом не испытывающие ее в данный момент, переносятся в первую очередь. Для вычислений используются соответствующие метрики томов, сохраненные в базе данных временных рядов Prometheus.
- **Продолжительные нагрузки на том**. Длительность промежутка времени для вычисления средней нагрузки на том, которая будет интерпретироваться как общая (продолжительная) нагрузка. Применяется для отбора наиболее подходящих для переноса томов. Тома, испытывающие высокую нагрузку в течении длительного промежутка времени, но при этом не испытывающие ее в данный момент, переносятся в первую очередь. Для вычислений используются соответствующие метрики томов, сохраненные в базе данных временных рядов Prometheus.

Параметры политики **Оптимизация использования пространства**

- **Периодичность циклов мониторинга**. Интервал времени между запусками мониторинга нагрузки на уровни хранилища. При мониторинге для каждого диска измеряются: текущая и максимальная скорости выполнения операций ввода-вывода, текущая и максимальная скорости передачи данных, объемы свободного и использованного дискового пространства,

а также время отклика. По этим данным вычисляются совокупные характеристики для каждого уровня хранилища.

- **Период ресурсоемких измерений, в циклах мониторинга**. Доля ресурсоемких измерений во всех измерениях, выполняемых при мониторинге нагрузки на уровни хранилища. К ресурсоемким относятся измерения максимальных скоростей выполнения операций ввода-вывода и передачи данных (используется утилита fio, которая создает дополнительную нагрузку). Например, если этому параметру задать значение 5, то на каждом пятом запуске мониторинга будут выполняться ресурсоемкие измерения.
- **Периодичность принятия решений**. Интервал времени между запусками балансировки нагрузки. Во время каждого запуска обрабатываются измерения нагрузки на уровни хранилища и тома, принимаются решения о перемещениях томов, осуществляются запланированные перемещения томов. Чем больше значение этого параметра, тем реже будут происходить перемещения томов.

Параметры политики **Обеспечение минимальной избыточности**

- **Периодичность циклов мониторинга**. Интервал времени между запусками мониторинга нагрузки на уровни хранилища. При мониторинге для каждого диска измеряются: текущая и максимальная скорости выполнения операций ввода-вывода, текущая и максимальная скорости передачи данных, объемы свободного и использованного дискового пространства, а также время отклика. По этим данным вычисляются совокупные характеристики для каждого уровня хранилища.
- **Период ресурсоемких измерений, в циклах мониторинга**. Доля ресурсоемких измерений во всех измерениях, выполняемых при мониторинге нагрузки на уровни хранилища. К ресурсоемким относятся измерения максимальных скоростей выполнения операций ввода-вывода и передачи данных (используется утилита fio, которая создает дополнительную нагрузку). Например, если этому параметру задать значение 5, то на каждом пятом запуске мониторинга будут выполняться ресурсоемкие измерения.
- **Периодичность принятия решений**. Интервал времени между запусками балансировки нагрузки. Во время каждого запуска обрабатываются измерения нагрузки на уровни хранилища и тома, принимаются решения о перемещениях томов, осуществляются запланированные перемещения томов. Чем больше значение этого параметра, тем реже будут происходить перемещения томов.
- **Нагрузки в данный момент на том**. Длительность промежутка времени для вычисления средней нагрузки на том, которая будет интерпретироваться как текущая (мгновенная) нагрузка. Применяется для отбора наиболее подходящих для переноса томов. Тома, испытывающие высокую нагрузку в течении длительного промежутка времени, но при этом не испытывающие ее в данный момент, переносятся в первую очередь. Для вычислений используются соответствующие метрики томов, сохраненные в базе данных временных рядов Prometheus.
- **Продолжительные нагрузки на том**. Длительность промежутка времени для вычисления средней нагрузки на том, которая будет интерпретироваться как общая (продолжительная) нагрузка. Применяется для отбора наиболее подходящих для переноса томов. Тома, испытывающие высокую нагрузку в течении длительного промежутка времени, но при этом

не испытывающие ее в данный момент, переносятся в первую очередь. Для вычислений используются соответствующие метрики томов, сохраненные в базе данных временных рядов Prometheus.

4. [Необязательно] По умолчанию балансировка нагрузки всегда включена и выполняется с заданной периодичностью в течение дня. Можно ограничить ее время работы частью дня, установив флажок **Задать график работы** и указав время начала и конца работы в полях **Начало** и **Конец**.
5. [Необязательно] Задайте расширенные параметры балансировки в зависимости от выбранной политики.

   Расширенные параметры политики **Уменьшение времени отклика**

   - **Разрешить автоматическое создание политик хранения для томов ВМ**. Определяет, можно ли автоматически создавать политики хранения томов ВМ и назначать их проектам в случаях, когда среди назначенных политик нет подходящих для перемещения томов.
   - **Выбирать схему избыточного кодирования с двойным запасом доменов отказа для перестроения**. Определяет, требуется ли перемещать тома с типом избыточности «помехоустойчивое кодирование» только на такие уровни, которые позволяют размещать двойное количество блоков четности. Например, при использовании этого параметра том с типом избыточности «помехоустойчивое кодирование» и схемой избыточности 5+2 (5 блоков данных и 2 блока четности) может быть перемещен только на такие уровни, где количество областей отказа не меньше, чем 9 (5+2*2).
   - **Порог занимаемого пространства, %**. Максимальный объем использованного дискового пространства уровня хранилища в процентах от его общего объема. Параметр позволяет исключить такие перемещения томов, в результате которых на уровнях-приемниках объем использованного дискового пространства будет больше максимального.
   - **Минимальный прирост производительности, %**. Минимальный прирост производительности в процентах от производительности тома, перемещаемого с уровня-источника на уровень-приемник. Параметр используется при принятии решений о перестановках томов между уровнями (например, когда более используемый том с уровня-источника может быть перемещен на уровень-приемник, а менее используемый том с уровня-приемника может быть перемещен на уровень-источник) и позволяет предотвратить малоэффективные перестановки томов. Перестановка томов выполняется при условии, что прирост производительности на уровне-источнике будет не меньше минимального.
   - **Перемещать один том не чаще <N единиц времени>**. Минимальная продолжительность промежутка времени между перемещениями одного и того же тома между уровнями. Этот параметр позволяет предотвратить слишком частые перемещения томов.
   - **Не перемещать тома размером более <N единиц размера>**. Максимальный размер томов для перемещения. Тома, размер которых превышает максимальный, не перемещаются автоматически.
   - **Количество циклов для принятия решения**. Количество последних запусков мониторинга нагрузки на уровни хранилища, по результатам которых принимается решение о перемещениях томов.

- **Граница низкой активности, %**. Минимальная нагрузка на том в процентах от средней нагрузки на тома одной и той же службы инфраструктуры. Тома, нагрузка на которые меньше минимальной, считаются «холодными» и подлежат переносу на менее производительные уровни хранилища. Этот параметр позволяет освободить более производительные уровни для часто используемых томов.
- **Ограничение времени миграции тома**. Максимальное время перемещения тома. Время перемещения оценивается на основе пропускных способностей уровня-источника и уровня-приемника. Если расчетное время перемещения тома превышает максимальное, том не будет перемещен.

Расширенные параметры политики **Увеличение IOPS**

- **Разрешить автоматическое создание политик хранения для томов ВМ**. Определяет, можно ли автоматически создавать политики хранения томов ВМ и назначать их проектам в случаях, когда среди назначенных политик нет подходящих для перемещения томов.
- **Выбирать схему избыточного кодирования с двойным запасом доменов отказа для перестроения**. Определяет, требуется ли перемещать тома с типом избыточности «помехоустойчивое кодирование» только на такие уровни, которые позволяют размещать двойное количество блоков четности. Например, при использовании этого параметра том с типом избыточности «помехоустойчивое кодирование» и схемой избыточности 5+2 (5 блоков данных и 2 блока четности) может быть перемещен только на такие уровни, где количество областей отказа не меньше, чем 9 (5+2*2).
- **Порог занимаемого пространства, %**. Максимальный объем использованного дискового пространства уровня хранилища в процентах от его общего объема. Параметр позволяет исключить такие перемещения томов, в результате которых на уровнях-приемниках объем использованного дискового пространства будет больше максимального.
- **Минимальный прирост производительности, %**. Минимальный прирост производительности в процентах от производительности тома, перемещаемого с уровня-источника на уровень-приемник. Параметр используется при принятии решений о перестановках томов между уровнями (например, когда более используемый том с уровня-источника может быть перемещен на уровень-приемник, а менее используемый том с уровня-приемника может быть перемещен на уровень-источник) и позволяет предотвратить малоэффективные перестановки томов. Перестановка томов выполняется при условии, что прирост производительности на уровне-источнике будет не меньше минимального.
- **Перемещать один том не чаще <N единиц времени>**. Минимальная продолжительность промежутка времени между перемещениями одного и того же тома между уровнями. Этот параметр позволяет предотвратить слишком частые перемещения томов.
- **Не перемещать тома размером более <N единиц размера>**. Максимальный размер томов для перемещения. Тома, размер которых превышает максимальный, не перемещаются автоматически.
- **Количество циклов для принятия решения**. Количество последних запусков мониторинга нагрузки на уровни хранилища, по результатам которых принимается решение о перемещениях томов.

- **Граница низкой активности, %**. Минимальная нагрузка на том в процентах от средней нагрузки на тома одной и той же службы инфраструктуры. Тома, нагрузка на которые меньше минимальной, считаются «холодными» и подлежат переносу на менее производительные уровни хранилища. Этот параметр позволяет освободить более производительные уровни для часто используемых томов.
- **Ограничение времени миграции тома**. Максимальное время перемещения тома. Время перемещения оценивается на основе пропускных способностей уровня-источника и уровня-приемника. Если расчетное время перемещения тома превышает максимальное, том не будет перемещен.

Расширенные параметры политики **Оптимизация использования пространства**

- **Разрешить автоматическое создание политик хранения для томов ВМ**. Определяет, можно ли автоматически создавать политики хранения томов ВМ и назначать их проектам в случаях, когда среди назначенных политик нет подходящих для перемещения томов.
- **Выбирать схему избыточного кодирования с двойным запасом доменов отказа для перестроения**. Определяет, требуется ли перемещать тома с типом избыточности «помехоустойчивое кодирование» только на такие уровни, которые позволяют размещать двойное количество блоков четности. Например, при использовании этого параметра том с типом избыточности «помехоустойчивое кодирование» и схемой избыточности 5+2 (5 блоков данных и 2 блока четности) может быть перемещен только на такие уровни, где количество областей отказа не меньше, чем 9 (5+2*2).
- **Порог занимаемого пространства, %**. Максимальный объем использованного дискового пространства уровня хранилища в процентах от его общего объема. Параметр позволяет исключить такие перемещения томов, в результате которых на уровнях-приемниках объем использованного дискового пространства будет больше максимального.
- **Перемещать один том не чаще <N единиц времени>**. Минимальная продолжительность промежутка времени между перемещениями одного и того же тома между уровнями. Этот параметр позволяет предотвратить слишком частые перемещения томов.
- **Не перемещать тома размером более <N единиц размера>**. Максимальный размер томов для перемещения. Тома, размер которых превышает максимальный, не перемещаются автоматически.
- **Количество циклов для принятия решения**. Количество последних запусков мониторинга нагрузки на уровни хранилища, по результатам которых принимается решение о перемещениях томов.
- **Ограничение времени миграции тома**. Максимальное время перемещения тома. Время перемещения оценивается на основе пропускных способностей уровня-источника и уровня-приемника. Если расчетное время перемещения тома превышает максимальное, том не будет перемещен.

Расширенные параметры политики **Обеспечение минимальной избыточности**

- **Разрешить автоматическое создание политик хранения для томов ВМ**. Определяет, можно ли автоматически создавать политики хранения томов ВМ и назначать их проектам в случаях, когда среди назначенных политик нет подходящих для перемещения томов.

- **Выбирать схему избыточного кодирования с двойным запасом доменов отказа для перестроения**. Определяет, требуется ли перемещать тома с типом избыточности «помехоустойчивое кодирование» только на такие уровни, которые позволяют размещать двойное количество блоков четности. Например, при использовании этого параметра том с типом избыточности «помехоустойчивое кодирование» и схемой избыточности 5+2 (5 блоков данных и 2 блока четности) может быть перемещен только на такие уровни, где количество областей отказа не меньше, чем 9 (5+2*2).
- **Порог занимаемого пространства, %**. Максимальный объем использованного дискового пространства уровня хранилища в процентах от его общего объема. Параметр позволяет исключить такие перемещения томов, в результате которых на уровнях-приемниках объем использованного дискового пространства будет больше максимального.
- **Минимальный прирост производительности, %**. Минимальный прирост производительности в процентах от производительности тома, перемещаемого с уровня-источника на уровень-приемник. Параметр используется при принятии решений о перестановках томов между уровнями (например, когда более используемый том с уровня-источника может быть перемещен на уровень-приемник, а менее используемый том с уровня-приемника может быть перемещен на уровень-источник) и позволяет предотвратить малоэффективные перестановки томов. Перестановка томов выполняется при условии, что прирост производительности на уровне-источнике будет не меньше минимального.
- **Перемещать один том не чаще <N единиц времени>**. Минимальная продолжительность промежутка времени между перемещениями одного и того же тома между уровнями. Этот параметр позволяет предотвратить слишком частые перемещения томов.
- **Не перемещать тома размером более <N единиц размера>**. Максимальный размер томов для перемещения. Тома, размер которых превышает максимальный, не перемещаются автоматически.
- **Количество циклов для принятия решения**. Количество последних запусков мониторинга нагрузки на уровни хранилища, по результатам которых принимается решение о перемещениях томов.
- **Граница низкой активности, %**. Минимальная нагрузка на том в процентах от средней нагрузки на тома одной и той же службы инфраструктуры. Тома, нагрузка на которые меньше минимальной, считаются «холодными» и подлежат переносу на менее производительные уровни хранилища. Этот параметр позволяет освободить более производительные уровни для часто используемых томов.
- **Ограничение времени миграции тома**. Максимальное время перемещения тома. Время перемещения оценивается на основе пропускных способностей уровня-источника и уровня-приемника. Если расчетное время перемещения тома превышает максимальное, том не будет перемещен.

6. Нажмите **Сохранить**.

Примечание
Перемещение отдельного тома можно запретить, сняв установленный по умолчанию флажок **Разрешить сервису "Балансировка уровней хранилища" автоматически перемещать этот том** в разделе сведений о томе.

Выключение автоматической балансировки нагрузки

На экране **Настройки** > **Системные настройки** > **Балансировка уровней хранилища** снимите флажок **Включить балансировку уровней хранилища**.

7.2 Управление хранилищем резервных копий

В этом разделе описываются действия администратора над хранилищем резервных копий, выполняемые со стороны Кибер Бэкап: обновление сертификата и повторная регистрация хранилища резервных копий в новом экземпляре Кибер Бэкап, изменение схемы резервирования, добавление узлов в кластер хранения резервных копий и их высвобождение из него. Кроме того, этот раздел также рассматривает георепликацию между двумя географически разнесенными центрами обработки данных или между двумя различными местами назначения резервных копий. Если потребуется удалить хранилище резервных копий, исключите из его состава все его узлы.

7.2.1 Добавление узлов в хранилище резервных копий

Можно добавить дополнительные серверы, которые будут служить местами размещения резервных копий из Кибер Бэкап и/или Кибер Бэкап Облачный, для высокой доступности и масштабируемости хранилища резервных копий.

Предварительные условия

- Кластер хранилища резервных копий создан и зарегистрирован в панели управления облаком, как описано в разделе "Подготовка пространства для хранилища резервных копий к работе" на странице 150.

Как добавить серверы к хранилищу резервных копий

Панель администратора

1. Перейдите на экран **Сервисы хранилища** > **Резервные копии** > **Серверы**.
2. Нажмите **Добавить сервер**.
3. Выберите серверы для присоединения к кластеру хранилища резервных копий и нажмите **Добавить**.

Серверы будут добавлены к хранилищу резервных копий, и на них будет работать сервис Backup Gateway.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service backup node add --nodes <nodes>
```

--nodes <nodes>

Разделенный запятыми список хостовых имен или идентификаторов серверов

Например, чтобы добавить сервер с идентификатором 2f3f6091-0d44-45aa-94e3-ebc2b65c0eeb в кластер хранилища резервных копий, выполните:

```
# vinfra service backup node add --nodes 2f3f6091-0d44-45aa-94e3-ebc2b65c0eeb
```

Добавленный сервер появится в выводе команды vinfra service backup node list:

```
# vinfra service backup node list
+--------------------------------------+-----------------------+-----------+
| id                                   | host                  | is_online |
+--------------------------------------+-----------------------+-----------+
| 2f3f6091-0d44-45aa-94e3-ebc2b65c0eeb | node003.vstoragedomain | True     |
| 74cbd22b-fb1b-4441-ae52-532078c54f9a | node001.vstoragedomain | True     |
| eeb06dce-4cfd-4c89-bc7f-4689ea5c7058 | node002.vstoragedomain | True     |
+--------------------------------------+-----------------------+-----------+
```

7.2.2 Обновление сертификата для хранилища резервных копий

При регистрации Backup Gateway в Кибер Бэкап Облачный или Кибер Бэкап они обмениваются сертификатами, которые действуют в течение трех лет. За полтора месяца до окончания этого периода вы получите уведомление о скором истечении срока действия сертификата на панели администрирования.

Предварительные требования

- Кластер хранилища резервных копий создан и зарегистрирован в панели управления облаком, как описано в разделе "Подготовка пространства для хранилища резервных копий к работе" на странице 150.
- Убедитесь, что для вашего тенанта партнера отключена двухфакторная проверка подлинности (2FA). Вы также можете отключить ее для конкретного пользователя при включенной двухфакторной проверке для тенанта, как описано в Руководстве администратора партнера в разделе "Управление двухфакторной проверкой подлинности для пользователей", и указать учетные данные этого пользователя.
- Если включен контроль входа для веб-интерфейса Кибер Бэкап Облачный, убедитесь, что внешний IP-адрес кластера хранилища резервных копий добавлен в список разрешенных IP-адресов, как описано в Руководстве администратора партнера в разделе "Ограничение доступа к веб-интерфейсу".

Чтобы обновить сертификат

Панель администратора

1. На экране **Сервисы хранилища** > **Резервное копирование** перейдите на вкладку **Настройки** и нажмите **Сертификат**.
2. Укажите данные партнерской учетной записи в облаке или учетные данные администратора организации на локальном сервере управления.
3. Нажмите **Обновить**.
4. На всех серверах, входящих в кластер хранилища резервных копий, перезапустите сервис:

   ```
   # systemctl restart vstorage-abgw
   ```

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service backup cluster renew-certificates --reg-account <reg-account>
                                  --reg-server <reg-server> [--stdin]
```

--stdin

Используется для настройки пароля регистрации из stdin.

--reg-account <reg-account>

Партнерская учетная запись в облаке или учетная запись администратора организации на локальном сервере управления

--reg-server <reg-server>

URL-адрес портала управления облаком или имя хоста/IP-адрес и порт локального сервера управления

Например, чтобы обновить сертификат кластера хранилища резервных копий, выполните:

```
# vinfra service backup cluster renew-certificates --reg-account account@example.com \
--reg-server https://cloud.example.com/ --stdin
```

Укажите пароль регистрации.

После обновления сертификата перезапустите сервис на всех серверах, входящих в кластер хранилища резервных копий:

```
# systemctl restart vstorage-abgw
```

7.2.3 Повторная регистрация хранилища резервных копий в новом экземпляре Кибер Бэкап

Чтобы переключить настроенное хранилище резервных копий на другой экземпляр Кибер Бэкап, необходимо перерегистрировать шлюз на этом экземпляре.

Предварительные требования

- Кластер хранилища резервных копий создан и зарегистрирован в панели управления облаком, как описано в разделе "Подготовка пространства для хранилища резервных копий к работе" на странице 150.

Как перерегистрировать хранилище резервных копий

Панель администратора

1. На экране **Сервисы хранилища** > **Резервные копии** перейдите на вкладку **Настройки** и нажмите **Перерегистрация**.
2. Укажите имя хоста или IP-адрес целевого сервера управления и порт 9877 (например, http://192.168.1.2:9877), а затем введите учетные данные для сервера управления.

   Примечание
   Адрес следует задавать с использованием протокола HTTP, а не HTTPS.

3. Нажмите **Сохранить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service backup cluster re-register --domain <domain>
                                          --reg-account <reg-account>
                                          --reg-server <reg-server> [--stdin]
```

--domain <domain>

Имя домена для резервного кластера

--reg-account <reg-account>

Партнерская учетная запись в облаке или учетная запись администратора организации на локальном сервере управления

--reg-server <reg-server>

URL-адрес портала управления облаком или имя хоста/IP-адрес и порт локального сервера управления

--stdin

Используется для настройки пароля регистрации из stdin.

Например, чтобы переключить кластер хранилища резервных копий на новый экземпляр Кибер Бэкап, выполните:

```
# vinfra service backup cluster re-register --domain newdns.example.com \
--reg-account account@example.com --reg-server https://cloud.example.com/ --stdin
```

Укажите пароль регистрации.

7.2.4 Изменение схемы избыточности для хранилища резервных копий

Можно обновить схему избыточности, которая используется для хранилища резервных копий, изменив политику хранилища. Такая настраиваемая схема избыточности обеспечивает высокую масштабируемость и максимальную эффективность хранилища резервных копий.

В процессе перекодирования данные частично хранятся с новой схемой избыточности и частично – со старой. При этом система использует политику хранилища с наименьшей избыточностью. Например, если вы меняете режим кодирования с 1+0 на 1+2, система будет использовать режим 1+0. В этом случае важно не отключать никакие серверы и диски хранилища до завершения процесса.

Внимание
Если вы изменили схему кодирования для кластера хранилища резервных копий с помощью специалистов технической поддержки, заново примените настройки избыточности на панели администрирования, чтобы гарантировать перекодирование всех данных.

Ограничения

- Избыточность за счет репликации не поддерживается для хранилищ резервных копий.

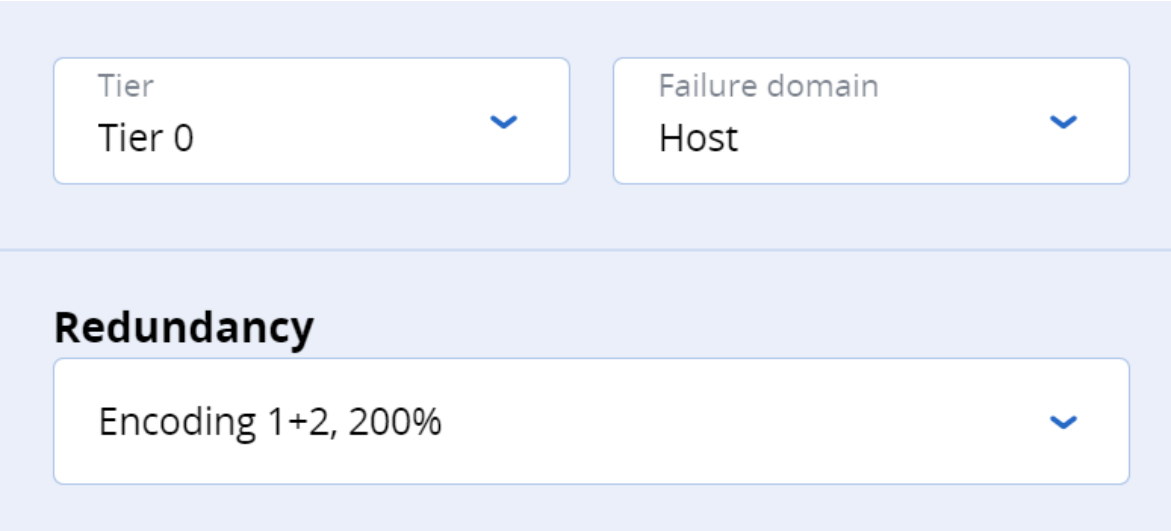
Предварительные требования

- Четкое понимание концепции "Политики хранения" на странице 37.
- Кластер хранилища резервных копий создан и зарегистрирован в панели управления облаком, как описано в "Подготовка пространства для хранилища резервных копий к работе" на странице 150.

Как изменить политику хранилища

Панель администратора

1. На экране **Сервисы хранилища** > **Резервные копии** перейдите на вкладку **Настройки** и нажмите **Политика хранения**.
2. Выберите нужный уровень хранилища, область отказов или режим избыточности данных.



3. Нажмите **Сохранить**.

После запуска процесса перекодирования на экране будет показан ход выполнения и приблизительное время завершения. Во время процесса можно выбрать другую схему избыточности. В этом случае текущий процесс перекодирования будет остановлен, а затем применена новая схема избыточности.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service backup volume-params change [--tier {0,1,2,3}]
                                           [--encoding <M>+<N>]
                                           [--failure-domain {disk,host,rack,row,room}]
```

--tier {0,1,2,3}

Уровень хранилища

--encoding <M>+<N>

Схема помехоустойчивого кодирования хранилища в формате:

- M: число блоков данных
- N: число паритетных блоков

--failure-domain {0,1,2,3,4}

Область отказа хранилища

Например, чтобы изменить уровень хранилища на 0, схему помехоустойчивого кодирования на 1+2, область отказа на «хост», выполните:

```
# vinfra service backup volume-params change --tier 0 --encoding 1+2 \
--failure-domain host
```

Обновленные параметры будут отображены в выводе команды vinfra service backup volume-params show:

```
# vinfra service backup volume-params show
+----------------+-------------+
| Field          | Value       |
+----------------+-------------+
| failure_domain | host        |
| redundancy     | m: 1        |
|                | n: 2        |
|                | type: raid6 |
| tier           | 0           |
+----------------+-------------+
```

7.2.5 Управление георепликацией для хранилища резервных копий

Кибер Инфраструктура позволяет включить репликацию хранилища резервных копий между двумя географически распределенными центрами обработки данных, зарегистрированными на облачной панели управления. Она обеспечивает защиту данных резервных копий от сбоя основного ЦОД. Георепликацию можно включить для хранилищ резервных копий, настроенных на различных серверных частях хранения данных: в локальном кластере хранилища данных, томе NFS или публичном облаке.

7.2.5.1 Включение георепликации

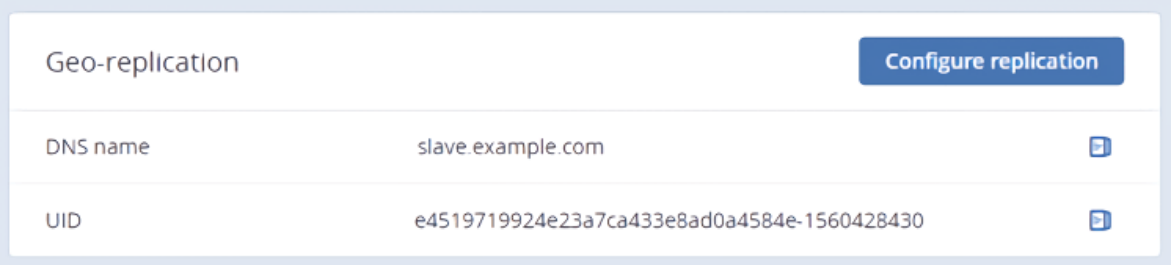
Предварительные требования

- Два кластера хранилища резервных копий должны быть развернуты и зарегистрированы на облачной панели управления, как описано в разделе "Подготовка пространства для хранилища резервных копий к работе" на странице 150.
- Обновить все кластеры хранения данных до последней версии.
- Обеспечить доступность всех кластеров хранилища данных друг для друга по доменным именам на порте TCP 44445.
- Каждый кластер хранилища должен иметь доступ сам к себе по собственному доменному имени через TCP-порт 44445. Это особенно важно, если кластеры расположены за NAT.

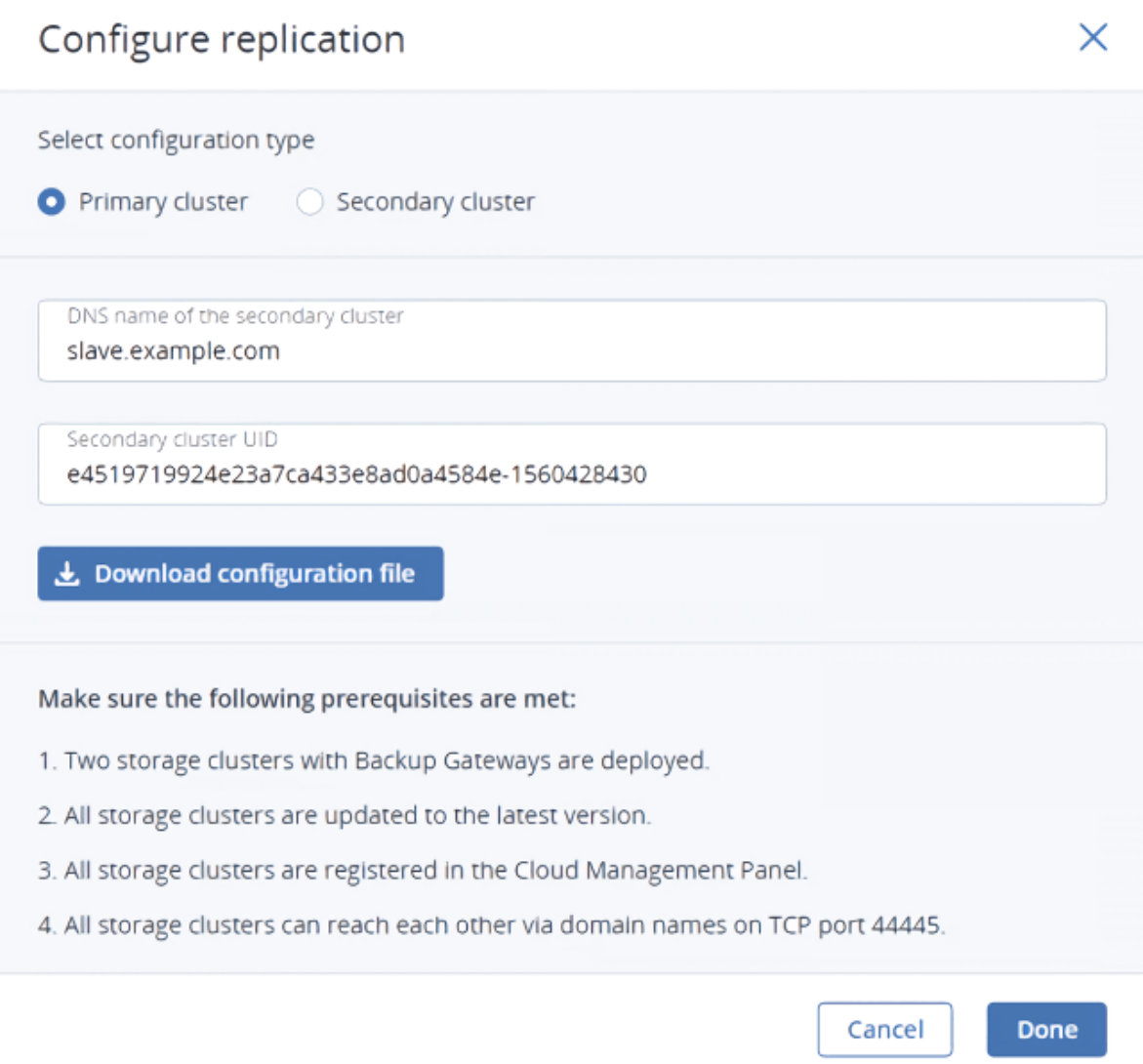
Чтобы настроить георепликацию между двумя кластерами хранилища

Панель администратора

1. На кластере, который будет настроен подчиненным, выберите **Сервисы хранилища** > **Резервные копии** > **Георепликация**. Щелкните по значку копирования рядом с полями **Доменное имя** и **UID**, чтобы скопировать его доменное имя и идентификатор пользователя UID в буфер обмена.

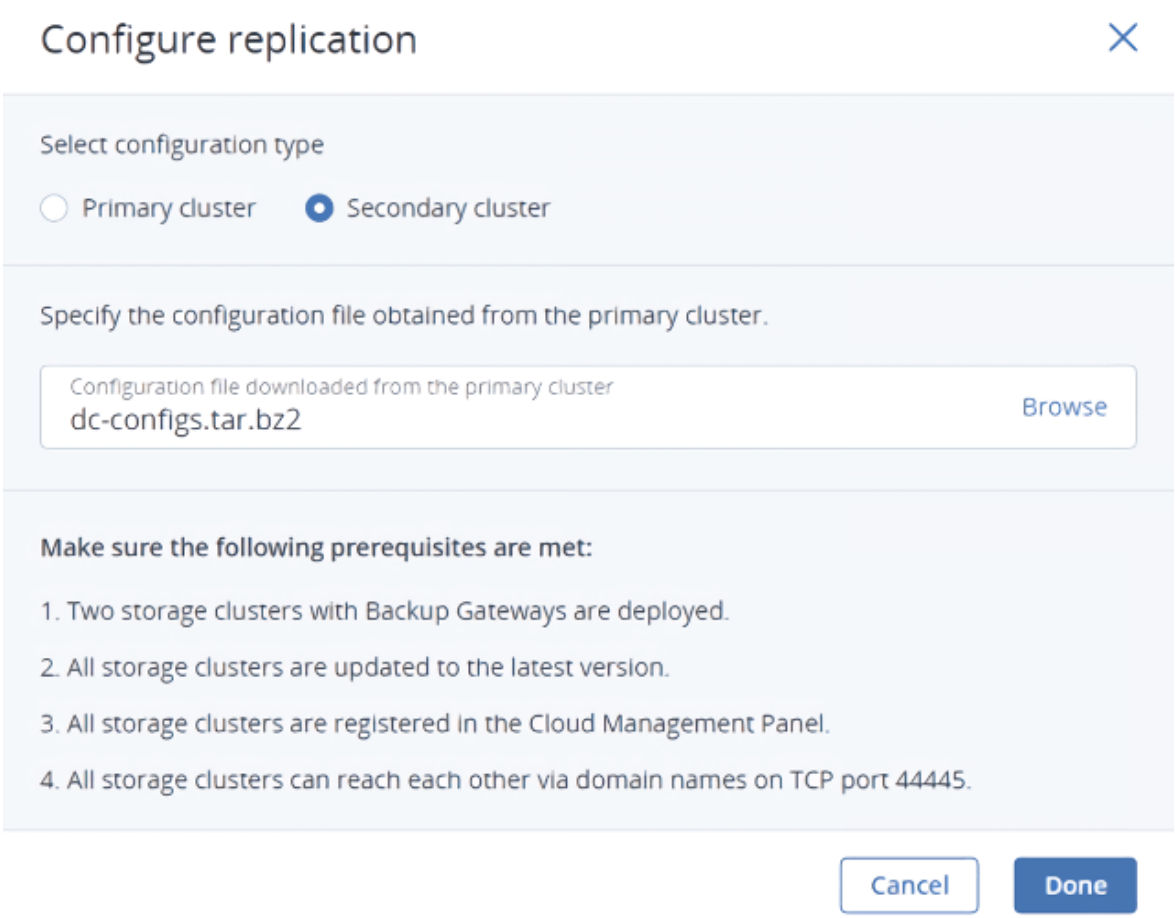


2. На кластере, который будет настроен как главный, выберите **Сервисы хранилища** > **Резервные копии** > **Георепликация**. Нажмите кнопку **Настроить репликацию** и выполните следующие действия в окне **Настроить репликацию**:
   a. Вставьте доменное имя и UID подчиненного кластера в соответствующие поля.
   b. Нажмите **Загрузить файл конфигурации**, чтобы загрузить файл конфигурации главного кластера на локальный сервер.
   c. Нажмите кнопку **Готово**.



Теперь главный кластер настроен и готов к подключению к подчиненному, который нужно настроить следующим образом.

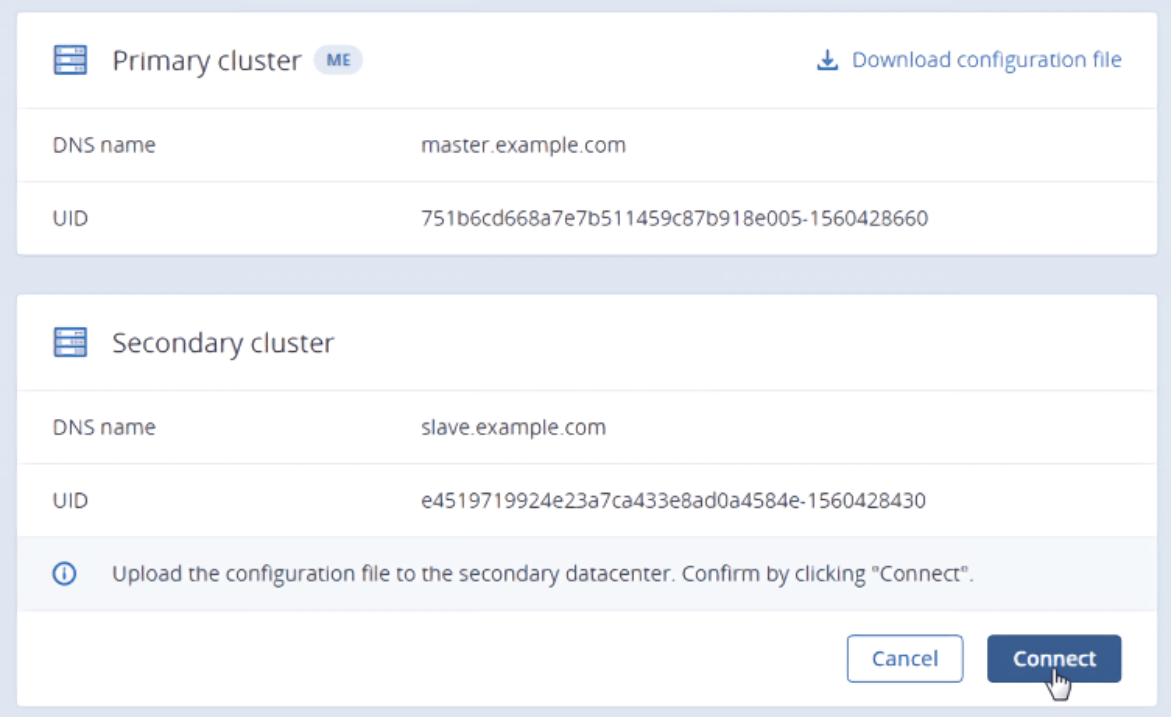
3. На подчиненном кластере нажмите **Настроить репликацию** и выполните следующие действия в окне **Настроить репликацию**.
   a. Выберите тип конфигурации **Подчиненный кластер**.
   b. Передайте файл конфигурации главного кластера с локального сервера.
   c. Нажмите кнопку **Готово**.



Теперь и подчиненный кластер настроен и готов к подключению к главному.

Примечание
Если после настройки подчиненного кластера по какой-либо причине потребуется изменить конфигурацию главного кластера, загрузите новую конфигурацию и передайте ее на подчиненный кластер, щелкнув по значку передачи рядом с полем **Файл конфигурации**. Перед этим убедитесь, что UID главного кластера не был изменен.

4. Вернувшись к главному кластеру, нажмите **Подключить** для включения репликации между двумя центрами обработки данных.



Интерфейс командной строки

1. На кластере, который будет настроен как подчиненный, выполните команду vinfra service backup geo-replication show, чтобы узнать его адрес и UID. Например:

```
# vinfra service backup geo-replication show
+-------+-----------------------------------------------------------+
| Field | Value                                                     |
+-------+-----------------------------------------------------------+
| self  | address: slave.example.com                                |
|       | datacenter_uid: e63a67388deb3c99d044eecbd7b79ad3-1577275849 |
+-------+-----------------------------------------------------------+
```

2. На кластере, который будет настроен как главный, выполните команду vinfra service backup geo-replication master setup с использованием адреса и UID подчиненного кластера. Например:

```
# vinfra service backup geo-replication master setup --slave-cluster-address \
slave.example.com --slave-cluster-uid e63a67388deb3c99d044eecbd7b79ad3-1577275849
```

3. На главном кластере выполните команду vinfra service backup geo-replication master download-configs, чтобы создать файл конфигурации главного кластера. Например:

```
# vinfra service backup geo-replication master download-configs --conf-file-path master_dc.conf
```

4. Загрузите файл конфигурации главного кластера на подчиненный кластер с помощью стандартной программы командной строки Linux. Например, с помощью scp:

```
# scp master_dc.conf node005.vstoragedomain:/root/master_dc.conf
root@node005.vstoragedomain's password:
```

5. На подчиненном кластере выполните команду vinfra service backup geo-replication slave setup, чтобы отправить файл конфигурации главного кластера. Например:

```
# vinfra service backup geo-replication slave setup --dc-config-file master_dc.conf
```

6. Если по какой-либо причине необходимо выключить георепликацию, выполните команду vinfra service backup geo-replication master cancel на главном кластере, а затем выполните команду vinfra service backup geo-replication slave cancel на подчиненном кластере.
7. На главном кластере выполните команду vinfra service backup geo-replication master establish, чтобы установить соединение между главным и подчиненным кластерами.

```
# vinfra service backup geo-replication master establish
```

7.2.5.2 Выполнение переключения при сбое

Если главный кластер окажется недоступным, можно вручную выполнить переключение, повысив подчиненный кластер до главного. При этом конфигурация подчиненного кластера, включая его DNS-имя, поменяется с конфигурацией главного. Переключение главного кластера при сбое можно выполнить в следующих случаях:

- Текущий главный кластер полностью нерабочий и изолирован от Интернета и любых агентов резервного копирования.
- Агенты резервного копирования не могут связаться с текущим главным кластером.
- Доменное имя главного кластера было перенастроено на его IP-адреса.

Предупреждение
Повышение подчиненного кластера до главного является необратимой операцией, которая сделает недействительными все данные на (бывшем) главном кластере. Ее следует использовать только в чрезвычайных случаях.

Предварительные требования

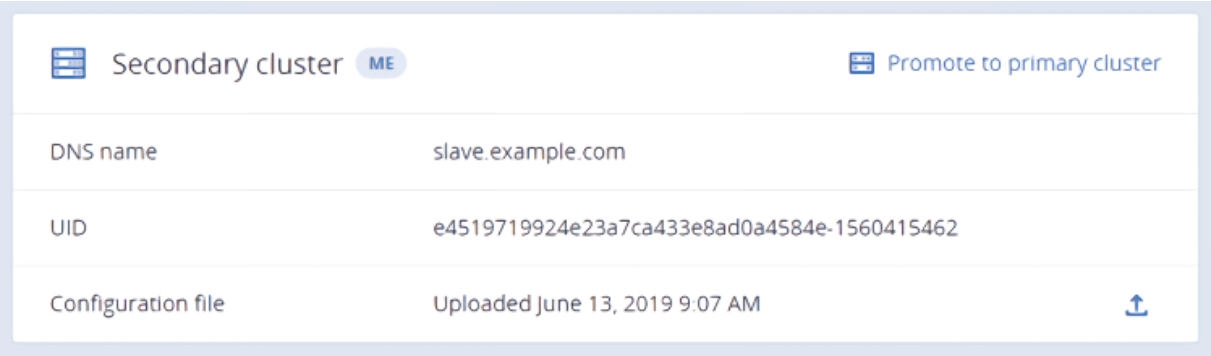
- Георепликация должна быть включена, как описано в разделе "Включение георепликации" на странице 356.
- Подчиненный кластер должен иметь доступ сам к себе по собственному доменному имени через TCP-порт 44445.

Чтобы выполнить переключение при сбое

Панель администратора

1. В подчиненном кластере выберите пункт меню **Сервисы хранилища** > **Резервные копии** > **Георепликация** и щелкните **Преобразовать в главный**.

2. Нажмите **Переход** в окне подтверждения.



Если текущий главный кластер остается работоспособным, сначала принудительно высвободите все его узлы из Backup Gateway, а затем выполните переключение при сбое.

Интерфейс командной строки

Используйте следующую команду:

```
# vinfra service backup geo-replication slave promote-to-master
```

7.2.5.3 Обновление конфигурации георепликации

Один раз в год необходимо обновлять сертификат хранилища резервных копий. При обновлении сертификата изменяется конфигурация кластера, что в свою очередь требует обновления конфигурации георепликации.

Предварительные требования

- Георепликация должна быть включена, как описано в разделе "Включение георепликации" на странице 356.

Чтобы обновить конфигурацию георепликации

Панель администратора

1. В главном кластере обновите сертификат, как описано в разделе "Обновление сертификата для хранилища резервных копий" на странице 351.
2. В главном кластере перейдите в пункт меню **Сервисы хранилища** > **Резервные копии** > **Георепликация**. Нажмите **Загрузить файл конфигурации**, чтобы загрузить его новую конфигурацию на локальный сервер.
3. На подчиненном кластере перейдите в пункт меню **Сервисы хранилища** > **Резервные копии** > **Георепликация**. Щелкните по значку отправки рядом с полем **Файл конфигурации**, чтобы передать новую конфигурацию на подчиненный кластер.

Интерфейс командной строки

1. На главном кластере обновите сертификат, выполнив команду vinfra service backup cluster renew-certificates. Например:

   ```
   # vinfra service backup cluster renew-certificates --reg-account account@example.com \
   --reg-server https://cloud.example.com/ --stdin
   ```

   Укажите регистрационный пароль.
2. На главном кластере загрузите его новую конфигурацию, выполнив команду vinfra service backup geo-replication master download-configs. Например:

   ```
   # vinfra service backup geo-replication master download-configs --conf-file-path master_dc.conf
   ```

3. Загрузите файл конфигурации главного кластера на подчиненный кластер с помощью стандартной программы командной строки Linux. Например, с помощью scp:

   ```
   # scp master_dc.conf node005.vstoragedomain:/root/master_dc.conf
   ```

   Укажите пароль администратора сервера.
4. На подчиненном кластере загрузите новую конфигурацию с помощью команды vinfra service backup geo-replication slave update-certificates. Например:

   ```
   # vinfra service backup geo-replication slave update-certificates \
   --dc-config-file primary_dc_updated.conf
   ```

7.2.5.4 Отключение георепликации

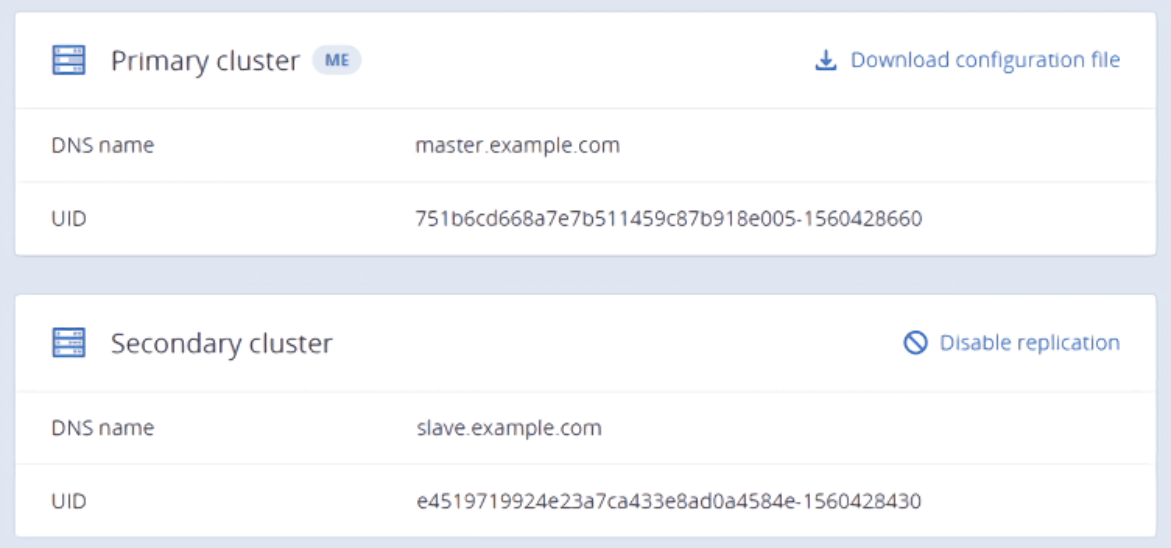
Предварительные требования

- Георепликация должна быть включена, как описано в разделе "Включение георепликации" на странице 356.

Чтобы отключить георепликацию

Панель администратора

1. В главном кластере перейдите на экран **Сервисы хранилища** > **Резервные копии** > **Георепликация** и щелкните **Отключить репликацию**.



2. Удалите подчиненный кластер из конфигурации георепликации, надлежащим образом по одному высвободив все его узлы из хранилища резервных копий.

Интерфейс командной строки

1. Отключите георепликацию на главном кластере с помощью команды infra service backup geo-replication master disable. Например:

```
# vinfra service backup geo-replication master disable
```

2. Удалите подчиненный кластер из конфигурации георепликации, надлежащим образом по одному высвободив все его узлы из хранилища резервных копий.

7.2.6 Настройка прокси для хранилища резервных копий

Использование хранилища резервных копий в режиме обратного прокси позволяет передавать данные резервного копирования в другие кластеры резервного копирования, служащие для выгрузки данных. Минимальная конфигурация прокси включает в себя одно хранилище резервных копий, работающее в режиме обратного прокси, и одно хранилище для выгрузки данных. При наличии дополнительных кластеров хранения резервных копий можно использовать их для выгрузки данных из хранилища резервных копий, работающего в режиме обратного прокси. Ниже дается описание конфигурации, которая включает в себя три кластера хранения резервных копий: одно хранилище резервных копий, работающее в режиме обратного прокси, и два хранилища для выгрузки данных.

Чтобы настроить прокси для хранилища резервных копий

1. В первом кластере хранения разверните автономное хранилище резервных копий, как описано в разделе "Подготовка пространства для хранилища резервных копий к работе" на странице 150. Как вариант, для развертывания можно использовать команду vinfra service backup cluster deploy-standalone. Например:

```
# vinfra service backup cluster deploy-standalone --nodes 2f3f6091-0d44-45aa-94e3-ebc2b65c0eeb \
--storage-type local --domain backup1.example.com --tier 0 --encoding 1+0 --failure-domain 0 \
--reg-account account@example.com --reg-server https://cloud.example.com/ --stdin
```

2. В первом кластере хранения превратите автономное хранилище резервных копий в хранилище для выгрузки данных резервного копирования с помощью команды vinfra service backup cluster turn-to-upstream. Например:

   ```
   # vinfra service backup cluster turn-to-upstream --address upstream1.example.com
   ```

   В этом примере upstream1.example.com — это адрес, который будет использоваться для хранилища для выгрузки данных резервного копирования.
3. Измените настройки сервера DNS следующим образом:
   a. Удалите имя DNS автономного хранилища из записей DNS.
   b. Добавьте имя DNS хранилища для выгрузки данных резервного копирования, которое может быть преобразовано в общедоступные IP-адреса для всех его узлов.
4. Во втором кластере хранения загрузите файл конфигурации хранилища для выгрузки данных резервного копирования с помощью команды vinfra service backup cluster download-upstream-info. Например:

   ```
   # vinfra service backup cluster download-upstream-info --output-file /root/upstream1.info \
   --vinfra-portal https://upstream1.example.com:8888 --vinfra-username admin --vinfra-password <password>
   ```

   В этом примере /root/upstream1.info — это файл конфигурации хранилища для выгрузки данных резервного копирования.
5. Во втором кластере хранения разверните хранилище резервных копий, которое будет работать в режиме обратного прокси, и зарегистрируйте для него хранилище для выгрузки данных. Для этого воспользуйтесь командой vinfra service backup cluster deploy-reverse-proxy. Например:

   ```
   # vinfra service backup cluster deploy-reverse-proxy --nodes 74cbd22b-fb1b-4441-ae52-532078c54f9a \
   --storage-type local --tier 0 --encoding 1+0 --failure-domain 0 --upstream-info-file /root/upstream1.info
   ```

   В этом примере /root/upstream1.info — это файл конфигурации хранилища для выгрузки данных резервного копирования, полученный ранее.
6. В записи DNS добавьте имя DNS первого хранилища резервных данных, которое может быть преобразовано в общедоступные IP-адреса для всех узлов, работающих в режиме обратного прокси.
7. В третьем кластере хранения разверните хранилище для выгрузки данных с помощью команды vinfra service backup cluster deploy-upstream. Например:

```
# vinfra service backup cluster deploy-upstream --nodes eeb06dce-4cfd-4c89-bc7f-
4689ea5c7058 \
--storage-type local --tier 0 --encoding 1+0 --failure-domain 0 --address upstream2.example.com
```

В этом примере upstream2.example.com — это адрес хранилища для выгрузки данных.

8. В записи DNS добавьте имя DNS нового хранилища для выгрузки данных, которое может быть преобразовано в общедоступные IP-адреса для всех его узлов.
9. Во втором кластере хранения загрузите файл конфигурации нового хранилища для выгрузки данных с помощью команды vinfra service backup cluster download-upstream-info. Например:

```
# vinfra service backup cluster download-upstream-info --output-file /root/upstream2.info \
--vinfra-portal https://upstream2.example.com:8888 --vinfra-username admin --vinfra-password
1q2w3e
```

10. Во втором кластере хранения зарегистрируйте для прокси новое хранилище для выгрузки данных с помощью команды vinfra service backup cluster add-upstream. Например:

```
# vinfra service backup cluster add-upstream --upstream-info-file /root/upstream2.info
```

Чтобы просматривать сведения о каждом процессе резервного копирования и возобновлять приостановленные процессы, используйте параметры --show и --retry команды vinfra service backup cluster process. Например, чтобы просмотреть сведения о состоянии процесса резервного копирования с идентификатором ee7e60c5-5447-4177-8581-26657ac380c0, выполните:

```
# vinfra service backup cluster process --show --process-id 15bf7eb1-9fbd-436a-8936-
33f7088c4933
+---------+--------------------------------------+
| Field   | Value                                |
+---------+--------------------------------------+
| failed  | False                                |
| id      | 15bf7eb1-9fbd-436a-8936-33f7088c4933 |
| message |                                      |
| state   | done                                 |
+---------+--------------------------------------+
```

Настройка обратного прокси для хранилища резервных данных завершена.

7.2.7 Настройка параметров TLS для хранилища резервных копий

Для фильтрации подключений к хранилищу резервных копий можно указать допустимые версии протокола TLS и криптографические алгоритмы.

Чтобы ограничить использование протоколов TLS 1.0 и 1.1

Укажите соответствующее значение для параметра advanced.min_tls_version в файле /etc/vstorage/abgw.config. Можно использовать следующие значения:

- 0: разрешить использование версий 1.0, 1.1 и 1.2 протокола TLS
- 1: разрешить использование версий 1.1 и 1.2 протокола TLS
- 2: разрешить использование только версии 1.2 протокола TLS

Например, чтобы разрешить использование всех версий протокола TLS, установите значение 0 следующим образом:

```
advanced.min_tls_version = 0
```

Чтобы разрешить подключения к хранилищу резервных копий только с использованием определенных криптографических алгоритмов

Укажите их в параметре advanced.tls_ciphers файла /etc/vstorage/abgw.config. Если клиент не использует ни один из указанных алгоритмов, подключение будет сброшено. Сведения о формате и полный набор алгоритмов см. на странице руководства по алгоритмам.

По умолчанию используются следующие алгоритмы:

- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA
- ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA
- DHE-RSA-AES128-SHA
- AES128-GCM-SHA256
- AES128-SHA256
- AES128-SHA

Обратите внимание на следующее:

- Если вы указали один алгоритм (например, RSA-AES128) и он не поддерживается, подключение будет сброшено.

- Если вы указали два алгоритма (например, CAMELIA и RSA-AES128) и поддерживается только один из них (например, CAMELIA), для подключения будет использован поддерживаемый алгоритм (в данном случае CAMELIA).
- Если указать пустое значение, все подключения будут завершаться сбоем.

Например, чтобы ограничить использование алгоритмов только алгоритмами ECDHE-ECDSA-CHACHA20-POLY1305 и ECDHE-RSA-CHACHA20-POLY1305, укажите их следующим образом, разделив двоеточием:

```
advanced.tls_ciphers = ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305
```

7.2.8 Просмотр и изменение параметров хранилища резервных копий

Предварительные требования

- Кластер хранилища резервных копий создан и зарегистрирован в панели управления облаком, как описано в разделе "Подготовка пространства для хранилища резервных копий к работе" на странице 150.

Чтобы просмотреть параметры хранилища резервных копий

Панель администратора

На экране **Сервисы хранилища** > **Резервные копии** > **Настройки** выберите раздел **Том NFS** или **Облачный сервис**. В выбранном разделе будут отображены параметры хранилища.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service backup storage-params show
```

Чтобы изменить параметры хранилища резервных копий

Панель администратора

1. На экране **Сервисы хранилища** > **Резервные копии** > **Настройки** выберите раздел **Том NFS** или **Облачный сервис**.
2. Измените значения параметров и нажмите **Сохранить**.

Интерфейс командной строки

Внимание
Изменяйте параметры хранилища с осторожностью и только в рамках существующей конфигурации. Можно изменить IP-адрес внешнего хранилища или учетные данные для доступа к нему.

Используйте следующую команду:

```
vinfra service backup storage-params change --storage-type {local,nfs,
                                            s3,swift,azure,google}
                                            [--nfs-host <host>]
                                            [--nfs-export <export>]
                                            [--nfs-version <version>]
                                            [--s3-flavor <flavor>]
                                            [--s3-region <region>]
                                            [--s3-bucket <bucket>]
                                            [--s3-endpoint <endpoint>]
                                            [--s3-access-key-id <access-key-id>]
                                            [--s3-secret-key-id <secret-key-id>]
                                            [--s3-cert-verify <cert-verify>]
                                            [--swift-auth-url <auth-url>]
                                            [--swift-auth-version <auth-version>]
                                            [--swift-user-name <user-name>]
                                            [--swift-api-key <api-key>]
                                            [--swift-domain <domain>]
                                            [--swift-domain-id <domain-id>]
                                            [--swift-tenant <tenant>]
                                            [--swift-tenant-id <tenant-id>]
                                            [--swift-tenant-domain <tenant-domain>]
                                            [--swift-tenant-domain-id <tenant-domain-id>]
                                            [--swift-trust-id <trust-id>]
                                            [--swift-region <region>]
                                            [--swift-internal <internal>]
                                            [--swift-container <container>]
                                            [--swift-cert-verify <cert-verify>]
                                            [--azure-endpoint <endpoint>]
                                            [--azure-container <container>]
                                            [--azure-account-name <account-name>]
                                            [--azure-account-key <account-key>]
                                            [--google-bucket <bucket>]
                                            [--google-credentials <credentials>]
```

--storage-type {local,nfs,s3,swift,azure,google}

Тип хранилища

Параметры хранилища типа nfs:

--nfs-host <host>

Имя хоста или IP-адрес NFS

--nfs-export <export>

Полный путь к экспорту NFS

--nfs-version <version>

Версия NFS (3 или 4)

Параметры хранилища типа s3:

--s3-flavor <flavor> (необязательно)

Имя типа BM

--s3-region <region> (необязательно)

Задайте регион для Amazon S3.

--s3-bucket <bucket>

Имя корзины

--s3-endpoint <endpoint>

URL-адрес оконечной точки

--s3-access-key-id <access-key-id>

Идентификатор ключа доступа

--s3-secret-key-id <secret-key-id>

Идентификатор секретного ключа

--s3-cert-verify <cert-verify> (необязательно)

Разрешить самозаверяющий сертификат оконечной точки S3

Параметры хранилища типа swift:

--swift-auth-url <auth-url>

URL аутентификации (Keystone)

--swift-auth-version <auth-version> (необязательно)

Версия протокола проверки подлинности

--swift-user-name <user-name>

Имя пользователя

--swift-api-key <api-key>

Ключ API (пароль)

--swift-domain <domain> (необязательно)

Имя домена

--swift-domain-id <domain-id> (необязательно)

Идентификатор домена

--swift-tenant <tenant> (необязательно)

Имя тенанта

--swift-tenant-id <tenant-id> (необязательно)

Идентификатор тенанта

--swift-tenant-domain <tenant-domain> (необязательно)

Имя домена тенанта

--swift-tenant-domain-id <tenant-domain-id> (необязательно)

Идентификатор домена тенанта

--swift-trust-id <trust-id> (необязательно)

Идентификатор Trust

--swift-region <region> (необязательно)

Имя региона

--swift-container <container> (необязательно)

Имя контейнера

--swift-cert-verify <cert-verify> (необязательно)

Разрешить самозаверяющий сертификат оконечной точки Swift (true или false)

Параметры хранилища типа azure:

--azure-endpoint <endpoint>

URL-адрес оконечной точки

--azure-container <container>

Имя контейнера

--azure-account-name <account-name>

Имя учетной записи

--azure-account-key <account-key>

Ключ учетной записи

Параметры хранилища типа google:

--google-bucket <bucket>

Имя корзины Google

--google-credentials <credentials>

Путь к файлу с учетными данными Google

Например, чтобы изменить параметры хранилища NFS, выполните:

```
# vinfra service backup storage-params change --storage-type nfs --nfs-host \
10.94.129.71 --nfs-export /myshare/myexport --nfs-version 4
Operation successful.
```

7.2.9 Высвобождение серверов из хранилища резервных копий

Хранилище резервных копий подключено к определенному месту назначения резервных копий. Если необходимо поменять место назначения, например с публичного облака на локальный кластер хранилища или с одной корзины облачного сервиса на другую, необходимо удалить хранилище резервных копий путем освобождения всех его серверов из кластера хранилища и создать новое.

При удалении хранилища резервных копий также отменяется его регистрация в продукте Кибер Бэкап, который теряет доступ к месту назначения резервных копий.

Ограничения

- Если выбрать принудительное освобождение и сохранить регистрацию Backup Gateway в продукте Кибер Бэкап, то в следующий раз необходимо будет зарегистрировать в продукте другой шлюз. Для этого придется удалить и создать заново не только хранилище резервных копий, но и весь кластер хранилища.

Предварительные требования

- Кластер хранилища резервных копий создан и зарегистрирован в панели управления облаком, как описано в разделе "Подготовка пространства для хранилища резервных копий к работе" на странице 150.

Как освободить сервер из хранилища резервных копий

Панель администратора

1. Перейдите на экран **Сервисы хранилища** > **Резервные копии** > **Серверы**.
2. Щелкните по нужному серверу, а затем на правой панели сервера нажмите **Освободить**.
3. Нажмите **Освободить** в окне подтверждения.

Хранилище резервных копий остается в рабочем состоянии, пока в нем есть хотя бы один сервер.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service backup node release --nodes <nodes>
```

--nodes <nodes>

Список имен хостов или идентификаторов серверов через запятую

Например, чтобы освободить сервер с идентификатором 2f3f6091-0d44-45aa-94e3-ebc2b65c0eeb из кластера хранилища резервных копий, выполните:

```
# vinfra service backup node release --nodes 2f3f6091-0d44-45aa-94e3-ebc2b65c0eeb
+---------+--------------------------------------+
| Field   | Value                                |
+---------+--------------------------------------+
| task_id | ea09642c-291c-4df8-87a5-a8958d6308c1 |
+---------+--------------------------------------+
```

Как освободить все серверы из хранилища резервных копий

Панель администратора

1. Перейдите на экран **Сервисы хранилища** > **Резервные копии** > **Серверы**.
2. Выберите все серверы резервного копирования или щелкните по единственному серверу в кластере хранилища резервных копий и нажмите **Освободить**.
3. В окне **Освободить серверы**:

- Выберите **(Рекомендуется) Корректно**, чтобы удалить шлюз Backup Gateway с сервера и отменить его регистрацию в продукте Кибер Бэкап.
- Выберите **Принудительно**, чтобы удалить шлюз Backup Gateway с сервера, но не отменять его регистрацию в продукте Кибер Бэкап.

  Внимание
  Выбирайте этот вариант, только если уверены, что регистрация шлюза в продукте Кибер Бэкап уже отменена.

4. Если вы выбрали штатное освобождение, укажите данные учетной записи администратора для продукта Кибер Бэкап.
5. Нажмите кнопку **Освободить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service backup cluster release [--reg-account <reg-account>] [--force] [--stdin]
```

--reg-account <reg-account>
: Партнерская учетная запись в облаке или учетная запись администратора организации на локальном сервере управления

--force
: Освобождает ресурсы резервного кластера, но не отменяет его регистрацию в программе резервного копирования.

  Примечание
  Выбирайте этот вариант, только если уверены, что регистрация кластера уже удалена из программы резервного копирования.

--stdin
: Используется для настройки пароля регистрации из stdin.

Например, чтобы удалить резервный кластер со всеми данными и отменить его регистрации в программе резервного копирования, выполните:

```
# vinfra service backup cluster release --reg-account account@example.com --stdin
```

Укажите пароль регистрации.

7.3 Управление блочным хранилищем

В этом разделе описывается, как управлять группами целевых устройств, целевыми устройствами и томами iSCSI. Также здесь приводятся инструкции по ограничению доступа к группам целевых устройств с помощью CHAP или списков ACL.

7.3.1 Управление группами целевых устройств

Предварительные требования

- Создана группа целевых устройств, как описано в разделе "Создание групп целевых устройств" на странице 199.

Чтобы запустить или остановить все целевые устройства в группе

Панель администратора

1. Откройте **Сервисы хранилища** > **Блочное хранилище** > **Группы целей**.
2. Щелкните по значку многоточия для нужной целевой группы и нажмите **Запустить цели** или **Остановить цели**.

Интерфейс командной строки

При создании группы ее целевые устройства изначально остановлены. Их можно запустить с помощью команды vstorage-target tg-start, например:

```
# vstorage-target tg-start -id 3d8364f5-b830-4211-85af-3a19d30ebac4
```

Эта команда запускает все целевые устройства в группе с идентификатором 3d8364f5-b830-4211-85af-3a19d30ebac4.

Все целевые устройства в группе могут быть либо запущены, либо остановлены, поэтому при добавлении целевых устройств в группу уже запущенных новые устройства запускаются автоматически.

Чтобы остановить группу целевых устройств, используйте команду vstorage-target tg-stop, например:

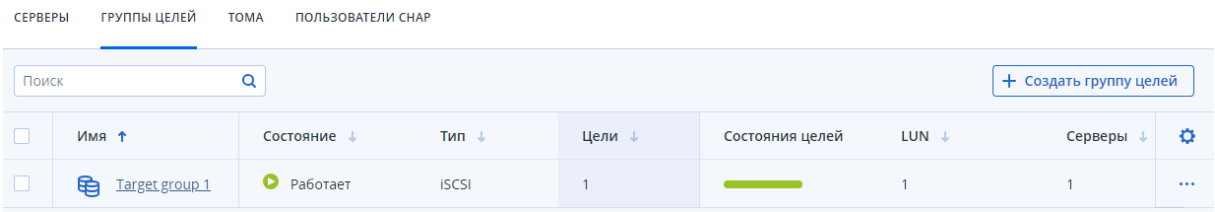
```
# vstorage-target tg-stop -id 3d8364f5-b830-4211-85af-3a19d30ebac4
```

Эта команда останавливает все целевые устройства в группе с идентификатором 3d8364f5-b830-4211-85af-3a19d30ebac4.

Чтобы просмотреть список групп целевых устройств

Панель администратора

На экране **Сервисы хранилища** > **Блочное хранилище** перейдите на вкладку **Группы целей**.



Интерфейс командной строки

Используйте команду vstorage-target tg-list, которая отображает базовую информацию о группах, например:

```
# vstorage-target tg-list
[
 {
  "Id": "3d8364f5-b830-4211-85af-3a19d30ebac4",
  "Name": "tg1",
  "Type": "ISCSI",
  "Running": true,
  "ACL": false,
  "ChapAuth": false,
  "CHAP": {},
  "Mode": 0
 },
 {
  "Id": "78c3b51e-fd9a-485b-91ce-bc0a8171c89d",
  "Name": "tg2",
  "Type": "ISCSI",
  "Running": false,
  "ACL": false,
  "ChapAuth": false,
  "CHAP": {},
  "Mode": 0
 }
]
```

Чтобы вывести полную информацию обо всех группах целевых устройств, используйте команду vstorage-target tg-list -all.

Чтобы просмотреть сведения о группе целевых устройств

Панель администратора

На экране **Сервисы хранилища** > **Блочное хранилище** > **Группы целей** щелкните по группе целевых устройств. В правой панели будут отображены сведения об этой группе целевых устройств.

Интерфейс командной строки

Используйте команду vstorage-target tg-status, например:

```
# vstorage-target tg-status -id faeacacd-eba6-416c-9a7f-b5ba9e372e16
```

Эта команда выводит полные сведения о группе целевых устройств с идентификатором faeacacd-eba6-416c-9a7f-b5ba9e372e16. Обратите внимание на параметр NodeState. Он указывает, синхронизирован ли сервер с группой целевых устройств, то есть имеет сведения о ее текущей конфигурации. Могут отображаться следующие состояния:

- synced: сервер синхронизирован с группой целевых устройств.
- syncing: сервер синхронизируется с группой целевых устройств.

- failed: серверу не удалось синхронизироваться с группой целевых устройств (сведения см. в параметре Error).
- offline: сервер не в сети.
- disabled: сервер отключен, его целевое устройство не в сети.

Чтобы включить или выключить постоянное резервирование SCSI

Резервирование SCSI-2 позволяет инициаторам получить эксклюзивный доступ к LUN и одновременно предотвращает изменения этого LUN другими инициаторами. Такое резервирование обычно снимается инициатором после внесения изменений в LUN. Однако оно также снимается при сбоях инициатора или сбросе логических единиц. В SCSI-3 вводится постоянное резервирование, которое сохраняется в случае сбоя или сброса и снимается самим инициатором при необходимости. Оно также позволяет нескольким инициаторам организованно обращаться к LUN.

В продукте Кибер Инфраструктура постоянное резервирование используется в основном для поддержки серверов Microsoft Hyper-V, работающих в отказоустойчивых кластерах.

Постоянное резервирование SCSI включено по умолчанию. Его можно включить или отключить для всех томов в группе целевых устройств следующим образом.

```
# vstorage-target tg-pr -id <tg_ID> -enable
# vstorage-target tg-pr -id <tg_ID> -disable
```

В этих командах tg_ID – это идентификатор группы целевых устройств, для которой задается постоянное резервирование.

Примечание
Для работы постоянного резервирования сервис vstorage-target-manager должен быть запущен на всех серверах MDS.

Чтобы удалить целевую группу

Панель администратора

1. Откройте **Сервисы хранилища** > **Блочное хранилище** > **Группы целей**.
2. Щелкните по значку многоточия для нужной целевой группы и нажмите **Удалить**.
3. Если для целевой группы имеются активные подключения, установите флажок в поле **Принудительно**.
4. Нажмите **Удалить** в окне подтверждения.

Интерфейс командной строки

Используйте команду vstorage-target tg-delete, например:

```
# vstorage-target tg-delete -id 3d8364f5-b830-4211-85af-3a19d30ebac4
```

Эта команда удаляет группу целевых устройств с идентификатором 3d8364f5-b830-4211-85af-3a19d30ebac4.

7.3.2 Управление целевыми устройствами и их порталами

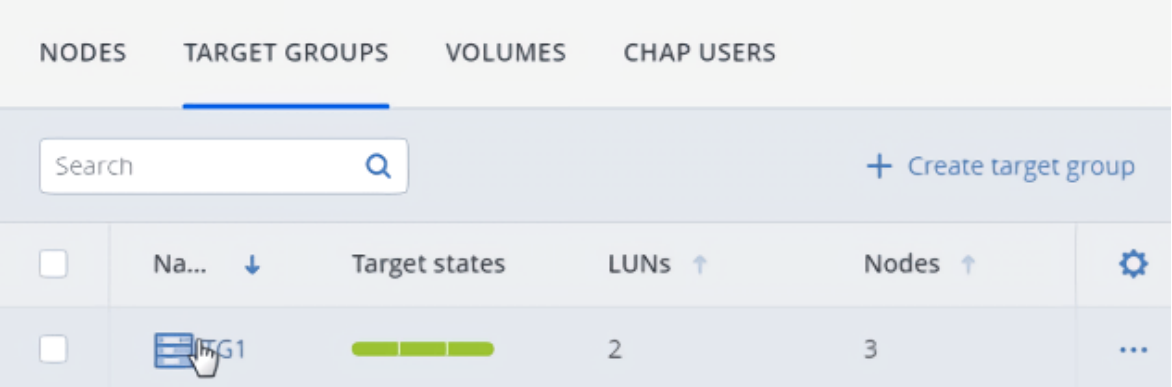
Предварительные требования

- Создана группа целевых устройств, как описано в разделе "Создание групп целевых устройств" на странице 199.

Чтобы добавить целевое устройство в группу

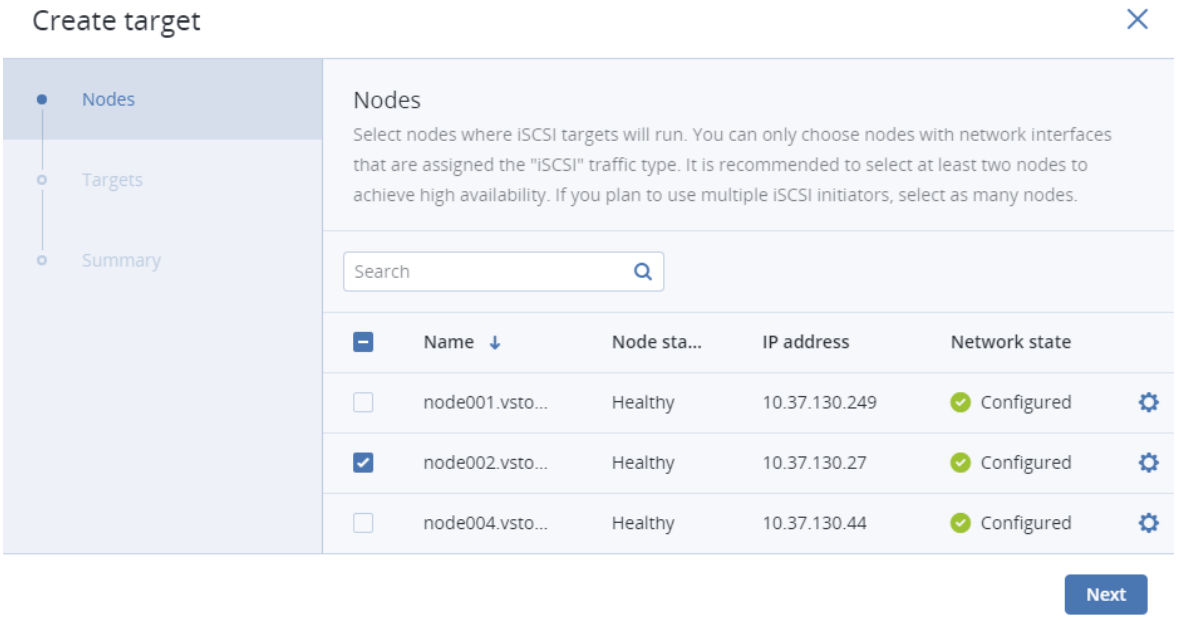
Панель администратора

1. Откройте **Сервисы хранилища** > **Блочное хранилище** > **Группы целей** и щелкните по имени нужной группы, чтобы открыть ее.

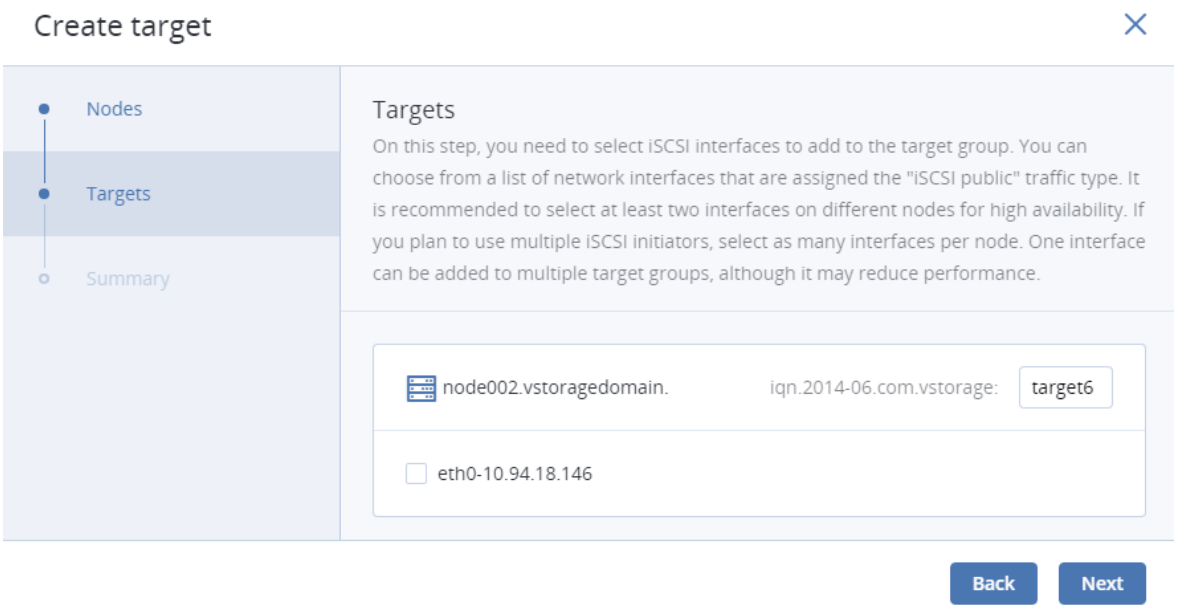


2. На вкладке **Цели** нажмите **Добавить цель**. Откроется мастер **Создать цель**.
3. На экране **Серверы** выберите серверы для добавления в группу целевых устройств. На этих серверах будут запускаться целевые устройства iSCSI. Можно выбирать только серверы с сетевыми интерфейсами, которым назначен тип трафика **iSCSI**. Рекомендуется добавить в группу целевых устройств как минимум два сервера для обеспечения высокой доступности. Если планируется использовать несколько инициаторов iSCSI, следует добавить столько же серверов в целевую группу. Оптимальный вариант – создать по одному целевому устройству на сервер.

   Если сетевые интерфейсы серверов не настроены, щелкните по значку шестерни, выберите необходимые сети и нажмите **Применить**.



4. На экране **Цели** выберите интерфейсы iSCSI для добавления в группу целевых устройств. Возможен выбор из списка сетевых интерфейсов, которым назначен тип трафика **iSCSI**. Если планируется использовать несколько инициаторов iSCSI, следует выбрать по такому же количеству интерфейсов на каждый сервер. Один интерфейс можно добавить в несколько групп целевых устройств, хотя это может снизить производительность.



5. На экране **Сводка** просмотрите сведения о целевом устройстве. При необходимости можно вернуться назад и изменить их. Нажмите кнопку **Далее**.

Созданное целевое устройство появится на вкладке **Цели**.

Интерфейс командной строки

Как правило, целевые устройства создаются автоматически при создании групп или добавлении в них серверов. Однако, поскольку можно удалить целевые устройства с сервера, не удаляя его из группы, на таком сервере можно снова создать целевые устройства. Используйте команду vstorage-target target-create, например:

```
# vstorage-target target-create -tg 3d8364f5-b830-4211-85af-3a19d30ebac4 \
-json target.json
```

Эта команда создает целевое устройство на базе файла конфигурации target.json в группе целевых устройств с идентификатором 3d8364f5-b830-4211-85af-3a19d30ebac4. В файле конфигурации перечислены сведения о целевом устройстве, такие как сервер для создания, WWN и портал, например:

```
{
 "NodeId": "bbfd0e7a26b1406d",
 "WWN": "iqn.2013-10.com.vstorage:test22",
 "Portals": [
  {
   "Addr": "10.94.104.90",
   "Port": 3260
  }
 ]
}
```

Чтобы добавить или удалить порталы целевых устройств

Используйте команду vstorage-target target-portal add, например:

```
# vstorage-target target-portal add -wwn iqn.2013-10.com.vstorage:test2 \
-addr 10.94.104.90 -tg 3d8364f5-b830-4211-85af-3a19d30ebac4
```

Эта команда добавляет портал с IP-адресом 10.94.104.90 и стандартным портом 3260 для целевого устройства с IQN iqn.2013-10.com.vstorage:test2 в группе целевых устройств с идентификатором 3d8364f5-b830-4211-85af-3a19d30ebac4.

Чтобы удалить портал для целевого устройства, используйте команду vstorage-target target-portal del, например:

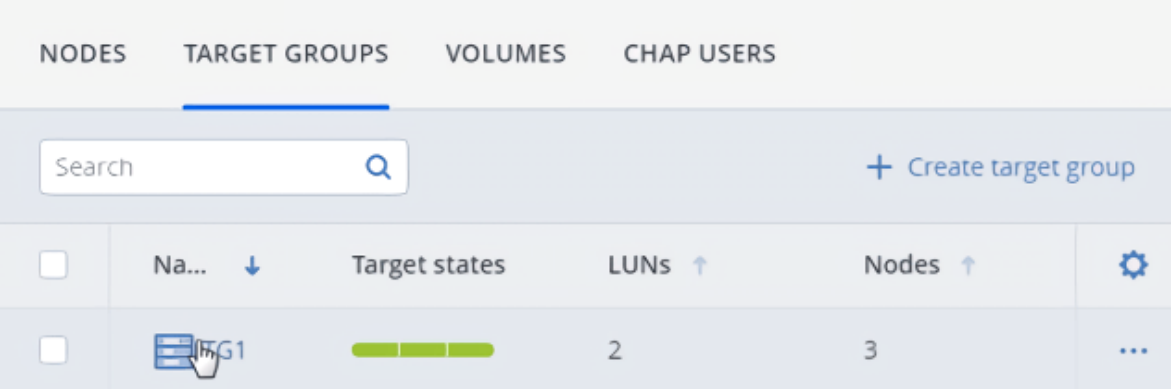
```
# vstorage-target target-portal del -wwn iqn.2013-10.com.vstorage:test2 \
-addr 10.94.104.90 -tg 3d8364f5-b830-4211-85af-3a19d30ebac4
```

Эта команда удаляет ранее созданный портал.

Чтобы удалить целевое устройство из группы

Панель администратора

1. Откройте **Сервисы хранилища** > **Блочное хранилище** > **Группы целей** и щелкните по имени нужной группы, чтобы открыть ее.



2. На вкладке **Цели** нажмите кнопку с многоточием для нужного целевого устройства, затем нажмите **Удалить**.
3. Нажмите **Удалить** в окне подтверждения. Чтобы удалить целевое устройство, у которого имеются активные подключения, установите флажок **Принудительно**.

Если удалить целевое устройство по активному/оптимизированному пути (указанному в сведениях о LUN), то этот путь переключится на другое целевое устройство.

Интерфейс командной строки

Используйте команду vstorage-target target-delete, например:

```
# vstorage-target target-delete -tg 3d8364f5-b830-4211-85af-3a19d30ebac4 \
-wwn iqn.2013-10.com.vstorage:test22
```

Эта команда удаляет целевое устройство с IQN iqn.2013-10.com.vstorage:test22 из группы с идентификатором 3d8364f5-b830-4211-85af-3a19d30ebac4, а также с сервера, на котором оно расположено.

Сервер, на котором не осталось целевых устройств, удаляется из группы.

7.3.3 Управление томами

Предварительные требования

- Том блочного хранилища создан в соответствии с инструкциями в разделе "Создание томов" на странице 204.
- Том подключен к целевой группе в соответствии с инструкциями в разделе "Присоединение томов к группам целевых устройств" на странице 205.

Чтобы вывести сведения о томах

Используйте команду vstorage-target vol-list, например:

```
# vstorage-target vol-list
[
 "3277153b-5296-49c5-9b66-4c200ddb343d",
```

```
  "a12110d5-cbbc-498a-acdd-a8567286f927",
  "d5cc3c13-cfb4-4890-a20d-fb80e2a56278"
]
```

Используйте команду vstorage-target vol-stat -all для печати подробных сведений обо всех томах. Чтобы напечатать сведения о конкретном томе, выполните команду vstorage-target vol-stat -id <vol_ID>.

Чтобы задать активный/оптимизированный путь для тома iSCSI

Используйте команду vstorage-target vol-set. Она будет работать, только если указанный сервер находится в состоянии STABLE.

Примечание
Убедитесь, что новый предпочитаемый сервер доступен для инициатора.

```
# vstorage-target vol-set -id 3d8364f5-b830-4211-85af-3a19d30ebac4 \
-pref-node bbfd0e7a26b1406d
```

Эта команда устанавливает активный/оптимизированный путь для тома с идентификатором 3d8364f5-b830-4211-85af-3a19d30ebac4 через сервер с идентификатором bbfd0e7a26b1406d.

Чтобы просмотреть и настроить параметры тома

Используйте команды vstorage-target vol-attr get и vstorage-target vol-attr set, например:

```
# vstorage-target vol-attr get -id d5cc3c13-cfb4-4890-a20d-fb80e2a56278
{
  "chunk-size": "268435456",
  "client-ssd-cache": "1",
  "failure-domain": "host",
  "replicas": "3:2",
  "tier": "0"
}
# vstorage-target vol-attr set -id d5cc3c13-cfb4-4890-a20d-fb80e2a56278 \
-vstorage-attr "replicas=2:1 tier=1"
```

Первая команда отображает параметры тома с идентификатором d5cc3c13-cfb4-4890-a20d-fb80e2a56278. Вторая команда устанавливает для этого тома режим избыточности с 2 репликами и уровень хранилища 1.

Чтобы просмотреть информацию ALUA для тома iSCSI

Используйте команду vstorage-target vol-info, например:

```
# vstorage-target vol-info -id 3d8364f5-b830-4211-85af-3a19d30ebac4
Volume ID:     3d8364f5-b830-4211-85af-3a19d30ebac4
Name:          vol1
Size:          1073741824
```

```
Used:        1073152
Serial:      d2be0e84fd7f
Attrs:       map[]
TG:          4708b908-8c2d-444c-91b1-a1e18a96d4fc
LUN:         0

                    *** Node #0 ***
                ------------------------
   NodeId:              bbfd0e7a26b1406d
    State:                    synced
     TPGs:              vstorage_tpg_0
     ALUA:                    active
Preferred:                         1
     WWNs: iqn.2014-06.com.vstorage:target1 [2]
  Portals:                  10.37.130.61
```

Эта команда отображает сведения ALUA для тома с идентификатором 3d8364f5-b830-4211-85af-3a19d30ebac4.

Чтобы увеличить размер тома

Панель администратора

1. Перейдите на экран **Сервисы хранилища** > **Блочное хранилище** > **Тома** и щелкните по имени нужного тома.
2. В правой панели щелкните значок карандаша рядом с параметром **Размер**.
3. В окне **Изменить размер тома** в поле **Размер** укажите необходимое значение и нажмите **Сохранить**.

Интерфейс командной строки

Используйте команду vstorage-target vol-grow, например:

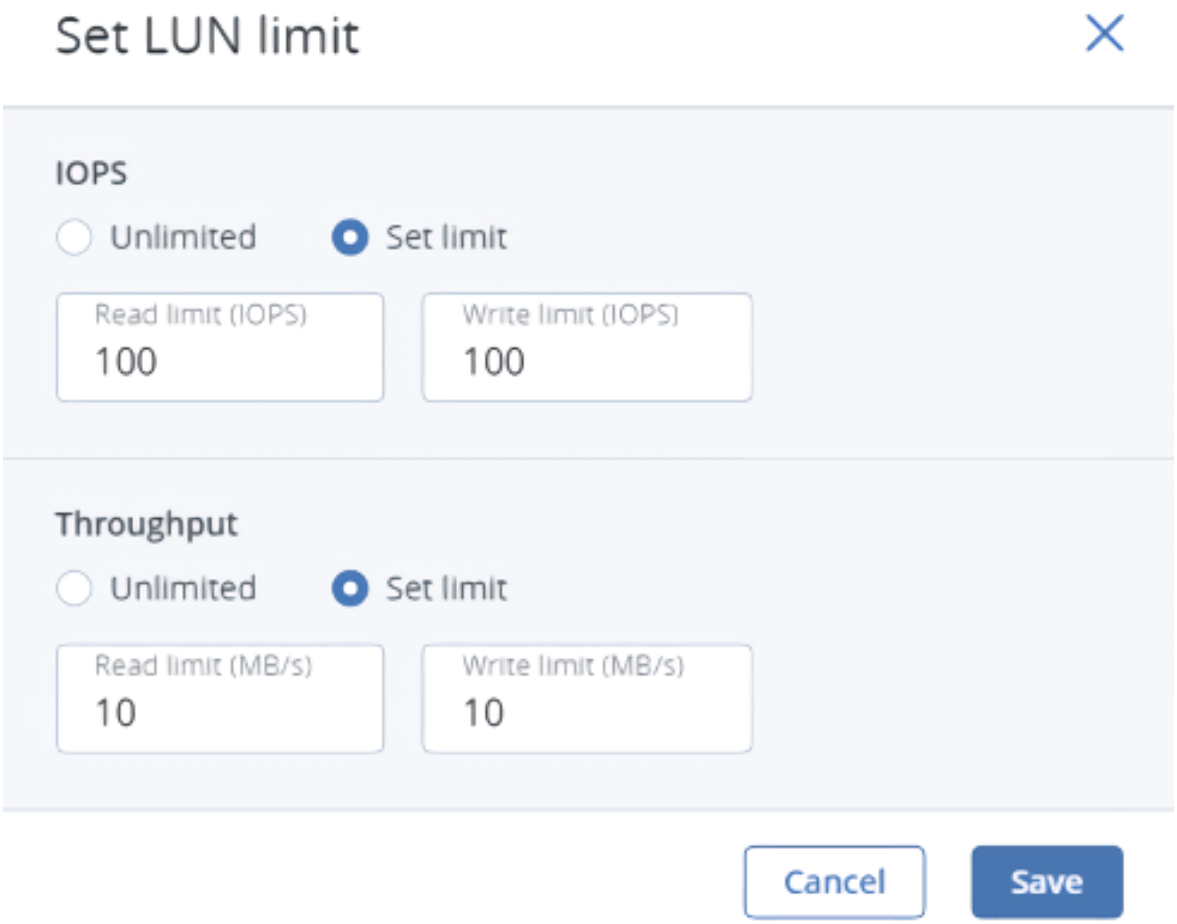
```
# vstorage-target vol-grow -id d5cc3c13-cfb4-4890-a20d-fb80e2a56278 -size 2G
```

Эта команда увеличивает размер тома с идентификатором d5cc3c13-cfb4-4890-a20d-fb80e2a56278 до 2 ГБ.

Чтобы задать ограничение на чтение/запись для тома, присоединенного как LUN

Панель администратора

1. Откройте **Сервисы хранилища** > **Блочное хранилище** > **Группы целей**, щелкните по имени нужной группы целевых устройств, чтобы открыть ее, и переключитесь на **LUN**.
2. Щелкните по нужному LUN, чтобы открыть сведения о нем, затем щелкните по значку карандаша в поле **Пределы**.
3. В окне **Установить пределы LUN** введите максимально допустимые значения и нажмите кнопку **Сохранить**.



Заданные квоты будут показаны в сведениях о LUN.

Интерфейс командной строки

Чтобы задать ограничения на чтение/запись для тома, используйте команду vstorage-target vol-limits, например:

```
# vstorage-target vol-limits -id d5cc3c13-cfb4-4890-a20d-fb80e2a56278 \
-read-bps 10485760 -write-bps 10485760
```

Эта команда задает для тома с идентификатором d5cc3c13-cfb4-4890-a20d-fb80e2a56278 скорость чтения/записи 10 485 760 байт в секунду.

Чтобы отсоединить том от целевой группы

Панель администратора

1. Откройте **Сервисы хранилища** > **Блочное хранилище** > **Группы целей**, щелкните по имени нужной группы целевых устройств, чтобы открыть ее, и переключитесь на **LUN**.
2. Нажмите кнопку многоточия для нужного LUN и выберите **Отсоединить**.

Либо можно открыть **Сервисы хранилища** > **Блочное хранилище** > **Тома**, щелкнуть по значку многоточия для нужного тома и нажать **Отсоединить**.

Интерфейс командной строки

Чтобы отсоединить том от группы целевых устройств, используйте команду vstorage-target tg-detach. LUN 0 должен быть отсоединен последним, например:

```
# vstorage-target tg-detach -id 3d8364f5-b830-4211-85af-3a19d30ebac4 \
-volume d5cc3c13-cfb4-4890-a20d-fb80e2a56278
```

Эта команда отсоединяет том с идентификатором d5cc3c13-cfb4-4890-a20d-fb80e2a56278 от целевой группы с идентификатором 3d8364f5-b830-4211-85af-3a19d30ebac4.

Чтобы удалить том, не подключенный к целевой группе

Панель администратора

1. Откройте **Сервисы хранилища** > **Блочное хранилище** > **Тома**.
2. Щелкните по значку многоточия для нужного тома и нажмите **Удалить**.

Интерфейс командной строки

Для удаления тома используйте команду vstorage-target vol-delete. Тома, присоединенные к группам целевых устройств, удалить нельзя, например:

```
# vstorage-target vol-delete -id d5cc3c13-cfb4-4890-a20d-fb80e2a56278
```

Эта команда удаляет том с идентификатором d5cc3c13-cfb4-4890-a20d-fb80e2a56278.

7.3.4 Ограничение доступа к группам целевых устройств

Можно ограничить доступ к целым группам целевых устройств (и всем присоединенным к ним томам) путем авторизации на основе ACL, а также проверки подлинности на основе пароля (CHAP).

Предварительные требования

- Созданная группа целевых устройств (как описано в разделе "Создание групп целевых устройств" на странице 199).

7.3.4.1 Управление списками управления доступом

Список управления доступом (ACL) позволяет контролировать доступ к LUN группы целевых устройств. Каждая запись списка содержит IQN инициатора и номера LUN, к которым этому инициатору разрешен доступ. Инициаторы, отсутствующие в списке, не обладают доступом к каким-либо LUN группы целевых устройств.

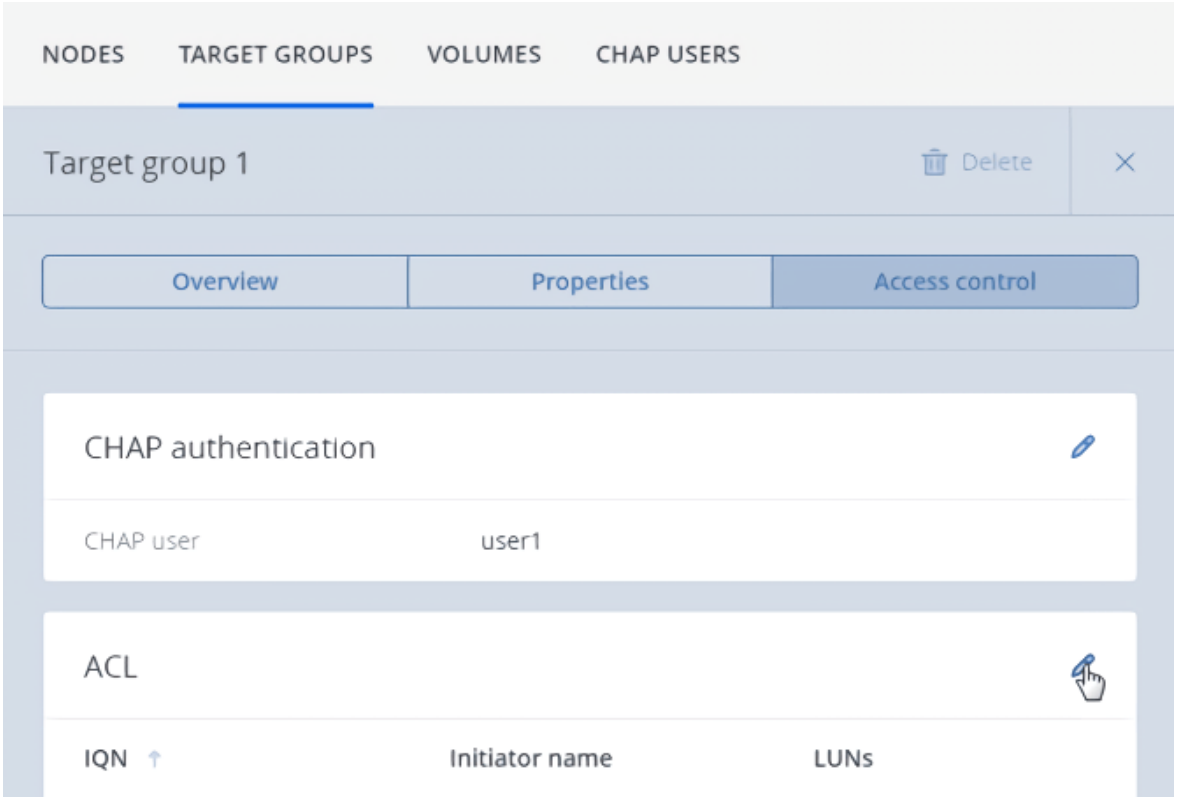
Примечание
Вышеописанное поведение списков контроля доступа введено в версии 5.5 продукта Кибер Инфраструктура. В предыдущих версиях инициаторы, указанные в списке, обладали доступом только к заданным LUN группы целевых устройств, а инициаторы вне списка – ко всем LUN группы. Для групп целевых устройств, созданных до обновления до версии 5.5, будет сохранено старое поведение списков контроля доступа, а сами группы будут помечены тегом **Не эксклюзивная**.

Предварительные требования

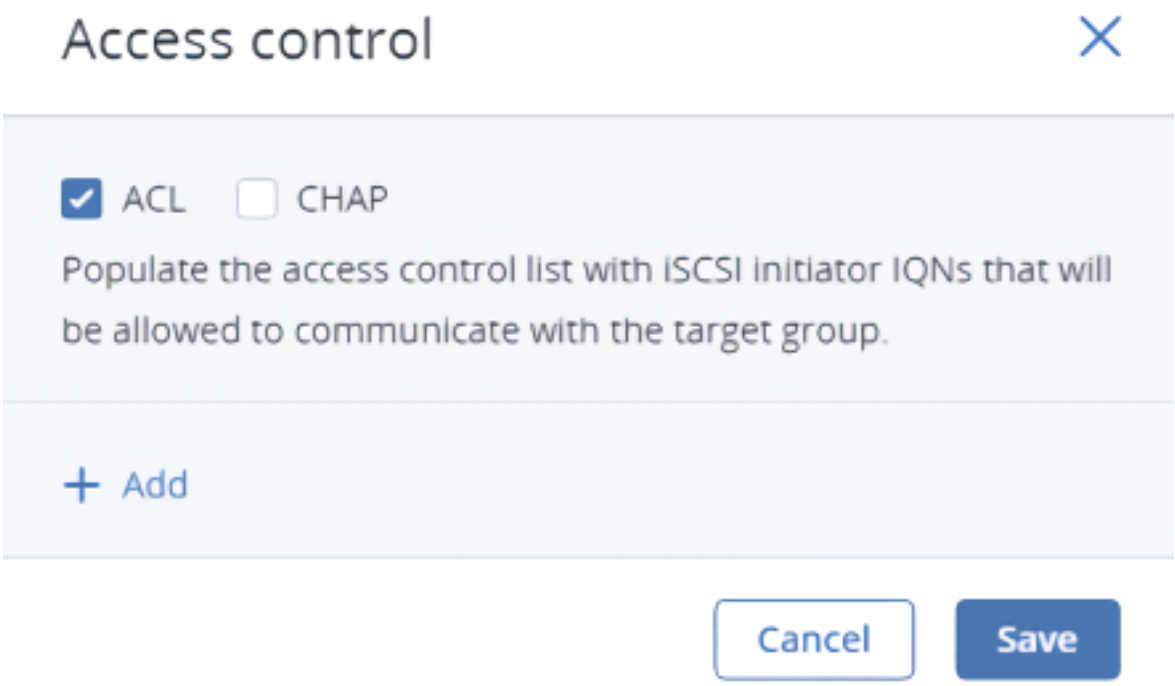
- Создана группа целевых устройств, как описано в разделе "Создание групп целевых устройств" на странице 199.

Чтобы добавить инициатор в список ACL группы целевых устройств

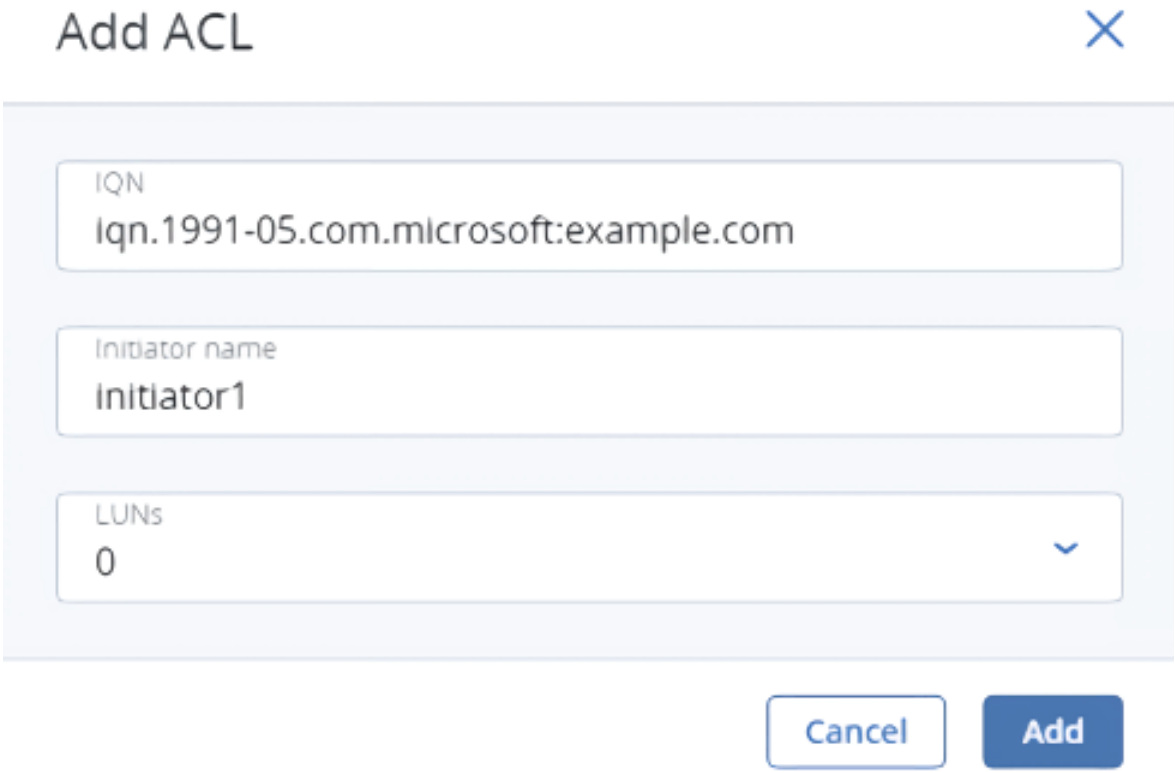
1. Откройте **Сервисы хранилища** > **Блочное хранилище** > **Группы целей** и щелкните по нужной группе целевых устройств в списке (в любом месте, кроме имени группы).
2. На правой панели группы нажмите **Контроль доступа**, затем щелкните по значку карандаша.



3. В окне **Контроль доступа** установите флажок **ACL** и нажмите кнопку **Добавить**.



4. В окне **Добавить список ACL** укажите IQN инициатора, введите псевдоним, выберите LUN, к которым он сможет получить доступ, и нажмите кнопку **Добавить**. Инициатор появится в списке ACL.



5. Заполнив список ACL инициаторами, нажмите кнопку **Сохранить**.

Чтобы изменить или удалить инициаторы в списке ACL

1. Щелкните по значку карандаша в сведениях о группе целевых устройств.
2. В окне **Контроль доступа** щелкните по значку карандаша для нужного инициатора и нажмите **Изменить** или **Удалить**.
3. Изменив список ACL, нажмите кнопку **Сохранить**.

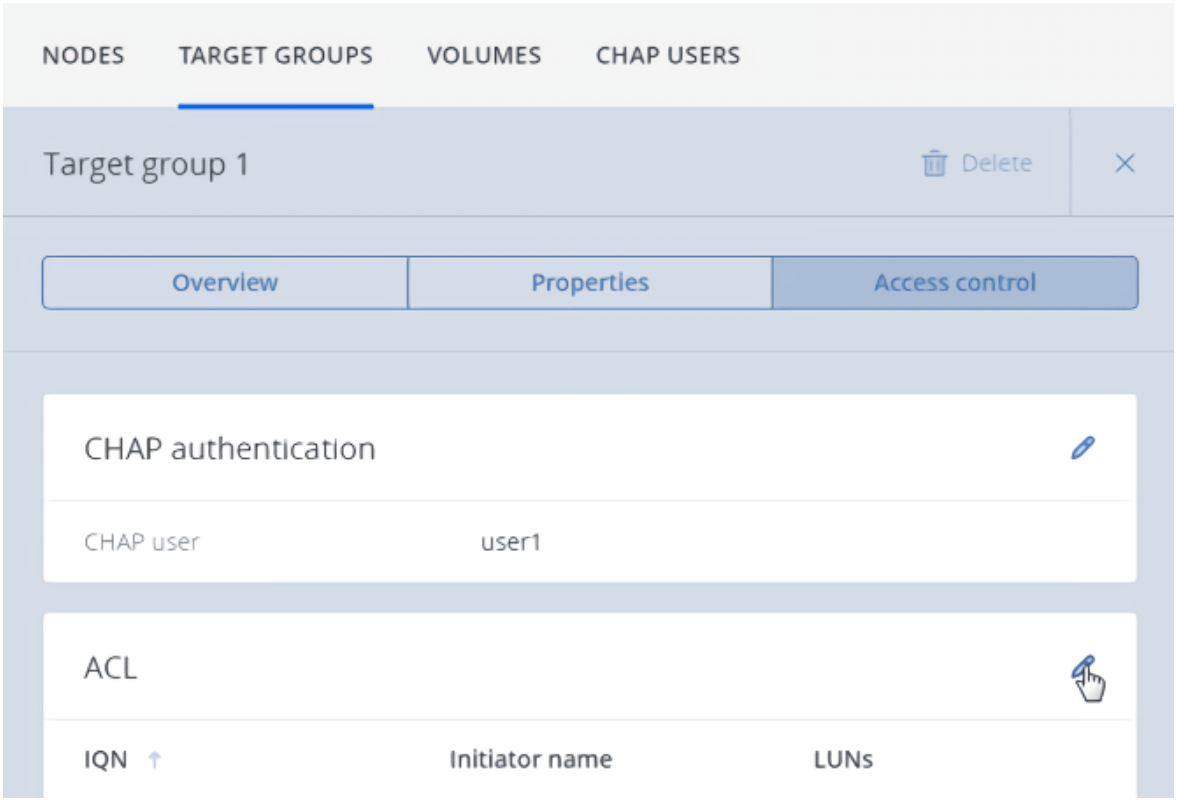
7.3.4.2 Управление пользователями CHAP

Протокол CHAP (Challenge-Handshake Authentication Protocol) предоставляет способ ограничить доступ к целевым устройствам и их LUN, требуя от инициатора имя пользователя и пароль. Учетные записи CHAP применяются к целым группам целевых устройств.

Чтобы ограничить доступ к группе целевых устройств определенным пользователем CHAP

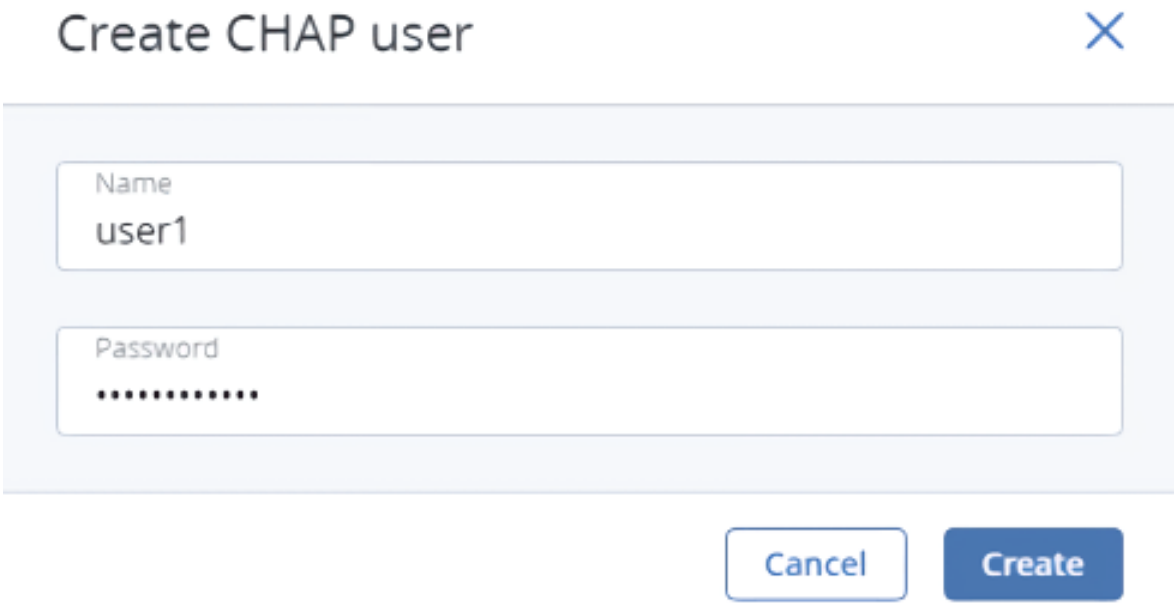
Панель администратора

1. Откройте **Сервисы хранилища** > **Блочное хранилище** > **Группы целей** и щелкните по нужной группе целевых устройств в списке (в любом месте, кроме имени группы).
2. На правой панели группы нажмите **Контроль доступа**, затем щелкните по значку карандаша.

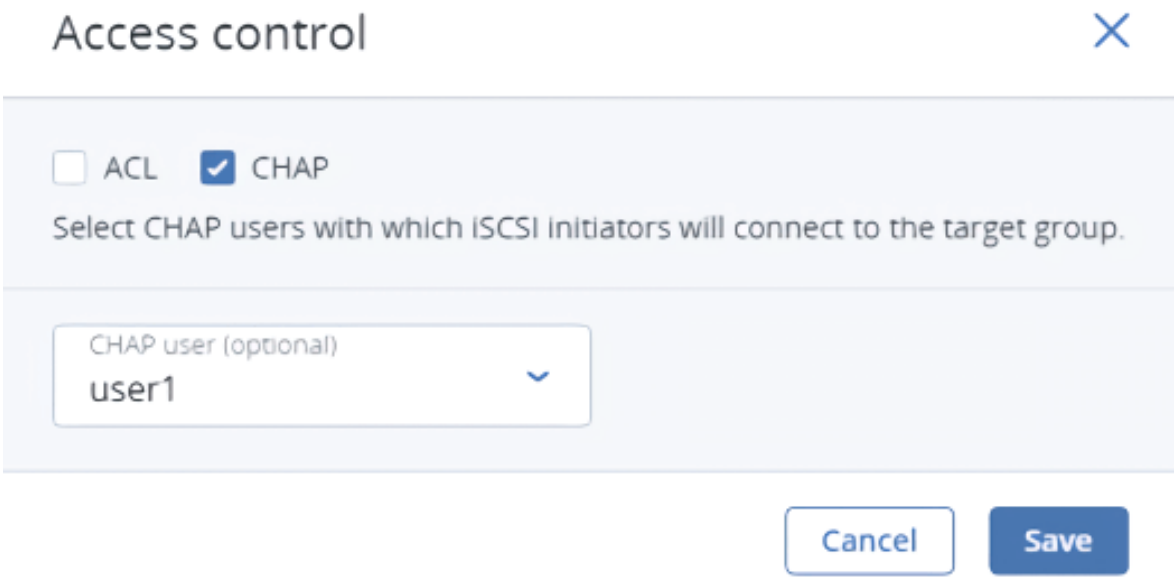


3. В окне **Контроль доступа** установите флажок **CHAP** и нажмите **Создать пользователя**.

4. В окне **Создать пользователя CHAP** введите имя пользователя и пароль (длиной от 12 до 16 символов). Нажмите кнопку **Создать**.



5. Вернувшись на экран **Контроль доступа**, выберите нужного пользователя CHAP и нажмите **Сохранить**.



Интерфейс командной строки

1. Включите авторизацию CHAP для нужной группы целевых устройств.

   ```
   # vstorage-target tg-auth -enable-chap -id <tg_id>
   ```

2. Создайте учетную запись CHAP, использовав команду vstorage-target account-create, например:

   ```
   # vstorage-target account-create -user user1 -desc "User for TG1"
   Enter Password:
   ```

   Пароль должен содержать от 12 до 16 символов.

3. Назначьте созданную учетную запись CHAP группе целевых устройств, использовав команду vstorage-target tg-chap, например:

   ```
   # vstorage-target tg-chap set -id faeacacd-eba6-416c-9a7f-b5ba9e372e16 \
   -user user1
   ```

Чтобы вывести список существующих учетных записей CHAP и сведения о них, используйте команду vstorage-target account-list.

Чтобы отменить назначение пользователя CHAP группе целевых устройств, используйте следующую команду:

```
# vstorage-target tg-chap del -id <tg_id> -user <user_id>
```

Чтобы изменить пароль пользователя CHAP

Панель администратора

1. Откройте **Сервисы хранилища** > **Блочное хранилище** > **Пользователи CHAP**, щелкните по пользователю, чтобы открыть сведения о нем, и нажмите значок карандаша.
2. В окне **Изменить пользователя CHAP** укажите новый пароль и нажмите **Применить**.

Интерфейс командной строки

Используйте команду vstorage-target account-set, например:

```
# vstorage-target account-set password -user user1
Enter Password:
```

Чтобы удалить неиспользуемого пользователя CHAP

Панель администратора

1. Откройте **Сервисы хранилища** > **Блочное хранилище** > **Пользователи CHAP**.
2. Щелкните по значку многоточия для нужного пользователя и нажмите **Удалить**.

Интерфейс командной строки

Используйте команду vstorage-target account-delete, например:

```
# vstorage-target account-delete -user user1
```

7.3.5 Управление серверами в группах целевых устройств

В этом разделе описывается управление серверами применительно к группам целевых устройств.

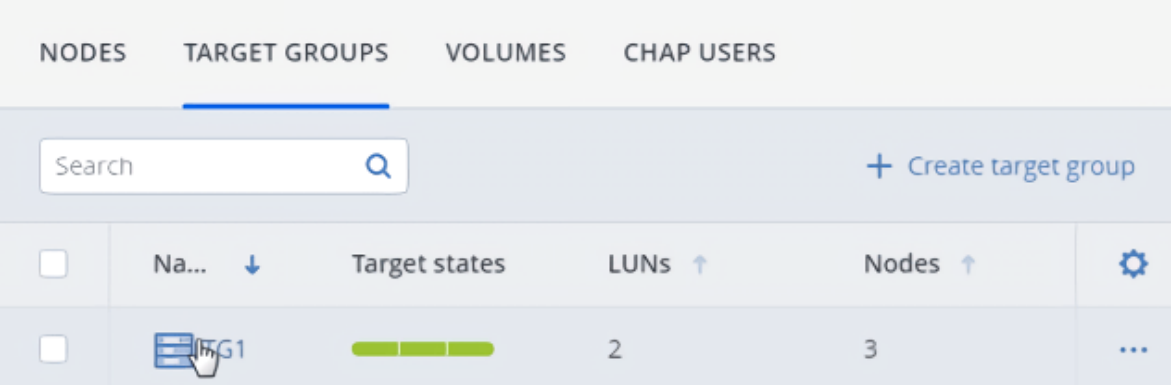
Предварительные требования

- Создана группа целевых устройств, как описано в разделе "Создание групп целевых устройств" на странице 199.

Добавление серверов в группы целевых устройств

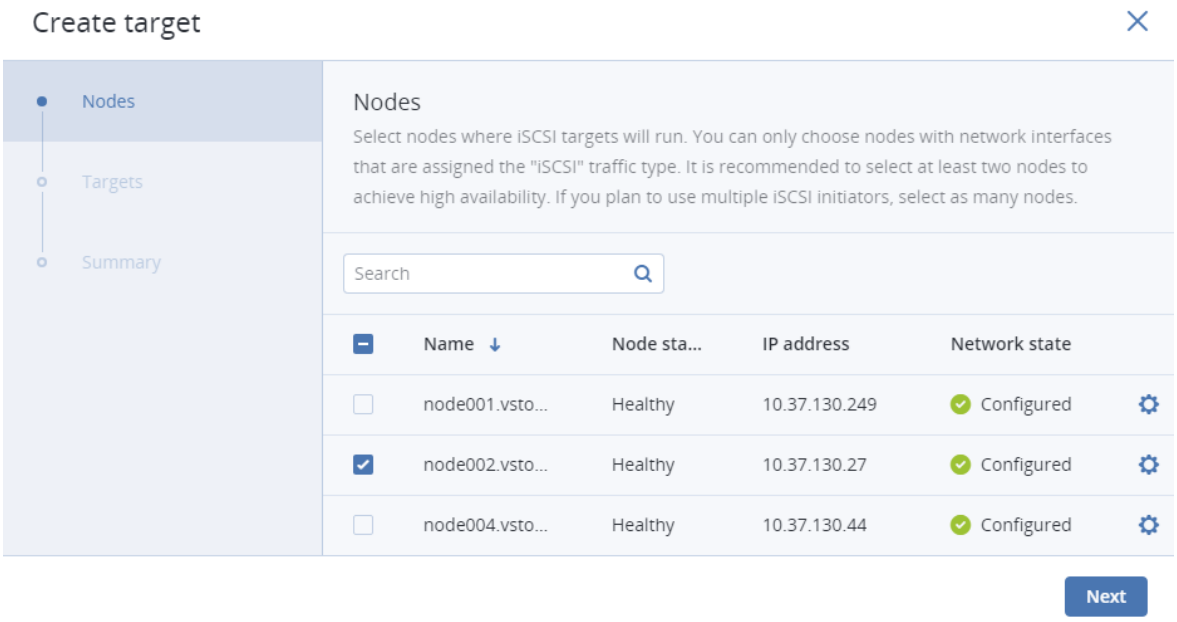
Панель администратора

1. Откройте **Сервисы хранилища** > **Блочное хранилище** > **Группы целей** и щелкните по имени нужной группы, чтобы открыть ее.

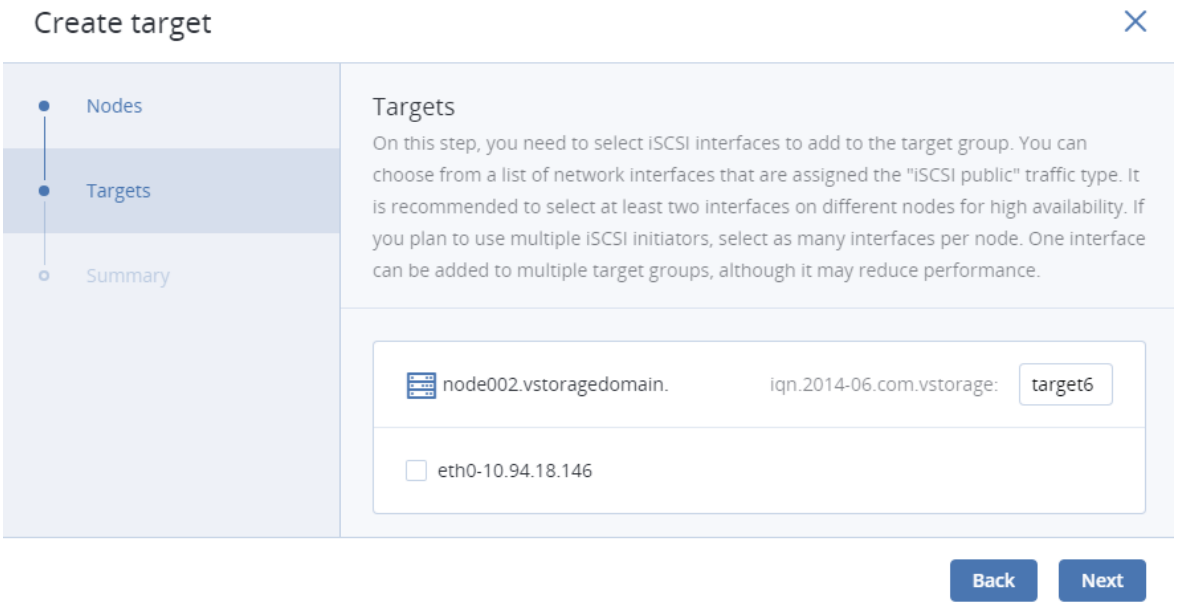


2. На вкладке **Цели** нажмите **Добавить цель**. Откроется мастер **Создать цель**.
3. На экране **Серверы** выберите серверы для добавления в группу целевых устройств. На этих серверах будут запускаться целевые устройства iSCSI. Можно выбирать только серверы с сетевыми интерфейсами, которым назначен тип трафика **iSCSI**. Рекомендуется добавить в группу целевых устройств как минимум два сервера для обеспечения высокой доступности. Если планируется использовать несколько инициаторов iSCSI, следует добавить столько же серверов в целевую группу. Оптимальный вариант – создать по одному целевому устройству на сервер.

   Если сетевые интерфейсы серверов не настроены, щелкните по значку шестерни, выберите необходимые сети и нажмите **Применить**.



4. На экране **Цели** выберите интерфейсы iSCSI для добавления в группу целевых устройств. Возможен выбор из списка сетевых интерфейсов, которым назначен тип трафика **iSCSI**. Если планируется использовать несколько инициаторов iSCSI, следует выбрать по такому же количеству интерфейсов на каждый сервер. Один интерфейс можно добавить в несколько групп целевых устройств, хотя это может снизить производительность.



5. На экране **Сводка** просмотрите сведения о целевом устройстве. При необходимости можно вернуться назад и изменить их. Нажмите кнопку **Далее**.

Созданное целевое устройство появится на вкладке **Цели**.

Интерфейс командной строки

Чтобы добавить сервер в группу целевых устройств, создайте файл конфигурации со сведениями о WWN и портале целевого устройства. Целевое устройство будет создано автоматически на добавленном сервере. Один сервер можно добавить в несколько групп целевых устройств, а его сетевые интерфейсы могут использоваться одновременно несколькими целевыми устройствами из разных групп.

Пример:

```
# vstorage-target node-add -node bbfd0e7a26b1406d \
-tg 3d8364f5-b830-4211-85af-3a19d30ebac4 -targets target.json
```

Эта команда добавляет сервер с идентификатором bbfd0e7a26b1406d в группу целевых устройств с идентификатором 3d8364f5-b830-4211-85af-3a19d30ebac4. Она также создает на нем целевое устройство в соответствии с файлом конфигурации target.json, который выглядит следующим образом:

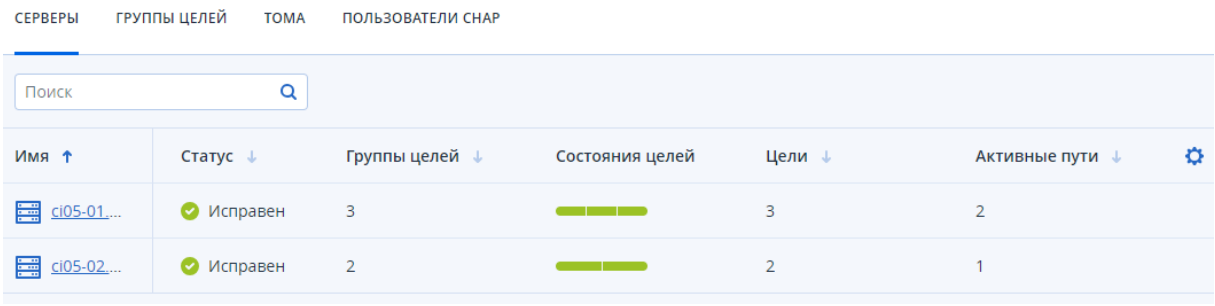
```
[
 {
  "NodeId": "bbfd0e7a26b1406d",
  "WWN": "iqn.2013-10.com.vstorage:test2",
  "Portals": [
   {
    "Addr": "10.94.104.89",
    "Port": 3260
```

```
    }
   ]
  }
 ]
```

Вывод списка серверов в группах целевых устройств

Панель администратора

На экране **Блочное хранилище** откройте вкладку **Серверы**.



Интерфейс командной строки

Чтобы вывести список всех серверов во всех группах целевых устройств и подробную информацию о них, используйте команду vstorage-target node-list, например:

```
# vstorage-target node-list
[
 {
  "ID": "bbfd0e7a26b1406d",
  "Status": "STABLE",
  "Enabled": true,
  "MonitorOnline": true,
  "Version": "7.10.32",
  "Address": "10.94.104.89:40135",
  "ActiveVolumes": [
   "0937f0e3-91a9-4dfc-8c10-6202bdc792c8"
  ]
 },
]
```

Включение и отключение серверов в группах целевых устройств

Чтобы включить или отключить сервер во всех группах целевых устройств, которым он принадлежит, используйте команду vstorage-target node-set. При включении сервера его целевые устройства запускаются, а при отключении они останавливаются и активный путь перемещается на другой сервер. Эти же операции выполняются, когда сервер выходит из режима обслуживания и входит в него.

Например, чтобы включить сервер с идентификатором bbfd0e7a26b1406d, выполните следующую команду:

```
# vstorage-target node-set -node bbfd0e7a26b1406d -enable
```

Перед отключением сервера убедитесь в наличии других серверов со статусом STABLE, куда можно переместить активный/оптимизированный путь. В противном случае произойдет ошибка ввода-вывода.

Чтобы отключить сервер с идентификатором bbfd0e7a26b1406d, выполните следующую команду:

```
# vstorage-target node-set -node bbfd0e7a26b1406d -disable
```

Статус сервера можно проверить с помощью команды vstorage-target node-list.

Удаление серверов из групп целевых устройств

Панель администратора

1. На экране **Блочное хранилище** > **Серверы** щелкните по имени сервера и перейдите на вкладку **Цели**.
2. Щелкните значок многоточия напротив целевого устройства, входящего в группу целевых устройств, из которой нужно удалить сервер, и нажмите **Освободить**.
3. В окне подтверждения нажмите **Освободить**.

Сервер будет удален из группы целевых устройств. Соответствующее целевое устройство будет автоматически удалено с сервера.

Интерфейс командной строки

Чтобы удалить сервер из группы целевых устройств, используйте команду vstorage-target node-del. Сервер можно удалить, только если он не находится на активном/оптимизированном пути. Иначе необходимо перенести путь на другой сервер посредством отключения этого сервера, использовав команду vstorage-target node-set (см. описание команды выше), или вручную, использовав команду vstorage-target vol-set (см. описание команды в разделе "Управление томами" на странице 379).

```
# vstorage-target node-del -tg 3d8364f5-b830-4211-85af-3a19d30ebac4 \
-node bbfd0e7a26b1406d
```

Эта команда удаляет сервер с идентификатором bbfd0e7a26b1406d из целевой группы с идентификатором 3d8364f5-b830-4211-85af-3a19d30ebac4.

7.3.6 Управление представлениями LUN

Представления LUN позволяют создавать и поддерживать список управления доступом (ACL).

Список управления доступом (ACL) позволяет контролировать доступ к LUN группы целевых устройств. Каждая запись списка содержит IQN инициатора и номера LUN, к которым этому инициатору разрешен доступ. Инициаторы, отсутствующие в списке, не обладают доступом к каким-либо LUN группы целевых устройств.

Примечание

Вышеописанное поведение списков контроля доступа введено в версии 5.5 продукта Кибер Инфраструктура. В предыдущих версиях инициаторы, указанные в списке, обладали доступом только к заданным LUN группы целевых устройств, а инициаторы вне списка – ко всем LUN группы. Для групп целевых устройств, созданных до обновления до версии 5.5, будет сохранено старое поведение списков контроля доступа, а сами группы будут помечены тегом **Не эксклюзивная**.

Включение авторизации на базе ACL

Чтобы использовать авторизацию на базе ACL, включите ее для группы целевых устройств.

```
# vstorage-target tg-auth -enable-acl -id <tg_ID>
```

Создание представлений LUN

Чтобы создать представление LUN для инициатора, используйте команду vstorage-target tg-initiator add или vstorage-target view-add. Первая команда добавляет инициатор в список ACL группы целевых устройств и создает для него представление. Вторая команда добавляет представления для инициаторов, которые уже есть в списке.

Пример:

```
# vstorage-target tg-initiator add -alias initiator2 -luns 0,1 \
-tg ee764519-80e3-406e-b637-8d63712badf1 -wwn iqn.1994-05.com.redhat:1535946874d
```

Эта команда добавляет инициатор с IQN iqn.1994-05.com.redhat:1535946874d в список ACL группы целевых устройств с идентификатором ee764519-80e3-406e-b637-8d63712badf1 и создает представление, разрешающее инициатору доступ к LUN с идентификаторами 0 и 1.

Другой пример:

```
# vstorage-target view-add -tg faeacacd-eba6-416c-9a7f-b5ba9e372e16 -lun 2 \
-map 2 -wwn iqn.1994-05.com.redhat:1535946874d
```

Эта команда добавляет для этого же инициатора представление, также разрешающее ему доступ к LUN 2.

Вывод списка представлений LUN

Чтобы вывести список представлений LUN для инициатора, используйте команду vstorage-target view-list, например:

```
# vstorage-target view-list -tg ee764519-80e3-406e-b637-8d63712badf1 \
-wwn iqn.1994-05.com.redhat:1535946874d
```

Эта команда выводит список представлений для инициатора с IQN iqn.1994-05.com.redhat:1535946874d.

Изменение сведений о представлениях LUN

Чтобы изменить представления LUN для инициатора, используйте команду vstorage-target view-set, например:

```
# vstorage-target view-set -luns 1 -tg ee764519-80e3-406e-b637-8d63712badf1 \
-wwn iqn.1994-05.com.redhat:1535946874d
```

Эта команда разрешает инициатору с IQN iqn.1994-05.com.redhat:1535946874d доступ только к LUN 1. По сути, она удаляет все представления LUN для инициатора, исключая указанное.

Удаление представлений LUN

Чтобы удалить представление LUN для инициатора, используйте команду vstorage-target view-del, например:

```
# vstorage-target view-del -lun 1 -tg ee764519-80e3-406e-b637-8d63712badf1 \
-wwn iqn.1994-05.com.redhat:1535946874d
```

Эта команда удаляет представление LUN 1 для инициатора с IQN iqn.1994-05.com.redhat:1535946874d.

7.4 Управление хранилищем объектов

В этом разделе дается краткое описание основных задач по администрированию кластеров, пользователей и корзин S3. Также здесь приведены рекомендации по использованию S3 в продукте Кибер Инфраструктура и списки поддерживаемых функций Amazon S3. Кроме того, в разделе даются инструкции по настройке георепликации S3 между центрами обработки данных.

7.4.1 Поддерживаемые функции Amazon S3

Помимо базовых операций Amazon S3, таких как GET, PUT, COPY, DELETE, реализация протокола Amazon S3 в продукте Кибер Инфраструктура поддерживает следующие функции:

- Передача по частям
- Списки управления доступом (ACL)
- Версии
- Подписанные URL-адреса
- Блокировка объектов
- Георепликация
- Ведение журнала доступа к серверам
- Классы хранилищ объектов
- Межрегиональная репликация (CRR)

Все поддерживаемые операции Amazon S3, методы, заголовки и схемы проверки подлинности перечислены далее.

7.4.1.1 Поддерживаемые операции и методы REST Amazon S3

Следующие операции и методы REST Amazon S3 в настоящее время поддерживаются реализацией протокола Amazon S3 в продукте Кибер Инфраструктура:

Поддерживаемые операции с сервисами: GET Service.

Поддерживаемые операции с корзинами:

- DELETE/HEAD/PUT Bucket
- GET Bucket (вывод списка объектов)
- GET/PUT Bucket acl
- GET Bucket location (возвращает Восточная часть США)
- GET Bucket Object versions
- GET/PUT Bucket versioning
- GET/PUT Bucket Logging (кроме элемента запроса TargetGrants)
- Вывод списка передач по частям

Поддерживаемые операции с объектами:

- DELETE/GET/HEAD/POST/PUT Object
- Удаление нескольких объектов
- PUT Object – копия
- GET/PUT Object acl
- Удаление нескольких объектов
- Прерывание передачи по частям
- Завершение передачи по частям
- Инициирование передачи по частям
- Вывод списка частей
- Передача части

Поддерживаемые методы:

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject
- CreateBucket

- CreateMultipartUpload
- DeleteBucket
- DeleteBucketPolicy
- DeleteBucketReplication
- DeleteBucketWebsite
- DeleteObject
- DeleteObjects
- GetBucketAcl
- GetBucketLocation
- GetBucketLogging
- GetBucketPolicy
- GetBucketReplication
- GetBucketVersioning
- GetBucketWebsite
- GetObject
- GetObjectAcl
- GetObjectLegalHold
- GetObjectLockConfiguration
- GetObjectRetention
- HeadBucket
- HeadObject
- ListBuckets
- ListMultipartUploads
- ListObjects
- ListObjectsV2
- ListObjectVersions
- ListParts
- PutBucketAcl
- PutBucketLogging
- PutBucketPolicy
- PutBucketReplication
- PutBucketVersioning
- PutBucketWebsite

- PutObject
- PutObjectAcl
- PutObjectLegalHold
- PutObjectLockConfiguration
- PutObjectRetention
- UploadPart

Примечание
Дополнительные сведения об операциях REST Amazon S3 см. в стандарте Amazon Simple Storage Service.

Дополнительные сведения о методах REST Amazon S3 см. в документации по API REST Amazon S3.

7.4.1.2 Поддерживаемые заголовки запросов Amazon

Следующие заголовки запросов REST Amazon S3 в настоящее время поддерживаются реализацией Кибер Инфраструктура протокола Amazon S3:

- Authorization
- Content-Length
- Content-Type
- Content-MD5
- Date
- Host
- x-amz-content-sha256
- x-amz-date
- x-amz-security-token
- x-amz-storage-class
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-mode
- x-amz-object-lock-legal-hold
- x-amz-bypass-governance-retention
- x-amz-bucket-object-lock-enabled
- x-amz-geo-endpoint
- x-amz-geo-access-key
- x-amz-geo-access-secret

Следующие заголовки запросов REST Amazon S3 игнорируются:

- Expect
- x-amz-security-token

Примечание
Дополнительные сведения о заголовках запросов REST Amazon S3 см. в документации по API REST Amazon S3.

7.4.1.3 Поддерживаемые заголовки ответов Amazon

Следующие заголовки ответов REST Amazon S3 в настоящее время поддерживаются реализацией Кибер Инфраструктура протокола Amazon S3:

- Content-Length
- Content-Type
- Connection
- Date
- ETag
- x-amz-delete-marker
- x-amz-request-id
- x-amz-version-id
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-mode
- x-amz-object-lock-legal-hold
- x-amz-geo-endpoint
- x-amz-geo-access-key
- x-amz-geo-access-secret

Следующие заголовки ответов REST Amazon S3 не используются:

- Server
- x-amz-id-2

Примечание
Дополнительные сведения о заголовках ответов REST Amazon S3 см. в документации по API REST Amazon S3.

7.4.1.4 Поддерживаемые заголовки ответов об ошибках Amazon

Следующие заголовки ответов об ошибках REST Amazon S3 в настоящее время поддерживаются реализацией Кибер Инфраструктура протокола Amazon S3:

- Code
- Error
- Сообщение

Следующие заголовки ответов об ошибках REST Amazon S3 не поддерживаются:

- RequestId (не используется)
- Ресурс

Примечание
Дополнительные сведения о заголовках ответов об ошибках REST Amazon S3 см. в документации по API REST Amazon S3.

7.4.1.5 Поддерживаемые схемы проверки подлинности

Реализация протокола Amazon S3 в Кибер Инфраструктура поддерживает следующие схемы проверки подлинности:

- Signature Version 2 (Подпись версии 2)
- Signature Version 4 (Подпись версии 4)

Реализация протокола Amazon S3 в Кибер Инфраструктура поддерживает следующие методы проверки подлинности:

- Использование заголовка авторизации
  - Передача пакета одним фрагментом
- Использование параметров запроса
- Браузерная загрузка с помощью POST

Следующий способ проверки подлинности не поддерживается:

- Передача пакета несколькими фрагментами

7.4.2 Добавление серверов в кластер S3

Вы можете добавлять дополнительные серверы для обеспечения высокой доступности и масштабирования вашего хранилища объектов.

Предварительные требования

- Кластер S3 должен быть создан в соответствии с указаниями из раздела "Создание кластера S3" на странице 208.

Чтобы добавить серверы в кластер S3

Панель администратора

1. Перейдите на экран **Сервисы хранилища** > **S3** > **Серверы**.
2. Выберите один или несколько серверов в разделе **Доступные серверы** и нажмите **Присоединить к кластеру S3**.

Серверы будут добавлены в кластер S3.

Интерфейс командной строки

Используйте команду:

```
vinfra service s3 node add --nodes <nodes>
```

--nodes <nodes>

Список имен хостов или идентификаторов серверов через запятую

Например, чтобы добавить сервер с идентификатором 2f3f6091-0d44-45aa-94e3-ebc2b65c0eeb в кластер S3, выполните:

```
# vinfra service s3 node add --nodes 2f3f6091-0d44-45aa-94e3-ebc2b65c0eeb
```

Добавленный сервер появится в выводе команды vinfra service s3 show:

```
# vinfra service s3 show
                    +----------------+-------------------------------------------+
                    | Field          | Value                                     |
                    +----------------+-------------------------------------------+
                    | failure_domain | 1                                         |
                    | id             | 0100000000000002                          |
                    | name           | cluster1                                  |
                    | nodes          | - id: ca334b1d-20a1-1241-96a5-eb9acadb8ecd |
                    |                | - id: ab36b523-91dc-e78d-53a7-88baed44541e |
                    |                | - id: 2f3f6091-0d44-45aa-94e3-ebc2b65c0eeb |
                    | np             |                                           |
                    | nusers         | 0                                         |
                    | protocol       | scheme: https                             |
                    | redundancy     | m: 1                                      |
                    |                | n: 2                                      |
                    |                | type: raid6                               |
                    | s3gw_domain    | dns.example.com                           |
                    | tier           | 0                                         |
                    +----------------+-------------------------------------------+
```

7.4.3 Управление пользователями S3

Концепция пользователя S3 – одна из базовых идей хранилища объектных данных наряду с концепциями объекта и корзины (контейнера для хранения объектов). В протоколе Amazon S3 используется модель разрешений на основе списков контроля доступа (ACL), где каждой корзине и каждому объекту назначается список ACL, в котором указаны все пользователи с доступом к данному ресурсу и тип доступа (чтение, запись, чтение ACL, запись ACL). Список пользователей

включает в себя владельца сущности, который назначается каждому объекту и корзине при создании. Владелец сущности имеет дополнительные права по сравнению с другими пользователями. Например, только владелец корзины может ее удалить.

Модель пользователей и политики доступа, реализованные в Кибер Инфраструктура, соответствуют модели пользователей и политикам доступа Amazon S3.

Сценарии управления пользователями в продукте Кибер Инфраструктура большей частью основаны на управлении пользователями в Amazon Web Services и включают следующие операции: создание, запрос и удаление пользователей, а также формирование и отзыв пар ключей доступа для пользователей.

7.4.3.1 Управление парами ключей доступа S3

У каждого пользователя S3 есть одна или две пары ключей (ключ доступа и секретный ключ) для доступа к облаку S3. Ключ доступа можно представить как имя входа, а секретный ключ — как пароль. (Дополнительные сведения о парах ключей S3 см. в документации Amazon.) Ключи доступа формируются и хранятся локально в кластере хранилища данных на серверах имен S3. У каждого пользователя может быть до двух пар ключей. Рекомендуется периодически отзывать старые пары ключей доступа и формировать новые.

Для доступа к корзине пользователю требуется следующая информация:

- IP-адрес панели администрирования
- Доменное имя кластера S3, указанное при настройке
- Идентификатор ключа доступа S3
- Секретный ключ доступа S3
- SSL-сертификат, если при настройке был выбран протокол HTTPS (файл сертификата можно найти в каталоге /etc/nginx/ssl/ на любом сервере, где размещен сервис шлюза S3)

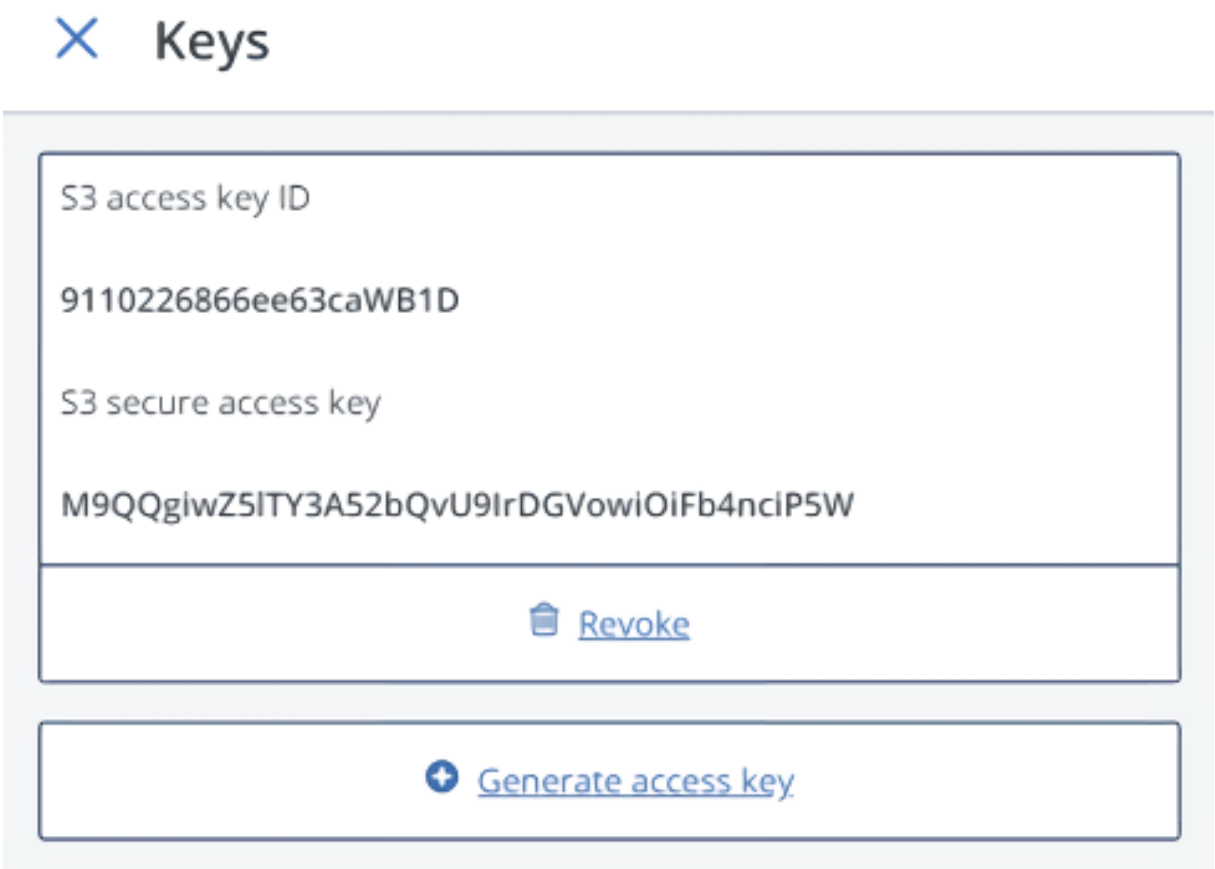
Предварительные требования

- Пользователи S3 созданы в соответствии с инструкциями в разделе "Добавление пользователей S3" на странице 214.
- Есть четкое понимание наилучших практик использования S3, приведенных в разделе "Рекомендации по использованию S3 в продукте Кибер Инфраструктура" на странице 404.

Чтобы просмотреть, добавить или отозвать пары ключей доступа S3 для пользователя S3

Выберите пользователя в списке и нажмите **Ключи**.

- Просмотрите существующие ключи на панели **Ключи**.
- Чтобы отозвать ключ, нажмите **Отозвать**.
- Чтобы добавить новый ключ, нажмите **Создать ключ доступа**.



7.4.4 Управление корзинами S3

Все объекты в хранилище, подобном Amazon S3, хранятся в контейнерах, называемых корзинами. Корзины адресуются по именам, уникальным для данного хранилища объектов, поэтому пользователь S3 не сможет создать корзину с таким же именем, как у другой корзины в том же хранилище объектов. Корзины используются в следующих случаях:

- Группировка объектов и их изоляция от объектов в других корзинах;
- Обеспечение механизмов управления ACL для объектов в корзинах;
- Задание политик доступа для каждой корзины, например управление версиями в корзине.

На экране **Сервисы хранилища** > **S3** > **Корзины** можно отслеживать пространство, используемое корзинами хранилища объектов. Нельзя создавать корзины хранилища объектов и управлять ими из панели администрирования Кибер Инфраструктура. Однако это можно сделать с помощью пользовательской панели Кибер Инфраструктура или стороннего приложения.

Сторонние приложения, указанные ниже, позволяют выполнять следующие действия:

- В CyberDuck: создание корзин и их содержимого и управление ими.
- В MountainDuck: подключение хранилища объектов в качестве диска и управление корзинами и их содержимым.

Предварительные требования

- Пользователи S3 созданы в соответствии с инструкциями в разделе "Добавление пользователей S3" на странице 214.
- Есть четкое понимание наилучших практик использования S3, приведенных в разделе "Рекомендации по использованию S3 в продукте Кибер Инфраструктура" ниже.

Чтобы получить доступ к корзинам из панели пользователя

1. На экране **Сервисы хранилища** > **S3** > **Пользователи** выберите пользователя.
2. Нажмите кнопку **Обзор**.

Для входа в систему используется SSL-сертификат. Убедитесь, что ваш сертификат действителен или добавьте его в исключения браузера как самозаверяющий.

Чтобы отобразить список содержимого корзины

- Откройте URL-адрес, состоящий из внешнего доменного имени конечной точки S3, указанного при создании кластера S3, и имени корзины, например **s3.example.com/mybucket** или **mybucket.s3.example.com** (в зависимости от конфигурации DNS).
- Скопируйте ссылку на содержимое корзины, щелкнув по ней правой кнопкой мыши в CyberDuck и выбрав **Копировать URL-адрес**.

7.4.5 Рекомендации по использованию S3 в продукте Кибер Инфраструктура

В этом разделе предлагаются рекомендации о том, как лучше всего использовать функцию S3 в продукте Кибер Инфраструктура.

7.4.5.1 Политики именования корзин и ключей S3

Рекомендуется использовать имена корзин, соответствующие соглашениям об именовании DNS:

- длиной от 3 до 63 символов;
- должны начинаться и заканчиваться буквой нижнего регистра или цифрой;
- могут содержать буквы нижнего регистра, цифры, точки (.), дефисы (-) и символы подчеркивания (_);
- могут представлять собой ряд допустимых частей имен (описанных ранее), разделенных точками.

Ключ объекта может быть строкой из любых символов в кодировке UTF-8 длиной до 1024 байт.

7.4.5.2 Использование передачи по частям для крупных объектов

Хранилище объектных данных поддерживает передачу объектов размером до 5 ГБ на один запрос PUT (50 ТБ при передаче по частям). Производительность передачи можно улучшить, разбив

большие объекты на фрагменты и передавая их параллельно (разделяя таким образом нагрузку между несколькими сервисами ОС) с помощью API передачи по частям.

Максимальное количество частей при передаче объекта по частям – 10 000.

Рекомендуется использовать передачу по частям для объектов размером больше 5 МБ.

7.4.5.3 Совместимые клиентские приложения для работы с S3

- CyberDuck - файловый менеджер для macOS, Linux и Windows.;
- boto - набор средств разработки для работы с сервисами AWS с поддержкой языков программирования Python 2.x и Python 3.x;
- boto3 - набор средств разработки для работы с сервисами AWS с поддержкой языков программирования Python 2.x и Python 3.x;
- aws cli - интерфейс командной строки для работы с сервисами AWS;
- s3cmd - консольный клиент (Linux, MacOS) для управления хранилищами объектов S3;
- s5cmd.

Пример использования boto3

До начала работы получите реквизиты доступа к Объектному хранилищу (адрес точки доступа S3, идентификатор ключа доступа к S3 и секретный ключ доступа к S3). Создайте в домашнем каталоге файл .aws/credentials и задайте ключ доступа в формате:

```
[default]
aws_access_key_id = <id>
aws_secret_access_key = <secretKey>
```

Задайте в файле .aws/config регион в формате:

```
[default]
region=us-east-1
```

Пример использования класса хранения

Создайте новый класс хранения TYPE_1:

```
ostor-ctl set-storage-class -s /mnt/vstorage/vols/ostor/ -V 0100000000000002 -C 1 -O 2 --vstorage-attr "replicas=2:1 tier=0"
```

Создайте объект, использующий класс хранения TYPE_1:

```
#!/usr/bin/python3
import boto3
import urllib3
```

```
urllib3.disable_warnings()
# boto3.set_stream_logger(name='botocore') # enable to see HTTP headers

s3_client = boto3.client(
   service_name='s3',
   endpoint_url='https://s3.example.com:443',
   aws_access_key_id='XXX',
   aws_secret_access_key='XXX',
   verify=False
)

obj_id='011010100101'
bucket_id='testbucket'

s3_client.create_bucket(Bucket=bucket_id)
s3_client.put_object(Body=b'Here we have some data', Bucket=bucket_id, Key=obj_id,
StorageClass='TYPE_1')

obj_info = s3_client.head_object(Bucket=bucket_id, Key=obj_id)
s3_client.delete_object(Bucket=bucket_id, Key=obj_id)

print(obj_info['StorageClass'])
```

Пример параллельной загрузки файлов и частей файлов

```
import os
import boto3
from boto3.s3.transfer import TransferConfig

from multiprocessing.pool import ThreadPool

access_key = 'XXX'
secret_key = 'XXX'
endpoint_url = 'https://s3.example.com'
bucket = 'bucket'

def get_resource():
   return boto3.Session().resource(
      's3',
      aws_access_key_id=access_key,
      aws_secret_access_key=secret_key,
      endpoint_url=endpoint_url,
      verify=False
   )

# Параллельная загрузка нескольких файлов (из директории)
def put_file(path, bucket, key):
   s3 = get_resource()
   s3.Bucket(bucket).upload_file(path, key)

# Параллельная загрузка частей файла
```

```
def put_file_multipart(path, bucket, key, chunk_size=100*1024, n_threads=20):
   s3 = get_resource()
   config = TransferConfig(multipart_threshold=chunk_size,
                           max_concurrency=n_threads,
                           multipart_chunksize=chunk_size,
                           use_threads=True)
   s3.Object(bucket, key).upload_file(path, Config=config)

def put_dir(bucket_name, directory_name, n_processes=20):
   p = ThreadPool(n_processes)
   files = [(os.path.join(directory_name, file),
          bucket_name, file) for file in os.listdir(directory_name)]
   p.starmap(put_file, files)
   # p.starmap(put_file_multipart, files)
```

7.4.6 Определение классов хранения объектов

Вы можете использовать до четырех классов хранения объектов для приложений с различными требованиями к производительности и резервированию. Первый класс хранилища задается автоматически при создании кластера S3. Остальные три класса можно определить вручную с помощью команды ostor-ctl set-storage-class.

Требования

- Создан кластер S3, как описано в разделе "Создание кластера S3" на странице 208.

Чтобы установить класс хранилища

1. Получите пароль для своего кластера хранения. Например:

   ```
   # vinfra cluster password show
   +----------+---------+
   | Field    | Value   |
   +----------+---------+
   | id       | 1       |
   | name     | cluster |
   | password | W3HMNq  |
   +----------+---------+
   ```

2. Узнайте идентификатор тома хранилища объектов. Например:

   ```
   # ostor-ctl get-config
   <...>
   VOL_ID           TYPE    STATE
   0100000000000002  OBJ    READY
   <...>
   ```

3. Определите класс хранения, указав его имя, количество объектных серверов, которые он будет включать, и требуемые параметры резервирования. При появлении запроса введите пароль, полученный на шаге 1. Например, чтобы создать хранилище класса 1 с 2 объектными

серверами и схемой резервирования из 2 реплик для уровня 1, выполните:

```
# ostor-ctl set-storage-class -s /mnt/vstorage/vols/ostor/ -V 0100000000000002 \
-C 1 -O 2 --vstorage-attr "replicas=2:1 tier=1"
Введите пароль для 'ostor-private.svc.vstoragedomain.':
Хранилище 1 класса успешно присвоено службам
```

Данная команда требует следующие параметры:

- -s: путь к каталогу хранения объектов
- -V: идентификатор тома, полученный на шаге 2
- -C: имя класса хранилища (может быть 1-3)
- -O: количество объектных серверов для создания
- --vstorage-attr: настройки резервирования, где можно указать желаемый уровень хранения данных, домен отказа и схему резервирования данных (см. справочное сообщение vstorage set-attr)

4. Убедитесь, что установлен новый класс хранения. Например, для хранилища класса 1 выполните:

```
# vstorage get-attr /mnt/vstorage/vols/ostor/0100000000000002/services/sc1/
connected to MDS#1
Путь: 'vstorage://hciHeat/vols/ostor/0100000000000002/services/sc1'
Атрибуты:
 directory
 client-ssd-cache=1
 replicas=2:1
 failure-domain=host
 failure-domain.int=1
 tier=1
 chunk-size=268435456
```

Для изменения параметров класса хранилища

Используйте команду ostor-ctl cfg-storage. Например:

```
# ostor-ctl cfg-storage -r /mnt/vstorage/vols/ostor/0100000000000002/ -C 1 \
--vstorage-attr "replicas=3:2 tier=0"
```

7.4.7 Репликация данных S3 между центрами обработки данных

Для репликации данных между центрами обработки данных пользователи S3 могут использовать либо георепликацию S3, либо межрегиональную репликацию (Cross-region replication или CRR):

- Георепликация предназначена для улучшения распространения данных между географически распределенными сетями данных. Георепликацию можно включить на панели администрирования.
- Межрегиональная репликация используется для асинхронного копирования объектов между корзинами S3, расположенными в различных кластерах и у различных поставщиков облачных

сервисов. Межрегиональную репликацию можно включить с помощью API, совместимого с API службы Amazon S3. Для подробных сведений см. справку по API оркестрации объектного хранилища.

Ограничения

- Георепликация и межрегиональная репликация несовместимы. При включенной георепликации межрегиональная репликация недоступна.

7.4.7.1 Включение георепликации S3

Кибер Инфраструктура может хранить реплики данных кластера S3 и поддерживать их в актуальном состоянии в нескольких географически распределенных центрах обработки данных. Георепликация уменьшает время отклика для локальных пользователей S3, обращающихся к данным в удаленном кластере S3, или удаленных пользователей S3, обращающихся к данным в локальном кластере S3, так как им не требуется подключения к Интернету.

Георепликация задает расписание обновления реплик сразу же после изменения каких-либо данных. Производительность георепликации зависит от скорости подключения к Интернету, режима избыточности и производительности кластера.

При наличии нескольких центров обработки данных с достаточным свободным пространством рекомендуется настроить георепликацию между кластерами S3, расположенными в этих ЦОД.

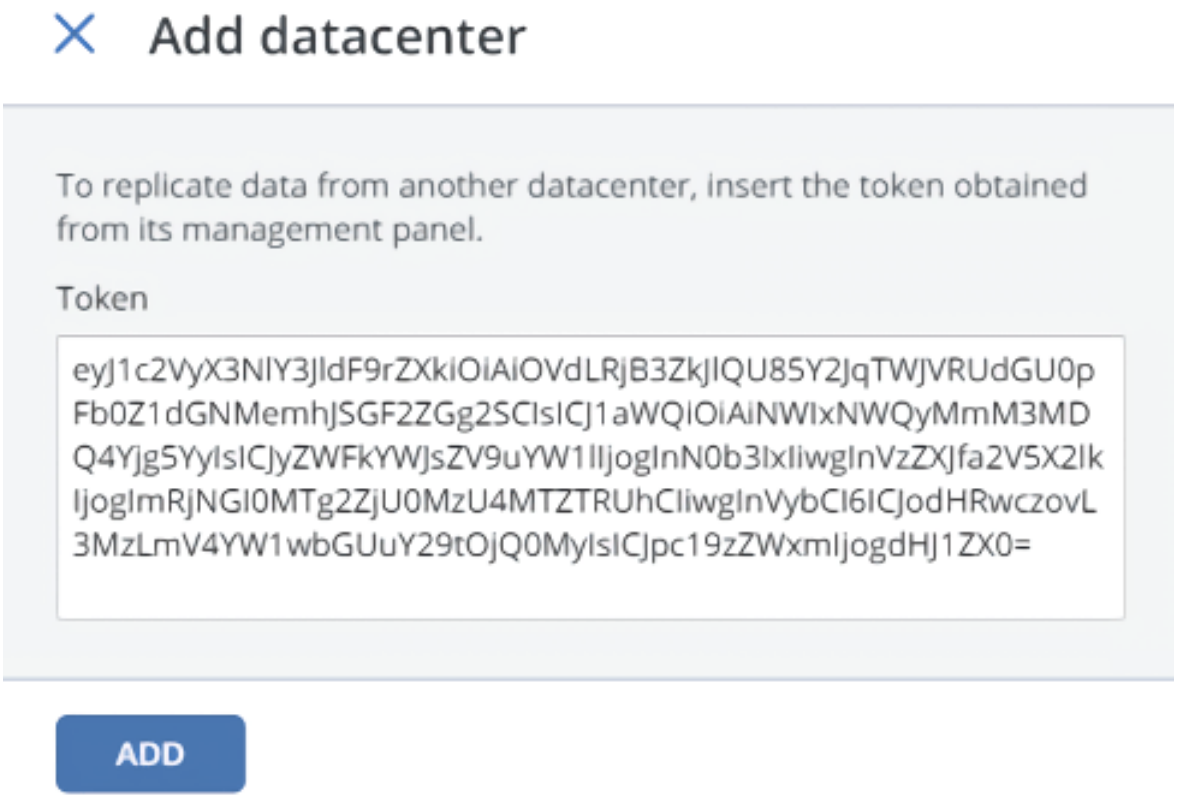
Предварительные требования

- Кластеры S3 созданы в соответствии с инструкциями в разделе "Создание кластера S3" на странице 208.
- У каждого кластера есть собственный SSL-сертификат, заверенный глобальным центром сертификации.

Чтобы настроить георепликацию между кластерами S3

1. На панели администрирования удаленного центра обработки данных откройте экран **Сервисы хранилища** > **S3** > **Георепликация**.

2. В разделе домашнего кластера S3 нажмите **Токен**. Скопируйте токен на панели **Получить токен**.
3. На панели администрирования локального центра обработки данных откройте экран **Сервисы хранилища** > **S3** > **Георепликация** и нажмите **Добавить ЦОД**.



4. Введите скопированный токен и нажмите **Готово**.
5. Таким же образом настройте и удаленный кластер S3.

После включения георепликации для кластеров можно реплицировать данные по корзинам.

Чтобы включить репликацию корзины

1. На экране **Сервисы хранилища** > **S3** > **Корзины** выберите корзину.
2. Щелкните **Включить георепликацию** на правой панели.

В столбце **Георепликация** для этой корзины будет отображаться **Включено**. Корзина будет скопирована в подключенный кластер.

Чтобы отключить репликацию корзины

1. На экране **Сервисы хранилища** > **S3** > **Корзины** выберите корзину.
2. Щелкните **Выключить георепликацию** на правой панели.

В столбце **Георепликация** для этой корзины будет отображаться **Отключено**. После отключения георепликации для корзины данные, скопированные до этого, сохранятся, но изменения больше не будут реплицироваться в другой кластер S3.

7.4.7.2 Включение межрегиональной репликации S3

Межрегиональная репликация (Cross-region replication или CRR) обеспечивает автоматическое асинхронное копирование объектов между корзинами S3, расположенными в разных регионах. Корзины, для которых настроена межрегиональная репликация, могут принадлежать одному и тому же пользователю. Репликация объектов может выполняться в одну или несколько целевых корзин.

Чтобы включить межрегиональную репликацию, необходимо добавить конфигурацию репликации к исходной корзине. Минимальная конфигурация должна обеспечивать корзины назначения, в которые будет выполняться репликация объектов, и пользователя с ролью, которая позволяет выполнение репликации объектов.

Ограничения

- После включения межрегиональной репликации репликация будет выполняться только для новых объектов S3.

Предварительные требования

- Кластеры S3 созданы в соответствии с инструкциями в разделе "Создание кластера S3" на странице 208.

Настройка межрегиональной репликации между корзинами кластера S3

1. Вам понадобятся одна исходная корзина и хотя бы одна целевая корзина. Если их нет, создайте их с помощью интерфейса командной строки AWS, стороннего приложения S3 или пользовательской панели Кибер Инфраструктура. Например, чтобы создать корзины с помощью интерфейса командной строки AWS, выполните следующие шаги на машине, где выполняется настройка репликации:
   a. Добавьте профиль пользователя S3 в конфигурационный файл %USERPROFILE%\.aws\credentials для Windows или $HOME/.aws/credentials для Linux:

```
[<s3-user-profile>]
aws_access_key_id = <key-id>
aws_secret_access_key = <key-secret>
```

Где:

<s3-user-profile>

Имя профиля пользователя S3

<key-id>

Идентификатор ключа доступа пользователя S3

<key-secret>

Секретный ключ доступа пользователя S3

b. Создайте целевую корзину и от одной до нескольких корзин назначения:

```
aws s3api create-bucket --bucket <bucket-name> --endpoint-url <s3-api-url> --profile <s3-user-profile>
```

Где:

<bucket-name>

Имя корзины

<s3-api-url>

Адрес S3 API

<s3-user-profile>

Имя профиля пользователя S3

2. Включите поддержку версий для каждой из этих корзин:

```
aws s3api put-bucket-versioning --bucket <bucket-name> --endpoint-url <s3-api-url> --profile <s3-user-profile> \
--versioning-configuration 'Status=Enabled'
```

Где:

<bucket-name>

Имя корзины

<s3-api-url>

Адрес S3 API

<s3-user-profile>

Имя профиля пользователя S3

3. Получите идентификатор пользователя-владельца исходной корзины из вывода команды ниже.

```
aws s3api list-buckets --endpoint-url <s3-api-url> --profile <s3-user-profile>
```

Где:

<s3-api-url>

Адрес S3 API

<s3-user-profile>

Имя профиля пользователя S3

Пример вывода команды:

```
{
  "Buckets": [
    {
      "Name": "destination",
      "CreationDate": "2023-07-27T13:01:08+00:00"
    },
    {
      "Name": "source",
      "CreationDate": "2023-07-27T12:58:21+00:00"
    }
  ],
  "Owner": {
    "DisplayName": "s3user",
    "ID": "e872c6783c209555"
  }
}
```

4. Создайте конфигурационный файл репликации на машине, где выполняется настройка репликации. Например, создайте файл replication.json со следующим содержимым:

```
{
    "Role": "arn:aws:iam::<s3-user-id>:role/service-role/s3crr_role",
    "Rules": [
        {
            "Priority": 1,
            "DeleteMarkerReplication": {"Status": "Disabled"},
            "Filter": {},
            "Status": "Enabled",
            "Destination": {
                "Bucket": "arn:aws:s3:::<destination-bucket-name>"
            }
        }
    ]
}
```

Где:

Role

Указывает роль, которая будет использоваться для репликации объектов. Задайте значение в формате arn:aws:iam::<s3-user-id>:role/service-role/s3crr_role, где <s3-user-id> – это идентификатор пользователя-владельца исходной корзины.

Rules

Правила репликации, указывающие, для каких объектов выполнять репликацию и где хранить реплики.

ID

Уникальный идентификатор правила длиной до 255 символов.

Priority

Указывает, какое правило обладает более высоким приоритетом, когда два или более правил конфликтуют.

Destination

Контейнер для информации о месте назначения репликации и его конфигурации.

Bucket

Указывает корзину, где необходимо хранить результаты. Задайте значение в формате arn:aws:s3:::<destination-bucket-name>, где <destination-bucket-name> – это имя корзины назначения.

Status

Указывает, включено ли правило. Возможные значения: Enabled или Disabled.

DeleteMarkerReplication

Указывает, выполнять ли репликацию маркеров удаления. Если указан элемент Filter, также необходимо указать элемент DeleteMarkerReplication.

Подробное описание формата файла конфигурации репликации и дополнительные примеры смотрите в документации AWS.

5. Настройте исходную корзину для межрегиональной репликации, указав конфигурационный файл репликации:

```
aws s3api put-bucket-replication --bucket <source-bucket-name> --endpoint-url <s3-api-url> --profile <s3-user-profile> \
--replication-configuration file://<replication-configuration-file>
```

Где:

<source-bucket-name>

Имя исходной корзины

<s3-api-url>

Адрес S3 API

s3-user-profile

Имя профиля пользователя S3

<replication-configuration-file>

Путь к файлу конфигурации репликации

Дополнительная информация:

- Чтобы просмотреть или проверить текущую конфигурацию репликации исходной корзины, выполните:

  ```
  aws s3api get-bucket-replication --bucket <source-bucket-name> --endpoint-url <s3-api-url> --profile <s3-user-profile>
  ```

- Чтобы просмотреть объекты в корзине и их ключи, выполните:

  ```
  aws s3api list-objects --bucket <bucket-name> --endpoint-url <s3-api-url> --profile <s3-user-profile>
  ```

- Чтобы просмотреть статус репликации объекта, выполните:

  ```
  aws s3api head-object --bucket <source-bucket-name> --key <object-key> --endpoint-url <s3-api-url> --profile <s3-user-profile>
  ```

- Для репликации из исходной корзины в несколько целевых корзин задайте несколько правил репликации в конфигурации репликации, указав соответствующие корзины назначения.
- Чтобы выключить репликацию, выполните:

  ```
  aws s3api delete-bucket-replication --bucket <source-bucket-name> --endpoint-url <s3-api-url> --profile <s3-user-profile>
  ```

7.4.8 Настройка параметров TLS для хранилища объектов

По умолчанию для подключений к кластеру S3 следует использовать только протокол TLS версии 1.2. Кроме того, допускается использование только следующих криптографических алгоритмов:

- ECDHE-ECDSA-AES128-GCM-SHA256,
- ECDHE-RSA-AES128-GCM-SHA256,
- DHE-RSA-AES128-GCM-SHA256,
- ECDHE-ECDSA-AES256-GCM-SHA384,
- ECDHE-RSA-AES256-GCM-SHA384,
- ECDHE-RSA-AES128-SHA256,
- DHE-RSA-AES128-SHA256,
- AES128-GCM-SHA256.

Эти параметры автоматически применяются ко всем кластерам S3, запущенным в Кибер Инфраструктура Версия 5.5, даже если какой-либо кластер был создан в более ранней версии.

Настройка версий протокола TLS для хранилища объектов

Чтобы разрешить входящие подключения к хранилищу объектов с использованием протоколов TLS 1.0 и 1.1, выполните следующие действия:

1. Перечислите необходимые протоколы TLS через пробел в параметре OSTOR_S3_GW_CUSTOM_SSL_PROTOCOLS файла конфигурации /usr/libexec/vstorage-ui-backend/etc/backend.cfg для каждого узла управления. Дополнительные сведения об этом параметре см. в документации nginx. Например, чтобы разрешить использование протокола TLS 1.1, использовавшегося в более ранних версиях, укажите следующее значение:

   ```
   OSTOR_S3_GW_CUSTOM_SSL_PROTOCOLS = 'TLSv1.1 TLSv1.2'
   ```

2. Перезапустите службу vstorage-ui-backend.

   ```
   # systemctl restart vstorage-ui-backend
   ```

3. На панели администрирования перейдите на экран **Сервисы хранилища** > **S3** > **Серверы**, щелкните **Настройки протокола** и нажмите **Готово**, чтобы применить изменения.

Настройка криптографических алгоритмов TLS для хранилища объектов

Чтобы разрешить использовать пользовательские криптографические алгоритмы для хранилища объектов, выполните следующие действия:

1. Перечислите необходимые алгоритмы через двоеточие в параметре OSTOR_S3_GW_CUSTOM_SSL_CIPHERS файла конфигурации /usr/libexec/vstorage-ui-backend/etc/backend.cfg для каждого узла управления. Дополнительные сведения об этом параметре см. в документации nginx. Например, чтобы разрешить использование алгоритмов, использовавшихся в более ранних версиях, укажите следующее значение:

   ```
   OSTOR_S3_GW_CUSTOM_SSL_CIPHERS = 'HIGH:!3DES:!RC4:!aNULL:!MD5:!kEDH'
   ```

2. Перезапустите службу vstorage-ui-backend.

   ```
   # systemctl restart vstorage-ui-backend
   ```

3. На панели администрирования перейдите на экран **Сервисы хранилища** > **S3** > **Серверы**, щелкните **Настройки протокола** и нажмите **Готово**, чтобы применить изменения.

7.4.9 Освобождение серверов из кластеров S3

Ограничения

- При удалении последнего сервера из кластера S3 кластер уничтожается и все данные удаляются.

Предварительные требования

- Кластер S3 создан в соответствии с инструкциями в разделе "Создание кластера S3" на странице 208.
- В кластере остается достаточно узлов, на которых работают серверы имен и объектов, а также достаточно шлюзов.

Чтобы освободить сервер из кластера S3

Панель администратора

1. На экране **Сервисы хранилища** > **S3** > **Серверы** выберите сервер.
2. Нажмите кнопку **Освободить**.
3. Нажмите **Да** в окне подтверждения.

Интерфейс командной строки

- Чтобы удалить сервер из кластера S3, который состоит из двух и более серверов, выполните:

  ```
  # vinfra service s3 node release --nodes <nodes>
  ```

  --nodes <nodes>

  Список имен хостов или идентификаторов серверов через запятую

- Чтобы удалить последний сервер из кластера S3 и удалить кластер, выполните:

  ```
  # vinfra service s3 cluster delete [--force]
  ```

7.5 Управление хранилищем файлов

В этом разделе описаны общие задачи администрирования серверов, томов и экспортов NFS.

Предварительные требования

- Экспорты NFS созданы в соответствии с инструкциями в разделе "Создание экспортов NFS" на странице 220.

7.5.1 Добавление серверов в кластер NFS

Для обеспечения высокой доступности и масштабирования хранилища файлов можно добавлять дополнительные серверы в кластер NFS.

Предварительные требования

- Создан кластер NFS, как описано в разделе "Создание кластера NFS" на странице 217.

Чтобы добавить серверы в кластер NFS

Панель администратора

1. Перейдите на экран **Сервисы хранилища** > **NFS** > **Серверы**.
2. Выберите один или несколько серверов в разделе **Доступные серверы** и нажмите **Присоединить к кластеру NFS**.

Серверы будут добавлены в кластер NFS.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service nfs node add --nodes <nodes>[:<ip_address>]
```

--nodes <nodes>[:<ip_address>]

Разделенный запятыми список хостовых имен или идентификаторов серверов (IP-адреса указываются при необходимости)

Например, чтобы добавить сервер node002 в кластер NFS, выполните:

```
# vinfra service nfs node add --nodes node002
```

Добавленный сервер появится в выводе команды vinfra service nfs node list:

```
# vinfra service nfs node list
+--------------------------------------+-----------------------+-------------+
| id                                   | ip_address            | has_configd |
+--------------------------------------+-----------------------+-------------+
| 923926da-a879-5f56-1b24-1462917ed335 | node001.vstoragedomain | True       |
| ef24c47c-620d-8726-2677-ed94d853de2e | node002.vstoragedomain | True       |
+--------------------------------------+-----------------------+-------------+
```

7.5.2 Настройка аутентификации и авторизации пользователей

Кибер Инфраструктура предоставляет следующие возможности:

- аутентификация пользователей томов NFS с помощью Kerberos;
- авторизация пользователей томов NFS с помощью LDAP.

7.5.2.1 Аутентификация пользователей томов NFS с помощью Kerberos

Кибер Инфраструктура позволяет выполнять аутентификацию пользователей томов NFS с помощью Kerberos.

Процедура включения аутентификации с помощью Kerberos состоит из следующих шагов:

1. Включение аутентификации Kerberos в панели администрирования продукта Кибер Инфраструктура.
2. Создание субъектов и таблиц ключей (keytabs) для клиента Kerberos и тома NFS на сервере Kerberos.
3. Настройка клиента Kerberos на машине, к которой будет подключен том NFS.
4. Включение аутентификации Kerberos для тома NFS.
5. Подключение тома NFS к машине с настроенным клиентом Kerberos.

Предварительные требования

- Тома NFS созданы и остановлены, как описано в разделах "Создание томов NFS" на странице 218 и "Управление томами NFS" на странице 422.

- Тому NFS назначено полное имя домена (FQDN). Для DNS-имени тома и его IP-адреса настроено прямое и обратное разрешение имен DNS.
- Если для исходящего трафика в кластере настроены ограничения, следует вручную добавить правило, чтобы разрешить исходящий трафик через порты TCP 88 и 749, а также порт UDP 88, как описано в разделе "Настройка правил брандмауэра для исходящих подключений" на странице 263.

Чтобы включить аутентификацию с помощью Kerberos

Панель администратора

1. Перейдите на экран **Настройки** > **Безопасность** > **Kerberos**.
2. Укажите следующие настройки Kerberos:
   a. В поле **Область** – имя области Kerberos (realm) заглавными буквами.
   b. В поле **Сервис KDC** – DNS-имя или IP-адрес сервера, на котором работает сервис центра распределения ключей (KDC) данной области.
   c. В поле **Сервис администрирования KDC** – DNS-имя или IP-адрес сервера, на котором работает сервис администрирования центра распределения ключей данной области.

   Примечание
   Как правило, центр распределения ключей и его сервис администрирования запускаются на одном и том же сервере.
3. Нажмите **Сохранить**, чтобы применить изменения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service nfs kerberos settings set --realm <realm> --kdc-service <kdc-service>
                                         --kdc-admin-service <kdc-admin-service>
```

--realm <realm>

Имя области Kerberos (realm) заглавными буквами

--kdc-service <kdc-service>

DNS-имя или IP-адрес сервера, на котором работает сервис центра распределения ключей (KDC) указанной области

--kdc-admin-service <kdc-admin-service>

DNS-имя или IP-адрес сервера, на котором работает сервис администрирования центра распределения ключей указанной области

Например, чтобы включить аутентификацию с помощью Kerberos, выполните:

```
# vinfra service nfs kerberos settings set --realm EXAMPLE.COM --kdc-service 10.136.10.10 \
--kdc-admin-service 10.136.10.10
```

Чтобы создать субъекты и их keytab-файлы

1. Войдите как администратор в программу администрирования баз данных Kerberos.
2. Создайте субъекты для клиента Kerberos и тома NFS с помощью команды addprinc -randkey nfs/<FQDN>@<realm>. Например, если DNS-имя клиента Kerberos — это krb-client.example.com, а DNS-имя тома NFS — это share1.example.com, выполните:

   ```
   # addprinc -randkey nfs/krb-client.example.com@EXAMPLE.COM
   # addprinc -randkey nfs/share1.example.com@EXAMPLE.COM
   ```

3. Сгенерируйте таблицы ключей для созданных субъектов и сохраните их файлы в папку, из которой вы их потом сможете скопировать. Например:

   ```
   # ktadd -k /tmp/krb-client.keytab nfs/krb-client.example.com@EXAMPLE.COM
   # ktadd -k /tmp/share.keytab nfs/share1.example.com@EXAMPLE.COM
   ```

   Внимание
   У каждого тома NFS и каждого клиента Kerberos (пользователя, подключающего экспорт NFS) должны быть собственные субъект и таблица ключей.

Чтобы настроить клиент Kerberos

1. На сервер, к которому будет подключен том NFS, установите необходимые пакеты. Например, на сервере с CentOS, выполните:

   ```
   # yum install krb5-workstation krb5-libs -y
   ```

2. [Необязательно] Настройте firewalld и selinux при необходимости. Для получения подробной информации обращайтесь к документации соответствующей операционной системы. Для операционной системы Red Hat Enterprise Linux, например, можно получить подробную информацию в Red Hat Enterprise Linux Security Guide в разделе Securing services.
3. Скопируйте файл конфигурации krb5.conf и файл таблицы ключей krb-client.keytab с сервера Kerberos на сервер, к которому будет подключен том NFS.
4. Проверьте, что том NFS и сервер Kerberos по доступны их DNS-именам с сервера, к которому будет подключен том NFS. Удостоверьтесь, что этому серверу назначено такое же DNS-имя, как у субъекта для клиента Kerberos.
5. Запустите службу nfs-client:

   ```
   # systemctl start nfs-client
   ```

Чтобы включить аутентификацию для тома NFS

Панель администратора

1. Перейдите на экран **Сервисы хранилища** > **NFS** > **Том** и выберите том NFS.
2. Если том запущен, остановите его с помощью кнопки **Стоп**.
3. Нажмите **Идентификация**.

4. В разделе **Идентификация** включите пользовательскую аутентификацию и загрузите файл таблицы ключей, сгенерированный для субъекта тома NFS.
5. Нажмите **Сохранить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service nfs share set [--krb-keytab <krb-keytab>] [--krb-auth <krb-auth>] <name>
```

--krb-keytab <krb-keytab>

Файл таблицы ключей Kerberos

--krb-auth <krb-auth>

Включение или отключение аутентификации с помощью Kerberos (true или false)

<name>

Имя тома NFS

Например, чтобы включить аутентификацию для тома share1 с использованием файла таблицы ключей /tmp/krb5.keytab, выполните:

```
# vinfra service nfs share set share1 --krb-auth true --krb-keytab share1.keytab
```

Чтобы подключить том NFS, для которого включена аутентификация с помощью Kerberos

Укажите параметр sec=krb5 в команде mount. Например, чтобы подключить том share1 с DNS-именем share1.example.com, выполните:

```
# mkdir /mnt/share
# mount -t nfs4 -o sec=krb5 share1.example.com:/share1 /mnt/share/
```

7.5.2.2 Авторизация пользователей томов NFS с помощью LDAP

Если настроить доступ к каталогу пользователей в LDAP, можно контролировать, какие пользователи к каким экспортам NFS могут получать доступ.

Предварительные условия

- Должны быть созданы экспорты NFS, как описано в разделе "Создание экспортов NFS" на странице 220.
- Включена аутентификация с помощью Kerberos, как описано в разделе "Аутентификация пользователей томов NFS с помощью Kerberos" на странице 418.
- Подготовлен каталог пользователей и указаны необходимые разрешения для доступа по NFS.

Чтобы настроить доступ к серверу LDAP

1. Перейдите на экран **Настройки** > **Безопасность** > **LDAP**.
2. Включите авторизацию с помощью LDAP и укажите следующую информацию:
   a. В поле **Адрес** укажите IP-адрес сервера LDAP.
   b. В поле **Base DN** укажите уникальное имя объекта каталога, начиная с которого будет осуществляться поиск записей.
   c. В полях **Bind DN** и **Пароль bind** укажите учетные данные для доступа к серверу LDAP.
3. Нажмите **Сохранить**, чтобы включить доступ к серверу LDAP.

7.5.3 Управление томами NFS

После того как том NFS создан, он запускается автоматически. Можно изменять его размер, уровень хранения, режим избыточности и область отказа, останавливать для смены IP-адреса, а также удалять.

Ограничения

- После создания тома NFS можно изменять его режим избыточности только тогда, когда избыточность обеспечивается с помощью репликации. Возможность изменить режим избыточности отключена для остальных случаев, так как это может снизить производительность кластера. Причина в том, что перекодировка данных требует большого количества ресурсов кластера на долгое время. Если вы все же хотите изменить режим избыточности, свяжитесь со службой технической поддержки.
- Смена IP-адреса возможна только для остановленных томов NFS.
- Нельзя удалить том NFS, у которого есть экспорты NFS.

Предварительные требования

- Создан том NFS, как описано в разделе "Создание томов NFS" на странице 218.

Чтобы остановить том NFS

Панель администратора

1. Перейдите на экран **Сервисы хранилища** > **NFS** > **Тома**.
2. Выберите работающий том NFS и нажмите **Стоп**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service nfs share stop [--force] <name>
```

--force

Остановить том NFS принудительно

<name>

Имя тома NFS

Например, чтобы остановить том share1, выполните:

```
# vinfra service nfs share stop share1
```

Чтобы запустить том NFS

Панель администратора

1. Перейдите на экран **Сервисы хранилища** > **NFS** > **Тома**.
2. Выберите остановленный том NFS и нажмите **Старт**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service nfs share start <name>
```

<name>
: Имя тома NFS

Например, чтобы запустить том share1, выполните:

```
# vinfra service nfs share start share1
```

Чтобы изменить конфигурацию тома NFS

Панель администратора

1. Перейдите на экран **Сервисы хранилища** > **NFS** > **Тома** и выберите необходимый том NFS.
2. Если вы хотите изменить IP-адрес тома, остановите том с помощью кнопки **Стоп**.
3. Нажмите **Настроить**.
4. В разделе **Параметры тома** измените его IP-адрес, размер, уровень хранения, режим избыточности и область отказа.
5. Нажмите **Сохранить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service nfs share set [--tier {0,1,2,3}] [--replicas <norm>] [--failure-domain {0,1,2,3,4}]
                             [--size <size>] <name>
```

--tier {0,1,2,3}
: Уровень хранилища

--replicas <norm>
: Схема репликации хранилища в формате:

  - norm: количество сохраняемых реплик

--failure-domain {0,1,2,3,4}

Область отказа хранилища

--size <size>

Размер тома NFS в байтах. Также можно использовать следующие единицы измерения: KiB для кибибайтов, MiB для мебибайтов, GiB для гибибайтов, TiB для тебибайтов и PiB для пебибайтов.

<name>

Имя тома NFS

Например, чтобы увеличить размер тома share1 до 200 GiB, выполните:

```
# vinfra service nfs share set share1 --size 200GiB
```

Чтобы удалить том NFS

Панель администратора

1. Перейдите на экран **Сервисы хранилища** > **NFS** > **Тома**.
2. Выберите необходимый том NFS и нажмите **Удалить**.
3. Нажмите **Да** в окне подтверждения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service nfs share delete <name>
```

<name>

Имя тома NFS

Например, чтобы удалить том share1, выполните:

```
# vinfra service nfs share delete share1
```

7.5.4 Управление экспортами NFS

Можно изменять конфигурацию и удалять существующие экспорты NFS.

Предварительные требования

- Должны быть созданы экспорты NFS, как описано в разделе "Создание экспортов NFS" на странице 220.

Чтобы изменить конфигурацию экспорта NFS

Панель администратора

1. На экране **Сервисы хранилища** > **NFS** > **Тома** щелкните по номеру в столбце **Экспорты** в строке нужного тома. Откроется экран тома.
2. Выберите экспорт NFS и нажмите **Настроить**.
3. В разделе **Настроить экспорт** измените настройки доступа и/или расширенные настройки и нажмите **Готово**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service nfs export set [--path <path>] [--access-type <access-type>] [--security-types
<security-types>]
                    [--client <address=ip_addresses:access=access_type:security=security_types>]
                    [--squash <squash>] [--anonymous-gid <anonymous-gid>] [--anonymous-uid
<anonymous-uid>]
                    <share-name> <export-name>
```

--path <path>

Путь экспорта NFS

--access-type <access-type>

Режим доступа экспорта NFS (none, rw или ro)

--security-types <security-types>

Режим безопасности экспорта NFS (none, sys, krb5, krb5i или krb5p)

--client <address=ip_addresses:access=access_type:security=security_types>

Список клиентского доступа экспорта NFS

--squash <squash>

Режим отображения пользователей клиентов NFS в пользователей сервера NFS (root_squash, root_id_squash, all_squash или none)

--anonymous-gid <anonymous-gid>

Идентификатор группы для анонимного доступа к экспорту NFS

--anonymous-uid <anonymous-uid>

Идентификатор пользователя для анонимного доступа к экспорту NFS

<share-name>

Имя тома NFS

<export-name>

Имя экспорта NFS

Например, чтобы включить режим доступа "только для чтения" для экспорта export1 тома share1, выполните:

```
# vinfra service nfs export set share1 export1 --access-type ro
```

Чтобы удалить экспорт NFS

Панель администратора

1. На экране **Сервисы хранилища** > **NFS** > **Тома** щелкните по номеру в столбце **Экспорты** в строке нужного тома. Откроется экран тома.
2. Выберите экспорт NFS и нажмите **Удалить**.
3. Нажмите **Да** в окне подтверждения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service nfs export delete <share-name> <export-name>
```

<share-name>

Имя тома NFS

<export-name>

Имя экспорта NFS

Например, чтобы удалить экспорт export1 тома share1, выполните:

```
# vinfra service nfs export delete share1 export1
```

7.5.5 Удаление серверов из кластера NFS

Ограничения

- После удаления последнего сервера из кластера NFS весь кластер и все его данные удаляются.

Предварительные требования

- Создан кластер NFS, как описано в разделе "Создание кластера NFS" на странице 217.

Чтобы удалить сервер из кластера NFS

Панель администратора

1. Перейдите на экран **Сервисы хранилища** > **NFS** > **Серверы**.
2. Выберите один или несколько серверов в разделе **Включено в кластер NFS** и нажмите **Освободить**.
3. Нажмите **Да** в окне подтверждения.

Интерфейс командной строки

- Чтобы удалить сервер из кластера NFS, в котором более одного сервера, выполните:

  ```
  vinfra service nfs node release --nodes <node>
  ```

- Чтобы удалить последний сервер из кластера NFS и удалить кластер, выполните:

```
vinfra service nfs cluster delete
```

7.6 Управление вычислительным кластером

В этом разделе описывается управление вычислительным кластером, его узлами и вычислительными сетями. В нем также рассказывается, как настраивать размещения, образы, типы ВМ и ключи SSH для виртуальных машин. Кроме того, здесь описывается выполнение операций над вычислительным хранилищем, его томами и политиками хранения.

7.6.1 Изменение параметров вычислительного кластера

После развертывания вычислительного кластера может потребоваться настроить клиент командной строки OpenStack, пользовательские параметры в файлах конфигурации OpenStack и резервирование ОЗУ для виртуальных машин.

Предварительные требования

- Должен быть создан вычислительный кластер, как описано в разделе "Создание вычислительного кластера" на странице 169.

7.6.1.1 Подключение к интерфейсу командной строки OpenStack

Для управления вычислительным кластером можно также использовать клиент командной строки OpenStack, который автоматически устанавливается вместе с продуктом Кибер Инфраструктура.

Чтобы подключиться к интерфейсу командной строки OpenStack и работать с ним

Выполните следующие действия:

1. Найдите сервер с ролью «управление» на панели администрирования. Откройте экран **Инфраструктура** > **Серверы**. На сервере управления работает сервис **Панель управления**.
2. Перейдите на сервер управления с помощью SSH и войдите в систему, используя учетные данные пользователя службы, например:

```
# ssh node001.vstoragedomain
# su - vstoradmin
```

3. Создайте скрипт администратора OpenRC, который устанавливает переменные среды.

```
# kolla-ansible post-deploy
```

Команда создаст Bash-скрипт /etc/kolla/admin-openrc.sh.

```
export OS_PROJECT_DOMAIN_NAME=Default
export OS_USER_DOMAIN_NAME=Default
export OS_PROJECT_NAME=admin
export OS_USERNAME=vstorage-service-user
export OS_PASSWORD=<password>
export OS_AUTH_URL=https://<MN_IP_address>:5000/v3
export OS_IDENTITY_API_VERSION=3
export OS_AUTH_TYPE=password
export OS_INSECURE=true
export PYTHONWARNINGS="ignore:Unverified HTTPS request is being made"
export NOVACLIENT_INSECURE=true
export NEUTRONCLIENT_INSECURE=true
export CINDERCLIENT_INSECURE=true
export OS_PLACEMENT_API_VERSION=1.22
```

По умолчанию скрипт создается, чтобы разрешить использование команд OpenStack в проекте admin. Это необходимо, чтобы пользователь vstorage-service-user мог использовать привилегии администратора для управления вычислительным кластером.

4. Для выполнения административных действий запустите следующий скрипт:

Внимание
Скрипт необходимо запускать для каждого сеанса.

```
# source /etc/kolla/admin-openrc.sh
```

Чтобы работать над другим проектом, используя другие учетные данные, внесите изменения в скрипт admin-openrc.sh. Например, чтобы разрешить использование команд OpenStack в проекте myproject пользователя myuser в домене mydomain, выполните следующие действия.

1. Скопируйте этот скрипт в новый каталог под новым именем, например:

```
# cp /etc/kolla/admin-openrc.sh /root/myscript.sh
```

2. Откройте скопированный скрипт для правки и измените первые пять переменных следующим образом.

```
export OS_PROJECT_DOMAIN_NAME=mydomain
export OS_USER_DOMAIN_NAME=mydomain
export OS_PROJECT_NAME=myproject
export OS_USERNAME=myuser
export OS_PASSWORD=<myuser_password>
```

Сохраните изменения.

3. Запустите измененный скрипт.

Внимание

Скрипт необходимо запускать для каждого сеанса.

```
# source /root/myscript.sh
```

Теперь для работы над проектом, в котором была выполнена авторизация, можно использовать команды OpenStack с параметром --insecure, например:

```
# openstack --insecure server list
+--------------------+------+--------+----------------------+-------+--------+
| ID                 | Name | Status | Networks             | Image | Flavor |
+--------------------+------+--------+----------------------+-------+--------+
| 32b0f95d-477f-<...> | vm1  | ACTIVE | private=192.168.128.87 |      | tiny   |
+--------------------+------+--------+----------------------+-------+--------+
```

7.6.1.2 Изменение параметров в файлах конфигурации OpenStack

В файлах конфигурации OpenStack можно изменить следующие параметры:

Параметр	Файл конфигурации	Описание	Значение
ram_weight_multiplier	/etc/kolla/nova-scheduler/nova.conf	Определяет, как взвешиваются вычислительные серверы с доступной оперативной памятью. При положительном значении параметра виртуальные машины размещаются на серверах, где больше доступный объем ОЗУ, и таким образом равномерно распределяются по всем вычислительным серверам. Однако в этом случае может возникнуть такая ситуация, когда вы не сможете запустить большие ВМ на определенных серверах, несмотря на более чем достаточный объем свободной памяти во всем кластере. Чтобы оптимизировать распределение ВМ и заполнять серверы по максимуму, можно установить для этого параметра отрицательное значение.	Допустимыми значениями являются целые числа и числа с плавающей запятой. Значение по умолчанию – 1.0.
scheduler_host_subset_size	/etc/kolla/nova-scheduler/nova.conf	Определяет количество вычислительных серверов, лучше всего подходящих для новой ВМ, один из которых случайным образом выбирается планировщиком.	Допустимым является значение, равное или больше 1. Любое значение меньше 1 рассматривается как 1. Чем больше значение, тем

Параметр	Файл конфигурации	Описание	Значение
			менее оптимальным для ВМ может быть выбранный сервер. Значение по умолчанию – 1.
vxlan_udp_port	/etc/kolla/neutron-openvswitch-agent/ml2_conf.ini	Указывает UDP-порт, который используется для туннелей VXLAN. При изменении порта правила iptables автоматически настраиваются для старого и нового порта.	Порт по умолчанию – 4789.
cpu_allocation_ratio	/etc/kolla/nova-compute/nova.conf	Определяет отношение выделяемых виртуальных ЦП к физическим. **Примечание** Изменение процессорных квот не повлияет на уже выделенные виртуальные ЦП для виртуальных машин.	Допустимыми значениями являются положительные целые числа и числа с плавающей запятой. Значение по умолчанию – 8.0.
ram_allocation_ratio	/etc/kolla/nova-compute/nova.conf	Определяет максимальное отношение зарезервированной ОЗУ к физической. **Примечание** Изменение квот ОЗУ не повлияет на уже выделенный объем ОЗУ для виртуальных машин.	Допустимыми значениями являются положительные целые числа и числа с плавающей запятой. Значение по умолчанию – 1.0. Максимальное рекомендуемое значение – 1.5.

Чтобы изменить параметр

Используйте следующую команду:

```
vinfra service compute set [--custom-param <service_name> <config_file> <section> <property> <value>]
                           [--nova-scheduler-ram-weight-multiplier <value>]
                           [--nova-compute-ram-allocation-ratio <value>]
                           [--neutron-openvswitch-vxlan-port <value>]
                           [--nova-scheduler-host-subset-size <value>]
                           [--nova-compute-cpu-allocation-ratio <value>]
```

--custom-param <service_name> <config_file> <section> <property> <value>

Установка пользовательских параметров для файлов конфигурации OpenStack:

- service_name – имя сервиса: nova-scheduler, nova-compute или neutron-openvswitch-agent
- config_file указывает файл конфигурации сервиса: nova.conf для nova-scheduler и nova-compute либо ml2_conf.ini для neutron-openvswitch-agent
- section указывает раздел в файле конфигурации сервиса, где определен нужный параметр: DEFAULT в nova.conf или agent в ml2_conf.ini
- property – параметр, который следует изменить: ram_weight_multiplier, ram_allocation_ratio, scheduler_host_subset и cpu_allocation_ratio в nova.conf; vxlan_udp_port в ml2_conf.ini
- value – новое значение параметра

--nova-scheduler-ram-weight-multiplier <value>

Сокращение для --custom-param nova-scheduler nova.conf DEFAULT ram_weight_multiplier <value>

--nova-compute-ram-allocation-ratio <value>

Сокращение для --custom-param nova-compute nova.conf DEFAULT ram_allocation_ratio <value>

--neutron-openvswitch-vxlan-port <value>

Сокращение для --custom-param neutron-openvswitch-agent ml2_conf.ini agent vxlan_udp_port <value>

--nova-scheduler-host-subset-size <value>

Сокращение для --custom-param nova-scheduler nova.conf DEFAULT scheduler_host_subset_size <value>

--nova-compute-cpu-allocation-ratio <value>

Сокращение для --custom-param nova-scheduler nova.conf DEFAULT cpu_allocation_ratio <value>

Например, чтобы изменить значения ram_weight_multiplier и vxlan_udp_port, выполните следующую команду:

```
# vinfra service compute set --nova-scheduler-ram-weight-multiplier -1 \
--neutron-openvswitch-vxlan-port 4787
```

Чтобы проверить, что настроенные параметры успешно изменены, выполните команду vinfra service compute show.

```
# vinfra service compute show
+-------------+-----------------------------------------+
| Field       | Value                                   |
+-------------+-----------------------------------------+
| <...>       | <...>                                   |
| options     | cpu_model: ''                           |
|             | custom_params:                          |
```

```
|           | - config_file: nova.conf              |
|           |   property: ram_weight_multiplier     |
|           |   section: DEFAULT                    |
|           |   service_name: nova-scheduler        |
|           |   value: -1.0                         |
|           | - config_file: ml2_conf.ini           |
|           |   property: vxlan_udp_port            |
|           |   section: agent                      |
|           |   service_name: neutron-openvswitch-agent |
|           |   value: 4787                         |
|           | notification_forwarding: disabled     |
| status    | active                                |
+-----------+---------------------------------------+
```

Изменения согласованно применяются на всех вычислительных серверах и не перезаписываются после обновлений продукта.

7.6.1.3 Настройка памяти для виртуальных машин

Для оптимизации использования памяти виртуальными машинами Кибер Инфраструктура использует технологию ядра Linux - Kernel Same-page Merging (KSM). Служба KSM периодически проверяет память на наличие страниц с одинаковым содержимым и объединяет их в одну страницу. Такая страница помечается как страница для копирования при записи (CoW), и, когда виртуальной машине необходимо изменить содержимое этой страницы, ядро создает копию страницы для виртуальной машины, а ВМ изменяет содержимое копии. Данная технология позволяет использовать перераспределение памяти и избегать использования пространства для подкачки, когда много похожих задач выполняются на одном и том же сервере. Однако настоятельно рекомендуется настроить пространство для подкачки при включении перераспределения памяти.

Кроме того, виртуальные машины, запущенные на сервере, привязаны к узлам NUMA, чтобы процессы виртуальных машин находились как можно ближе к памяти, к которой они обращаются. Когда разница в нагрузке на узлы NUMA превышает 50 %, происходит перебалансировка размещенных ВМ с учетом объема ОЗУ и количества ядер ЦП, которые они потребляют.

Чтобы настроить объем памяти, выделяемой виртуальным машинам, установите коэффициент перераспределения ОЗУ. Коэффициент представляет собой соотношение максимального объема зарезервированной памяти к объему физической памяти. По умолчанию это соотношение равно 1. Это означает, что нельзя выделить объем памяти, превышающий общий объем физической памяти на всех вычислительных узлах. Увеличивая коэффициент, можно увеличить количество виртуальных машин, запущенных на вычислительном узле, за счет снижения их производительности. Рекомендуемый максимальный коэффициент перераспределения равен 1,5.

Перераспределение памяти для виртуальных машин доступно, только если на всех вычислительных узлах достаточно места для подкачки. Прежде чем включить эту функцию, рассчитайте необходимое пространство для подкачки и настройте его на каждом узле.

Добавление пространства подкачки

Чтобы обеспечить коэффициент перераспределения ОЗУ, необходимо добавить пространство подкачки. Размер пространства подкачки зависит от установленного коэффициента перераспределения ОЗУ. Для его расчета можно использовать следующую формулу:

```
(total RAM – RAM used for system) * (RAM overcommitment ratio – 1)
```

Чтобы лучше понять, как вычисляется минимальный размер пространства подкачки, рассмотрим следующие примеры.

- Общий объем физической памяти на вычислительном узле составляет 24 ГиБ
- 8 ГиБ ОЗУ зарезервировано под систему
- Рекомендуемый коэффициент перераспределения ОЗУ составляет 1,5

По этой формуле минимальный обязательный размер пространства подкачки будет составлять 8 ГиБ. Рассчитав необходимое пространство подкачки, переходим к созданию и настройке файла подкачки.

Ограничения

- После создания файла подкачки, его размер невозможно изменить.

Предварительные требования

- Для создания файла подкачки в корневом каталоге должно оставаться не менее 100 ГиБ свободного пространства после создания файла. Например, чтобы создать файл подкачки размером 8 ГиБ, убедитесь, что в корневом каталоге есть не менее 108 ГиБ доступного пространства.

Чтобы создать файл подкачки

На всех узлах вычислительного кластера выполните скрипт configure-swap.sh, чтобы задать желаемый размер файла подкачки:

```
# /usr/libexec/vstorage-ui-agent/bin/configure-swap.sh -s 8192
```

Используйте этот скрипт, чтобы создать файл подкачки, подготовить пространство подкачки и добавить для него точку подключения к /etc/fstab.

Чтобы убедиться в успешном создании файла подкачки, выполните следующую команду:

```
# swapon -s
Filename        Type      Size   Used   Priority
/dev/sda3       partition  8258556  0   -2
/swapfile0      file      8389628  0   -3
```

Чтобы увеличить размер пространства подкачки

Создайте дополнительный файл с помощью следующей команды:

```
# /usr/libexec/vstorage-ui-agent/bin/configure-swap.sh -s 8192 --append
```

Включение и отключение перераспределения ОЗУ

Перераспределение ОЗУ для виртуальных машин доступно только при наличии достаточного пространства подкачки на всех вычислительных узлах.

Предварительные требования

- Создан файл подкачки, как указано в разделе "Добавление пространства подкачки" на предыдущей странице.

Чтобы включить перераспределение ОЗУ для виртуальных машин

Используйте команду vinfra service compute create или vinfra service compute set с параметром --custom-param или --nova-compute-ram-allocation-ratio. Например, чтобы настроить коэффициент перераспределения ОЗУ, равный 1,5, выполните следующую команду:

```
# vinfra service compute set --nova-compute-ram-allocation-ratio 1.5
```

Чтобы убедиться, что соотношение успешно изменено, выполните команду vinfra service compute show.

```
# vinfra service compute show
+--------------+-------------------------------------------+
| Field        | Value                                     |
+--------------+-------------------------------------------+
| <...>        | <...>                                     |
| options      | cpu_model: ''                             |
|              | custom_params:                            |
|              | - config_file: nova.conf                  |
|              |   property: ram_allocation_ratio          |
|              |   section: DEFAULT                        |
|              |   service_name: nova-compute              |
|              |   value: 1.5                              |
| <...>        | <...>                                     |
+--------------+-------------------------------------------+
```

Чтобы выключить перераспределение ОЗУ для виртуальных машин

Задайте коэффициенту перераспределения ОЗУ значение 1 с помощью следующей команды:

```
# vinfra service compute set --nova-compute-ram-allocation-ratio 1
```

В этом случае пространство для подкачки больше не требуется и файл подкачки можно удалить с помощью следующей команды:

```
# /usr/libexec/vstorage-ui-agent/bin/configure-swap.sh --remove-all
```

Запустите этот скрипт на всех узлах вычислительного кластера, чтобы удалить файл подкачки с каждого из них.

7.6.2 Управление виртуальными машинами

Каждая виртуальная машина (ВМ) – это независимая система с независимым набором виртуального оборудования. Она имеет следующие основные характеристики.

- Виртуальная машина представляет собой подобие обычного компьютера и работает аналогичным образом. Она имеет собственное виртуальное оборудование. Программные приложения могут работать в виртуальных машинах без каких-либо изменений или специальных настроек.
- Конфигурацию виртуальной машины можно легко изменить, например добавив новые виртуальные диски или память.
- Хотя виртуальные машины совместно используют одни физические аппаратные ресурсы, они полностью изолированы друг от друга (имеют отдельные файловые системы, процессы, переменные sysctl) и от вычислительного сервера.
- На виртуальной машине может работать любая поддерживаемая гостевая операционная система.

В таблице ниже перечислены текущие ограничения для конфигурации виртуальных машин.

Ресурс	Ограничение
ОЗУ	1 ТиБ
ЦП	64 виртуальных ЦП
Хранилище	15 томов по 512 ТиБ каждый
Сеть	15 сетевых адаптеров

Предварительные требования

- Должен быть создан вычислительный кластер, как описано в разделе "Создание вычислительного кластера" на странице 169.

7.6.2.1 Поддерживаемые гостевые операционные системы

Перечисленные ниже гостевые операционные системы прошли тестирование и поддерживаются в виртуальных машинах.

Примечание
Поддерживается только архитектура x64.

Linux

Дистрибутив	Версия	Поддержка горячего подключения ЦП	Поддержка горячего подключения ОЗУ
Alma Linux	9, 8	Да	Да
Astra Linux Common Edition	2.12, 2.11	Да	Да
Astra Linux Special Edition	1.6, 1.5	Да	Да
CentOS	9.x, 8.x, 7.x	Да	Да
	6.x	Нет	Нет
Debian	11.x, 10.x, 9.x	Да	Да
Red Hat Enterprise Linux	9.x, 8.x, 7.x	Да	Да
Rocky Linux	9, 8	Да	Да
Ubuntu	22.04.x, 20,04.x, 18,04.x	Да	Да
	16,04.x	Нет	Нет
Альт Рабочая станция	10, 9	Да	Да
Альт Сервер	10, 9	Да	Да
РЕД ОС	7	Да	Да
РОСА FRESH	R12, R11	Да	Да
РОСА КОБАЛЬТ	7	Да	Да
РОСА ХРОМ	12	Да	Да

Windows

Версия	Выпуск	Поддержка горячего подключения ЦП	Поддержка горячего подключения ОЗУ
Windows Server 2022	Essentials	Нет	Нет
	Standard, Datacenter	Да	Да
Windows Server 2019	Essentials	Нет	Нет
	Standard, Datacenter	Да	Да

Версия	Выпуск	Поддержка горячего подключения ЦП	Поддержка горячего подключения ОЗУ
Windows Server 2016	Essentials	Нет	Нет
	Standard, Datacenter	Да*	Да
Windows Server 2012 R2	Essentials, Standard, Datacenter	Да	Да
Windows Server 2012	Standard, Datacenter	Да	Да
Windows Server 2008 R2	Standard, Datacenter	Нет	Нет
Windows 10	Home, Professional, Enterprise, Enterprise 2016 LTSB	Нет	Нет
Windows 8.1	Home, Professional, Enterprise	Нет	Нет
Windows 7	Home, Professional, Enterprise	Нет	Нет

*Горячее подключение ЦП работает некорректно из-за ошибки Windows с неправильно установленным драйвером. Чтобы устранить эту проблему, используйте это решение.

7.6.2.2 Подготовка загрузочного носителя для виртуальных машин

Перед созданием виртуальной машины необходимо подготовить образ-источник с гостевой операционной системой, чтобы ВМ загружалась с него. Можно использовать следующие типы носителей:

- ISO-образ – это стандартный формат дистрибутивов ОС, которые необходимо устанавливать на диск. ISO-образ можно загрузить в вычислительный кластер.
- Шаблон – это готовый загрузочный том в формате QCOW2 с установленной операционной системой и приложениями. Многие поставщики ОС предлагают шаблоны своих операционных систем, называя их облачными образами. Облачный образ можно загрузить из официального репозитория ОС, также можно подготовить собственный шаблон в вычислительном кластере.
- Загрузочный том с установленной операционной системой и приложениями. Загрузочный том можно подготовить в вычислительном кластере.

Предварительные требования

- Знакомство с поддерживаемыми операционными системами, перечисленными в разделе "Поддерживаемые гостевые операционные системы" на странице 435.

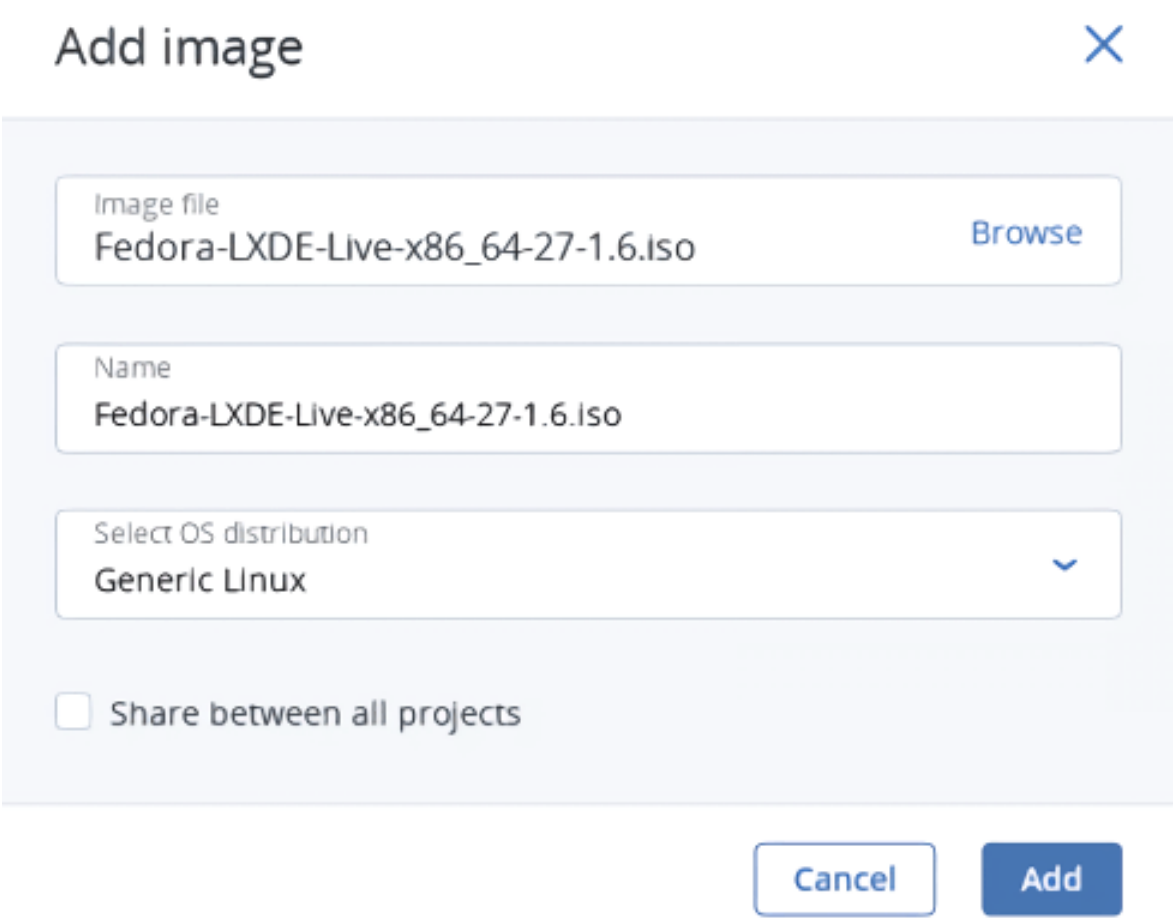
Загрузка образов виртуальных машин

Как загрузить образ

Панель администратора

1. Перейдите на экран **Вычисления** > **Виртуальные машины** > **Образы** и нажмите **Добавить образ**.
2. В окне **Добавить образ** выполните следующие действия.
   a. Нажмите **Обзор** и выберите файл в одном из поддерживаемых форматов: .iso, .img, .qcow2, .raw.
   b. Укажите имя образа, которое будет отображаться на панели администратора.
   c. Выберите правильный тип ОС из раскрывающегося списка.

   Внимание
   Тип ОС влияет на параметры ВМ, такие как настройки гипервизора. ВМ, созданные из образа с неверным типом ОС, могут работать неправильно, например могут происходить сбои.



3. [Необязательно] Установите флажок **Использовать во всех проектах**. Если этот параметр отключен, образ будет доступен только в проекте **admin** домена **Default** (По умолчанию).
4. Нажмите **Добавить**, чтобы начать передачу образа. Индикатор хода загрузки будет отображаться в правом нижнем углу.

Всплывающее окно можно скрыть, не прерывая процесса загрузки. Индикатор хода загрузки будет доступен в центре уведомлений.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute image create [--min-disk <size-gb>] [--min-ram <size-mb>] [--os-distro <os-distro>]
                                    [--protected | --unprotected] [--public] [--public] [--disk-format <disk_format>]
                                    [--container-format <format>] [--tags <tags>] --file <file> <image-name>
```

--min-disk <size-gb>

Минимальный размер диска, необходимый для загрузки с образа, в гигабайтах.

--min-ram <size-mb>

Минимальный размер ОЗУ, необходимый для загрузки с образа, в мегабайтах.

--os-distro <os-distro>

Дистрибутив ОС. Чтобы вывести список доступных дистрибутивов, выполните команду vinfra service compute show.

--protected

Защита образа от удаления.

--unprotected

Разрешает удалять образ.

--public

Делает образ доступным для всех пользователей.

--private

Делает образ доступным только владельцам.

--disk-format <disk_format>

Формат диска: detect, iso, qcow2, raw (по умолчанию detect).

--container-format <format>

Формат контейнера: bare.

--tags <tags>

Список тегов через запятую.

--file <file>

Создание образа из локального файла.

<image-name>

Имя образа.

Например, чтобы создать образ Cirros из локального файла и загрузить его в вычислительный кластер, выполните:

```
# vinfra service compute image create mycirrosimg --file /distr/cirros-0.4.0-x86_64-disk.img
Uploading image to server [elapsed time: 0:00:04]... |
```

Информация о ходе загрузки образа будет отображаться в выводе команды. Для просмотра всех образов вычислительного кластера выполните:

```
# vinfra service compute image list
+--------------------+-------------+----------+--------+-------------+
| id                 | name        |     size | status | disk_format |
+--------------------+-------------+----------+--------+-------------+
| 179f45ef-c5d6-<...> | mycirrosimg | 12716032 | active | qcow2       |
| 4741274f-5cca-<...> | cirros      | 12716032 | active | qcow2       |
+--------------------+-------------+----------+--------+-------------+
```

Подготовка шаблонов

Создание шаблона может потребоваться в следующих случаях:

- Аварийное восстановление виртуальной машины.
- Создание ВМ, доступной через SSH.
- Создание ВМ, настраиваемой с пользовательскими данными.

Общая схема подготовки

1. Установите Cloudbase-Init и OpenSSH Server в виртуальную машину.
2. [Необязательно] Включите ведение журнала для виртуальных машин, которые будут создаваться из шаблона.
3. Преобразуйте загрузочный том ВМ в шаблон.

Получение шаблонов Linux

Поскольку во всех гостевых ОС Linux по умолчанию предустановлен OpenSSH Server, необходимо только убедиться, что в шаблоне Linux установлен пакет cloud-init.

Самый простой способ получить шаблон Linux с установленным пакетом cloud-init – загрузить из официального репозитория или создать с помощью diskimage-builder. Либо можно создать шаблон Linux из существующего загрузочного тома.

Ограничения

- Образ диска создается только с пользователем root, у которого нет ни пароля, ни SSH-ключей. Можно использовать методы user data и cloud-init для выполнения задач начальной конфигурации на ВМ, которые будут развернуты из этого образа, например для создания определенных учетных записей пользователей. Другие параметры для настройки ВМ во время загрузки см. в документации по cloud-init.

Чтобы создать шаблон Linux

1. Установите пакет diskimage-builder:

```
# yum install diskimage-builder
```

2. Для гостевой ОС RHEL 7 загрузите облачный образ с клиентского портала Red Hat (требуется вход) и выполните следующую команду:

```
# export DIB_LOCAL_IMAGE=<path_to_rhel7_image>
```

3. Выполните команду disk-image-create, чтобы создать образ диска с установленным пакетом cloud-init для нужной гостевой системы Linux, например:

```
# disk-image-create vm centos7 -t qcow2 -o centos7
```

где:

- centos7 — имя гостевой ОС. Может иметь одно из следующих значений: centos6, centos7, debian, rhel7 или ubuntu.

  По умолчанию при использовании варианта ubuntu будет создан образ диска для Ubuntu 16.04. Чтобы создать образ для Ubuntu 18.04, добавьте в команду DIB_RELEASE=bionic: DIB_RELEASE=bionic disk-image-create vm ubuntu -t qcow2 -o ubuntu18.
- -o задает имя итогового файла образа диска.

4. Отправьте созданный образ диска в вычислительный кластер с помощью инструмента vinfra:

```
# vinfra service compute image create centos7-image --os-distro centos7 \
--disk-format qcow2 --file centos7.qcow2
```

где:

- centos7-image — имя нового образа.
- centos7 — дистрибутив ОС. Может иметь одно из следующих значений: centos6, centos7, debian9, rhel7, ubuntu16.04 и ubuntu18.04.
- centos7.qcow2 — образ QCOW2, созданный на шаге 3.

Чтобы развернуть виртуальную машину из загруженного шаблона

1. Создайте файл конфигурации user-data с нужной учетной записью пользователя:

```
# cat <<EOF > user-data
#cloud-config
user: myuser
password: password
chpasswd: {expire: False}
ssh_pwauth: True
EOF
```

где myuser — имя пользователя, а password — пароль для учетной записи.

2. Запустите развертывание ВМ из образа диска, используя файл конфигурации в качестве данных пользователя:

```
# vinfra service compute server create centos7-vm --flavor medium \
--network public --user-data user-data --volume source=image,\
id=centos7-image,size=10
```

где:

- centos7-vm – имя новой ВМ.
- user-data – файл конфигурации, созданный на шаге 1.
- centos7-image – образ, добавленный в вычислительный кластер.

Настройка загрузочных томов Windows

В гостевых ОС Windows по умолчанию не предустановлены ни Cloudbase-Init, ни OpenSSH Server. Их необходимо установить и настроить вручную.

Как установить Cloudbase-Init и OpenSSH Server в виртуальную машину Windows

1. Выполните вход в ВМ Windows.
2. Создайте новую учетную запись администратора, которая будет использоваться для SSH-подключений, и выполните вход с этой учетной записью.
3. Чтобы установить и настроить OpenSSH Server
   a. Запустите Windows PowerShell с правами администратора и установите для политики выполнения значение Unrestricted, чтобы иметь возможность выполнять скрипты.

      ```
      > Set-ExecutionPolicy Unrestricted
      ```

   b. Загрузите OpenSSH Server (например, из репозитория GitHub), распакуйте архив в папку C:\Program Files и установите его, выполнив следующую команду:

      ```
      > & 'C:\Program Files\OpenSSH-Win64\install-sshd.ps1'
      ```

   c. Запустите сервис sshd и задайте для него автоматический тип запуска.

      ```
      > net start sshd
      > Set-Service sshd -StartupType Automatic
      ```

   d. Откройте порт TCP 22 для сервиса OpenSSH в брандмауэре Windows.
      - В Windows 8.1, Windows Server 2012 и более новых версиях выполните следующую команду:

        ```
        > New-NetFirewallRule -Protocol TCP -LocalPort 22 -Direction Inbound -Action Allow -
        DisplayName OpenSSH
        ```

      - В Windows 7, Windows Server 2008 и Windows Server 2008 R2 выполните следующую команду:

```
> netsh advfirewall firewall add rule name=sshd dir=in action=allow protocol=TCP
localport=22
```

e. Откройте файл C:\ProgramData\ssh\sshd_config.

```
> notepad 'C:\ProgramData\ssh\sshd_config'
```

Закомментируйте следующие строки в конце файла:

```
#Match Group administrators
#AuthorizedKeysFile __PROGRAMDATA__/ssh/administrators_authorized_keys
```

Сохраните изменения.

f. Создайте папку .ssh в C:\Users\<current_user> и пустой файл authorized_keys внутри нее.

```
> cd C:\Users\<current_user>
> mkdir .ssh
> notepad .\.ssh\authorized_keys
```

Удалите расширение .txt у созданного файла.

```
> move .\.ssh\authorized_keys.txt .\.ssh\authorized_keys
```

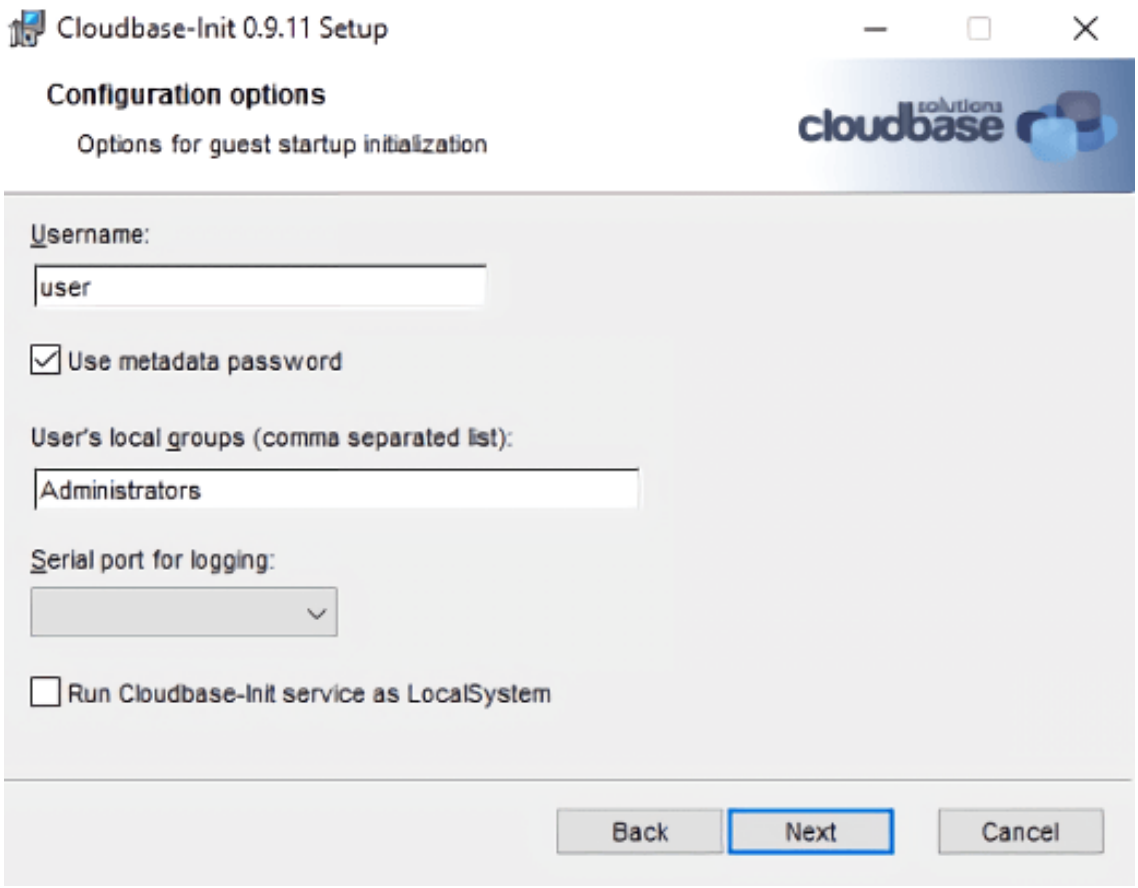
g. Измените разрешения для созданного файла, чтобы отключить наследование.

```
> icacls .\.ssh\authorized_keys /inheritance:r
```

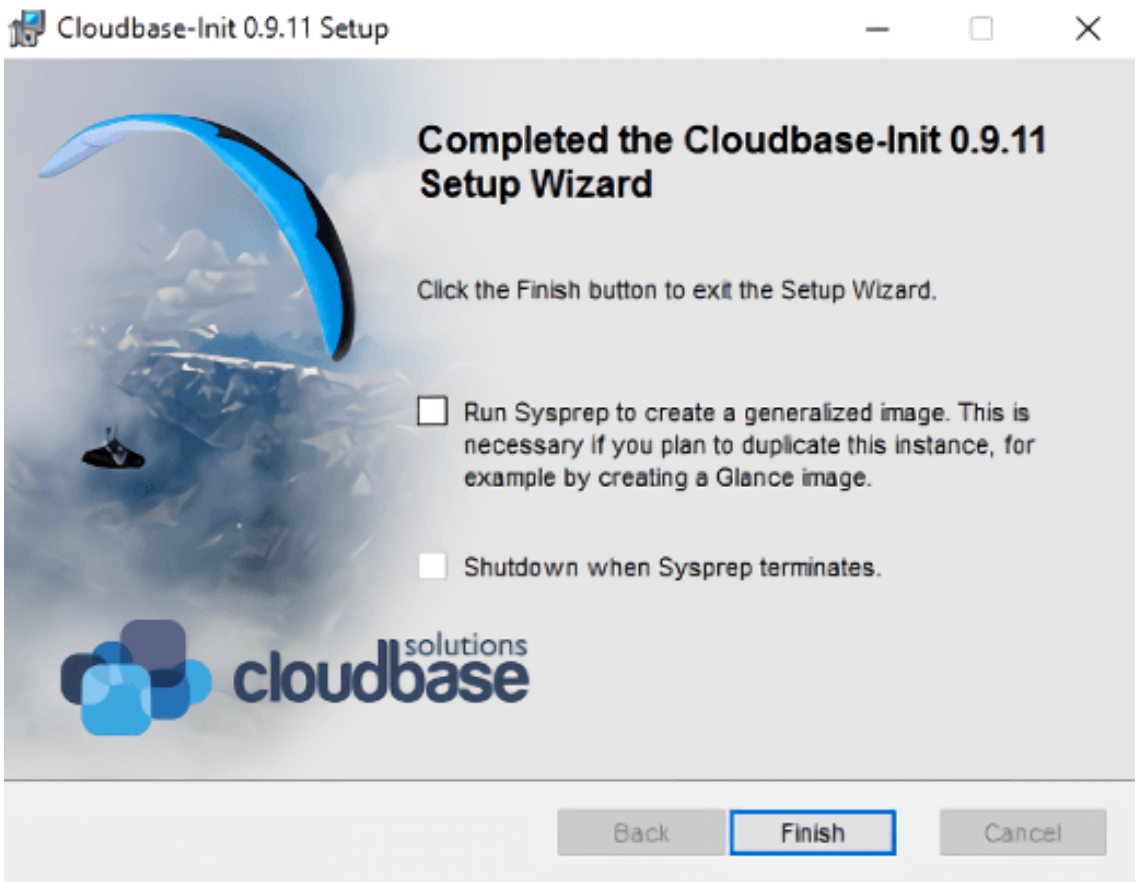
4. Загрузите Cloudbase-Init (например, с официального сайта), запустите установку и следуйте инструкциям на экране.

a. В окне **Параметры конфигурации** введите текущее имя пользователя в поле **Имя пользователя**.

Внимание
Пароль учетной записи будет сброшен при следующем запуске ВМ. Вы сможете выполнить вход с этой учетной записью, используя метод аутентификации с ключом, либо установить новый пароль с помощью скрипта настройки.



b. После окончания установки не запускайте Sysprep и нажмите **Завершить**.



c. Запустите Windows PowerShell с правами администратора и откройте файл C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\cloudbase-init.conf.

```
> notepad 'C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\cloudbase-init.conf'
```

Добавьте metadata_services и plugins в две строки.

```
metadata_services=\
cloudbaseinit.metadata.services.configdrive.ConfigDriveService,\
cloudbaseinit.metadata.services.httpservice.HttpService\
plugins=cloudbaseinit.plugins.common.mtu.MTUPlugin,\
cloudbaseinit.plugins.windows.ntpclient.NTPClientPlugin,\
cloudbaseinit.plugins.common.sethostname.SetHostNamePlugin,\
cloudbaseinit.plugins.windows.createuser.CreateUserPlugin,\
cloudbaseinit.plugins.common.networkconfig.NetworkConfigPlugin,\
cloudbaseinit.plugins.windows.licensing.WindowsLicensingPlugin,\
cloudbaseinit.plugins.common.sshpublickeys.SetUserSSHPublicKeysPlugin,\
cloudbaseinit.plugins.windows.extendvolumes.ExtendVolumesPlugin,\
cloudbaseinit.plugins.common.setuserpassword.SetUserPasswordPlugin,\
cloudbaseinit.plugins.common.userdata.UserDataPlugin,\
cloudbaseinit.plugins.windows.winrmlistener.ConfigWinRMListenerPlugin,\
cloudbaseinit.plugins.windows.winrmcertificateauth.\
ConfigWinRMCertificateAuthPlugin,\
cloudbaseinit.plugins.common.localscripts.LocalScriptsPlugin
```

Примечание
Не забудьте удалить все символы обратной косой черты в строках выше.

Сохраните изменения.

Включение ведения журнала для виртуальных машин

Журнал консоли виртуальной машины можно использовать для диагностики проблем с загрузкой. Журнал содержит сообщения, только если ведение журнала включено внутри ВМ, иначе журнал будет пустым.

Ведение журнала можно активировать, включив уровни ведения журнала TTY1 и TTYS0 в ВМ Linux или перенаправление на консоль сервисов аварийного управления (EMS) в ВМ Windows. Также можно включить ведение журнала состояния драйверов в ВМ Windows, чтобы просматривать список загруженных драйверов. Это может пригодиться для диагностики неисправного драйвера или долгого процесса загрузки.

Как включить ведение журнала TTY1 и TTYS0 в виртуальных машинах Linux

1. Добавьте строку GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0" в файл /etc/default/grub.
2. В зависимости от загрузчика выполните команду

   ```
   # grub-mkconfig -o /boot/grub/grub.cfg
   ```

   или

   ```
   # grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

3. Перезагрузите ВМ.

Как включить перенаправление на консоль EMS в виртуальных машинах Windows

1. Запустите **Windows PowerShell** с правами администратора.
2. В консоли PowerShell задайте COM-порт и скорость передачи данных для перенаправления на консоль EMS. Поскольку виртуальные машины Windows имеют только порт COM1 со скоростью передачи 9600 бит/с, выполните следующую команду:

   ```
   bcdedit /emssettings EMSPORT:1
   ```

3. Включите EMS для текущей загрузочной записи:

   ```
   bcdedit /ems on
   ```

Как включить ведение журнала состояния драйверов в виртуальных машинах Windows

1. Запустите программу **Конфигурация системы** с правами администратора.
2. В окне **Конфигурация системы** откройте вкладку **Загрузка** и установите флажки **Информация об ОС** и **Сделать эти параметры загрузки постоянными**.
3. Подтвердите изменения и перезапустите систему.

Создание шаблонов

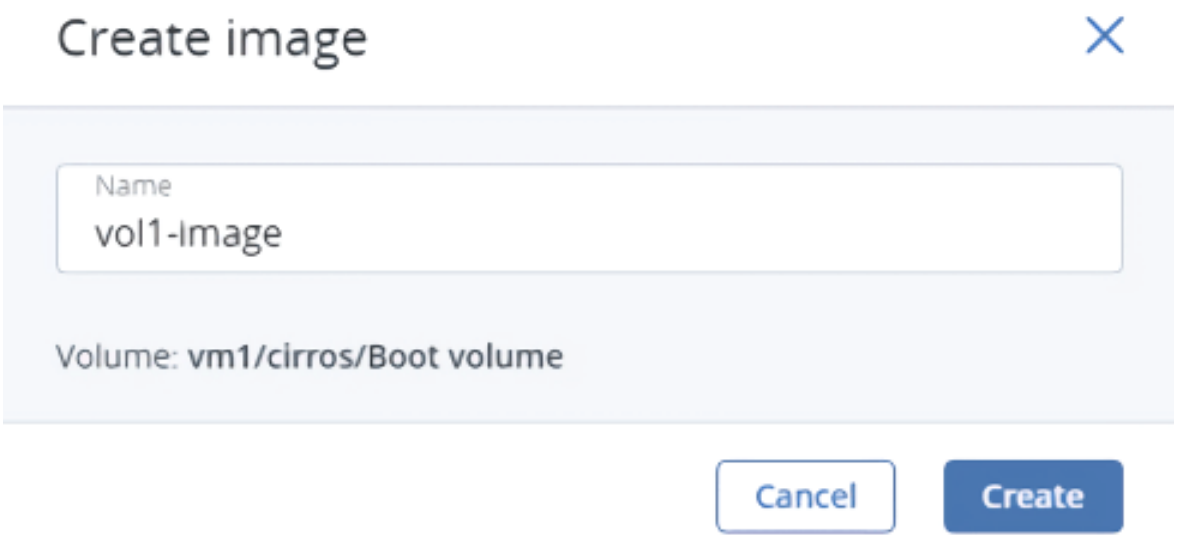
Предварительные требования

- На виртуальных машинах Linux должен быть установлен пакет cloud-init, как описано в разделе "Получение шаблонов Linux" на странице 440.
- На виртуальных машинах Windows должны быть установлены Cloudbase-Init и OpenSSH Server, как описано в разделе "Настройка загрузочных томов Windows" на странице 442.
- [Необязательно] Ведение журнала должно быть включено внутри виртуальной машины, как указано в разделе "Включение ведения журнала для виртуальных машин" на предыдущей странице.

Как создать шаблон из загрузочного тома

Панель администратора

1. Выключите ВМ, к которой присоединен исходный том.
2. Перейдите на экран **Вычисления** > **Виртуальные машины** > **Образы**, нажмите значок с многоточием рядом с томом и выберите **Создать образ**.
3. В окне **Создать образ** введите имя образа и нажмите **Создать**.



Новый образ появится на экране **Образы**.

Интерфейс командной строки

1. Остановите ВМ, загрузочный том которой следует использовать. Например:

```
# vinfra service compute server stop myvm
```

2. Получите идентификатор загрузочного тома. Например:

```
# vinfra service compute server show myvm
+--------------+------------------------------------------+
| Field        | Value                                    |
+--------------+------------------------------------------+
| config_drive |                                          |
| created      | 2021-06-10T08:55:53Z                     |
| description  |                                          |
| fault        |                                          |
| flavor       | disk: 0                                  |
|              | ephemeral: 0                             |
|              | extra_specs: {}                          |
|              | original_name: tiny                      |
|              | ram: 512                                 |
|              | swap: 0                                  |
|              | vcpus: 1                                 |
| ha_enabled   | True                                     |
| host         | amigai-ac-ve0.vstoragedomain             |
| host_status  | UP                                       |
| id           | 6d0fc132-7ea7-41f0-81ca-a4a2b2a2c893     |
| key_name     |                                          |
| metadata     | {}                                       |
| name         | myvm                                     |
| networks     | - id: bd17c207-5291-4096-be6a-0a8a4bf67792 |
|              | ipam_enabled: true                       |
|              | ips:                                     |
|              | - 192.168.128.100                        |
|              | mac_addr: fa:16:3e:6b:6c:83              |
|              | name: private                            |
|              | spoofing_protection: true                |
| orig_hostname | amigai-ac-ve0                           |
| placements   | []                                       |
| power_state  | SHUTDOWN                                 |
| project_id   | dfd99654b8c94b939b638f94abb2ad73         |
| status       | SHUTOFF                                  |
| task_state   |                                          |
| updated      | 2021-06-15T11:24:05Z                     |
| user_data    |                                          |
| vm_state     | stopped                                  |
| volumes      | - delete_on_termination: false           |
|              | id: 49be1057-c026-494f-b85d-e013728d41bd |
|              | - delete_on_termination: false           |
|              | id: eca9f679-7e35-4768-ad20-9bcb6af6fd59 |
+--------------+------------------------------------------+
```

Первый том в выводе команды – загрузочный том.

3. Загрузите том как образ, указав имя образа. Например:

```
# vinfra service compute volume upload-to-image 49be1057-c026-494f-b85d-e013728d41bd \
--name image_from_volume
```

Новый образ появится в выводе команды vinfra service compute image list:

```
# vinfra service compute image list
+--------------------------------------+------------------+-----------+--------+-------------+
| id                                   | name             | size      | status | disk_format |
+--------------------------------------+------------------+-----------+--------+-------------+
| d51ad587-6524-4685-b54c-56b7f3e0591d | image_from_volume | 171966464 | active | qcow2       |
| cd964608-edef-479e-b10e-9851dbc0b431 | cirros           | 12716032  | active | qcow2       |
+--------------------------------------+------------------+-----------+--------+-------------+
```

Подготовка загрузочных томов

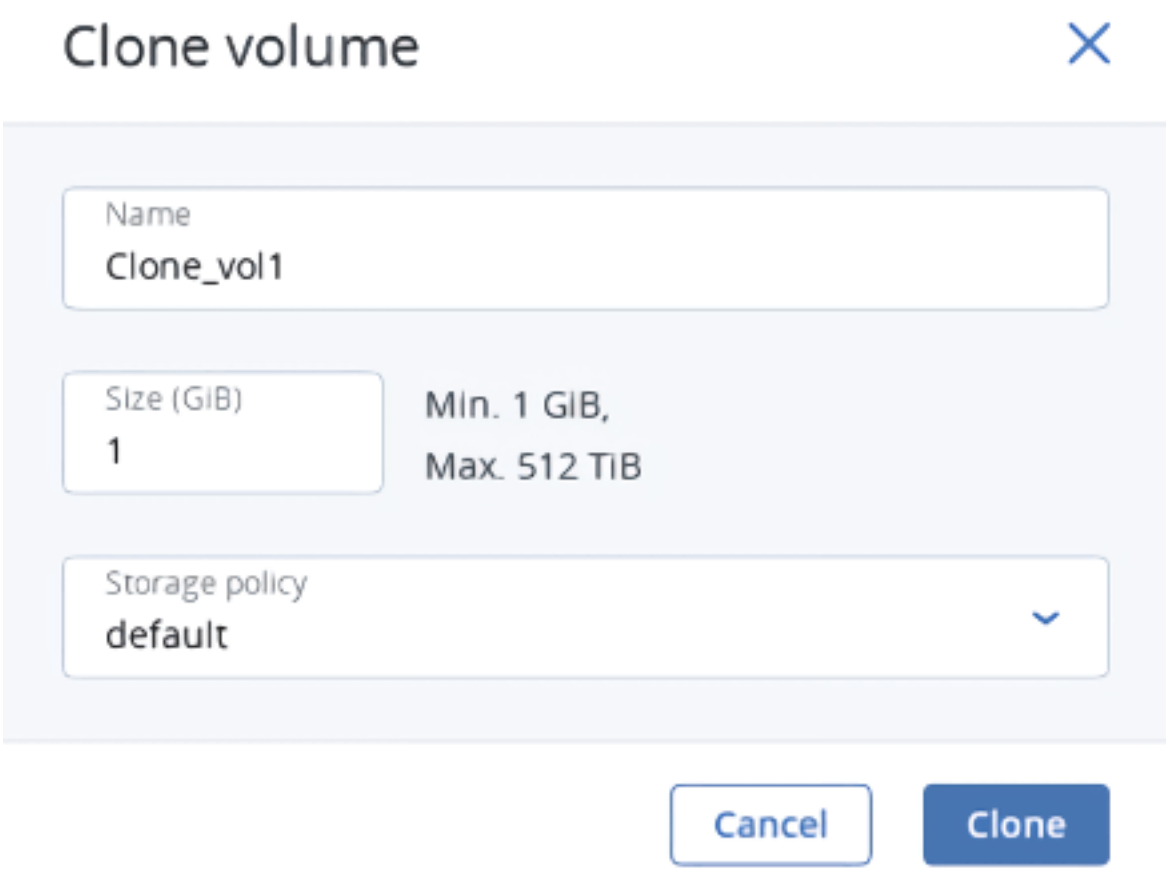
Указания по подготовке загрузочного тома зависят от типа его источника.

Чтобы создать загрузочный том на основе существующей виртуальной машины

Панель администратора

1. Остановите ВМ, загрузочный том с которой вы намерены использовать.
2. На правой панели ВМ перейдите в раздел **Свойства** и щелкните по диску, помеченному как **Загрузочный**.
3. На правой панели тома нажмите **Клонировать**.
4. В окне **Клонировать том** укажите имя тома, размер и политику хранения. Нажмите

Клонировать.



Интерфейс командной строки

1. Остановите ВМ, загрузочный том которой следует использовать. Например:

```
# vinfra service compute server stop myvm
```

2. Узнайте идентификатор загрузочного тома. Например:

```
# vinfra service compute server show myvm
+---------------+--------------------------------------------+
| Field         | Value                                      |
+---------------+--------------------------------------------+
| config_drive  |                                            |
| created       | 2021-06-10T08:55:53Z                       |
| description   |                                            |
| fault         |                                            |
| flavor        | disk: 0                                    |
|               | ephemeral: 0                               |
|               | extra_specs: {}                            |
|               | original_name: tiny                        |
|               | ram: 512                                   |
|               | swap: 0                                    |
```

```
|            | vcpus: 1                                  |
| ha_enabled   | True                                      |
| host         | amigai-ac-ve0.vstoragedomain              |
| host_status  | UP                                        |
| id           | 6d0fc132-7ea7-41f0-81ca-a4a2b2a2c893      |
| key_name     |                                           |
| metadata     | {}                                        |
| name         | myvm                                      |
| networks     | - id: bd17c207-5291-4096-be6a-0a8a4bf67792 |
|              |   ipam_enabled: true                      |
|              |   ips:                                    |
|              |   - 192.168.128.100                       |
|              |   mac_addr: fa:16:3e:6b:6c:83             |
|              |   name: private                           |
|              |   spoofing_protection: true               |
| orig_hostname | amigai-ac-ve0                            |
| placements   | []                                        |
| power_state  | SHUTDOWN                                  |
| project_id   | dfd99654b8c94b939b638f94abb2ad73          |
| status       | SHUTOFF                                   |
| task_state   |                                           |
| updated      | 2021-06-15T11:24:05Z                      |
| user_data    |                                           |
| vm_state     | stopped                                   |
| volumes      | - delete_on_termination: false            |
|              |   id: 49be1057-c026-494f-b85d-e013728d41bd |
|              | - delete_on_termination: false            |
|              |   id: eca9f679-7e35-4768-ad20-9bcb6af6fd59 |
+--------------+-------------------------------------------+
```

В выводе команды первый том — это загрузочный том.

3. Создайте копию загрузочного тома, указав имя нового тома. Например:

```
# vinfra service compute volume clone 49be1057-c026-494f-b85d-e013728d41bd \
--name cloned_volume
```

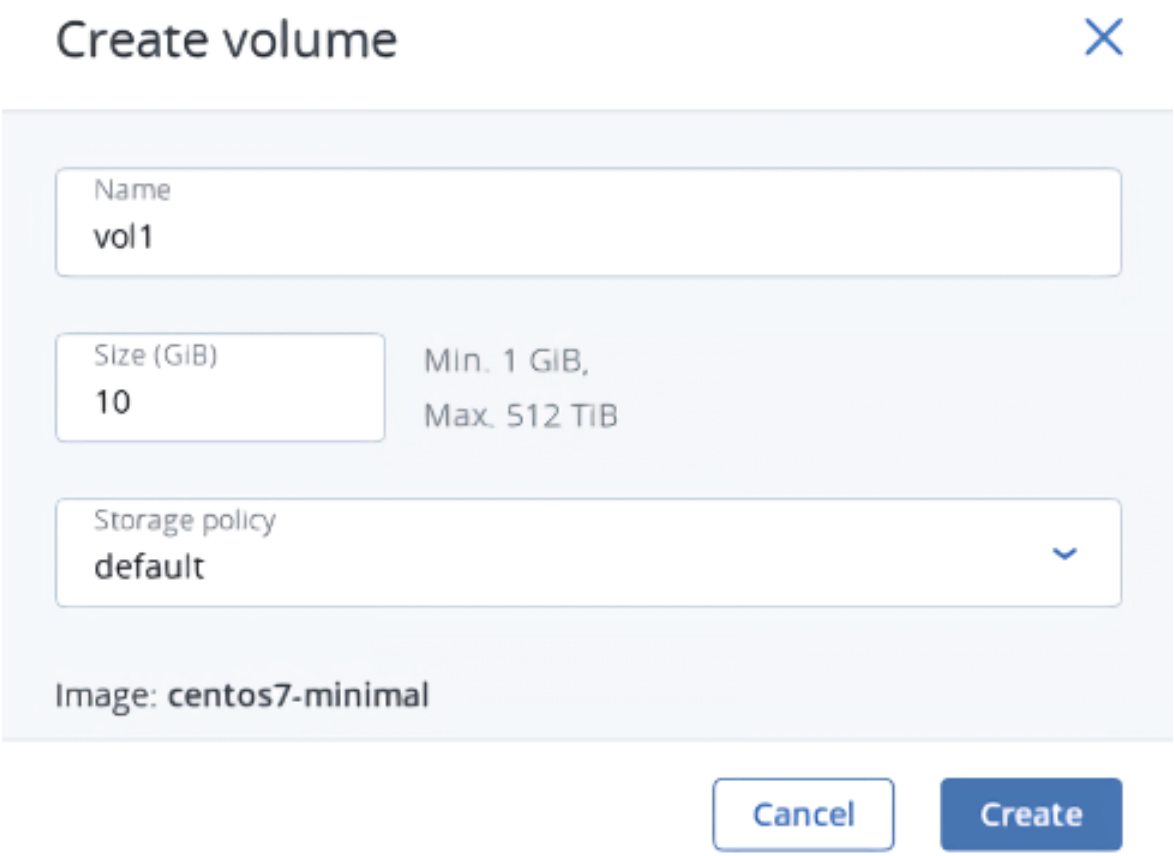
Копия загрузочного тома появится в выводе команды vinfra service compute volume list:

```
# vinfra service compute volume list
+-----------------+------------------------+------+-----------+--------------------------+
| id              | name                   | size | status    | os-vol-host-attr:host    |
+-----------------+------------------------+------+-----------+--------------------------+
| 14f4053e-cff5<…> | cloned_volume          | 1    | available | node003.vstoragedomain<…> |
| 504078c7-9035<…> | myvm/cirros/Boot volume | 1    | in-use    | node002.vstoragedomain<…> |
+-----------------+------------------------+------+-----------+--------------------------+
```

Чтобы создать загрузочный том на основе шаблона

Панель администратора

1. Перейдите на экран **Вычисления** > **Виртуальные машины** > **Образы** и нажмите на нужный образ.
2. На панели образа нажмите **Создать том**.
3. В окне **Создать том** укажите имя и размер тома и выберите политику хранилища.



4. Нажмите кнопку **Создать**.

Новый том появится на экране **Тома**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute volume create [--description <description>] [--image <image>]
                                     --storage-policy <storage_policy> --size <size-gb> <volume-name>
```

--description <description>

Описание тома

--image <image>

Идентификатор или имя исходного образа вычислений

--storage-policy <storage_policy>

Идентификатор или имя политики хранилища

--size <size-gb>

Размер тома в гигабайтах

<volume-name>

Имя тома

Например, чтобы создать том cirros_volume размером в 1 ГБ с политикой хранилища по умолчанию, использовав шаблон cirros, выполните:

```
# vinfra service compute volume create cirros_volume --image cirros --storage-policy default --size 1
```

Новый том появится в выводе команды vinfra service compute volume list:

```
# vinfra service compute volume list
+------------------+-------------------------+------+-----------+--------------------------+
| id               | name                    | size | status    | os-vol-host-attr:host    |
+------------------+-------------------------+------+-----------+--------------------------+
| 232d09db-bc75<…> | cirros_volume           | 1    | available | node003.vstoragedomain<…> |
| 14f4053e-cff5<…> | cloned_volume           | 1    | available | node003.vstoragedomain<…> |
| 504078c7-9035<…> | myvm/cirros/Boot volume | 1    | in-use    | node002.vstoragedomain<…> |
+------------------+-------------------------+------+-----------+--------------------------+
```

7.6.2.3 Создание пользовательских типов виртуальных машин

Тип ВМ в вычислительном кластере представляет собой шаблон конфигурации для виртуальных машин. Типы ВМ упрощают развертывание виртуальных машин. Они позволяют задать количество виртуальных ядер ЦП и объем ОЗУ, которые будут использоваться виртуальной машиной. По умолчанию создаются пять стандартных типов ВМ со следующими параметрами:

Имя	Виртуальные ЦП	Память
tiny	1	512 МиБ
small	1	2 ГиБ
medium	2	4 ГиБ
large	4	8 ГиБ
xlarge	8	16 ГиБ

Можно создавать пользовательские типы ВМ с разным количеством виртуальных ядер ЦП и объемом ОЗУ: общие типы ВМ (по умолчанию), доступные для всех проектов, и частные типы ВМ, доступные только для отдельных проектов. Кроме того, можно удалять существующие типы ВМ, включая созданные по умолчанию.

Предварительные условия

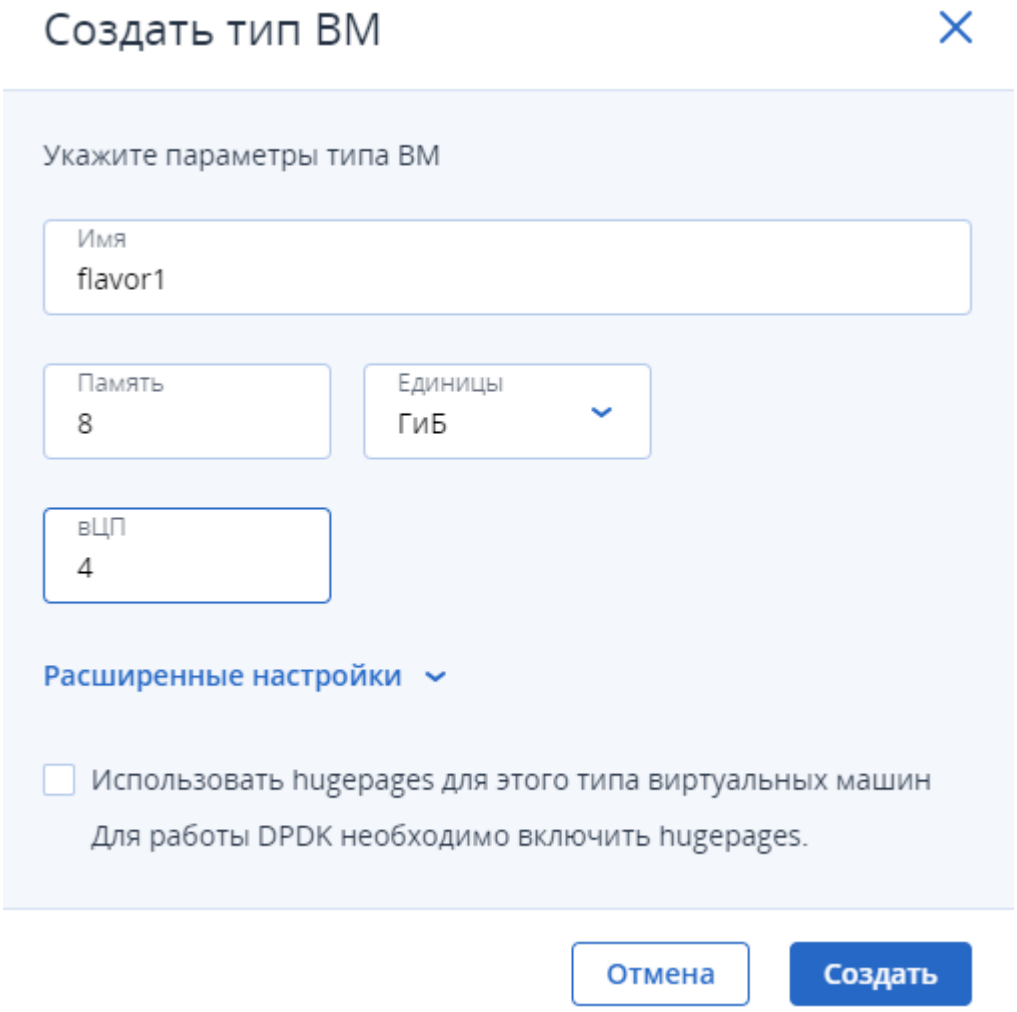
- Для авторизации выполнения приведенных ниже команд настроен клиент командной строки OpenStack, как описано в разделе "Подключение к интерфейсу командной строки OpenStack" на

странице 427.

Чтобы создать общий тип ВМ

Панель администратора

1. На экране **Вычисления** > **Виртуальные машины** > **Типы ВМ** нажмите **Создать тип ВМ**.
2. В окне **Создать тип ВМ** укажите имя типа ВМ, количество виртуальных ядер ЦП и объем ОЗУ.



3. Если планируется подключать ВМ этого типа к быстрой сети DPDK, включите поддержку больших страниц, установив флажок **Использовать hugepages для этого типа виртуальных машин** в области **Расширенные настройки**.
4. Нажмите кнопку **Создать**.

Созданный тип ВМ будет доступен для всех проектов.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute flavor create [--swap <size-mb>]
                                     --vcpus <vcpus>
                                     --ram <size-mb>
                                     [--huge-pages <huge_pages>]
                                     <flavor-name>
```

--swap <size-mb>

Размер пространства подкачки в мегабайтах.

--vcpus <vcpus>

Количество виртуальных ЦП.

--ram <size-mb>

Размер памяти в мегабайтах.

--huge-pages <huge_pages>

Поддержка больших страниц (true – включена или false – выключена). Должна быть включена, если планируется подключать ВМ этого типа к быстрой сети DPDK. Выключена по умолчанию.

<flavor-name>

Имя типа ВМ.

Например, чтобы создать тип ВМ с именем myflavor, одним виртуальным ядром ЦП и 3 ГБ ОЗУ, выполните:

```
# vinfra service compute flavor create myflavor --vcpus 1 --ram 3072
```

Новый тип ВМ появится в выводе команды vinfra service compute flavor list:

```
# vinfra service compute flavor list
+--------------------------------------+----------+-------+------+-------+
| id                                   | name     | ram   | swap | vcpus |
+--------------------------------------+----------+-------+------+-------+
| 100                                  | tiny     | 512   | 0    | 1     |
| 101                                  | small    | 2048  | 0    | 1     |
| 102                                  | medium   | 4096  | 0    | 2     |
| 103                                  | large    | 8192  | 0    | 4     |
| 104                                  | xlarge   | 16384 | 0    | 8     |
| 2e32ebd2-5d83-45fd-a526-3ae4a6658078 | myflavor | 3072  | 0    | 1     |
+--------------------------------------+----------+-------+------+-------+
```

Чтобы создать частный тип ВМ

1. Создайте тип ВМ, указав параметр --private. Например, чтобы создать тип ВМ private_tiny с одним виртуальным ядром ЦП, 512 МиБ ОЗУ и автоматически сгенерированным UUID, выполните:

   ```
   # openstack --insecure flavor create private_tiny --private --id auto --ram 512 --disk 0 --vcpus 1
   ```

2. Назначьте тип ВМ проекту. Например, чтобы назначить тип ВМ private_tiny проекту myproject домена mydomain, выполните:

```
# openstack --insecure flavor set private_tiny --project myproject --project-domain mydomain
```

Созданный тип ВМ будет доступен только для того проекта, которому он был назначен.

Чтобы просмотреть сведения о типе ВМ

Панель администратора

На экране **Вычисления** > **Виртуальные машины** > **Типы ВМ** выберите необходимый тип ВМ. На правой панели будут отображены сведения об этом типе.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute flavor show <flavor>
```

<flavor>

Идентификатор или имя типа ВМ

Например, чтобы вывести сведения о типе ВМ myflavor, выполните:

```
# vinfra service compute flavor show myflavor
+------------------+--------------------------------------+
| Field            | Value                                |
+------------------+--------------------------------------+
| Memory page size | small                                |
| id               | 561a48ea-0c1c-4152-8b7d-e4b4af276c2d |
| name             | myflavor                             |
| placements       | []                                   |
| ram              | 3072                                 |
| swap             | 0                                    |
| vcpus            | 1                                    |
+------------------+--------------------------------------+
```

Чтобы удалить тип ВМ

Панель администратора

1. На экране **Вычисления** > **Виртуальные машины** > **Типы ВМ** выберите тип ВМ, который необходимо удалить, и нажмите **Удалить**.
2. Нажмите **Удалить** в окне подтверждения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute flavor delete <flavor>
```

<flavor>

Идентификатор или имя типа ВМ

Например, чтобы удалить тип ВМ myflavor, выполните:

```
# vinfra service compute flavor delete myflavor
```

7.6.2.4 Добавление ключей SSH для виртуальных машин

SSH-ключи применяются для защищенного SSH-доступа к виртуальным машинам. Можно создать пару ключей на клиенте, с которого вы будете подключаться к виртуальным машинам через SSH. Закрытый ключ будет храниться на клиенте, и его можно будет скопировать на другие серверы. Открытый ключ необходимо будет загрузить в продукт Кибер Инфраструктура и указать при создании ВМ. Он внедряется в виртуальную машину посредством cloud-init и используется для аутентификации OpenSSH. Внедрение ключей поддерживается для виртуальных машин под управлением как Linux, так и Windows.

Ограничения

- SSH-ключ можно указать, только если ВМ развертывается из шаблона или загрузочного тома (не ISO-образа).
- Если ключ внедрен в одну или несколько ВМ, он останется в них даже после его удаления из панели.

Предварительные требования

- Утилита cloud-init и OpenSSH Server установлены на загрузочный том или в шаблон ВМ, как указано в разделе "Подготовка шаблонов" на странице 440.

Как добавить открытый ключ

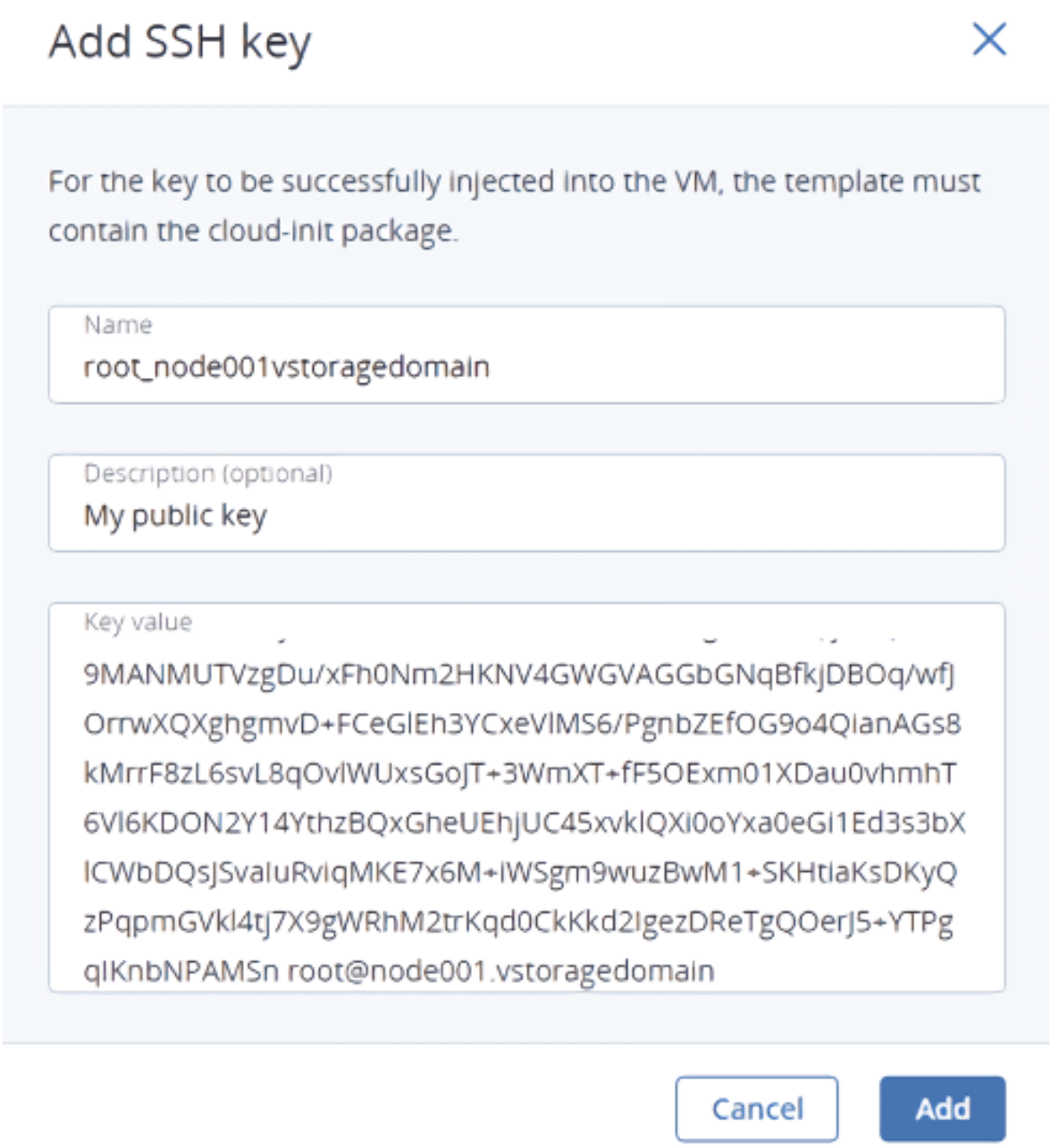
Панель администратора

1. Создайте пару SSH-ключей на клиенте с помощью утилиты ssh-keygen.

   ```
   # ssh-keygen -t rsa
   ```

2. На экране **Вычисления** > **Виртуальные машины** > **SSH-ключи** нажмите **Добавить ключ**.
3. В окне **Добавить SSH-ключ** укажите имя ключа и скопируйте значение из созданного открытого ключа, который находится в /root/.ssh/id_rsa.pub. При необходимости можно

добавить описание ключа.



Интерфейс командной строки

1. Создайте пару SSH-ключей на клиенте с помощью утилиты ssh-keygen.

   ```
   # ssh-keygen -t rsa
   ```

2. Загрузите открытый ключ в вычислительный кластер. Например, чтобы создать открытый SSH-ключ mykey, выполните:

   ```
   # vinfra service compute key create --public-key /root/.ssh/id_rsa.pub mykey
   ```

Новый SSH-ключ появится в выводе команды vinfra service compute key list:

```
# vinfra service compute key list
+-------+-------------+----------------------------------+
| name  | description | created_at                       |
+-------+-------------+----------------------------------+
| mykey |             | 2021-06-15T12:24:27.814043+00:00 |
+-------+-------------+----------------------------------+
```

Как просмотреть сведения об открытом ключе

Панель администратора

На экране **Вычисления** > **Виртуальные машины** > **SSH-ключи** щелкните по ключу, сведения о котором вы хотите просмотреть. На правой панели будут отображены его имя, описание, а также дата и время его создания.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute key show <ssh-key>
```

<ssh-key>

Имя SSH-ключа

Например, чтобы вывести сведения о SSH-ключе publickey, выполните:

```
# vinfra service compute key show publickey
+-----------------------+-------------------------------------------------+
| Field                 | Value                                           |
+-----------------------+-------------------------------------------------+
| created_at            | 2019-04-25T13:41:14.241736+00:00                |
| description           | public key                                      |
| name                  | publickey                                       |
| public_key_fingerprint | 1a:fb:de:d8:1e:0a:84:30:fc:ff:e4:fd:89:e7:96:a9 |
+-----------------------+-------------------------------------------------+
```

Как удалить открытый ключ

Панель администратора

1. На экране **Вычисления** > **Виртуальные машины** > **SSH-ключи** выберите SSH-ключ, который следует удалить, и нажмите **Удалить**.
2. В окне подтверждения нажмите **Удалить**.

Если SSH-ключ был внедрен в какие-либо виртуальные машины, он останется внутри них.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute key delete <ssh-key>
```

<ssh-key>

Имя SSH-ключа

Например, чтобы удалить SSH-ключ mykey, выполните:

```
# vinfra service compute key delete mykey
```

7.6.2.5 Создание виртуальных машин

Ограничения

- Виртуальные машины по умолчанию создаются с той же моделью ЦП, что и у хоста. Наличие вычислительных серверов с разными типами ЦП может привести к проблемам при динамической миграции. Чтобы избежать этого, можно вручную задать модель ЦП для всех новых ВМ, как описано в разделе "Настройка модели ЦП виртуальных машин" на странице 178. Либо можно создать размещение для каждой группы вычислительных серверов с одной моделью ЦП, следуя инструкциям в разделе "Управление размещениями для вычислительных узлов" на странице 643.

Предварительные требования

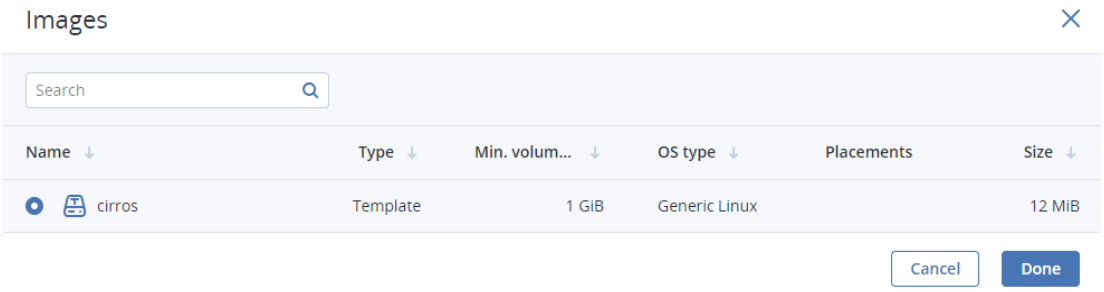
- Подготовлен источник гостевой ОС, как описано в разделе "Подготовка загрузочного носителя для виртуальных машин" на странице 437.
- Созданы одна или несколько вычислительных сетей автоматически в процессе развертывания вычислительного кластера или вручную с использованием инструкций из "Создание физических вычислительных сетей" на странице 532 и "Создание виртуальных вычислительных сетей" на странице 540.
- [Необязательно] Настроены пользовательские группы безопасности, как указано в разделе "Управление группами безопасности" на странице 550.
- [Необязательно] Создан пользовательский тип ВМ, как описано в разделе "Создание пользовательских типов виртуальных машин" на странице 453. Также можно использовать предварительно настроенные типы.
- [Необязательно] В вычислительный кластер добавлен SSH-ключ, как показано в разделе "Добавление ключей SSH для виртуальных машин" на странице 457. SSH-ключ можно указать только при создании ВМ из шаблона или загрузочного тома.
- [Необязательно] Для томов создана пользовательская политика хранилища, как описано в разделе "Управление политиками хранения" на странице 619.

Чтобы создать виртуальную машину

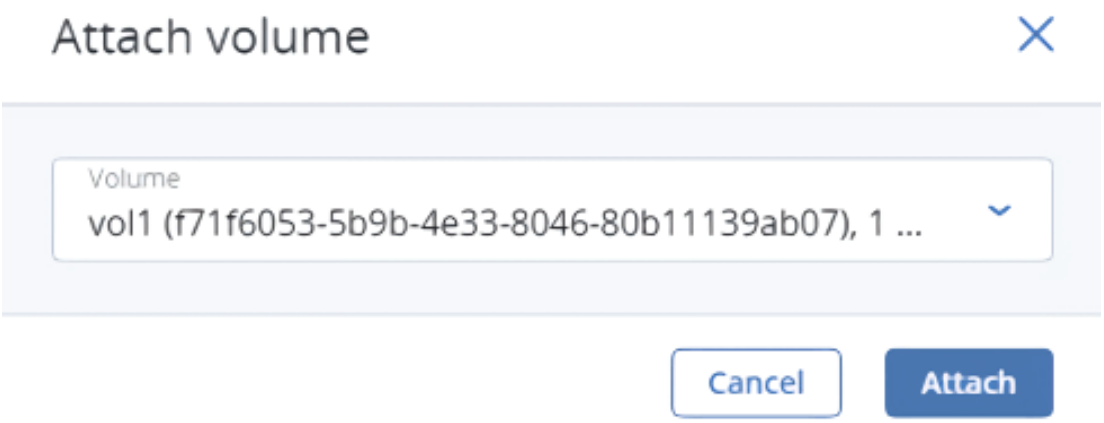
Панель администратора

1. На экране **Виртуальные машины** нажмите **Создать виртуальную машину**. Откроется окно, где нужно будет указать параметры ВМ.
2. Укажите имя новой ВМ.
3. Выберите загрузочный носитель ВМ.

- Если у вас есть ISO-образ или шаблон
  a. Выберите **Образ** в разделе **Развернуть из**, а затем нажмите **Указать** в разделе **Образ**.
  b. В окне **Образы** выберите ISO-образ или шаблон и нажмите **Готово**.



- Если у вас есть вычислительный загрузочный том
  a. Выберите **Том** в разделе **Развернуть из**, а затем нажмите **Указать** в разделе **Тома**.
  b. В окне **Тома** нажмите **Присоединить**.
  c. В окне **Присоединить том** найдите и выберите том и нажмите **Присоединить**.



Если вы присоединяете более одного тома, то первый присоединенный том становится загрузочным по умолчанию. Чтобы выбрать другой том в качестве загрузочного, сделайте его первым в списке, нажимая кнопку со стрелкой вверх.

Примечание
Если выбрать образ или том с назначенным размещением, то созданная ВМ унаследует это размещение.

После выбора загрузочного носителя необходимые для загрузки тома будут автоматически добавлены в раздел **Тома**.

4. Настройте диски ВМ.
   a. В окне **Тома** убедитесь, что загрузочный том по умолчанию достаточно большой для размещения гостевой ОС. В противном случае нажмите значок с многоточием и выберите

Изменить. Измените размер тома и нажмите **Сохранить**.

b. [Необязательно] Добавьте дополнительные диски в ВМ путем создания или присоединения томов. Для этого щелкните по значку карандаша в разделе **Тома**, а затем нажмите **Добавить** или **Присоединить** в окне **Тома**.

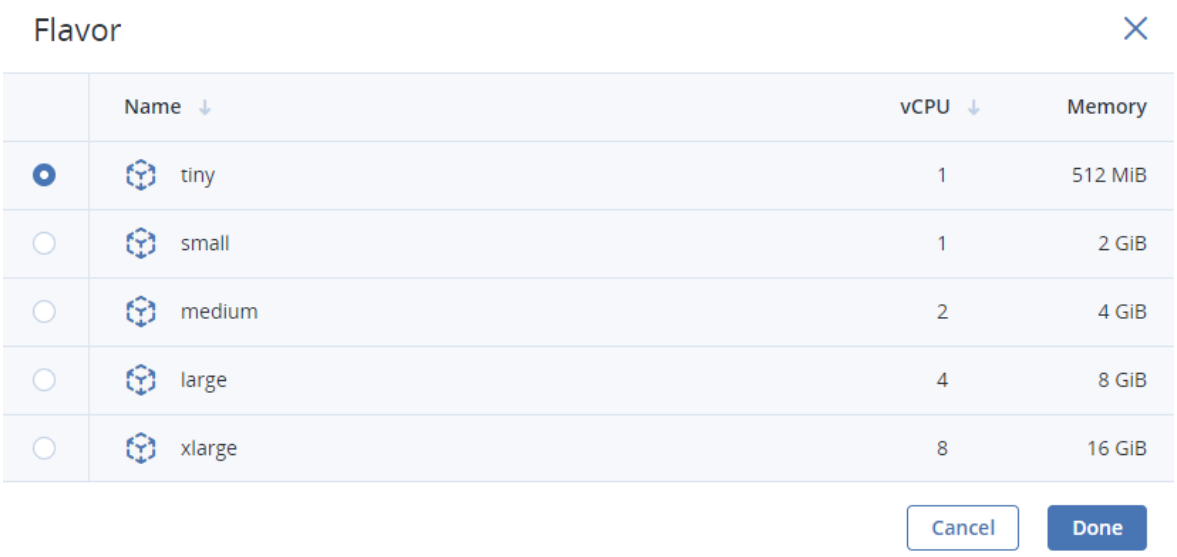
c. Выберите тома, которые будут удалены при удалении ВМ. Для этого щелкните по значку карандаша в разделе **Тома**, нажмите значок с многоточием напротив нужного тома и выберите **Изменить**. Включите параметр **Удалить по завершении** и нажмите **Сохранить**.

d. Завершив настройку дисков ВМ, нажмите **Готово**.

5. Выберите объем ОЗУ и ресурсов ЦП, которые будут выделены ВМ, в разделе **Тип ВМ**. В окне **Тип ВМ** выберите тип и нажмите **Готово**.

Внимание
При выборе типа для ВМ убедитесь, что он удовлетворяет требованиям к оборудованию гостевой ОС.

Примечание
Если выбрать тип ВМ с назначенным размещением, то созданная ВМ унаследует это размещение.



6. Добавьте сетевые интерфейсы для ВМ в разделе **Сети**.

a. В окне **Сетевые интерфейсы** нажмите **Добавить**, чтобы присоединить сетевой интерфейс.

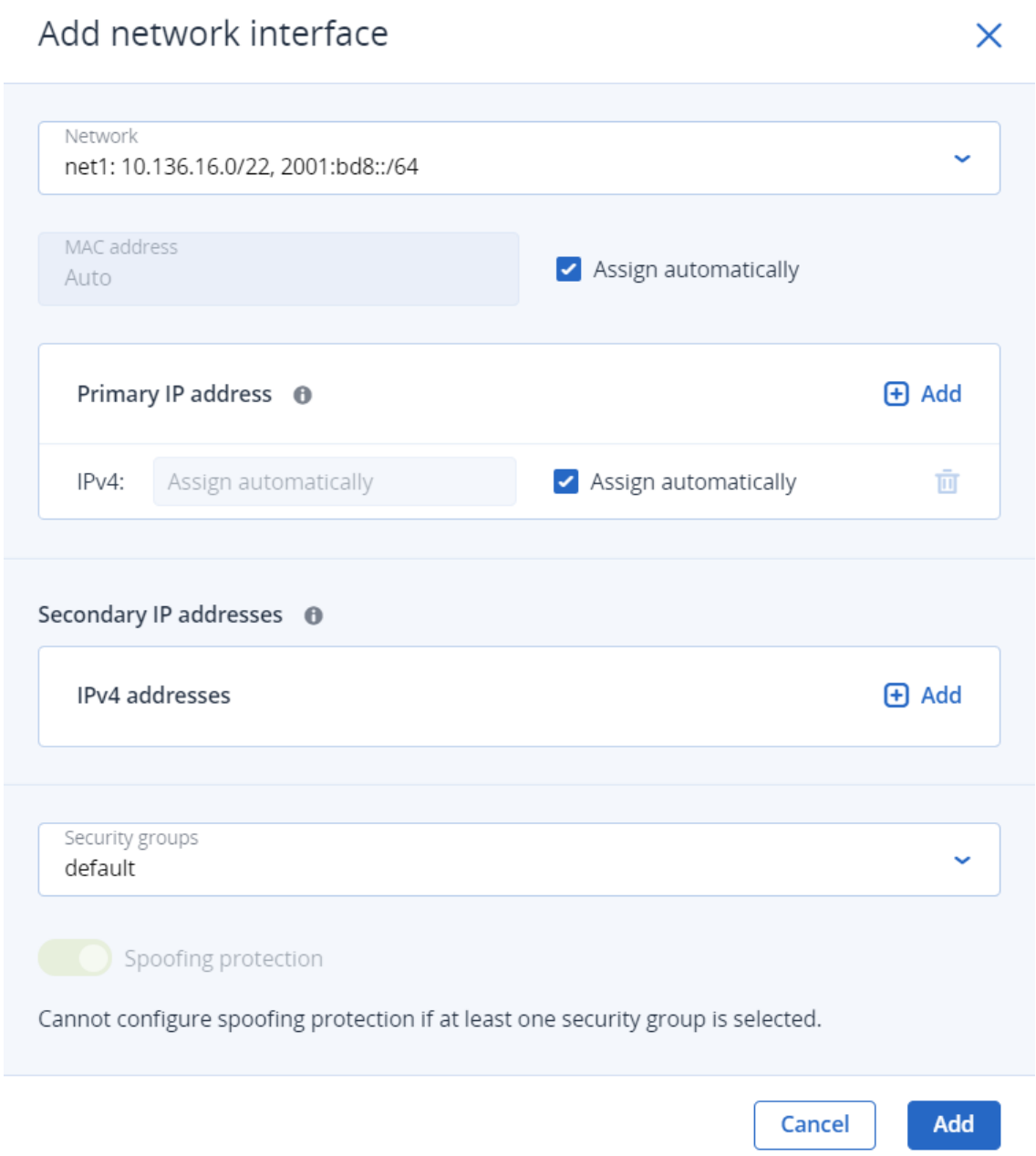
b. В окне **Добавить сетевой интерфейс** выберите вычислительную сеть, к которой следует подключиться, и укажите MAC-адрес, адреса IPv4 и/или IPv6 и группы безопасности. По умолчанию MAC-адрес и основной IP-адрес назначаются автоматически. Чтобы указать их вручную, снимите флажки **Назначить автоматически** и введите нужные адреса. При необходимости можно назначить сетевому интерфейсу дополнительные IP-адреса в разделе **Вторичные IP-адреса**. Учтите, что вторичный адрес IPv6 недоступен для подсети

IPv6, которая работает в режиме SLAAC или DHCPv6 без отслеживания состояния.

Примечание
Вторичные IP-адреса, в отличие от основного, не будут автоматически назначены сетевому интерфейсу внутри гостевой ОС виртуальной машины. Их следует назначать вручную.

- Если выбрана виртуальная сеть со включенным управлением IP-адресами
  В этом случае по умолчанию будет включена защита от спуфинга и выбрана группа безопасности **default**. Эта группа безопасности разрешает весь входящий и исходящий трафик на всех портах ВМ. При необходимости можно выбрать другую группу безопасности или несколько групп.

  Чтобы отключить защиту от спуфинга, снимите все флажки и установите переключатель в положение «выкл». С отключенной защитой от спуфинга нельзя настроить группы безопасности.
- Если выбрана виртуальная сеть с отключенным управлением IP-адресами
  В этом случае защита от спуфинга отключена по умолчанию и ее нельзя включить. Для такой сети нельзя настроить группы безопасности.



Указав параметры сетевого интерфейса, нажмите **Добавить**. Интерфейс появится в списке **Сетевые интерфейсы**.

c. [Необязательно] При необходимости измените IP-адреса и группы безопасности добавленных сетевых интерфейсов. Для этого щелкните по значку с многоточием, выберите **Изменить** и задайте нужные параметры.

d. Завершив настройку сетевых интерфейсов ВМ, нажмите **Готово**.

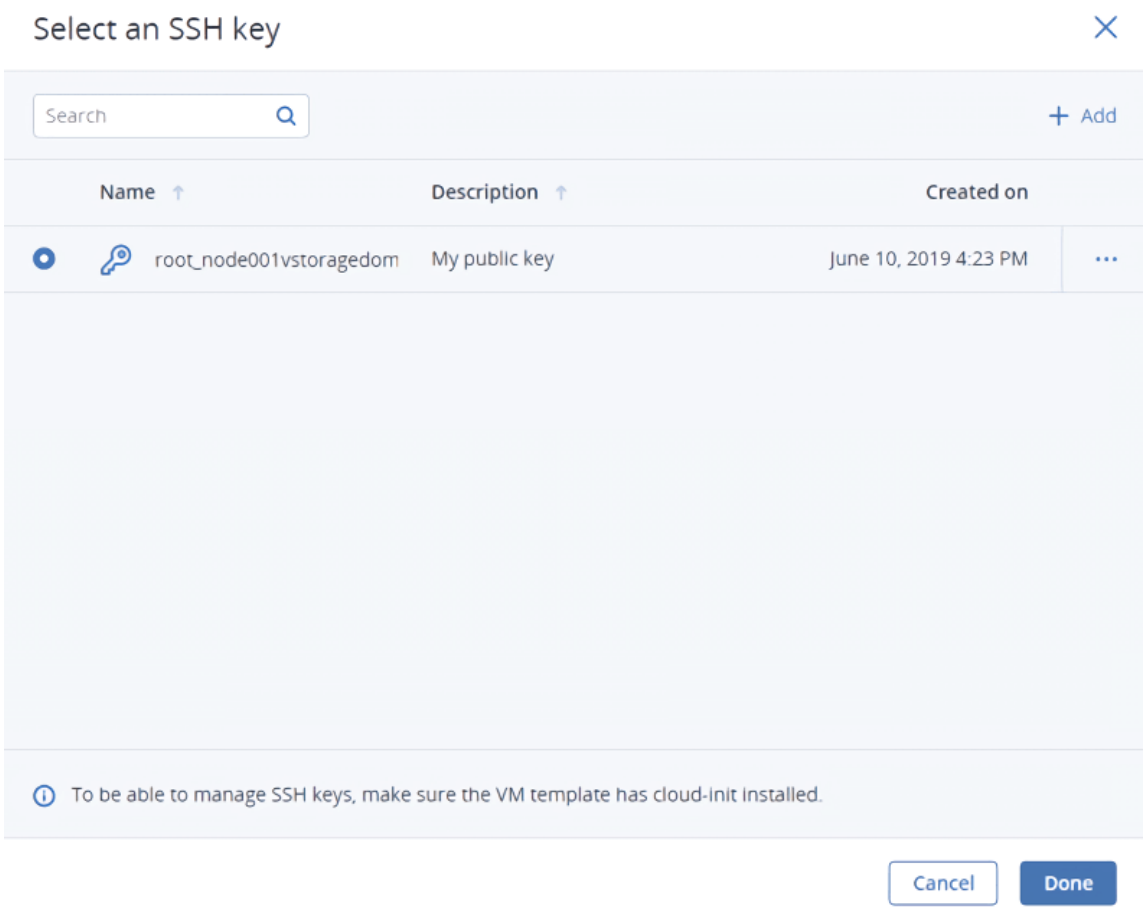
Примечание

Включите EUI-64 в сетевых настройках ВМ для корректного назначения IP-адреса.

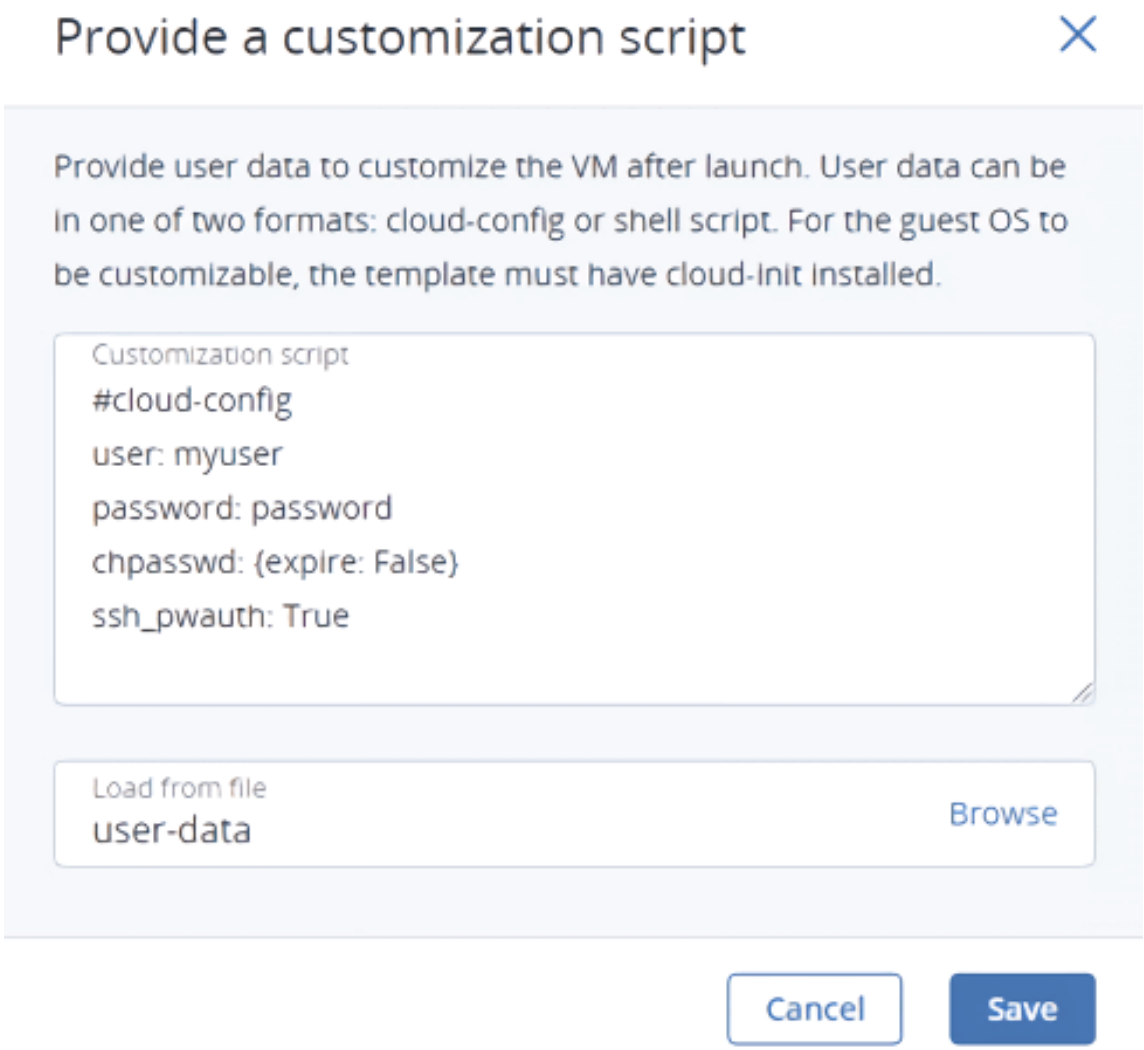
7. [Необязательно] Если вы выбрали загрузку из шаблона или тома, на котором установлены cloud-init и OpenSSH:

Внимание
Поскольку у облачных образов нет пароля по умолчанию, доступ к ВМ, развернутым из этих образов, можно получить только с помощью метода аутентификации с ключом SSH.

- Добавьте SSH-ключ в ВМ, чтобы она была доступна через SSH без пароля.
  В окне **Выберите SSH-ключ** выберите ключ и нажмите **Готово**.



- Добавьте пользовательские данные для настройки ВМ после запуска, например, для изменения пароля пользователя.
  Введите скрипт cloud-config или скрипт оболочки в поле **Скрипт настройки** или укажите файл на локальном сервере, из которого следует загрузить скрипт.



Чтобы внедрить скрипт в виртуальную машину Windows, см. документацию по Cloudbase-Init. Например, можно задать новый пароль для учетной записи с помощью следующего скрипта:

```
#ps1
net user <username> <new_password>
```

8. [Необязательно] В разделе **Расширенные параметры** выполните следующее:
   - Разрешите горячее подключение ресурсов ЦП и ОЗУ для ВМ, чтобы можно было изменить тип работающей ВМ. Горячее подключение также можно разрешить после создания ВМ.
   - Запретите автоматические перемещения ВМ, связанные с работой DRS, сняв установленный по умолчанию флажок **Разрешить автоматические миграции для этой виртуальной машины**. Снять флажок также можно после создания ВМ.
9. Настроив все параметры ВМ, нажмите **Развернуть**, чтобы создать и загрузить ВМ.

Если вы развертываете ВМ из ISO-образа, потребуется установить гостевую ОС внутри ВМ с помощью встроенной консоли VNC. Виртуальные машины, созданные из шаблона или загрузочного тома, уже имеют предустановленную гостевую ОС.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server create [--description <description>]
                                     [--metadata <metadata>]
                                     [--user-data <user-data>]
                                     [--key-name <key-name>]
                                     [--config-drive] [--count <count>]
                                     [--ha-enabled {true,false}]
                                     [--placements <placements>]
                                     [--allow-live-resize]
                                     [--allow-auto-migration <allow_auto_migration>]
                                     --network id|<id=id[,key=value,...]>
                                     --volume <source=source[,key=value,...]>
                                     --flavor <flavor> <server-name>
```

--description <description>

Описание виртуальной машины.

--metadata <metadata>

Метаданные виртуальной машины.

--user-data <user-data>

Файл пользовательских данных.

--key-name <key-name>

Пара ключей для внедрения.

--config-drive

Использовать временный (эфемерный) диск.

--count <count>

Если указано число и оно больше 1, то аргумент имя рассматривается как шаблон присвоения имен.

--ha-enabled {true,false}

Включение или отключение высокой доступности для виртуальной машины.

--placements <placements>

Имена или идентификаторы размещений, в которые следует добавить виртуальную машину.

--allow-live-resize

Разрешает изменение размера виртуальной машины в онлайн-режиме.

--allow-auto-migration <allow_auto_migration>

Разрешает или запрещает автоматические перемещения ВМ, связанные с работой DRS (true — разрешить или false — запретить).

--network id|<id=id[,key=value,...]>

Создает виртуальную машину с заданной сетью. Укажите этот параметр несколько раз, чтобы создать несколько сетей.

- id: присоединить сетевой интерфейс к указанной (по идентификатору или имени) сети
- разделенные запятыми пары key=value с ключами (необязательно):
  - mac: MAC-адрес для сетевого интерфейса
  - fixed-ip: фиксированный IP-адрес или None для автоматического выделения IP-адреса. Этот параметр можно использовать несколько раз.
  - spoofing-protection-enable:: включение защиты от спуфинга пакетов на сетевом интерфейсе
  - spoofing-protection-disable:: отключение защиты от спуфинга пакетов на сетевом интерфейсе
  - security-group: имя или идентификатор группы безопасности. Этот параметр можно использовать несколько раз.
  - no-security-group: не использовать группу безопасности

--volume <source=source[,key=value,...]>

Создает виртуальную машину с заданным томом. Укажите этот параметр несколько раз, чтобы создать несколько томов.

- source: тип источника (volume для тома, image для образа, snapshot для снимка или blank — пустой)
- разделенные запятыми пары key=value с ключами (необязательно):
  - id: идентификатор или имя ресурса для указанного типа источника (требуется для источников типа volume — том, image — образ и snapshot — снимок)
  - size: размер блочного устройства в гигабайтах (требуется для источников типа image — образ и blank — пустой)
  - boot-index: загрузочный индекс блочного устройства (требуется при наличии нескольких томов с типом источника volume)
  - bus: тип контроллера блочного устройства (scsi)
  - type: тип блочного устройства (disk или cdrom)
  - rm: удалить блочное устройство по завершении работы виртуальной машины (yes или no)
  - storage-policy: политика хранилища блочного устройства

--flavor <flavor>

Идентификатор или имя типа ВМ.

<server-name>

Имя для виртуальной машины.

Например, чтобы создать виртуальную машину myvm, основанную на образа cirros и типе BM tiny, и подключить ее к виртуальной сети private с фиксированным IP-адресом192.168.128.100, выполните:

```
# vinfra service compute server create myvm --network id=private,fixed-ip=192.168.128.100 \
--volume source=image,id=cirros,size=1 --flavor tiny
+-------------+----------------------------------------------+
| Field             | Value                                    |
+-------------+----------------------------------------------+
| allow_auto_migration | True                                  |
| config_drive       |                                        |
| created            | 2019-05-29T11:24:04Z                   |
| description        |                                        |
| flavor             | disk: 0                                |
|                    | ephemeral: 0                           |
|                    | extra_specs: {}                        |
|                    | original_name: tiny                    |
|                    | ram: 512                               |
|                    | swap: 0                                |
|                    | vcpus: 1                               |
| ha_enabled         | True                                   |
| host               |                                        |
| id                 | 8cd29296-8bee-4efb-828d-0e522d816c6e |
| key_name           |                                        |
| metadata           | {}                                     |
| name               | myvm                                   |
| networks           | []                                     |
| power_state        | NOSTATE                                |
| project_id         | b4267de6fd0c442da99542cd20f5932c     |
| status             | BUILD                                  |
| task_state         | scheduling                             |
| updated            | 2019-05-29T11:24:21Z                   |
| user_data          |                                        |
| vm_state           | building                               |
| volumes            | []                                     |
+-------------+----------------------------------------------+
```

Новая виртуальная машина появится в выводе команды vinfra service compute server list:

```
# vinfra service compute server list
+--------------------------------------+------+--------+-------------------------+
| id                                   | name | status | host                    |
+--------------------------------------+------+--------+-------------------------+
| 8cd29296-8bee-4efb-828d-0e522d816c6e | myvm | BUILD  | node002.vstoragedomain |
+--------------------------------------+------+--------+-------------------------+
```

7.6.2.6 Подключение к виртуальным машинам

Предварительные требования

- Созданы виртуальные машины, как описано в разделе "Создание виртуальных машин" на странице 460.
- Чтобы к виртуальной машине можно было подключиться через SSH, в ней должны быть установлены cloud-init и OpenSSH.

Чтобы подключиться к виртуальной машине через консоль VNC

Выберите ВМ и нажмите **Консоль** на ее правой панели. Консоль откроется в новом окне браузера. В консоли можно отправить сочетание клавиш на ВМ, создать снимок экрана окна консоли или скачать файл журнала консоли (см. раздел "Поиск и устранение неисправностей виртуальных машин" на странице 527) .

Чтобы подключиться к виртуальной машине через SSH

Укажите имя пользователя и IP-адрес ВМ в терминале SSH.

```
# ssh <username>@<VM_IP_address>
```

Облачные образы Linux имеют имя входа по умолчанию в зависимости от операционной системы, например centos или ubuntu. Чтобы подключиться к ВМ Windows, введите имя пользователя, указанное вами при установке Cloudbase-Init.

Если развертывание ВМ выполнено без указания SSH-ключа, необходимо также ввести пароль для входа в ВМ.

7.6.2.7 Управление дополнениями гостевой ОС

В этом разделе описывается, как установить и удалить дополнения гостевой ОС.

Дополнения гостевых ОС обеспечивают следующие возможности:

- Выполнение команд внутри ВМ с помощью virsh x-exec. См. пример использования в разделе "Выполнение команд в виртуальных машинах без сетевого подключения" на странице 511.
- Автоматический вызов fstrim -a внутри ВМ для освобождения не используемых файловыми системами блоков дисков.
- Поддержка технологии Memory Ballooning, которая позволяет перераспределять ОЗУ сервера между работающими виртуальными машинами.
- Создание согласованных моментальных снимков дисков работающей ВМ.

Ограничения

- Дополнения гостевой ОС зависят от гостевого агента QEMU, который устанавливается вместе с ними. Для работы дополнений должна быть запущена служба агента.

Предварительные требования

- Созданы виртуальные машины, как описано в разделе "Создание виртуальных машин" на странице 460.
- В виртуальной машине установлена гостевая операционная система.

Установка дополнений гостевой ОС

Установка дополнений гостевой ОС в виртуальную машину включает шаги, выполняемые пользователями с разными ролями: системный администратор и пользователь ВМ.

Примечание
Виртуальная машина должна иметь доступ к Интернету.

В роли системного администратора

Загрузите ISO-файлы с дополнениями гостевой ОС, расположенные в каталоге /usr/share/vz-guest-tools/ на любом вычислительном узле, в вычислительный кластер:

- для гостевой ОС Windows загрузите vz-guest-tools-win.iso, выполнив следующую команду:

  ```
  # vinfra service compute image create vz-guest-tools-win --file /usr/share/vz-guest-tools/vz-guest-tools-win.iso --public
  ```

- для гостевой ОС Linux загрузите vz-guest-tools-lin.iso, выполнив следующую команду:

  ```
  # vinfra service compute image create vz-guest-tools-lin --file /usr/share/vz-guest-tools/vz-guest-tools-lin.iso --public
  ```

В роли пользователя виртуальной машины

Панель администратора

1. Создайте вычислительный том из образа **vz-guest-tools-win** или **vz-guest-tools-lin** в зависимости от операционной системы ВМ.

   Примечание
   Если в вашем проекте нет этих образов, обратитесь к системному администратору.

   a. Перейдите на **Вычисления** > **Виртуальные машины** > вкладка **Образы** и нажмите на образ **vz-guest-tools-win** или **vz-guest-tools-lin**.
   b. На правой панели образа нажмите **Создать том**.
   c. В окне **Создать том из образа** укажите имя для тома и нажмите **Создать**.
2. Присоедините том с дополнениями гостевой ОС к виртуальной машине.
   a. Перейдите на **Вычисления** > **Виртуальные машины** > вкладка **Виртуальные машины** и щелкните по нужной ВМ.
   b. На правой панели ВМ нажмите значок карандаша в поле **Тома**.
   c. В окне **Тома** нажмите **Присоединить**.
   d. В окне **Присоединить том** выберите созданный том с дополнениями гостевой ОС и нажмите **Присоединить**. Присоединенный том будет помечен как ISO.
   e. В окне **Тома** нажмите **Готово**, чтобы сохранить изменения.

3. Выполните вход в виртуальную машину.
4. Внутри ВМ выполните следующие действия.
   - Внутри ВМ Windows перейдите на подключенный оптический диск в проводнике и установите дополнения гостевой ОС, запустив файл setup.exe. После завершения установки перезапустите ВМ.
   - Внутри ВМ Linux установите пакет с заголовками или исходными кодами ядра. Версия пакета должна соответствовать версии ядра.

     Затем создайте точку подключения для оптического диска с образом дополнений гостевой ОС и запустите установщик.

     ```
     # mkdir /mnt/cdrom
     # mount <path_to_guest_tools_iso> /mnt/cdrom
     # bash /mnt/cdrom/install
     ```

Интерфейс командной строки

1. Создайте вычислительный том из образа **vz-guest-tools-win** или **vz-guest-tools-lin** в зависимости от операционной системы ВМ. Например:

   ```
   # vinfra service compute volume create guest-tools-lin --image vz-guest-tools-lin \
   --storage-policy default --size 1
   ```

2. Присоедините том с дополнениями гостевой ОС к виртуальной машине. Например:

   ```
   # vinfra service compute server volume attach guest-tools-lin --server centos7
   +--------+--------------------------------------+
   | Field  | Value                                |
   +--------+--------------------------------------+
   | device | /dev/sda                             |
   | id     | 132908e4-3543-419f-a4bf-c219f74e2640 |
   +--------+--------------------------------------+
   ```

3. Выполните вход в виртуальную машину.
4. Внутри ВМ выполните следующие действия:
   - Внутри ВМ Windows перейдите на подключенный оптический диск в проводнике и установите дополнения гостевой ОС, запустив файл setup.exe. После завершения установки перезапустите ВМ.
   - Внутри ВМ Linux установите пакет с заголовками или исходными кодами ядра. Версия пакета должна соответствовать версии ядра.

     Затем создайте точку подключения для оптического диска с образом дополнений гостевой ОС и запустите установщик.

     ```
     # mkdir /mnt/cdrom
     # mount <path_to_guest_tools_iso> /mnt/cdrom
     # bash /mnt/cdrom/install
     ```

Удаление дополнений гостевой ОС

Если окажется, что дополнения гостевой ОС несовместимы с каким-либо ПО внутри виртуальной машины, их можно удалить.

Предварительные требования

- Внутри виртуальной машины должны быть установлены дополнения гостевой ОС, как описано в разделе "Установка дополнений гостевой ОС" на странице 471.

Чтобы удалить дополнения гостевой ОС

- Внутри ВМ Windows:
  1. Удалите драйверы устройств QEMU из диспетчера устройств.

     Внимание
     Не удаляйте драйвер жесткого диска VirtIO/SCSI и сетевой драйвер NetKVM. Без первого драйвера ВМ не будет загружаться, а без второго потеряет возможность подключения к сети.

  2. Удалите гостевой агент QEMU и дополнения гостевой ОС из списка установленных приложений.
  3. Остановите и удалите **Guest Tools Monitor**.

     ```
     > sc stop VzGuestToolsMonitor
     > sc delete VzGuestToolsMonitor
     ```

  4. Отмените регистрацию **Guest Tools Monitor** в **журнале событий**.

     ```
     > reg delete HKLM\SYSTEM\CurrentControlSet\services\eventlog\Application\\
     VzGuestToolsMonitor
     ```

  5. Удалите раздел реестра для автозапуска **RebootNotifier**.

     ```
     > reg delete HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v \
     VzRebootNotifier
     ```

  6. Удалите папку C:\Program Files\Qemu-ga\.

     Если файл VzGuestToolsMonitor.exe заблокирован, закройте все окна средства просмотра событий. Если файл остается заблокированным, перезапустите службу eventlog.

     ```
     > sc stop eventlog
     > sc start eventlog
     ```

  После удаления дополнений гостевой ОС перезапустите виртуальную машину.
- Внутри ВМ Linux:

1. Удалите пакеты.
   - В системах на базе RPM (CentOS и др.):

     ```
     # yum remove dkms-vzvirtio_balloon prl_nettool qemu-guest-agent-vz \
     vz-guest-udev
     ```

   - В системах на базе DEB (Debian и Ubuntu):

     ```
     # apt-get remove vzvirtio-balloon-dkms prl-nettool qemu-guest-agent-vz \
     vz-guest-udev
     ```

     Если какие-либо из перечисленных выше пакетов не установлены в системе, выполнение команды завершится ошибкой. В этом случае исключите эти пакеты из команды и выполните ее снова.
2. Удалите файлы.

   ```
   # rm -f /usr/bin/prl_backup /usr/share/qemu-ga/VERSION \
   /usr/bin/install-tools \
   /etc/udev/rules.d/90-guest_iso.rules /usr/local/bin/fstrim-static \
   /etc/cron.weekly/fstrim
   ```

3. Перезагрузите правила udev.

   ```
   # udevadm control --reload
   ```

После удаления дополнений гостевой ОС перезапустите виртуальную машину.

7.6.2.8 Управление состоянием активности виртуальных машин

Предварительные требования

- Созданы виртуальные машины, как описано в разделе "Создание виртуальных машин" на странице 460.

Как управлять состоянием активности виртуальной машины

Панель администратора

Щелкните по виртуальной машине или значку многоточия рядом с ней, чтобы открыть полный список действий, доступных для текущего состояния.

- Для запуска ВМ нажмите **Запустить**.
- Чтобы корректно завершить работу работающей виртуальной машины, нажмите кнопку **Выключить**. По умолчанию время ожидания остановки, после которого виртуальная машина будет выключена, составляет 10 минут. Вы можете настроить это время ожидания для каждой виртуальной машины с помощью команды vinfra service compute server stop --wait-time.
- Для принудительной остановки ВМ нажмите **Принудительно выключить**.
- Для мягкой перезагрузки работающей ВМ нажмите **Перезагрузить**.
- Для перезагрузки ВМ без штатной остановки гостевой ОС нажмите **Аппаратная перезагрузка**.

- Для сохранения текущего состояния ВМ в файл нажмите **Приостановить**. Это может пригодиться, например, если необходимо перезапустить хост без выхода из приложений, работающих на ВМ, и без перезапуска ее гостевой ОС.
- Для возвращения ВМ из состояния приостановки нажмите **Возобновить работу**.

Интерфейс командной строки

Используйте следующие команды:

- Для запуска виртуальной машины:

  ```
  vinfra service compute server start <server>
  ```

- Для корректного завершения работы виртуальной машины:

  ```
  vinfra service compute server stop <server> [--wait-time <seconds>]
  ```

  --wait-time <seconds>

  Время ожидания остановки, после которого виртуальная машина будет выключена. Укажите значение -1, чтобы задать неограниченное время ожидания.

- Для принудительной остановки работы виртуальной машины:

  ```
  vinfra service compute server stop <server> --hard
  ```

- Для мягкой перезагрузки виртуальной машины:

  ```
  vinfra service compute server reboot <server>
  ```

- Для перезагрузки виртуальной машины без штатной остановки гостевой ОС:

  ```
  vinfra service compute server reboot <server> --hard
  ```

- Для замораживания состояния виртуальной машины:

  ```
  vinfra service compute server suspend <server>
  ```

  Это может пригодиться, например, если необходимо перезапустить хост без выхода из приложений, работающих на ВМ, и без перезапуска ее гостевой ОС.

- Для возобновления работы виртуальной машины, состояние которой было заморожено:

  ```
  vinfra service compute server resume <server>
  ```

- Для приостановки виртуальной машины:

  ```
  vinfra service compute server pause <server>
  ```

- Для возобновления работы виртуальной машины после приостановки:

```
vinfra service compute server unpause <server>
```

7.6.2.9 Присоединение ISO-образов к виртуальным машинам

Можно присоединить ISO-образы к запущенным или остановленным виртуальным машинам, например, для установки на них дополнительного ПО или восстановления их операционной системы в аварийном режиме. Чтобы присоединить ISO-образ, необходимо преобразовать его в том, а затем присоединить этот том к ВМ.

После завершения установки с ISO-тома его можно отсоединить без предварительной остановки ВМ.

Как создать том из ISO-образа

Панель администратора

1. Перейдите на экран **Вычисления** > **Виртуальные машины** > **Образы** и щелкните по нужному ISO-образу.
2. На правой панели образа нажмите **Создать том**.
3. В окне **Создать том из образа** укажите имя для тома и нажмите **Создать**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute volume create [--description <description>] [--image <image>]
                                     --storage-policy <storage_policy> --size <size-gb> <volume-name>
```

--description <description>

Описание тома

--image <image>

Идентификатор или имя исходного образа

--storage-policy <storage_policy>

Идентификатор или имя политики хранилища

--size <size-gb>

Размер тома в гигабайтах

<volume-name>

Имя тома

Например, чтобы создать том guest-tools-lin размером 1 ГБ из образа guest-tools-lin-iso и задать для тома политику хранилища по умолчанию, выполните:

```
# vinfra service compute volume create guest-tools-lin --image guest-tools-lin-iso \
--storage-policy default --size 1
```

Новый том появится в выводе команды vinfra service compute volume list:

```
#  vinfra service compute volume list | grep guest-tools
| 132908e4-3543-419f-a4bf-c219f74e2640 | guest-tools-lin | 1    | available | node003.vstorage<…> |
```

Как присоединить ISO-том к виртуальной машине

Панель администратора

1. Перейдите на экран **Вычисления** > **Виртуальные машины** > **Виртуальные машины** и щелкните по нужной ВМ.
2. На вкладке **Сводка** нажмите значок карандаша в поле **Тома**.
3. В окне **Тома** нажмите **Присоединить**.
4. В окне **Присоединить том** выберите созданный том и нажмите **Присоединить**. Присоединенный том будет помечен как ISO.
5. В окне **Тома** нажмите **Готово**, чтобы сохранить изменения.

Присоединенный том появится внутри операционной системы ВМ.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server volume attach --server <server> <volume>
```

--server <server>

Идентификатор или имя виртуальной машины

<volume>

Идентификатор или имя тома

Например, чтобы присоединить том guest-tools-lin к ВМ centos7, выполните:

```
# vinfra service compute server volume attach guest-tools-lin --server centos7
+--------+--------------------------------------+
| Field  | Value                                |
+--------+--------------------------------------+
| device | /dev/sda                             |
| id     | 132908e4-3543-419f-a4bf-c219f74e2640 |
+--------+--------------------------------------+
```

Присоединенный том появится в выводе команды vinfra service compute server volume list:

```
# vinfra service compute server volume list --server centos7
+--------------------------------------+----------+
```

```
| id                                   | device   |
+--------------------------------------+----------+
| 1dc6750e-22ee-4fa5-8718-7cbcb7553c59 | /dev/vda |
| 132908e4-3543-419f-a4bf-c219f74e2640 | /dev/sda |
+--------------------------------------+----------+
```

Как отсоединить ISO-том от виртуальной машины

Панель администратора

1. Перейдите на экран **Вычисления** > **Виртуальные машины** > **Виртуальные машины** и щелкните по нужной ВМ.
2. На вкладке **Сводка** нажмите значок карандаша в поле **Тома**.
3. В окне **Тома** нажмите значок с многоточием напротив ISO-тома и выберите **Отсоединить принудительно**.
4. Нажмите **Готово**, чтобы сохранить изменения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server volume detach --server <server> <volume>
```

--server <server>

Идентификатор или имя виртуальной машины

<volume>

Идентификатор или имя тома

Например, чтобы отсоединить том guest-tools-lin от ВМ centos7, выполните:

```
# vinfra service compute server volume detach guest-tools-lin --server centos7
Operation successful.
```

7.6.2.10 Изменение конфигурации виртуальных машин

После создания виртуальной машины можно управлять ее ресурсами ЦП и ОЗУ, а также сетевыми интерфейсами и томами.

Предварительные требования

- Созданы виртуальные машины, как описано в разделе "Создание виртуальных машин" на странице 460.

Изменение ресурсов виртуальных машин

Можно изменить объем ресурсов ЦП и ОЗУ, используемых виртуальной машиной, применив к ней другой тип ВМ. Для изменения размера работающей ВМ необходимо сначала разрешить для нее

горячее подключение ЦП и ОЗУ. Настройки горячего подключения можно изменить как для новых, так и для существующих ВМ.

Запущенная виртуальная машина имеет лимит изменения размера, определяющий максимальное число виртуальных ЦП и максимальный объем ОЗУ, которые можно выделить этой ВМ. Лимит изменения размера для виртуальных ЦП является статическим и равен 64 для всех ВМ. Лимит изменения размера для ОЗУ, напротив, является динамическим и зависит от объема ОЗУ, который запущенная ВМ использует в настоящее время. Этот лимит обновляется при запуске ВМ, а его значения перечислены в таблице ниже.

Текущий размер ОЗУ в ГиБ	Ограничение размера ОЗУ в ГиБ
1-4	16
5-8	32
9-16	64
17-32	128
33-64	256
65-128	512
129-256	1024

Например, можно изменить размер запущенной ВМ, изменив тип ВМ с 16 ГиБ ОЗУ на тип ВМ с 256 ГиБ в два подхода.

1. Измените размер ВМ, установив тип ВМ с 64 ГиБ.
2. Выключите ВМ и запустите ее снова, чтобы обновить лимит изменения размера.
3. Измените размер ВМ, установив тип ВМ с 256 ГиБ.

Ограничения

- Нельзя изменить тип для ВМ с освобожденными ресурсами. Чтобы изменить размер такой ВМ, сначала назначьте ей ресурсы.
- Нельзя уменьшить число ЦП и объем ОЗУ для запущенных ВМ.
- [Для всех гостевых систем Linux] Если в ВМ не установлены дополнения гостевой ОС, новые ядра могут быть в состоянии офлайн после горячего подключения ЦП. Проверить, какие ядра ЦП находятся в состоянии онлайн, можно с помощью команды cat /sys/devices/system/cpu/online. Чтобы активировать ядра ЦП в состоянии офлайн, выполните команду echo 1 > /sys/devices/system/cpu/cpu<cpu_number>/online.

Предварительные требования

- Перед изменением типа ВМ убедитесь, что сервер, на котором размещена ВМ, имеет достаточно ресурсов ЦП и ОЗУ для нового размера ВМ.

- Перед изменением размера запущенной ВМ убедитесь, что гостевая операционная система поддерживает горячее подключение ЦП и ОЗУ (см. раздел "Поддерживаемые гостевые операционные системы" на странице 435). Учтите, что в противном случая после изменения размера гостевая ОС может работать нестабильно. Чтобы увеличить ресурсы ЦП и ОЗУ для такой гостевой ОС, необходимо сначала остановить виртуальную машину.
- Перед изменением размера запущенной ВМ убедитесь, что в гостевой операционной системе установлены последние обновления.

Как разрешить или запретить горячее подключение ЦП и ОЗУ для виртуальной машины

Панель администратора

1. Перейдите на экран **Вычисления** > **Виртуальные машины** > **Виртуальные машины** и убедитесь, что нужная виртуальная машина находится в состоянии «Выключена», а затем щелкните по ней.
2. На вкладке **Сводка** нажмите значок карандаша в поле **Горячее подключение ЦП и ОЗУ**.
3. Установите или снимите флажок **Разрешить горячее подключение**, а затем нажмите галочку, чтобы сохранить изменения.

Если горячее подключение ЦП и ОЗУ разрешено, можно изменять тип для работающей ВМ.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server set <server> {--allow-live-resize | --deny-live-resize}
```

--allow-live-resize

Разрешает изменение размера виртуальной машины в онлайн-режиме.

--deny-live-resize

Запрещает изменение размера виртуальной машины в онлайн-режиме.

<server>

Идентификатор или имя виртуальной машины.

Например, чтобы разрешить горячее подключение ЦП и ОЗУ для виртуальной машины myvm, выполните:

```
# vinfra service compute server set myvm --allow-live-resize
```

Как изменить тип виртуальной машины

Панель администратора

1. Перейдите на экран **Вычисления** > **Виртуальные машины** > **Виртуальные машины** и щелкните по нужной ВМ.
2. На вкладке **Сводка** щелкните по значку карандаша в поле **Тип ВМ**.
3. В окне **Тип ВМ** выберите новый тип ВМ и нажмите **Готово**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server resize --flavor <flavor> <server>
```

--flavor <flavor>

Применение типа с идентификатором или именем.

<server>

Идентификатор или имя виртуальной машины.

Например, чтобы изменить тип виртуальной машины myvm на small, выполните:

```
# vinfra service compute server resize myvm --flavor small
```

Настройка сетевых интерфейсов виртуальных машин

Можно добавить новые сетевые интерфейсы к виртуальным машинам, изменить IP-адреса и группы безопасности для существующих интерфейсов, а также удалить сетевые интерфейсы, отсоединив их.

Ограничения

- Нельзя управлять сетевыми интерфейсами ВМ с освобожденными ресурсами.
- ВМ, подключенная к сети с двойным стеком, всегда получает адрес IPv6, если подсеть IPv6 работает в режиме SLAAC или DHCPv6 без отслеживания состояния.

Чтобы присоединить сетевой интерфейс к виртуальной машине

Панель администратора

1. Перейдите на **Вычисления** > **Виртуальные машины** > экран **Виртуальные машины**. На экране **Виртуальные машины** щелкните по нужной ВМ.
2. На вкладке **Сводка** нажмите **Изменить** в разделе **Сетевые интерфейсы**.
3. В окне **Сетевые интерфейсы** нажмите **Добавить**, чтобы присоединить сетевой интерфейс.
4. В окне **Добавить сетевой интерфейс** выберите вычислительную сеть, к которой следует подключиться, и укажите MAC-адрес, адреса IPv4 и/или IPv6 и группы безопасности. По умолчанию MAC-адрес и основной IP-адрес назначаются автоматически. Чтобы указать их вручную, снимите флажки **Назначить автоматически** и введите нужные адреса. При необходимости можно назначить сетевому интерфейсу дополнительные IP-адреса в разделе **Вторичные IP-адреса**. Учтите, что вторичный адрес IPv6 недоступен для подсети IPv6, которая работает в режиме SLAAC или DHCPv6 без отслеживания состояния.

Примечание
Вторичные IP-адреса, в отличие от основного, не будут автоматически назначены сетевому интерфейсу внутри гостевой ОС виртуальной машины. Их следует назначать вручную.

- Если выбрана виртуальная сеть со включенным управлением IP-адресами
  В этом случае по умолчанию будет включена защита от спуфинга и выбрана группа безопасности **default**. Эта группа безопасности разрешает весь входящий и исходящий трафик на всех портах ВМ. При необходимости можно выбрать другую группу безопасности или несколько групп.

  Чтобы отключить защиту от спуфинга, снимите все флажки и установите переключатель в положение «выкл». С отключенной защитой от спуфинга нельзя настроить группы безопасности.
- Если выбрана виртуальная сеть с отключенным управлением IP-адресами
  В этом случае защита от спуфинга отключена по умолчанию и ее нельзя включить. Для такой сети нельзя настроить группы безопасности.

Указав параметры сетевого интерфейса, нажмите **Добавить**.

5. Нажмите **Готово**, чтобы завершить настройку сетевых интерфейсов ВМ и сохранить изменения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server iface attach [--fixed-ip <ip-address | ip-address=
                                    <ip-address>,subnet=<subnet> |
                                    ip-version=<ip-version>>]
                                    [--spoofing-protection-enable |
                                    --spoofing-protection-disable]
                                    [--security-group <security-group> |
                                    --no-security-groups]
                                    --server <server>
                                    --network <network> [--mac <mac>]
```

--fixed-ip <ip-address|ip-address=<ip-address>,subnet=<subnet>|ip-version=<ip-version>>

Нужный IP-адрес и/или подсеть. Этот параметр можно использовать несколько раз.

--spoofing-protection-enable

Включает защиту от спуфинга пакетов на сетевом интерфейсе

--spoofing-protection-disable

Выключает защиту от спуфинга пакетов на сетевом интерфейсе

--security-group <security-group>

Имя или идентификатор группы безопасности. Этот параметр можно использовать несколько раз.

--no-security-groups

Не устанавливать группы безопасности

--server <server>

Идентификатор или имя виртуальной машины

--network <network>

Идентификатор или имя сети

--mac <mac>

MAC-адрес

Например, чтобы присоединить виртуальную машину myvm к виртуальной сети myprivnet и назначить ей IP-адрес 192.168.129.8, выполните:

```
# vinfra service compute server iface attach --network myprivnet --fixed-ip 192.168.129.8 --server myvm
```

Созданный сетевой интерфейс появится в выводе команды vinfra service compute server iface list:

```
# vinfra service compute server iface list --server myvm
+---------------+---------------+-------------------+-----------------+
| id            | network_id    | mac_address       | fixed_ips       |
+---------------+---------------+-------------------+-----------------+
| 690ed3f2-<...> | 0710372e-<...> | fa:16:3e:54:59:08 | 192.168.129.8   |
| a5b13bf3-<...> | 1bf2c9da-<...> | fa:16:3e:b9:33:bb | 192.168.128.100 |
+---------------+---------------+-------------------+-----------------+
```

Чтобы изменить сетевой интерфейс виртуальной машины

Панель администратора

1. Перейдите на **Вычисления** > **Виртуальные машины** > экран **Виртуальные машины**. На экране **Виртуальные машины** щелкните по нужной ВМ.
2. На вкладке **Сводка** нажмите **Изменить** в разделе **Сетевые интерфейсы**.
3. В окне **Сетевые интерфейсы** нажмите кнопку с многоточием напротив нужного сетевого интерфейса и выберите **Изменить**.
4. В окне **Изменить сетевой интерфейс** измените параметры сетевого интерфейса следующим образом:
   - Измените основной IP-адрес. Чтобы обновить адрес внутри гостевой ОС виртуальной машины, перезапустите сетевой интерфейс.
   - Добавьте или удалите вторичные IP-адреса.
   - Измените группы безопасности, назначенные виртуальной машине.

   Обновив нужные параметры, нажмите **Сохранить**.
5. Нажмите **Готово**, чтобы завершить настройку сетевых интерфейсов ВМ и сохранить изменения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server iface set [--fixed-ip <ip-address | ip-address=
                                <ip-address>,subnet=<subnet> |
                                ip-version=<ip-version>>]
                                [--spoofing-protection-enable |
                                --spoofing-protection-disable]
                                [--security-group <security-group> |
                                --no-security-groups]
                                --server <server> <interface>
```

--fixed-ip <ip-address|ip-address=<ip-address>,subnet=<subnet>|ip-version=<ip-version>>

Нужный IP-адрес и/или подсеть. Этот параметр можно использовать несколько раз.

--spoofing-protection-enable

Включает защиту от спуфинга пакетов на сетевом интерфейсе

--spoofing-protection-disable

Выключает защиту от спуфинга пакетов на сетевом интерфейсе

--security-group <security-group>

Имя или идентификатор группы безопасности. Этот параметр можно использовать несколько раз.

--no-security-groups

Не устанавливать группы безопасности

--server <server>

Идентификатор или имя виртуальной машины

<interface>

Идентификатор сетевого интерфейса

Например, чтобы отменить назначение групп безопасности сетевому интерфейсу с идентификатором 611abc06-7557-44c9-bbf8-31fef817e802, присоединенному к виртуальной машине myvm, выполните:

```
# vinfra service compute server iface set --server myvm --no-security-groups 611abc06-7557-44c9-
bbf8-31fef817e802
```

Чтобы отсоединить сетевой интерфейс от виртуальной машины

Панель администратора

1. Перейдите на **Вычисления** > **Виртуальные машины** > экран **Виртуальные машины**. На экране **Виртуальные машины** щелкните по нужной ВМ.
2. На вкладке **Сводка** нажмите **Изменить** в разделе **Сетевые интерфейсы**.
3. В окне **Сетевые интерфейсы** нажмите кнопку с многоточием напротив сетевого интерфейса, который следует отсоединить, и выберите **Удалить**.
4. Нажмите **Готово**, чтобы завершить настройку сетевых интерфейсов ВМ и сохранить изменения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server iface detach --server <server> <interface>
```

--server <server>

Идентификатор или имя виртуальной машины

<interface>

Идентификатор сетевого интерфейса

Например, чтобы отсоединить сетевой интерфейс с идентификатором 471e37fd-13ae-4b8f-b70c-90ac02cc4386 от ВМ myvm, выполните:

```
# vinfra service compute server iface detach 471e37fd-13ae-4b8f-b70c-90ac02cc4386 --server myvm
```

Настройка томов виртуальных машин

Можно добавлять новые тома к виртуальным машинам, присоединять существующие тома и отсоединять ненужные.

Ограничения

- Нельзя изменить, отсоединить или удалить загрузочный том.
- Присоединять и отсоединять можно только незагрузочные тома.
- Нельзя управлять томами ВМ с освобожденными ресурсами.

Предварительные требования

- Чтобы можно было использовать тома, присоединенные к ВМ, они должны быть инициализированы внутри гостевой ОС стандартными средствами.

Как присоединить том к виртуальной машине

Панель администратора

1. Перейдите на экран **Вычисления** > **Виртуальные машины** > **Виртуальные машины** и щелкните по нужной ВМ.
2. На вкладке **Сводка** нажмите значок карандаша в поле **Тома**.
3. В окне **Тома**:
   - Нажмите **Присоединить** для присоединения существующего тома, а затем выберите том в окне **Присоединить том**.
   - Нажмите **Добавить**, чтобы создать новый том, а затем укажите для него имя, размер и политику хранилища. Созданный том будет автоматически добавлен к дискам ВМ.
4. Нажмите **Готово**, чтобы завершить настройку дисков ВМ и сохранить изменения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server volume attach --server <server> <volume>
```

--server <server>

Идентификатор или имя виртуальной машины

<volume>

Идентификатор или имя тома

Например, чтобы присоединить том с идентификатором e4cb5363-1fb2-41f5-b24b-18f98a388cba к виртуальной машине myvm, выполните:

```
# vinfra service compute server volume attach e4cb5363-1fb2-41f5-b24b-18f98a388cba --server
myvm
+--------+--------------------------------------+
| Field  | Value                                |
+--------+--------------------------------------+
| device | /dev/vdb                             |
| id     | e4cb5363-1fb2-41f5-b24b-18f98a388cba |
+--------+--------------------------------------+
```

Имя нового устройства будет отображено в выводе команды. Чтобы просмотреть все тома ВМ, выполните:

```
# vinfra service compute server volume list --server myvm
+--------------------------------------+----------+
| id                                   | device   |
+--------------------------------------+----------+
| e4cb5363-1fb2-41f5-b24b-18f98a388cba | /dev/vdb |
| b325cc6e-8de1-4b6c-9807-5a497e3da7e3 | /dev/vda |
+--------------------------------------+----------+
```

Как отсоединить том от виртуальной машины

Панель администратора

1. Перейдите на экран **Вычисления** > **Виртуальные машины** > **Виртуальные машины** и щелкните по нужной ВМ.
2. На вкладке **Сводка** нажмите значок карандаша в поле **Тома**.
3. В окне **Тома**:
   - Нажмите **Отсоединить**, чтобы отсоединить том от остановленной виртуальной машины.
   - Нажмите **Отсоединить принудительно**, чтобы отсоединить том от работающей виртуальной машины.

     Предупреждение

При этом есть риск потери данных.

4. Нажмите **Готово**, чтобы завершить настройку дисков ВМ и сохранить изменения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server volume detach --server <server> <volume>
```

--server <server>

Идентификатор или имя виртуальной машины

<volume>

Идентификатор или имя тома

Например, чтобы отсоединить том с идентификатором e4cb5363-1fb2-41f5-b24b-18f98a388cba от виртуальной машины myvm, выполните:

```
# vinfra service compute server volume detach e4cb5363-1fb2-41f5-b24b-18f98a388cba \
--server 871fef54-519b-4111-b18d-d2039e2410a8
```

7.6.2.11 Настройка высокой доступности виртуальных машин

Высокая доступность сохраняет виртуальные машины в работоспособном состоянии, если узел, на котором они располагаются, выйдет из строя из-за сбоя ядра, нарушения электроснабжения и т. п. или станет недоступен по сети. Штатное завершение работы не считается отказом узла.

В случае отказа система попытается эвакуировать затронутые ВМ автоматически, то есть выполнить их автономную миграцию с автоматическим переназначением на другие исправные вычислительные узлы в следующем порядке:

- Виртуальные машины со статусом «Активная» эвакуируются первыми и автоматически запускаются.
- Виртуальные машины со статусом «Завершение работы» эвакуируются следующими и остаются остановленными.
- Все прочие виртуальные машины игнорируются и остаются на вышедшем из строя узле.

Если что-либо препятствует эвакуации, например на вычислительных узлах назначения не хватает ресурсов для размещения затронутых виртуальных машин, эти ВМ остаются на отказавшем узле и получают статус «Ошибка». Их можно эвакуировать вручную после устранения проблемы (обеспечения достаточного объема ресурсов, присоединения новых узлов к кластеру и т. д.).

По умолчанию высокая доступность для виртуальных машин включается автоматически после создания вычислительного кластера. При необходимости ее можно отключить вручную. Не забывайте, что виртуальные машины с отключенной высокой доступностью не будут эвакуироваться на работоспособные узлы в случае переключения при сбое.

Ограничения

- Вычислительный кластер может выдержать выход из строя только одного узла.

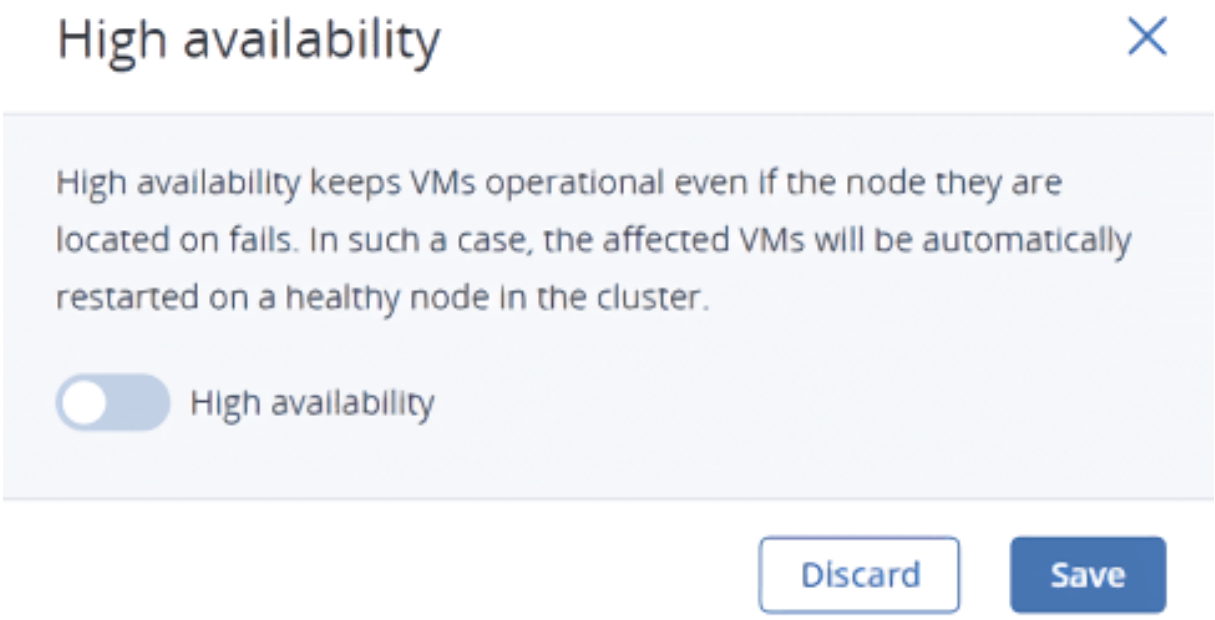
Предварительные требования

- Созданы виртуальные машины, как описано в разделе "Создание виртуальных машин" на странице 460.

Чтобы отключить высокую доступность для виртуальных машин

Панель администратора

1. Щелкните по виртуальной машине, для которой нужно отключить высокую доступность.
2. На правой панели ВМ щелкните по значку карандаша рядом с параметром **Высокая доступность**.
3. В окне **Высокая доступность** отключите высокую доступность для ВМ и нажмите кнопку **Сохранить**.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server set <server> --ha-enabled {true,false}
```

--ha-enabled {true,false}

Включение или отключение высокой доступности для виртуальной машины

<server>

Идентификатор или имя виртуальной машины

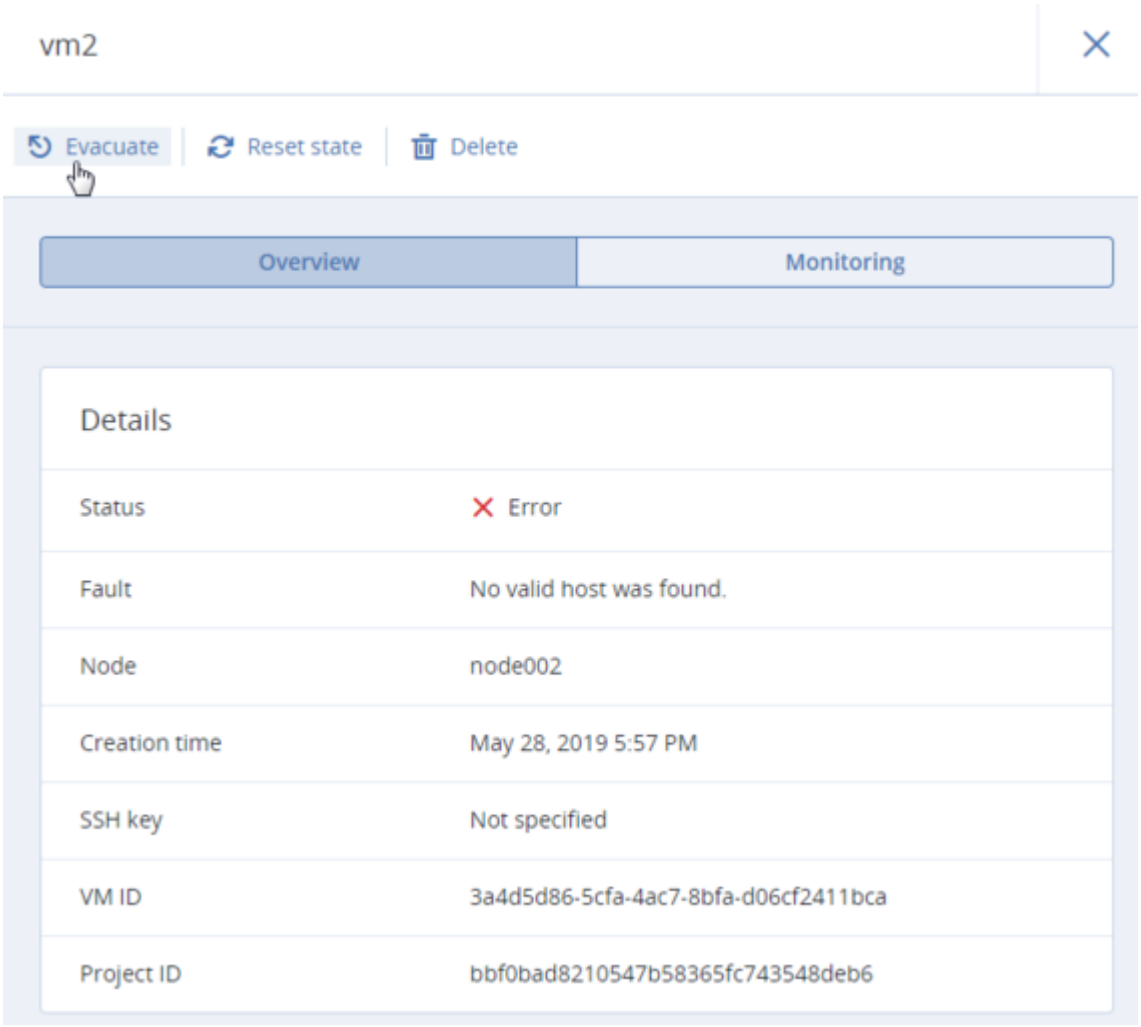
Например, чтобы отключить высокую доступность для виртуальной машины myvm, выполните:

```
# vinfra service compute server set myvm --ha-enabled false
```

Чтобы выполнить эвакуацию виртуальной машины вручную

Панель администратора

1. Щелкните по виртуальной машине с состоянием «Ошибка».
2. Нажмите **Эвакуировать** на правой панели ВМ.



Интерфейс командной строки

Используйте следующую команду:

```
# vinfra service compute server set myvm --ha-enabled false
```

<server>

Идентификатор или имя виртуальной машины

Например, чтобы эвакуировать остановленную ВМ myvm с ее сервера на работоспособный вычислительный сервер, выполните:

```
# vinfra service compute server evacuate myvm
```

7.6.2.12 Управление виртуальными машинами в размещениях

Размещение назначается виртуальной машине при ее создании из образа или типа ВМ с назначенным размещением. ВМ также может унаследовать размещение от тома, созданного с помощью назначенного образа. Однако ВМ не наследует размещение и его изменения от сервера. Например, если назначить размещение серверу с существующими ВМ, то размещение будет иметь только сервер. ВМ не унаследуют это размещение. Аналогично, если у вас есть сервер с ВМ, которым назначено то же размещение, и вы удалите такой сервер из размещения, то размещение изменится только у сервера. ВМ на этом сервере сохранят прежнее размещение.

Предварительные требования

- Созданы виртуальные машины, как описано в разделе "Создание виртуальных машин" на странице 460.
- Должны быть созданы размещения для вычислительных узлов, как описано в разделе "Создание размещений" на странице 647.
- На узле и размещенных на нем виртуальных машинах должна быть одна и та же конфигурация размещений.

Чтобы изменить размещение ВМ

Используйте следующую команду:

```
vinfra service compute server set [--no-placements |--placement placement] <server>
```

--no-placements

Отзыв у виртуальной машины всех назначенных размещений

--placement placement

Имя или идентификатор размещения, которое следует назначить виртуальной машине. Укажите этот параметр несколько раз, чтобы назначить несколько размещений виртуальной машине.

<server>

Идентификатор или имя виртуальной машины

Например, чтобы отозвать у виртуальной машины myvm все назначенные размещения, выполните:

```
# vinfra service compute server set myvm --no-placements
```

7.6.2.13 Миграция виртуальных машин

Миграция виртуальных машин помогает упростить обновление кластеров и балансировку рабочих нагрузок между вычислительными узлами. Кибер Инфраструктура позволяет выполнять два типа миграции:

- **Холодная миграция** – для остановленных и приостановленных виртуальных машин.
- **Горячая миграция** – для запущенных виртуальных машин (позволяет избежать простоя ВМ).

При обоих типах миграции виртуальная машина переносится между вычислительными узлами, использующими общее хранилище, поэтому миграция блочных устройств хранения данных не производится.

Горячая миграция состоит из следующих этапов:

1. Вся память ВМ копируется на узел назначения, в то время как виртуальная машина продолжает работать на исходном узле. Если та или иная страница памяти ВМ изменится, она будет скопирована заново.
2. Когда остается скопировать только несколько страниц памяти, ВМ на исходном узле останавливается, оставшиеся страницы передаются и ВМ перезапускается на узле назначения.

Большие виртуальные машины с интенсивными нагрузками записи записывают новые данные в память быстрее, чем изменения памяти могут быть переданы на узел назначения, что препятствует сходимости миграции. Для таких ВМ применяется механизм автоматической сходимости. При обнаружении отсутствия сходимости во время активной миграции скорость работы виртуального ЦП виртуальной машины снижается, что также замедляет запись в память ВМ. Изначально виртуальный ЦП виртуальной машины замедляется на 20 процентов, а затем еще на 10 процентов при каждой итерации. Этот процесс продолжается до тех пор, пока запись в память ВМ не будет достаточно замедлена для завершения миграции или пока виртуальный ЦП не будет замедлен на 99 процентов.

Ограничения

- Виртуальные машины по умолчанию создаются с той же моделью ЦП, что и у хоста. Наличие вычислительных серверов с разными типами ЦП может привести к проблемам при динамической миграции. Чтобы избежать этого, можно вручную задать модель ЦП для всех новых ВМ, как описано в разделе "Настройка модели ЦП виртуальных машин" на странице 178. Либо можно создать размещение для каждой группы вычислительных серверов с одной моделью ЦП, следуя инструкциям в разделе "Управление размещениями для вычислительных узлов" на странице 643.

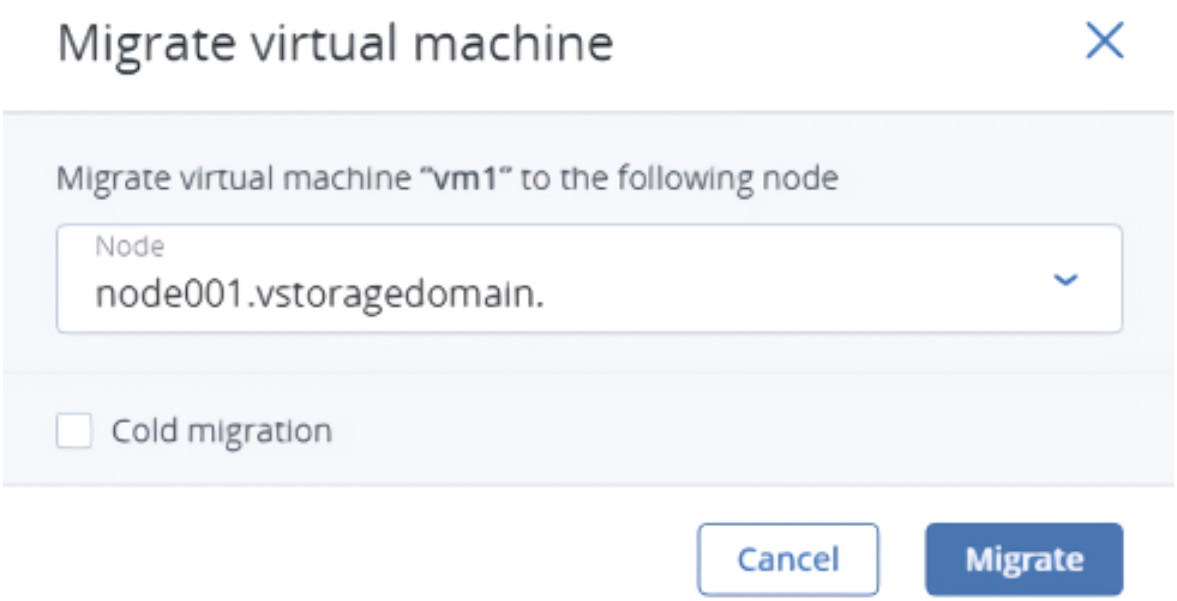
Предварительные требования

- Созданы виртуальные машины, как описано в разделе "Создание виртуальных машин" на странице 460.

Чтобы произвести миграцию виртуальной машины

Панель администратора

1. На вкладке **Вычисления** > **Виртуальные машины** > **Виртуальные машины** щелкните по виртуальной машине, которую необходимо перенести.
2. Щелкните по значку многоточия рядом с виртуальной машиной и выберите **Миграция**.
3. В новом окне укажите узел назначения:
   - **Автоматически**. Оптимальное место назначения будет автоматически выбрано среди узлов кластера в зависимости от доступных на них ресурсов ЦП и ОЗУ.
   - Выберите узел назначения вручную из раскрывающегося списка.



4. [Необязательно] По умолчанию запущенные ВМ переносятся активными. Можно изменить режим миграции на автономный, установив флажок **Холодная миграция**. Виртуальная машина будет остановлена и перезапущена на сервере назначения после миграции.
5. Нажмите **Мигрировать**, чтобы зарезервировать ресурсы на узле назначения и начать миграцию.

Ход миграции будет отображаться на панели администрирования.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server migrate [--cold] [--node <node>] <server>
```

--cold

Выполнение холодной миграции. Если параметр не установлен, тип миграции определяется автоматически.

--node <node>

Идентификатор или имя хоста для сервера назначения

<server>

Идентификатор или имя виртуальной машины

Например, чтобы начать миграцию виртуальной машины myvm на вычислительный сервер node003.vstoragedomain, выполните:

```
# vinfra service compute server migrate myvm --node node003
```

7.6.2.14 Освобождение ресурсов виртуальных машин

Можно отменить привязку остановленной ВМ к серверу, где она была размещена, и высвободить ее зарезервированные ресурсы, такие как ЦП и ОЗУ. При этом ВМ остается загружаемой и сохраняет свою конфигурацию, включая IP-адреса.

Предварительные требования

- Созданы виртуальные машины, как описано в разделе "Создание виртуальных машин" на странице 460.

Как освободить ресурсы остановленной виртуальной машины

Панель администратора

1. Щелкните по остановленной виртуальной машине.
2. На правой панели ВМ нажмите **Освободить ресурсы**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server shelve <server>
```

<server>

Идентификатор или имя виртуальной машины

Например, чтобы освободить ресурсы виртуальной машины myvm, выполните:

```
# vinfra service compute server shelve myvm
```

Как освободить ресурсы работающей или приостановленной виртуальной машины

Панель администратора

1. Щелкните по работающей или приостановленной виртуальной машине.
2. На правой панели ВМ нажмите **Выключить** или **Принудительно выключить**, а затем выберите **Освободить ресурсы ВМ** в окне подтверждения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server shelve <server>
```

<server>

Идентификатор или имя виртуальной машины

Например, чтобы освободить ресурсы виртуальной машины myvm, выполните:

```
# vinfra service compute server shelve myvm
```

Как воссоздать освобожденную ВМ на сервере с достаточным для нее количеством ресурсов

Панель администратора

1. Щелкните по виртуальной машине с освобожденными ресурсами.
2. На правой панели ВМ нажмите **Назначить ресурсы**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server unshelve <server>
```

<server>

Идентификатор или имя виртуальной машины

Например, чтобы воссоздать освобожденную виртуальную машину myvm, выполните:

```
# vinfra service compute server unshelve myvm
```

7.6.2.15 Присоединение физических устройств PCI к виртуальным машинам

Путем присоединения различных устройств с вычислительных серверов к виртуальным машинам можно снизить сетевую задержку ВМ или ускорить визуализацию внутри гостевой операционной системы. Поддерживаются следующие PCI-устройства:

- Графические карты. С помощью сквозной передачи (GPU passthrough) можно предоставить в распоряжение отдельной ВМ целый физический графический процессор, тогда как виртуальные графические процессоры (vGPUs) позволяют разделить ресурсы одной физической графической карты между несколькими ВМ. Можно одновременно использовать обе возможности, сквозную передачу и виртуальные графические процессоры, на одном и том же сервере.
- Сетевые адаптеры с возможностями Single Root I/O Virtualization (SR-IOV). Технология SR-IOV позволяет разделить один физический адаптер (физическую функцию) на несколько виртуальных адаптеров (виртуальных функций). Каждая виртуальная функция воспринимается как отдельное PCI-устройство, которое можно присоединить к виртуальной машине.

- Хост-адаптеры шины. Для присоединения HBA-устройств к виртуальным машинам используйте шаги, описанные для настройки сквозной передачи.

Ограничения

- Сквозной режим PCI-устройств доступен на серверах, поддерживающих блок управления памятью для операций ввода-вывода (IOMMU). Список оборудования с поддержкой IOMMU см. в этой статье.
- Виртуальные графические процессоры поддерживается для графических карт NVIDIA.

Обзор процедуры

1. Подготовьте вычислительные серверы в зависимости от физических устройств, для которых необходимо включить режим сквозной передачи или виртуализацию.
2. Перенастройте вычислительный кластер, чтобы включить режим сквозной передачи или поддержку vGPU.
3. Создайте виртуальные машины с присоединенными физическими устройствами PCI или виртуальными графическими картами.

Подготовка серверов для сквозной передачи GPU

Для сквозной передачи GPU отсоедините графические карты, которые необходимо присоединить к виртуальным машинам сервера, а затем включите поддержку IOMMU. Можно отсоединять сразу несколько графических карт с одинаковыми VID (идентификатор производителя) и PID (идентификатор продукта), а также отсоединять только отдельные графические карты, используя их PCI-адреса.

Если были отсоединены несколько графических карт сервера с помощью pci-helper.py detach, но необходимо использовать только одну из них для сквозной передачи, нужно отменить отсоединение и отсоединить необходимую графическую карту с помощью pci-helper.py bind-to-stub. В этом случае остальные графические карты сервера можно использовать для предоставления виртуальных графических карт.

Чтобы отсоединить несколько графических карт сервера

Выведите список всех графических карт сервера и получите их VID и PID:

```
# lspci -nnD | grep NVIDIA
0000:01:00.0 3D controller [0302]: NVIDIA Corporation TU104GL [Tesla T4] [10de:1eb8] (rev a1)
0000:81:00.0 3D controller [0302]: NVIDIA Corporation TU104GL [Tesla T4] [10de:1eb8] (rev a1)
```

[10de:1eb8] содержит VID и PID графической карты.

Запустите сценарий pci-helper.py detach, чтобы отсоединить все графические карты с одинаковыми VID и PID. Для графических карт NVIDIA дополнительно внесите в черный список драйвер Nouveau. Например:

```
# /usr/libexec/vstorage-ui-agent/bin/pci-helper.py detach 10de:1eb8 --blacklist-nouveau
```

Эта команда отсоединяет графические карты сервера, у которых VID:PID — это 10de:1eb8, а также выключает загрузку драйвера Nouveau.

Чтобы отменить отсоединение нескольких графических карт сервера

1. В файле /etc/sysconfig/grub найдите переменную GRUB_CMDLINE_LINUX, а затем удалите pci-stub.ids=<gpu_vid>:<gpu_pid> rd.driver.blacklist=nouveau nouveau.modeset=0 из ее значения. Получившийся файл будет выглядеть следующим образом:

   ```
   # cat /etc/sysconfig/grub | grep CMDLINE
   GRUB_CMDLINE_LINUX="crashkernel=auto tcache.enabled=0 quiet iommu=pt"
   ```

2. Сгенерируйте файл конфигурации GRUB.
   - Для системы с BIOS выполните:

     ```
     # /usr/sbin/grub2-mkconfig -o /etc/grub2.cfg
     ```

   - Для системы с UEFI выполните:

     ```
     # /usr/sbin/grub2-mkconfig -o /etc/grub2-efi.cfg
     ```

3. Удалите файл /etc/modprobe.d/blacklist-nouveau.conf.
4. Пересоздайте загрузочный образ Linux, выполнив:

   ```
   # dracut -f
   ```

5. Перезагрузите сервер, чтобы применить изменения:

   ```
   # reboot
   ```

Чтобы отсоединить отдельную графическую карту сервера

Получите список всех графических карт сервера и узнайте их PCI-адреса:

```
# lspci -nnD | grep NVIDIA
0000:01:00.0 3D controller [0302]: NVIDIA Corporation TU104GL [Tesla T4] [10de:1eb8] (rev a1)
0000:81:00.0 3D controller [0302]: NVIDIA Corporation TU104GL [Tesla T4] [10de:1eb8] (rev a1)
```

0000:01:00.0 и 0000:81:00.0 — это PCI-адреса графических карт.

Выполните сценарий pci-helper.py bind-to-stub, чтобы назначить драйвер pci-stub графической карте по ее PCI-адресу. Например:

```
# /usr/libexec/vstorage-ui-agent/bin/pci-helper.py bind-to-stub 0000:01:00.0
```

Эта команда отсоединяет графическую карту сервера с PCI-адресом 0000:01:00.0 и выключает загрузку драйвера Nouveau.

Чтобы включить поддержку IOMMU на сервере

Выполните сценарий pci-helper.py, а затем перезагрузите сервер, чтобы применить изменения:

```
# /usr/libexec/vstorage-ui-agent/bin/pci-helper.py enable-iommu
# reboot
```

Сценарий работает как для процессоров Intel, так и для AMD.

Проверить успешное включение поддержки IOMMU можно в выводе dmesg:

```
# dmesg | grep -e DMAR -e IOMMU
[    0.000000] DMAR: IOMMU enabled
```

Подготовка серверов для виртуализации графических карт

Для включения поддержки виртуализации графических карт необходимо установить модуль ядра NVIDIA. Если необходимо включить поддержку виртуализации для графической карты, которая ранее была отсоединена для ее использования в режиме сквозной передачи, нужно дополнительно модифицировать конфигурационный файл GRUB.

Предварительные требования

- Для авторизации команд OpenStack должен быть настроен клиент интерфейса командной строки OpenStack, как описано в разделе "Подключение к интерфейсу командной строки OpenStack" на странице 427.

Чтобы включить поддержку виртуализации графических карт на сервере

1. На сервере с физической графической картой выполните следующие действия:
   - Если физическая графическая карта сервера соединена
     Добавьте драйвер Nouveau в черный список:

     ```
     # rmmod nouveau
     # echo -e "blacklist nouveau\noptions nouveau modeset=0" >
     /usr/lib/modprobe.d/nouveau.conf
     # echo -e "blacklist nouveau\noptions nouveau modeset=0" > /etc/modprobe.d/nouveau.conf
     ```

   - Если физическая графическая карта сервера отсоединена
     a. В файле /etc/sysconfig/grub найдите переменную GRUB_CMDLINE_LINUX, а затем удалите pci-stub.ids=<gpu_vid>:<gpu_pid> из ее значения. Например, для графической карты, у которой VID:PID – это 10de:1eb8, удалите pci-stub.ids=10de:1eb8 и проверьте получившийся файл:

     ```
     # cat /etc/sysconfig/grub | grep CMDLINE
     GRUB_CMDLINE_LINUX="crashkernel=auto tcache.enabled=0 quiet iommu=pt
     rd.driver.blacklist=nouveau nouveau.modeset=0"
     ```

     b. Сгенерируйте конфигурационный файл GRUB.
        - Для системы с BIOS выполните:

        ```
        # /usr/sbin/grub2-mkconfig -o /etc/grub2.cfg
        ```

- Для системы с UEFI выполните:

```
# /usr/sbin/grub2-mkconfig -o /etc/grub2-efi.cfg
```

c. Перезагрузите сервер, чтобы применить изменения:

```
# reboot
```

2. Установите модуль ядра vGPU KVM из пакета NVIDIA GRID:

```
# bash NVIDIA-Linux-x86_64-460.73.02-vgpu-kvm.run
```

3. Пересоздайте загрузочный образ Linux, выполнив:

```
# dracut -f
```

4. Перезагрузите сервер, чтобы завершить установку модуля ядра:

```
# reboot
```

Чтобы проверить, что поддержка виртуальных графических карт включена для физической графической карты

Получите список всех графических карт сервера и их PCI-адреса:

```
# lspci -D | grep NVIDIA
0000:01:00.0 3D controller: NVIDIA Corporation TU104GL [Tesla T4] (rev a1)
0000:81:00.0 3D controller: NVIDIA Corporation TU104GL [Tesla T4] (rev a1)
```

0000:01:00.0 и 0000:81:00.0 – это PCI-адреса графических карт.

Проверьте, что поддержка виртуальных графических карт включена для физической графической карты:

```
ls /sys/bus/pci/devices/0000\:03:00.0/mdev_supported_types
nvidia-222  nvidia-223  nvidia-224  nvidia-225  nvidia-226  nvidia-227  nvidia-228  nvidia-229  nvidia-
230  nvidia-231
nvidia-232  nvidia-233  nvidia-234  nvidia-252  nvidia-319  nvidia-320  nvidia-321
```

Для физической графической карты, для которой включена виртуализация, папка содержит список типов поддерживаемых виртуальных графических карт. Тип виртуальной графической карты – это конфигурация виртуальной графической карты, которая определяет объем виртуальной памяти, максимальное разрешение, максимальное количество графических процессоров и другие параметры.

Чтобы проверить, что на сервере есть ресурсы виртуальных графических карт для выделения

Получите список поставщиков ресурсов вычислительного кластера, чтобы узнать их идентификаторы. Например:

```
# openstack --insecure resource provider list
+--------------------------------------+---------------------------------------+------------+--------------------------------------+--------------------------------------+
| uuid                                 | name                                  | generation | root_provider_uuid                   | parent_provider_uuid                 |
+--------------------------------------+---------------------------------------+------------+--------------------------------------+--------------------------------------+
| 359cccf7-9c64-4edc-a35d-f4673e485a04 | node001.vstoragedomain_pci_0000_03_00_0 |          1 | 4936695a-4711-425a-b0e4-fdab5e4688d6 | 4936695a-4711-425a-b0e4-fdab5e4688d6 |
| b8443d1b-b941-4bf5-ab4b-2dc7c64ac7d1 | node001.vstoragedomain_pci_0000_81_00_0 |          1 | 4936695a-4711-425a-b0e4-fdab5e4688d6 | 4936695a-4711-425a-b0e4-fdab5e4688d6 |
| 4936695a-4711-425a-b0e4-fdab5e4688d6 | node001.vstoragedomain                |        823 | 4936695a-4711-425a-b0e4-fdab5e4688d6 | None                                 |
+--------------------------------------+---------------------------------------+------------+--------------------------------------+--------------------------------------+
```

В этом выводе поставщик ресурсов с идентификатором 4936695a-4711-425a-b0e4-fdab5e4688d6 обладает двумя дочерними поставщиками ресурсов для двух физических графических карт с PCI-адресами 0000:03:00.0 и 0000:81:00.0.

Используйте полученный идентификатор дочернего поставщика ресурсов, чтобы получить его инвентарный список. Например:

```
# openstack --insecure resource provider inventory list 359cccf7-9c64-4edc-a35d-f4673e485a04
+----------------+------------------+----------+----------+-----------+----------+-------+
| resource_class | allocation_ratio | max_unit | reserved | step_size | min_unit | total |
+----------------+------------------+----------+----------+-----------+----------+-------+
| VGPU           |              1.0 |        8 |        0 |         1 |        1 |     8 |
+----------------+------------------+----------+----------+-----------+----------+-------+
```

Этот дочерний поставщик ресурсов обладает ресурсами виртуальных графических карт, которые могут быть выделены виртуальным машинам.

Подготовка серверов для использования SR-IOV

Чтобы использовать возможности SR-IOV, убедитесь, что сетевой адаптер можно виртуализировать, а затем включите поддержку IOMMU. Для сетевых адаптеров Mellanox необходимо дополнительно включить SR-IOV в микропрограмме.

Чтобы проверить, что сетевой адаптер поддерживает SR-IOV

Выведите список всех сетевых адаптеров на сервере и получите их VID и PID:

```
# lspci -nnD | grep Ethernet
0000:00:03.0 Ethernet controller [0200]: Mellanox Technologies MT27800 Family [ConnectX-5] [15b3:1017]
0000:00:04.0 Ethernet controller [0200]: Mellanox Technologies MT27800 Family [ConnectX-5] [15b3:1017]
```

[15b3:1017] содержит VID и PID сетевого адаптера.

Убедитесь, что выбранный сетевой адаптер поддерживает SR-IOV, указав его VID и PID:

```
# lspci -vv -d 15b3:1017 | grep SR-IOV
Capabilities: [180 v1] Single Root I/O Virtualization (SR-IOV)
Capabilities: [180 v1] Single Root I/O Virtualization (SR-IOV)
```

Чтобы включить поддержку IOMMU на сервере

Выполните сценарий pci-helper.py, а затем перезагрузите сервер, чтобы применить изменения:

```
# /usr/libexec/vstorage-ui-agent/bin/pci-helper.py enable-iommu
# reboot
```

Сценарий работает как для процессоров Intel, так и для AMD.

Проверить успешное включение поддержки IOMMU можно в выводе dmesg:

```
# dmesg | grep -e DMAR -e IOMMU
[    0.000000] DMAR: IOMMU enabled
```

Чтобы включить поддержку SR-IOV в микропрограмме сетевых адаптеров Mellanox

1. Скачайте Mellanox Firmware Tools (MFT) с официального сайта и распакуйте архив на сервере, например:

   ```
   # wget https://www.mellanox.com/downloads/MFT/mft-4.17.0-106-x86_64-rpm.tgz
   # tar -xvzf mft-4.17.0-106-x86_64-rpm.tgz
   ```

2. Установите пакет, а затем запустите Mellanox Software Tools (MST):

   ```
   # yum install rpm-build
   # . mft-4.17.0-106-x86_64-rpm/install.sh
   # mst start
   ```

3. Определите путь к устройству Mellanox:

   ```
   # mst status
   ```

4. Запросите текущую конфигурацию устройства:

   ```
   # mlxconfig -d /dev/mst/mt4119_pciconf0 q
   ...
   Configurations:
   ...
           NUM_OF_VFS          4           # Number of activated VFs
           SRIOV_EN            True(1)     # SR-IOV is enabled
   ...
   ```

5. При необходимости задайте нужные значения. Например, чтобы увеличить число виртуальных функций до 8, выполните следующую команду:

```
# mlxconfig -d /dev/mst/mt4119_pciconf0 set SRIOV_EN=1 NUM_OF_VFS=8
```

6. Перезагрузите сервер, чтобы применить изменения.

Включение поддержки сквозной передачи и виртуализации графических карт в вычислительном кластере

Чтобы включить поддержку сквозной передачи и виртуализации графических карт в вычислительном кластере, необходимо создать конфигурационный файл в формате YAML, а затем использовать его для перенастройки вычислительного кластера.

Предварительные требования

- Серверы вычислительного кластера подготовлены для использования режима сквозной передачи, виртуализации графических карт или использования SR-IOV, как описано в разделах "Подготовка серверов для сквозной передачи GPU" на странице 495, "Подготовка серверов для виртуализации графических карт" на странице 497 и "Подготовка серверов для использования SR-IOV" на странице 499.

Чтобы создать конфигурационный файл для режима сквозной передачи и виртуализации графических карт

Укажите идентификатор сервера, где расположены PCI-устройства, а затем добавьте устройства, для которых необходимо использовать режим сквозной передачи или виртуализацию:

- Чтобы создать виртуальную функцию для сетевого адаптера, добавьте следующие строки:

  ```
  - device_type: sriov
    device: enp2s0
    physical_network: sriovnet
    num_vfs: 8
  ```

  Где:

  - sriov – тип устройства для сетевого адаптера
  - enp2s0 – имя устройства для сетевого адартера
  - sriovnet – произвольное имя, которое будет использоваться в качестве псевдонима для сетевого адаптера
  - num_vfs – количество виртуальных функций, которые будут созданы для сетевого адаптера

  Макисмальное количество виртуальных функций, поддерживаемое PCI-устройством, указано в файле /sys/class/net/<device_name>/device/sriov_totalvfs. Например:

  ```
  # cat /sys/class/net/enp2s0/device/sriov_totalvfs
  63
  ```

- Чтобы включить поддержку сквозной передачи для графическиой карты, добавьте следующие строки:

```
- device_type: generic
  device: 1b36:0100
  alias: gpu
```

Где:

- generic – тип устройства для физической графической карты, для которой будет включен режим сквозной передачи
- 1b36:0100 – VID и PID физической графической карты
- gpu – произвольное имя, которое будет использоваться как псевдоним для физической графической карты

- Чтобы включить поддержку виртуализации для физической графической карты, добавьте следующие строки:

```
- device_type: pgpu
  device: "0000:03:00.0"
  vgpu_type: nvidia-224
```

Где:

- pgpu – тип устройства для физической графической карты, которая будет виртуализована
- "0000:03:00.0" – PCI-адрес физической графической карты
- nvidia-224 – тип виртуальной графической карты, который будет включен для указанной физической графической карты

Пример конфигурационного файла, который должен получиться в итоге:

```
# cat config.yaml
- node_id: c3b2321a-7c12-8456-42ce-8005ff937e12
  devices:
    - device_type: sriov
      device: enp2s0
      physical_network: sriovnet
      num_vfs: 8
    - device_type: generic
      device: 1b36:0100
      alias: gpu
    - device_type: pgpu
      device: "0000:01:00.0"
      vgpu_type: nvidia-232
- node_id: 1d6481c2-1fd5-406b-a0c7-330f24bd0e3d
  devices:
    - device_type: generic
      device: 10de:1eb8
      alias: gpu
    - device_type: pgpu
      device: "0000:03:00.0"
      vgpu_type: nvidia-224
    - device_type: pgpu
```

```
    device: "0000:81:00.0"
    vgpu_type: nvidia-228
```

Чтобы настроить вычислительный кластер для использования режима сквозной передачи и виртуализации графических карт

Укажите конфигурационный файл, который был подготовлен ранее, при запуске команды vinfra service compute set. Например:

```
# vinfra service compute set --pci-passthrough-config config.yaml
```

Если перенастройка вычислительного кластера завершается ошибкой

Проверьте, есть ли следующая ошибка в /var/log/vstorage-ui-backend/ansible.log:

```
2021-09-23 16:42:59,796 p=32130 u=vstoradmin | fatal: [32c8461b-92ec-48c3-ae02-
4d12194acd02]: FAILED! => {"changed": true, "cmd": "echo 4 > /sys/class/net/
enp103s0f1/device/sriov_numvfs", "delta": "0:00:00.127417", "end": "2021-09-23
19:42:59.784281", "msg": "non-zero return code", "rc": 1, "start": "2021-09-23
19:42:59.656864", "stderr": "/bin/sh: line 0: echo: write error: Cannot allocate
memory", "stderr_lines": ["/bin/sh: line 0: echo: write error: Cannot allocate memory"],
"stdout": "", "stdout_lines": []}
```

В этом случае запустите сценарий pci-helper.py и перезагрузите сервер:

```
# /usr/libexec/vstorage-ui-agent/bin/pci-helper.py enable-iommu --pci-realloc
# reboot
```

Когда сервер возобновит работу, выполните команду vinfra service compute set еще раз.

Переключение между режимом сквозной передачи и виртуализацией графических карт

Если в вычислительном кластере был включен режим сквозной передачи для графических карт, но необходимо использовать виртуализацию графических карт (или наоборот), перенастройте сервер с физической графической картой и вычислительный кластер.

Предварительные требования

- Вычислительный кластер настроен для использования сквозной передачи или виртуализации графических карт, как описано в разделе "Включение поддержки сквозной передачи и виртуализации графических карт в вычислительном кластере" на странице 501.

Чтобы переключить вычислительный кластер из режима сквозной передачи в режим виртуализации графических карт

1. На сервере с физической графической картой найдите службу, которая связана с данным устройством. Например:

```
# systemctl | grep stub
pcistub-0000:01:00.0.service      loaded active exited    Bind device to pci-stub driver
```

2. Отключите эту службу. Например:

```
# systemctl disable pcistub-0000:01:00.0.service
```

3. Перезагрузите сервер, чтобы применить изменения:

```
# reboot
```

4. Измените конфигурационный файл:
   - Измените device_type с generic на pgpu.
   - Укажите PCI-адрес физической графической карты в device.
   - Удалите поле alias.
   - Укажите необходимый тип виртуальной графической карты в vgpu_type.

   В итоге получится следующий конфигурационный файл config.yaml:

```
- node_id: c3b2321a-7c12-8456-42ce-8005ff937e12
  devices:
    - device_type: pgpu
      device: "0000:01:00.0"
      vgpu_type: nvidia-224
```

5. Укажите конфигурационный файл при запуске команды vinfra service compute set. Например:

```
# vinfra service compute set --pci-passthrough-config config.yaml
```

Чтобы переключить вычислительный кластер из режима виртуализации графических карт в режим сквозной передачи

1. Удалите из конфигурационного файла config.yaml информацию, относящуюся к виртуальным графическим картам. Например, удалите следующие строки:

```
- device_type: pgpu
  device: "0000:01:00.0"
  vgpu_type: nvidia-224
```

2. Перенастройте вычислительный кластер, используя обновленный конфигурационный файл config.yaml. Например:

```
# vinfra service compute set --pci-passthrough-config config.yaml
```

3. На сервере с физической графической картой выполните сценарий pci-helper.py, чтобы назначить драйвер pci-stub физической графической карте по ее PCI-адресу. Например:

```
# /usr/libexec/vstorage-ui-agent/bin/pci-helper.py bind-to-stub 0000:01:00.0
```

4. Добавьте физическую графическую карту в конфигурационный файл как устройство типа generic. Например:

```
- device_type: generic
  device: 1b36:0100
  alias: gpu
```

5. Укажите конфигурационный файл при запуске команды vinfra service compute set. Например:

```
# vinfra service compute set --pci-passthrough-config config.yaml
```

Изменение типа виртуальной графической карты для физических графических карт

После включения поддержки виртуальных графических карт в вычислительном кластере, при необходимости, можно изменить тип виртуальной графической карты, указанный для физической графической карты.

Предварительные требования

- Вычислительный кластер настроен для поддержки виртуальных графических карт, как описано в разделе "Включение поддержки сквозной передачи и виртуализации графических карт в вычислительном кластере" на странице 501.
- В вычислитетельном кластере нет виртуальных машин, использующих виртуальные графические карты указанного типа.

Чтобы изменить тип виртуальной графической карты для физической графической карты

1. Измените конфигурационный файл. Например, замените nvidia-224 на nvidia-228 в поле vgpu_type:

```
- device_type: pgpu
  device: "0000:01:00.0"
  vgpu_type: nvidia-228
```

2. Укажите конфигурационный файл при запуске команды vinfra service compute set. Например:

```
# vinfra service compute set --pci-passthrough-config config.yaml
```

3. Перезагрузите сервер с физической графической картой, чтобы применить изменения:

```
# reboot
```

Создание виртуальных машин с физическим графическим процессором

Ограничения

- Для виртуальных машин, к которым подключен физический графический процессор, нельзя использовать живую миграцию.

Предварительные требования

- В вычислительном кластере включена поддержка сквозной передачи для графических карт, как описано в разделе "Включение поддержки сквозной передачи и виртуализации графических карт в вычислительном кластере" на странице 501.
- Для авторизации команд OpenStack настроен клиент интерфейса командной строки OpenStack, как описано в разделе "Подключение к интерфейсу командной строки OpenStack" на странице 427.

Чтобы создать виртуальную машину, использующую физический графический процессор

1. Создайте тип BM, указав в свойстве pci_passthrough псевдоним графического процессора из файла pci-passthrough.yaml и число графических процессоров, которые будут использоваться. Например, чтобы создать тип BM gpu-flavor с 8 виртуальными ЦП и 16 ГиБ ОЗУ, выполните следующую команду:

   ```
   # openstack --insecure flavor create --ram 16 --vcpus 8 --property "pci_
   passthrough:alias"="gpu:1" gpu-flavor
   ```

2. Для некоторых драйверов может потребоваться скрыть подпись гипервизора. Для этого добавьте свойство hide_hypervisor_id к типу BM.

   ```
   # openstack --insecure flavor set gpu-flavor --property hide_hypervisor_id=true
   ```

3. Создайте виртуальную машину, указав тип BM gpu-flavor. Например, чтобы создать BM gpu-vm из тома vol2, выполните следующую команду:

   ```
   # openstack --insecure server create --volume vol2 --flavor gpu-flavor gpu-vm
   ```

Создание виртуальных машин с виртуальными графическими процессорами

Ограничения

- Для виртуальных машин, к которым подключены виртуальные графические процессоры, нельзя использовать живую миграцию. Виртуальные машины с виртуальными графическими процессорами нельзя приостановить.
- Драйвер по умолчанию QLX для консоли VNC несовместим с драйвером NVIDIA GPU
  После установки драйвера NVIDIA GPU внутри BM с виртуальным графическим процессором консоль VNC перестает работать. Можно использовать RDP для удаленного подключения. Кроме того, в шаблонах, в которых драйвер NVIDIA GPU уже установлен, можно установить свойство hw_use_vgpu_display, чтобы выключить драйвер QLX. Например:

  ```
  # openstack --insecure image set --property hw_use_vgpu_display 007db63f-9b41-4918-b572-
  2c5eef4c8f4b
  ```

Предварительные требования

- Вычислительный кластер настроен для поддержки виртуальных графических карт, как описано в разделе "Включение поддержки сквозной передачи и виртуализации графических карт в вычислительном кластере" на странице 501.

- Для авторизации команд OpenStack настроен клиент интерфейса командной строки OpenStack, как описано в разделе "Подключение к интерфейсу командной строки OpenStack" на странице 427.

Чтобы создать виртуальную машину с виртуальным графическим процессором произвольного типа, доступного на вычислительном сервере

1. Создайте тип ВМ со свойством resources, указывающим, какое количество виртуальных графических процессоров доступно для использования. Например, чтобы создать тип ВМ vgpu-flavor с 2 виртуальными ЦП и 4 ГиБ ОЗУ, выполните:

   ```
   # openstack --insecure flavor create --ram 4096 --vcpus 2 --property resources:VGPU=1 --public vgpu-flavor
   ```

2. Создайте ВМ, указав тип ВМ vgpu-flavor. Например, чтобы создать ВМ vgpu-vm из тома vol2, выполните:

   ```
   # openstack --insecure server create --volume vol2 --flavor vgpu-flavor vgpu-vm
   ```

Созданная ВМ будет иметь виртуальный графический процессор, тип которого выбран случайным образом из доступных на вычислительном сервере типов виртуальных графических процессоров.

Чтобы создать виртуальную машину с виртуальным графическим процессором определенного типа

1. Создайте тип ВМ со свойствами resources и trait, указывающих количество виртуальных графических процессоров и их тип. Например, чтобы создать тип ВМ vgpu228-flavor с 2 виртуальными ЦП, 4 ГиБ ОЗУ и виртуальным графическим процессором типа nvidia-228, выполните:

   ```
   # openstack --insecure flavor create --ram 4096 --vcpus 2 --property resources:VGPU=1 \
   --property trait:CUSTOM_NVIDIA_228=required --public vgpu228-flavor
   ```

2. Создайте ВМ, указав тип ВМ vgpu228-flavor. Например, чтобы создать ВМ vgpu-vm из тома vol2, выполните:

   ```
   # openstack --insecure server create --volume vol2 --flavor vgpu228-flavor vgpu-vm
   ```

Созданная ВМ будет иметь виртуальный графический процессор типа nvidia-228.

Создание виртуальных машин с сетевыми портами SR-IOV

Ограничения

- Для виртуальных машин, к которым присоединены PCI-устройства, живая миграция не поддерживается.

Предварительные требования

- В вычислительном кластере включена поддержка сквозной передачи для PCI-устройств, как описано в разделе "Включение поддержки сквозной передачи и виртуализации графических карт в вычислительном кластере" на странице 501.
- Для авторизации команд OpenStack настроен клиент интерфейса командной строки OpenStack, как описано в разделе "Подключение к интерфейсу командной строки OpenStack" на странице 427.

Чтобы создать виртуальную машину с сетевым портом SR-IOV

1. Создайте физическую вычислительную сеть, указав псевдоним сетевого адаптера из файла pci-passthrough.yaml. Например, чтобы создать сеть sriov-net, выполните следующую команду:

   ```
   # openstack --insecure network create --provider-physical-network sriovnet --provider-network-type flat sriov-net
   ```

2. Создайте подсеть для сети sriov-net, отключив встроенный DHCP-сервер и указав желаемый диапазон IP-адресов. Например, чтобы создать подсеть sriov-subnet с диапазоном IP-адресов 10.10.10.0/24, выполните следующую команду:

   ```
   # openstack --insecure subnet create --no-dhcp --subnet-range 10.10.10.0/24 --network sriov-net sriov-subnet
   ```

3. Создайте сетевой порт в сети sriov-net с прямой сквозной передачей PCI. Например, чтобы создать порт sriov-port с IP-адресом 10.10.10.10 из подсети sriov-subnet, выполните следующую команду:

   ```
   # openstack --insecure port create --network sriov-net --vnic-type=direct --fixed-ip subnet=sriov-subnet,ip-address=10.10.10.10 sriov-port
   ```

4. Создайте виртуальную машину, указав порт sriov-port. Включите параметр --config-drive, чтобы автоматически назначить IP-адрес внутри гостевой операционной системы. Например, чтобы создать ВМ sriov-vm из тома vol1 с типом ВМ large, выполните следующую команду:

   ```
   # openstack --insecure server create --port sriov-port --volume vol1 --flavor large sriov-vm --config-drive True
   ```

Если создание ВМ завершается с ошибкой

Если создание ВМ завершается следующей ошибкой в файле /var/log/hci/nova/nova-compute.log:

```
2021-08-27 17:56:21.349 6 ERROR nova.compute.manager [instance: 9fb738bf-afe5-40ef-943c-22e43696bfd9] libvirtError: internal error: qemu unexpectedly closed the monitor: 2021-08-27T14:56:20.294985Z qemu-kvm: -device vfio-pci,host=01:00.3,id=hostdev0, bus=pci.0,addr=0x6: vfio error: 0000:01:00.3: group 1 is not viable
2021-08-27 17:56:21.349 6 ERROR nova.compute.manager [instance: 9fb738bf-afe5-40ef-943c-22e43696bfd9] Please ensure all devices within the iommu_group are bound to their vfio bus driver.
```

В этом случае физические и виртуальные функции сетевого адаптера должны принадлежать к одной группе IOMMU. Это можно проверить с помощью команды virsh nodedev-dumpxml, указав имена устройств физических и виртуальных функций, например:

```
# virsh nodedev-dumpxml pci_0000_00_03_0 | grep iommuGroup
  <iommuGroup number='1'>
  </iommuGroup>
# virsh nodedev-dumpxml pci_0000_00_03_1 | grep iommuGroup
  <iommuGroup number='1'>
  </iommuGroup>
```

Имена устройств имеют формат pci_0000_<номер_шины>_<номер_устройства>_<номер_функции>. Эти номера можно получить с помощью команды lspci:

```
# lspci -nn | grep Ethernet
00:03.0 Ethernet controller [0200]: Mellanox Technologies MT27800 Family [ConnectX-5]
[15b3:1017]
...
```

В этих выходных данных 00 – номер шины, 03 – номер устройства и 0 – номер функции.

Если физическая и виртуальные функции принадлежат к одной группе IOMMU, необходимо отключить физическую функцию от сервера, выполнив сценарий pci-helper.py с указанием VID и PID, например:

```
# /usr/libexec/vstorage-ui-agent/bin/pci-helper.py detach 15b3:1017
```

7.6.2.16 Создание виртуальных машин с загрузкой UEFI

Виртуальные машины с загрузкой UEFI можно создать из шаблонов (образов QCOW2) или ISO-образов.

Предварительные требования

- Загрузочный носитель добавлен в вычислительный кластер, как описано в разделе "Подготовка загрузочного носителя для виртуальных машин" на странице 437.
- Чтобы создать ВМ с загрузкой UEFI из шаблона, в образе QCOW2 уже должна быть включена загрузка UEFI.
- Для авторизации команд OpenStack должен быть настроен клиент интерфейса командной строки OpenStack, как описано в разделе "Подключение к интерфейсу командной строки OpenStack" на странице 427.

Чтобы создать виртуальную машину с загрузкой UEFI из шаблона

1. Определите идентификатор нужного шаблона с UEFI, например:

   ```
   # openstack --insecure image list | grep centos.qcow2
   | 007db63f-9b41-4918-b572-2c5eef4c8f4b | centos7.qcow2 | active |
   ```

2. Укажите микропрограмму UEFI для этого шаблона с помощью свойства hw_firmware_type, например:

```
# openstack --insecure image set --property hw_firmware_type=uefi 007db63f-9b41-4918-b572-2c5eef4c8f4b
```

3. Создайте ВМ из этого шаблона в интерфейсе командной строки или пользовательском интерфейсе.

Чтобы создать виртуальную машину с загрузкой UEFI из образа ISO

1. Определите идентификатор нужного ISO-образа, например:

```
# openstack --insecure image list | grep centos.iso
| c9d6f6e9-9c6d-4d1c-824f-c3542f70fdb0 | centos7.iso | active |
```

2. Укажите микропрограмму UEFI для этого ISO-образа с помощью свойства hw_firmware_type, например:

```
# openstack --insecure image set --property hw_firmware_type=uefi c9d6f6e9-9c6d-4d1c-824f-c3542f70fdb0
```

3. Создайте ВМ из этого ISO-образа в интерфейсе командной строки или пользовательском интерфейсе.
4. Когда ВМ запустится, выключите ее, а затем укажите микропрограмму UEFI для загрузочного тома этой ВМ с помощью свойства hw_firmware_type. Например, если идентификатор загрузочного тома – 12d360f4-afe8-48c9-af24-7f048dcec0c9, выполните следующую команду:

```
# openstack --insecure volume set --image-property hw_firmware_type=uefi 12d360f4-afe8-48c9-af24-7f048dcec0c9
```

5. Запустите ВМ и продолжите установку гостевой ОС.

7.6.2.17 Создание дисков virtIO для виртуальных машин

Чтобы повысить производительность ввода-вывода виртуальных машин, с ними можно использовать диски virtIO. По умолчанию виртуальные машины создаются с дисками, присоединенными к шине SCSI, что нельзя изменить позже.

Можно создать том для ВМ и присоединить его к шине virtIO во время развертывания ВМ с помощью утилиты vinfra. Этот метод может применяться для создания загрузочных томов из образов ISO и шаблонов (QCOW2). Его также можно использовать для присоединения незагрузочных томов. Обратите внимание, что нужно будет использовать утилиту vinfra каждый раз при создании виртуальной машины.

Как вариант, можно применить свойство шины virtIO к образу через средство командной строки OpenStack. Это свойство позволяет создать несколько ВМ из настроенных образов в интерфейсе командной строки, а также на панелях администрирования и самообслуживания. Однако оно работает только для шаблонов.

Предварительные требования

- Образ загружен в вычислительный кластер, как описано в разделе "Подготовка загрузочного носителя для виртуальных машин" на странице 437.
- Для авторизации выполнения приведенных ниже команд настроен клиент командной строки OpenStack, как описано в разделе "Подключение к интерфейсу командной строки OpenStack" на странице 427.

Чтобы создать виртуальную машину с томом virtIO

Используйте параметр --volume bus=virtio при выполнении команды vinfra service compute server create.

Пример 1. Чтобы создать ВМ из QCOW2-образа mytemplate, выполните:

```
# vinfra service compute server create myvm1 --network id=private,fixed-ip=192.168.128.100 --flavor medium\
--volume source=image,id=mytemplate,bus=virtio,size=100
```

Пример 2. Чтобы создать ВМ из ISO-образа myiso, выполните:

```
# vinfra service compute server create myvm2 --network id=private,fixed-ip=192.168.128.100 --flavor medium\
--volume source=blank,size=100,bus=virtio,boot-index=0,type=disk \
--volume source=image,id=myiso,size=5,boot-index=1,type=cdrom
```

После создания ВМ все добавляемые к ней тома будут присоединяться к шине virtIO.

Чтобы создать виртуальную машину из шаблона virtIO

1. Примените свойство шины virtIO к шаблону. Например:

   ```
   # openstack --insecure image set mytemplate --property hw_disk_bus=virtio
   ```

2. Создайте том из шаблона virtIO. Например:

   ```
   # openstack --insecure volume create --image=mytemplate --size=10 myvolume
   ```

3. Создайте ВМ с новым томом. Например:

   ```
   # openstack --insecure server create myvm --volume=myvolume --flavor small --network public
   ```

После создания ВМ все добавляемые к ней тома будут присоединяться к шине virtIO.

7.6.2.18 Выполнение команд в виртуальных машинах без сетевого подключения

Если по какой-то причине у ВМ нет доступа к сети, вы все равно можете выполнять на ней команды с сервера, на котором она расположена.

Вам потребуется идентификатор ВМ, который можно получить с помощью команды vinfra service compute server list. Вы также можете использовать имя домена virsh, которое можно получить с помощью команды virsh list.

Предварительные требования

- На ВМ должны быть установлены дополнения гостевой ОС (см. раздел "Установка дополнений гостевой ОС" на странице 471).

Чтобы выполнять команды внутри ВМ без сетевого подключения

Windows

Чтобы выполнить произвольную команду внутри ВМ Windows и получить вывод на консоль, используйте команду virsh x-exec, например:

```
# virsh x-exec bbf4a6ec-865f-4e2c-ac21-8639d1bfb85c --shell dir c:\\
 Volume in drive C has no label.
 Volume Serial Number is D0BE-A8D1

 Directory of c:\

06/10/2009  01:42 PM            24 autoexec.bat
06/10/2009  01:42 PM            10 config.sys
07/13/2009  06:37 PM    <DIR>      PerfLogs
11/12/2018  07:45 AM    <DIR>      Program Files
11/12/2018  07:55 AM    <DIR>      test
11/12/2018  06:23 AM    <DIR>      Users
11/12/2018  07:53 AM    <DIR>      Windows
               2 File(s)         34 bytes
               5 Dir(s)  59,329,495,040 bytes free
```

Чтобы скопировать файл на ВМ Windows, используйте команды virsh x-exec и prl_cat, например:

```
# virsh x-exec bbf4a6ec-865f-4e2c-ac21-8639d1bfb85c \
--shell '%programfiles%\\qemu-ga\\prl_cat' 'c:\test\test.file' < /home/test.file
```

Чтобы получить файл с ВМ Windows, используйте команды virsh x-exec и type, например:

```
# virsh x-exec bbf4a6ec-865f-4e2c-ac21-8639d1bfb85c \
--shell type 'c:\test\test.file' > test.file
```

Linux

Чтобы выполнить произвольную команду внутри ВМ Linux и получить вывод на консоль, используйте команду virsh x-exec, например:

```
# virsh x-exec 1d45a54b-0e20-4d5e-8f11-12c8b4f300db /usr/bin/bash -c 'lsblk'
NAME      MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
loop0       7:0    0 945.9M  1 loop
loop1       7:1    0     5G  1 loop
```

```
├ —live-rw  253:0   0    5G  0 dm  /
└ —live-base 253:1   0    5G  1 dm
loop2       7:2    0   32G  0 loop
└ —live-rw  253:0   0    5G  0 dm  /
sda         8:0    0   64G  0 disk
sdc         8:32   0    1G  1 disk
sr0        11:0    1    2G  0 rom  /run/initramfs/live
```

Чтобы скопировать файл на ВМ Linux, используйте команды virsh x-exec и cat, например:

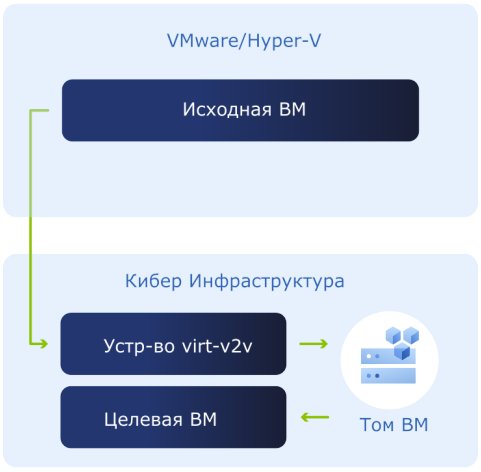
```
# virsh x-exec 1d45a54b-0e20-4d5e-8f11-12c8b4f300db \
--shell 'cat > test.file' < /home/test.file
```

Чтобы получить файл с ВМ Linux, используйте те же команды virsh x-exec и cat, например:

```
# virsh x-exec 1d45a54b-0e20-4d5e-8f11-12c8b4f300db \
--shell 'cat /home/test.file' > test.file
```

7.6.2.19 Миграция виртуальных машин в Кибер Инфраструктуру

Начиная с версии Кибер Инфраструктура 3.5 миграция виртуальных машин из VMware vCenter 5.0 (и выше) и Hyper-V в Кибер Инфраструктура может осуществляться с помощью инструмента virt-v2v. Для этого необходимо создать виртуальную машину устройства virt-v2v для передачи и преобразования данных.



Миграция виртуальных машин из VMware vCenter доступна в автономном и онлайн режимах, миграция виртуальных машин из Hyper-V доступна только в автономном режиме (подробнее см. в разделах "Миграция виртуальных машин в Кибер Инфраструктуру в автономном режиме" на странице 515 и "Миграция виртуальных машин в Кибер Инфраструктуру онлайн" на странице 518).

Примечание

Для миграции виртуальных машин также можно использовать Кибер Бэкап (есть ограничения). Подробные сведения см. в документации по Кибер Бэкап.

Развертывание виртуальной машины устройства

Чтобы создать ВМ устройства virt-v2v, выполните следующие действия:

1. Загрузите образ устройства virt-v2v из официального репозитория.
2. Загрузите образ в Кибер Инфраструктура. Например:

   ```
   # vinfra service compute image create virt-v2v-img --file cyber-infrastructure-migration-appliance.qcow2
   ```

3. Создайте ключ SSH для устройства, если у вас его нет. Например:

   ```
   # vinfra service compute key create publickey --public-key virt-v2v-app-key.pub
   ```

4. Создайте виртуальную машину и разверните в ней загруженный образ. Виртуальной машине необходимы 2 ЦП, 4 ГБ ОЗУ и достаточно места для хранения, чтобы разместить самую большую виртуальную машину, подлежащую миграции в Кибер Инфраструктура. Также необходимо подключение к сети, обрабатывающей тип трафика **Compute API**.

   Если планируется миграция ВМ в онлайн режиме (подробнее см. в разделе "Миграция виртуальных машин в Кибер Инфраструктуру онлайн" на странице 518), необходимо подключение к сети с доступом к VMware vCenter API.

   Например:

   ```
   # vinfra service compute server create virt-v2v-appliance --flavor medium --key-name <key> --network id=<compute_API> --network id=<vcenter_API> --volume source=image,id=virt-v2v-img,size=<size>
   ```

   Где:

   - <key> – ключ SSH для авторизации в виртуальной машине устройства.
   - <compute_API> – сеть с типом трафика **Compute API**.
   - <vcenter_API> – сеть с доступом к VMware vCenter API.
   - <size> – размер диска (должен соответствовать размеру самой большой виртуальной машины для онлайн-миграции и превышать его в два раза для оффлайн-миграции).

Настройка аутентификации на виртуальной машине устройства

Предварительные требования

- Виртуальная машина устройства virt-v2v развернута в соответствии с инструкциями в разделе "Развертывание виртуальной машины устройства" выше.

Для настройки аутентификации виртуальной машины устройства необходимо

1. Войти в виртуальную машину устройства как пользователь admin с ключом SSH.
2. Получить привилегии администратора с помощью команды sudo -i, например.
3. Создать скрипт, который будет экспортировать учетные данные OpenStack:

```
# cat > user-openrc.sh << EOF
export OS_PROJECT_DOMAIN_NAME=Domain_name
export OS_USER_DOMAIN_NAME=Domain_name
export OS_PROJECT_NAME=Project_name
export OS_USERNAME=user_name
export OS_PASSWORD=Password
export OS_AUTH_URL=https://<admin_panel_IP_addr>:5000/v3
export OS_IDENTITY_API_VERSION=3
export OS_INSECURE=true
export NOVACLIENT_INSECURE=true
export NEUTRONCLIENT_INSECURE=true
export CINDERCLIENT_INSECURE=true
export LIBGUESTFS_BACKEND=direct
EOF
```

Примечание
Вам потребуются учетные данные администратора для проекта, которому принадлежит виртуальная машина устройства.

4. Скопировать корневой сертификат ЦС OpenStack и ключи ЦС с узла управления Кибер Инфраструктура:

```
# scp root@<MN_IP>:/usr/libexec/vstorage-ui-backend/ca/ca.* /etc/pki/ca-trust/source/anchors/
# update-ca-trust extract
```

Где <MN_IP> – это IP-адрес узла управления. Для дополнительной информации см. раздел "Защита трафика API OpenStack с помощью SSL" на странице 181.

5. Для миграции виртуальных машин из VMware vCenter необходимо создать файл с паролем VMware vCenter для передачи в virt-v2v. Например:

```
# echo $vCenterPass > password.txt
```

Также вы можете ввести пароль во время миграции или предоставить его virt-v2v с опцией --password-file.

Миграция виртуальных машин в Кибер Инфраструктуру в автономном режиме

Для миграции виртуальных машин в Кибер Инфраструктуру в автономном режиме скопируйте виртуальную машину VMware vCenter/Hyper-V на виртуальную машину устройства virt-v2v (например, с помощью USB-накопителя) и преобразуйте ВМ в формат, используемый в Кибер Инфраструктуре.

Ограничения

- Миграция виртуальных машин возможна на основе VMware vCenter версии 5.0 или более поздней.

Предварительные требования

- Аутентификация настроена на виртуальной машине устройства, как описано в разделе "Настройка аутентификации на виртуальной машине устройства" на странице 514.
- Необходимо удалить инструменты VMware с виртуальных машин Windows перед миграцией, чтобы избежать проблем при последующей загрузке. Инструменты VMware будут автоматически удалены из гостевых систем Linux.

Миграция виртуальной машины из VMware vCenter в автономном режиме

1. Скопируйте все файлы виртуальной машины, включая vmdk и vmx, на USB-накопитель.
2. Подключите USB-накопитель к хосту в той же локальной сети, что и виртуальная машина устройства.
3. Войдите в виртуальную машину устройства как пользователь admin, используя ключ SSH.
4. Получите привилегии администратора с помощью команды sudo -i.
5. Скопируйте файлы виртуальной машины, используя, например, команду rsync или scp.
6. Установите учетные данные OpenStack:

   ```
   # source user-openrc.sh
   ```

7. Перенесите виртуальную машину в том Кибер Инфраструктуры, указав политику хранения. Для получения списка доступных политик хранения, запустите команду vinfra service compute storage-policy list в Кибер Инфраструктуре. Например:

   ```
   # virt-v2v -i libvirtxml <VM_config> -o openstack \
   -oo server-id=635ae4cc-4c01-461a-ae63-91ca4187a7b1 -os <policy_name>
   ```

   Где <VM_config> – это файл конфигурации виртуальной машины в формате vmx, а <policy_name> – это политика хранения преобразованного тома.
8. Узнайте идентификатор или имя нового тома. Например:

   ```
   # openstack --insecure volume list
   +----------------------+------+-----------+------+-------------+
   | ID                   | Name | Status    | Size | Attached to |
   +----------------------+------+-----------+------+-------------+
   | 024b6843-2de3-<...> | sda1 | available |   64 |             |
   +----------------------+------+-----------+------+-------------+
   ```

9. При использовании виртуальной машиной микропрограммы UEFI, вручную установите правильный дистрибутив ОС и тип микропрограммы UEFI для преобразованного тома. Чтобы получить список доступных дистрибутивов, запустите команду vinfra service compute show в Кибер Инфраструктура. Например:

```
# openstack --insecure volume set sda1 --image-property os_distro=win2k8
# openstack --insecure volume set sda1 --image-property hw_firmware_type=uefi
```

10. Создайте виртуальную машину на основе нового тома в Кибер Инфраструктуре. Например:

```
# vinfra service compute server create migratedvm --network id=private \
--network id=public --volume source=volume,id=sda1,size=64 --flavor medium
```

После миграции рекомендуется установить гостевые инструменты внутри виртуальной машины. Установка гостевых инструментов предотвратит возможные проблемы с взаимодействием с гостевой ОС через консоль VNC.

Миграция виртуальной машины из Hyper-V в автономном режиме

1. Скопируйте все файлы виртуальной машины из Hyper-V на виртуальную машину с virt-v2v (например, с помощью USB-накопителя).
2. Установите учетные данные OpenStack:

```
# source user-openrc.sh
```

3. Преобразуйте диски виртуальной машины из Hyper-V в тома Кибер Инфраструктуры. Например, для виртуальной машины с одним диском:

```
# virt-v2v -i disk <hyper-v-vm-disk>.vhdx -o openstack -oo server-id=<virt-v2v-vm-id>
```

Где <hyper-v-vm-disk> – это имя диска скопированной виртуальной машины, а <virt-v2v-vm-id> – это имя или идентификатор ВМ устройства virt-v2v.

Или для виртуальной машины с несколькими дисками:

```
# virt-v2v -i libvirtxml <libvirt-xml> -o openstack -oo server-id=<virt-v2v-vm-id>
```

Где libvirt-xml – это XML-файл, который содержит пути к дискам ВМ, скопированной из Hyper-V.

Пример XML-файла:

```
<domain type='kvm'>
    <name>hyp-ws22-migrated</name>
    <devices>
        <disk type='file' device='disk'>
            <source file='/root/hyp-ws22.vhdx'/>
        </disk>
        <disk type='file' device='disk'>
            <source file='/root/hyp-ws22-d2.vhdx'/>
        </disk>
        <disk type='file' device='disk'>
            <source file='/root/hyp-ws22-d3.vhdx'/>
        </disk>
    </devices>
</domain>
```

4. Узнайте идентификатор или имя нового тома. Например:

```
# openstack --insecure volume list
+--------------------+------+-----------+------+-------------+
| ID                 | Name | Status    | Size | Attached to |
+--------------------+------+-----------+------+-------------+
| 024b6843-2de3-<...> | sda1 | available |   64 |             |
+--------------------+------+-----------+------+-------------+
```

5. При использовании виртуальной машиной микропрограммы UEFI, вручную установите правильный дистрибутив ОС и тип микропрограммы UEFI для преобразованного тома. Чтобы получить список доступных дистрибутивов, запустите команду vinfra service compute show в Кибер Инфраструктура. Например:

```
# openstack --insecure volume set sda1 --image-property os_distro=win2k8
# openstack --insecure volume set sda1 --image-property hw_firmware_type=uefi
```

6. Создайте виртуальную машину на основе нового тома в Кибер Инфраструктуре. Например:

```
# vinfra service compute server create migratedvm --network id=private \
--network id=public --volume source=volume,id=sda1,size=64 --flavor medium
```

После миграции рекомендуется установить гостевые инструменты внутри виртуальной машины. Установка гостевых инструментов предотвратит возможные проблемы с взаимодействием с гостевой ОС через консоль VNC.

Миграция виртуальных машин в Кибер Инфраструктуру онлайн

Ограничения

- Миграция виртуальных машин возможна на основе VMware vCenter версии 5.0 или более поздней.

Предварительные требования

- Аутентификация настроена на виртуальной машине устройства, как описано в разделе "Настройка аутентификации на виртуальной машине устройства" на странице 514.
- Необходимо удалить инструменты VMware с виртуальных машин Windows перед миграцией, чтобы избежать проблем при последующей загрузке. Инструменты VMware будут автоматически удалены из гостевых систем Linux.

Миграция виртуальной машины из VMware vCenter онлайн

1. Войдите в виртуальную машину устройства как пользователь admin, используя ключ SSH.
2. Получите привилегии администратора с помощью команды sudo -i.
3. Установите учетные данные OpenStack:

```
# source user-openrc.sh
```

4. Проверьте соединение между libvirt и VMware vCenter. Например:

```
# virsh -c 'vpx://<domain>%5c<user>@<hostname>?no_verify=1' list --all
Enter root's password for vcenter.example.com: ***
+----+--------------+----------+
| Id | Name         | <...>    |
+----+--------------+----------+
| -  | Fedora 20    | <...>    |
| -  | Windows 2008 | <...>    |
+----+--------------+----------+
```

Где <hostname> — это имя хоста VMware ESXi, на котором работают виртуальные машины. Его полный путь выглядит как <vCenter_hostname>/<datacenter_name>/<cluster_name>/<server_hostname>, и его можно найти в VMware vCenter.

Если имя пользователя VPX содержит обратную косую черту (например, <domain>\<user>), замените ее с помощью %5c: <domain>%5c<user>. Также замените пробелы с помощью %20.

5. Проверьте соединение с OpenStack и узнайте идентификатор устройства virt-v2v. Например:

```
# openstack --insecure server list
+--------------------------------------+--------------------+--------+--------+
| ID                                   | Name               | Status | <...> |
+--------------------------------------+--------------------+--------+--------+
| 635ae4cc-4c01-461a-ae63-91ca4187a7b1 | virt-v2v-appliance | ACTIVE | <...> |
+--------------------------------------+--------------------+--------+--------+
```

6. Выключите виртуальную машину. Сеансы виртуальных машин Windows должны быть корректно завершены, чтобы миграция прошла успешно.
7. Перенесите виртуальную машину в том Кибер Инфраструктуры, указав политику хранения. Чтобы получить список доступных политик хранения, запустите команду vinfra service compute storage-policy list в Кибер Инфраструктуре. Например:

```
# virt-v2v -ip password.txt -ic 'vpx://<domain>%5c<user>@<hostname>\
?no_verify=1' 'Windows 2008' -o openstack -oo server-id=635ae4cc-\
4c01-461a-ae63-91ca4187a7b1 -os <policy_name>
```

Где <policy_name> — это политика хранения преобразованного тома.

8. Узнайте идентификатор или имя нового тома. Например:

```
# openstack --insecure volume list
+--------------------+------+-----------+------+-------------+
| ID                 | Name | Status    | Size | Attached to |
+--------------------+------+-----------+------+-------------+
| 024b6843-2de3-<...> | sda1 | available |   64 |             |
+--------------------+------+-----------+------+-------------+
```

9. При использовании виртуальной машиной микропрограммы UEFI, вручную установите правильный дистрибутив ОС и тип микропрограммы UEFI для преобразованного тома. Чтобы получить список доступных дистрибутивов, запустите команду vinfra service compute show в Кибер Инфраструктуре. Например:

```
# openstack --insecure volume set sda1 --image-property os_distro=win2k8
# openstack --insecure volume set sda1 --image-property hw_firmware_type=uefi
```

10. Создайте виртуальную машину на основе нового тома в Кибер Инфраструктуре. Например:

```
# vinfra service compute server create migratedvm --network id=private \
--network id=public --volume source=volume,id=sda1,size=64 --flavor medium
```

После миграции рекомендуется установить гостевые инструменты внутри виртуальной машины. Установка гостевых инструментов предотвратит возможные проблемы с взаимодействием с гостевой ОС через консоль VNC.

7.6.2.20 Аварийное восстановление виртуальных машин

Если возникают проблемы с загрузкой ВМ, можно перевести ее в режим аварийного восстановления для доступа к загрузочному тому. Когда ВМ в состоянии «Запущена» переводится в режим аварийного восстановления, сначала выполняется мягкая остановка. После того как ВМ перейдет в режим аварийного восстановления, к ней можно подключиться через SSH или консоль. Предыдущий загрузочный диск ВМ теперь присоединен как вторичный. Можно подключить этот диск и исправить на нем ошибки.

Ограничения

- В режиме аварийного восстановления ISO-образы могут использоваться для загрузки виртуальных машин как Linux, так и Windows, а образы (шаблоны) QCOW2 – для загрузки ВМ Linux. Для инструкций о создании шаблонов см. раздел "Подготовка шаблонов" на странице 440.
- ВМ можно перевести в режим аварийного восстановления, только если ее текущее состояние «Запущена» или «Выключена».
- Для ВМ в режиме аварийного восстановления доступны только три действия: **Консоль**, **Выйти из режима восстановления** и **Удалить**.
- Если в образе для аварийного восстановления установлен пакет cloud-init, то к ВМ, загруженной из образа, можно будет получить доступ с помощью того же SSH-ключа, который использовался для ее создания.

Предварительные требования

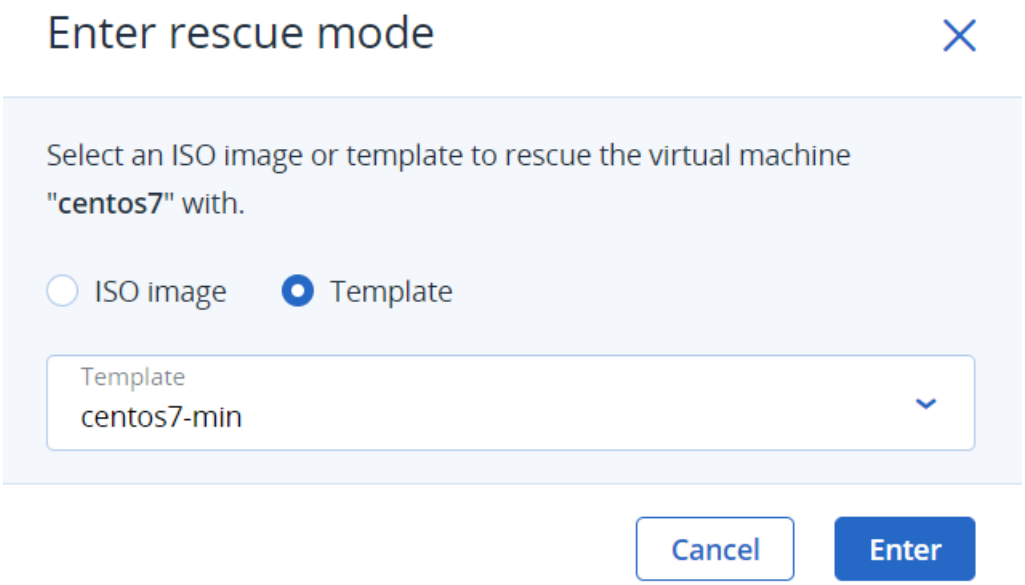
- Созданы виртуальные машины, как описано в разделе "Создание виртуальных машин" на странице 460.

Чтобы перевести виртуальную машину в режим аварийного восстановления

Панель администратора

1. Перейдите на **Вычисления** > **Виртуальные машины** > вкладка **Виртуальные машины**. На вкладке **Виртуальные машины** щелкните по нужной ВМ в списке.
2. На правой панели ВМ нажмите кнопку с многоточием на панели инструментов. Затем нажмите **Войти в режим восстановления**.

3. В окне **Войти в режим восстановления** выберите образ для восстановления ВМ. По умолчанию выбран образ, который использовался для создания ВМ. Нажмите **Войти**.



Статус машины изменится на «Восстановление».

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server rescue [--image <image>] <server>
```

<server>

Идентификатор или имя виртуальной машины

--image <image>

Загрузка из образа с указанным идентификатором или именем

Напрмир, чтобы перевести виртуальную машину myvm в режим аварийного восстановления с использованием образа cirros, выполните:

```
# vinfra service compute server rescue myvm --image cirros
```

Чтобы вернуть виртуальную машину в режим нормальной работы

Панель администратора

1. Перейдите на **Вычисления** > **Виртуальные машины** > вкладка **Виртуальные машины**. На вкладке **Виртуальные машины** щелкните по нужной ВМ в списке.
2. На правой панели ВМ нажмите **Выйти из режима восстановления**.
3. В окне **Выйти из режима восстановления** нажмите **Выйти**. ВМ автоматически перезагрузится.

Статус ВМ сменится на «Запущена», и ВМ загрузится с исходного корневого диска.

Примечание

Если при выходе из режима аварийного восстановления статус ВМ изменится на «Ошибка», его можно сбросить с помощью действия **Сбросить состояние**. После этого ВМ должна вернуться в состояние «Восстановление».

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server unrescue <server>
```

<server>

Идентификатор или имя виртуальной машины

Например, чтобы вернуть виртуальную машину myvm в нормальные режим работы, выполните:

```
# vinfra service compute server unrescue myvm
```

Выход из режима аварийного восстановления для виртуальных машин Windows

При выходе ВМ Windows из режима аварийного восстановления может возникать проблема. Если в этом режиме установить статус «в сети» для исходного системного диска, то его идентификатор становится таким же, как идентификатор диска аварийного восстановления. После этого при попытке выйти из режима аварийного восстановления загрузчик не может найти правильный загрузочный диск. Чтобы разрешить конфликт идентификаторов, выполните следующие действия.

1. Когда ВМ находится в режиме аварийного восстановления, откройте окно **Управление дисками** и запомните номер исходного системного диска (не в сети) и диска аварийного восстановления (в сети). Установите для исходного системного диска статус **В сети**.
2. Чтобы изменить конфигурацию загрузки, введите следующую команду в окне **Командная строка**:

   ```
   > bcdedit /store <the original system disk name>:\boot\bcd
   ```

3. Просмотрите выходные данные и убедитесь, что диск аварийного восстановления является целевым для объектов (partition=<the rescue disk name>).

   Если объекты не указывают на диск C, исправьте это следующими командами:

   ```
   > bcdedit /store <the original system disk name>:\boot\bcd \
   /set {default} osdevice partition=<the rescue disk name>:
   > bcdedit /store <the original system disk name>:\boot\bcd \
   /set {default} device partition=<the rescue disk name>:
   > bcdedit /store <the original system disk name>:\boot\bcd \
   /set {bootmgr} device partition=<the rescue disk name>:
   > bcdedit /store <the original system disk name>:\boot\bcd \
   /set {memdiag} device partition=<the rescue disk name>:
   ```

4. Чтобы просмотреть доступные диски, введите в командной строке следующие команды:

```
> DISKPART
> LIST DISK
```

   Сопоставьте номер и имя диска с указанными в окне **Управление дисками**.

5. Чтобы получить идентификатор диска аварийного восстановления, выполните следующие команды:

```
> SELECT DISK <the rescue disk number>
> UNIQUEID DISK
```

   Запишите идентификатор диска, он понадобится позже.

6. Измените этот идентификатор с помощью следующей команды:

```
> UNIQUEID DISK id=<any hex value of 8 characters>
```

   Убедитесь, что значение изменилось, с помощью команды UNIQUEID DISK.

7. Назначьте исходному системному диску записанный ранее идентификатор.

```
> SELECT DISK <the original system disk number>
> UNIQUEID DISK id=<the recorded disk ID>
```

   Убедитесь, что значение изменилось, с помощью команды UNIQUEID DISK.

Теперь можно будет выйти из режима аварийного восстановления.

Как добавить драйверы дисков в среду восстановления Windows (Windows Recovery Environment)

Для отображения дисков виртуальной машины в среде восстановления Windows необходимо, чтобы в WIM-образе, используемом для загрузки среды восстановления, присутствовали необходимые драйверы. Эти драйверы расположены на диске A:, который подключен по умолчанию к виртуальным машинам с операционной системой Windows.

Например, чтобы добавить необходимые драйверы в WIM-образ среды восстановления Windows на рабочей виртуальной машине, выполните следующие действия:

1. Запустите интерпретатор командной строки от имени администратора.
2. Создайте папку, к которой будет подключен WIM-образ среды восстановления. Например:

```
md C:\mount
```

3. Подключите WIM-образ среды восстановления к созданной папке. Например:

```
ReAgentC.exe /mountre /path c:\mount
```

4. Добавьте необходимые драйверы в подключенный WIM-образ. Например:

```
Dism /Image:C:\mount /Add-Driver /Driver:"A:\Drivers\NetKVM\w10\amd64\netkvm.inf"
Dism /Image:C:\mount /Add-Driver /Driver:"A:\Drivers\vioscsi\w10\amd64\vioscsi.inf"
Dism /Image:C:\mount /Add-Driver /Driver:"A:\Drivers\viostor\w10\amd64\viostor.inf"
```

5. Сохраните изменения и отключите WIM-образ от папки. Например:

```
ReAgentC.exe /unmountre /path c:\mount /commit
```

После загрузки среды восстановления Windows, использующей обновленный WIM-образ, будут отображаться диски виртуальной машины.

7.6.2.21 Управление образами

Образы, хранящиеся в вычислительном кластере, можно загружать на клиентские машины, также их можно изменять и удалять.

Ограничения

- Образы хранятся в соответствии с политикой хранения по умолчанию.
- При установке балансировщика нагрузки или сервиса Kubernetes в вычислительном кластере появляются специальные образы, которые используются системой для создания ВМ сервиса. Такие образы имеют метку **Система** и не могут быть изменены или удалены на панели администрирования.

Предварительные требования

- Образы должны быть добавлены в вычислительный кластер, как описано в разделе "Загрузка образов виртуальных машин" на странице 437.

Чтобы загрузить образ

Панель администратора

1. Перейдите на вкладку **Вычисления** > **Виртуальные машины** > **Образы** и нажмите кнопку с многоточием рядом с нужным образом.
2. Нажмите **Загрузить образ**.

Образ будет загружен на вашу машину.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute image save [--file <filename>] <image>
```

--file <filename>

Файл, в который следует сохранить образ (по умолчанию stdout)

<image>

Идентификатор или имя образа

Например, чтобы загрузить стандартный образ Cirros на локальный диск как cirros.qcow2, выполните:

```
# vinfra service compute image save cirros --file cirros.qcow2
```

Чтобы изменить образ

Панель администратора

1. Перейдите на вкладку **Вычисления** > **Виртуальные машины** > **Образы** и щелкните по нужному образу.
2. На правой панели образа щелкните по значку карандаша рядом с параметром, который необходимо изменить. Можно изменить имя образа, тип операционной системы и параметры доступа сети. Для шаблонов здесь также можно изменять минимальный размер тома.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute image set [--min-disk <size-gb>] [--min-ram <size-mb>] [--os-distro <os-distro>]
                                 [--protected | --unprotected] [--public] [--private] [--name <name>] <image>
```

--min-disk <size-gb>
: Минимальный размер диска, необходимый для загрузки с образа, в гигабайтах

--min-ram <size-mb>
: Минимальный размер ОЗУ, необходимый для загрузки с образа, в мегабайтах

--os-distro <os-distro>
: Дистрибутив ОС. Чтобы вывести список доступных дистрибутивов, выполните команду vinfra service compute show.

--protected
: Защита образа от удаления

--unprotected
: Разрешает удалять образ.

--public
: Делает образ доступным для всех пользователей.

--private
: Делает образ доступным только владельцам.

--name <name>
: Имя образа

<image>
: Идентификатор или имя образа

Например, чтобы сделать образ cirros доступным для всех пользователей и задать для него минимальный размер ОЗУ в 1 ГБ, выполните:

```
# vinfra service compute image set cirros --public --min-ram 1
```

Чтобы просмотреть сведения об образе

Панель администратора

Перейдите на вкладку **Вычисления** > **Виртуальные машины** > **Образы** и щелкните по нужному образу. На правой панели будут отображены сведения об этом образе.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute image show <image>
```

<image>

Идентификатор или имя образа

Например, чтобы вывести сведения о стандартном образе Cirros, выполните:

```
# vinfra service compute image show 4741274f-5cca-4205-8f66-a2e89fb346cc
+------------------+------------------------------------------------------+
| Field            | Value                                                |
+------------------+------------------------------------------------------+
| checksum         | 443b7623e27ecf03dc9e01ee93f67afe                     |
| container_format | bare                                                 |
| created_at       | 2018-09-11T13:29:10Z                                 |
| disk_format      | qcow2                                                |
| file             | /api/v2/compute/images/4741274f-5cca-<...>/file/     |
| id               | 4741274f-5cca-4205-8f66-a2e89fb346cc                 |
| min_disk         | 1                                                    |
| min_ram          | 0                                                    |
| name             | cirros                                               |
| os_distro        | linux                                                |
| os_type          | linux                                                |
| placements       | []                                                   |
| project_id       | 72a5db3a033c403a86756021e601ef34                     |
| protected        | False                                                |
| public           | True                                                 |
| size             | 12716032                                             |
| status           | active                                               |
| tags             | []                                                   |
| updated_at       | 2018-09-11T13:29:13Z                                 |
| virtual_size     |                                                      |
+------------------+------------------------------------------------------+
```

Чтобы удалить образ

Панель администратора

1. Перейдите на вкладку **Вычисления** > **Виртуальные машины** > **Образы** и нажмите кнопку с многоточием рядом с нужным образом.
2. Нажмите кнопку **Удалить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute image delete <image>
```

<image>

Идентификатор или имя образа

Например, чтобы удалить образ cirros, выполните:

```
# vinfra service compute image delete cirros
```

7.6.2.22 Поиск и устранение неисправностей виртуальных машин

Если не удается развернуть виртуальную машину

Просмотрите сообщение об ошибке на правой панели ВМ. Одной из возможных причин сбоя может быть нехватка свободных ресурсов ОЗУ или ЦП для размещения ВМ.

Если виртуальная машина зависла в состоянии сбоя или переходном состоянии

Панель администратора

Сбросьте ВМ в последнее стабильное состояние: активное, выключенное или с освобожденными ресурсами.

1. Щелкните по зависшей ВМ.
2. На правой панели ВМ нажмите **Сбросить состояние**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server reset-state [--state-error] <server>
```

--state-error

Сброс виртуальной машины в состояние ERROR

<server>

Идентификатор или имя виртуальной машины

Например, чтобы перевести виртуальную машину myvm из переходного состояния в предыдущее состояние, выполните:

```
# vinfra service compute server reset-state myvm
```

Если виртуальная машина зависла в процессе выполнения задачи "Выключение"

В этом случае ВМ будет иметь статус "Активна (Выключение)" на правой панели.

Вы можете отменить эту задачу, выполнив следующую команду:

```
vinfra service compute server cancel-stop <server>
```

<server>

Идентификатор или имя виртуальной машины

Например, чтобы отменить завершение работы гостевой ОС и вернуть виртуальную машину в активное состояние, выполните:

```
# vinfra service compute server cancel-stop myvm
```

Если не удается загрузить виртуальную машину

Панель администратора

Просмотрите журнал консоли виртуальной машины, щелкнув **Загрузить журнал консоли** на правой панели виртуальной машины. Журнал будет содержать сообщения только в том случае, если ведение журнала включено внутри самой виртуальной машины.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server log <server>
```

<server>

Идентификатор или имя виртуальной машины

Например, чтобы сохранить журнал виртуальной машины myvm в файл myvm.log, выполните:

```
# vinfra service compute server log myvm > myvm.log
```

Журнал будет содержать сообщения только в том случае, если ведение журнала включено внутри самой виртуальной машины.

7.6.2.23 Удаление виртуальных машин

Ограничения

- ВМ удаляется вместе с ее дисками, у которых при развертывании ВМ был включен параметр **Удалить по завершении**.

Предварительные требования

- Созданы виртуальные машины, как описано в разделе "Создание виртуальных машин" на странице 460.

Удаление одной виртуальной машины

Панель администратора

1. Нажмите кнопку с многоточием напротив ВМ, которую следует удалить, и выберите **Удалить**.
2. Нажмите **Удалить** в окне подтверждения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server delete <server>
```

<server>
    Идентификатор или имя виртуальной машины

Например, чтобы удалить виртуальную машину myvm, выполните:

```
# vinfra service compute server delete myvm
```

Удаление нескольких виртуальных машин

1. Установите флажки напротив ВМ, которые следует удалить.
2. Над списком ВМ нажмите **Удалить**.
3. Нажмите **Удалить** в окне подтверждения.

7.6.3 Управление вычислительной сетью

В продукте Кибер Инфраструктура в состав сетевых вычислительных компонентов входят вычислительные сети, группы безопасности, виртуальные маршрутизаторы, плавающие общедоступные IP-адреса и сетевые балансировщики нагрузки.

Предварительные требования

- Должен быть создан вычислительный кластер, как описано в разделе "Создание вычислительного кластера" на странице 169.

7.6.3.1 Управление вычислительными сетями

Кибер Инфраструктура защищает и изолирует виртуальные сети для виртуальных машин с помощью инкапсуляции VXLAN. Распределенная виртуальная коммутация и маршрутизация упрощают конфигурацию сетей на ВМ, а встроенный брандмауэр повышает их защищенность. Интегрированный DHCP-сервер, а также управление IP-адресами и DNS обеспечивают эффективную конфигурацию сети.

В вычислительном кластере можно создавать и контролировать два типа сетей:

- Виртуальные сети представляют собой оверлейные сети на основе VXLAN, которые могут использоваться для обмена данными между виртуальными машинами (ВМ). Каждая виртуальная сеть изолируется от других виртуальных сетей, так же как от физических. Виртуальные сети поддерживают управление только адресами IPv4.
- Физические сети используют диапазоны IP-адресов публичных сетей инфраструктуры. Такие сети могут использоваться для предоставления виртуальным машинам доступа к Интернету. Физические сети поддерживают управление адресами как IPv4, так и IPv6.

Ограничения

- При создании балансировщиков нагрузки или кластеров Kubernetes с высокой доступностью мастер-серверов в вычислительном кластере появляется виртуальная сеть **lb-mgmt-net**. Эта сеть используется системой для балансировки нагрузки. Она имеет метку **Система** и не может быть изменена или удалена.

Подключение виртуальных коммутаторов к магистральным интерфейсам

Если вы планируете использовать для виртуальных машин большое количество сетей на базе VLAN, можно воспользоваться автоматической процедурой создания таких сетей. При создании в вычислительном кластере сети на базе VLAN система автоматически создает связанную сеть инфраструктуры и настраивает сетевые интерфейсы VLAN на всех вычислительных узлах с помощью распределенного виртуального коммутатора.

Чтобы использовать автоматическое создание сетей на базе VLAN, рассмотрим следующие примеры:

- Если у магистральных сетевых интерфейсов есть виртуальный коммутатор (их имена имеют формат **br-<interface>**), можно приступать к созданию в вычислительном кластере сетей на базе VLAN.
- Если для магистральных сетевых интерфейсов не настроены ни сети VLAN, ни виртуальный коммутатор, назначьте инфраструктурной сети, подключенной к этим магистральным интерфейсам, тип трафика **ВМ внешн.** Виртуальный коммутатор будет автоматически настроен на магистральных сетевых интерфейсах после создания сети на базе VLAN.
- Если у вас есть сети VLAN, но на магистральных сетевых интерфейсах не настроен виртуальный коммутатор, сначала преобразуйте конфигурацию магистральных интерфейсов в конфигурацию виртуального коммутатора, как описано ниже.

Если сетевая конфигурация включает небольшое количество сетей на базе VLAN, можно создать сетевые интерфейсы VLAN отдельно на каждом вычислительном узле, как описано в разделе "Создание интерфейсов VLAN" на странице 131.

Ограничения

- Для сетей на базе VLAN соответствующие идентификаторы VLAN должны быть настроены на физических коммутаторах, подключенных к вычислительным узлам.

Чтобы подключить магистральный сетевой интерфейс к виртуальному коммутатору

1. Проверьте, могут ли сетевые интерфейсы VLAN, подключенные к вашей сети, быть преобразованы в Open vSwitch VLAN. Например:

```
# vinfra cluster network conversion precheck --network mynet
+--------------------+-------------------------------------------------+
| Field              | Value                                           |
+--------------------+-------------------------------------------------+
| affected_interfaces | - interface: eth0                              |
|                    |   node_id: 13cb6cbf-0b9b-be0f-bb56-8ed6a0e9225c |
|                    |   vlans:                                        |
|                    |   - eth0.1                                      |
|                    | - interface: eth0                               |
|                    |   node_id: 6e5d9e91-5c4e-a874-38cd-fe6f4bef10a4 |
|                    |   vlans:                                        |
|                    |   - eth0.1                                      |
|                    | - interface: eth0                               |
|                    |   node_id: 1053e85b-351c-6113-5623-e0c6c64995e7 |
|                    |   vlans:                                        |
|                    |   - eth0.1                                      |
| affected_networks  | - mynet                                         |
| physical_network   | Public                                          |
+--------------------+-------------------------------------------------+
```

2. Преобразуйте сетевые интерфейсы VLAN в Open vSwitch VLAN. Во время преобразования могут возникать перебои в подключении. Например:

```
# vinfra cluster network conversion start --network mynet
+---------+--------------------------------------+
| Field   | Value                                |
+---------+--------------------------------------+
| task_id | 058fc247-03a8-49fa-90e1-1e073dbafec9 |
+---------+--------------------------------------+
```

   Если магистральные сетевые интерфейсы не назначены ни одной инфраструктурной сети, укажите имя новой инфраструктурной сети, использовав параметр --physical-network-name <name>. Новая инфраструктурная сеть будет автоматически создана с указанным именем и назначена магистральным интерфейсам.

3. Проверьте статус преобразования. Например:

```
# vinfra cluster network conversion status 058fc247-03a8-49fa-90e1-1e073dbafec9
+--------------------+-------------------------------------------------+
| Field              | Value                                           |
+--------------------+-------------------------------------------------+
| affected_interfaces | - interface: eth0                              |
|                    |   node_id: 13cb6cbf-0b9b-be0f-bb56-8ed6a0e9225c |
|                    |   vlans:                                        |
|                    |   - eth0.1                                      |
|                    | - interface: eth0                               |
|                    |   node_id: 6e5d9e91-5c4e-a874-38cd-fe6f4bef10a4 |
|                    |   vlans:                                        |
|                    |   - eth0.1                                      |
```

```
|                | - interface: eth0                          |
|                |   node_id: 1053e85b-351c-6113-5623-e0c6c64995e7 |
|                |   vlans:                                   |
|                |   - eth0.1                                 |
| flow           | done                                       |
| physical_network | Public                                   |
| state          | success                                    |
| task_id        | 058fc247-03a8-49fa-90e1-1e073dbafec9       |
+----------------+--------------------------------------------+
```

По завершении преобразования можно будет создавать дополнительные сети VLAN на магистральных сетевых интерфейсах с помощью упрощенной процедуры.

Создание физических вычислительных сетей

В физических сетях могут размещаться несколько подсетей IPv4, IPv6 и с двойным стеком. Подсети IPv6 поддерживают три режима назначения IP-адресов: автоматическая конфигурация без отслеживания состояния (SLAAC), DHCPv6 без отслеживания состояния и DHCPv6 с отслеживанием состояния. Эти режимы описаны в следующей таблице:

Режим адресации IPv6	Назначение адреса ВМ	Конфигурация внешнего маршрутизатора	Конфигурация DHCP-сервера
SLAAC	ВМ получает адрес IPv6, шлюз по умолчанию и префикс подсети через объявления маршрутизатора (RA) с внешнего маршрутизатора. DNS-серверы и имя хоста не настраиваются автоматически.	Внешний маршрутизатор должен отправлять сообщения RA без флагов M (управляемая конфигурация адресов) и O (другая конфигурация).	Встроенный сервер DHCPv6 автоматически отключается.
DHCPv6 без отслеживания состояния	ВМ получает адрес IPv6 и шлюз по умолчанию через сообщения RA с внешнего маршрутизатора, а другую информацию (префикс подсети, DNS-серверы, имя хоста) со встроенного сервера DHCPv6.	Внешний маршрутизатор должен отправлять сообщения RA с флагом O.	Встроенный сервер DHCPv6 автоматически включается.
DHCPv6 с отслеживанием состояния	ВМ получает адрес IPv6 и другую информацию (префикс подсети, DNS-серверы, имя хоста) со встроенного сервера DHCPv6, а шлюз по умолчанию – через сообщения RA с внешнего маршрутизатора.	Внешний маршрутизатор должен отправлять сообщения RA с флагом M.	Встроенный сервер DHCPv6 автоматически включается.

Внимание

Назначение адреса IPv6 внутри виртуальной машины также зависит от сетевых параметров гостевой операционной системы.

Ограничения

- Поверх сети инфраструктуры можно создать только одну нетегированную физическую сеть.
- Когда предоставляется сетевой доступ ко всему домену, он настраивается только для существующих проектов внутри этого домена. Вновь созданные проекты не будут иметь доступа к сети.
- Нельзя подключать подсети IPv6 к маршрутизаторам. Как следствие, плавающие адреса IPv6 не поддерживаются.
- Адреса IPv6 не поддерживаются для балансировщиков нагрузки и кластеров Kubernetes.
- Виртуальная машина, которая подключена к сети с двойным стеком, всегда получает адрес IPv6, если для сети включен режим SLAAC или DHCPv6 без отслеживания состояния.
- Чтобы работать в подсети IPv6 с включенным режимом SLAAC посредством cloud-init, гостевая операционная система ВМ должна иметь версию cloud-init 19.4 или выше.

Предварительные требования

- Четкое понимание архитектуры вычислительных сетей, которая разъясняется в разделе "Архитектура вычислительных сетей" на странице 23.
- Для сетей на базе VLAN виртуальный коммутатор подключен к магистральному сетевому интерфейсу, как описано в разделе "Подключение виртуальных коммутаторов к магистральным интерфейсам" на странице 530.

Как добавить физическую вычислительную сеть

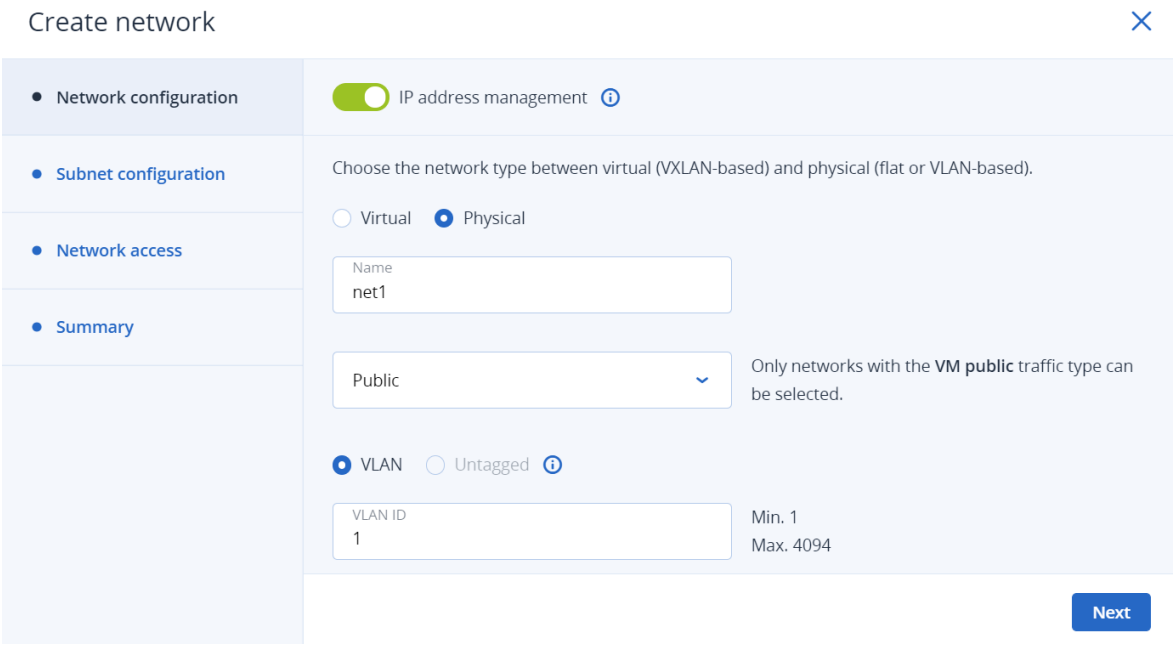
Панель администратора

1. На экране **Вычисления** > **Сеть** > **Сети** нажмите **Создать сеть**.
2. На шаге **Конфигурация сети** выполните следующие действия:
   a. Включите или отключите управление IP-адресами:
      - Если управление IP-адресами включено, встроенный DHCP-сервер автоматически назначит ВМ, подключенным к сети, IP-адреса из пулов IP-адресов, а также задаст для ВМ настраиваемые DNS-серверы. Кроме того, по умолчанию для всех сетевых портов ВМ будет включена защита от спуфинга. Каждый сетевой интерфейс ВМ сможет принимать и отправлять IP-пакеты, только если ему назначены IP- и MAC-адреса. При необходимости защиту от спуфинга для интерфейса ВМ можно отключить вручную.
      - Если управление IP-адресами отключено, то ВМ, подключенные к сети, получат IP-адреса от DHCP-серверов в этой сети (при их наличии). Кроме того, защита от спуфинга будет отключена для всех сетевых портов ВМ, и ее нельзя будет включить вручную. Это означает, что каждый сетевой интерфейс ВМ с назначенными IP- и MAC-адресами или без них сможет принимать и отправлять IP-пакеты.

      В любом случае можно будет вручную назначить статические IP-адреса изнутри виртуальных машин.
   b. Выберите тип сети **Физическая**.
   c. Укажите имя сети, а затем выберите сеть инфраструктуры с типом трафика **ВМ внешн**.

d. Чтобы создать сеть на базе VLAN, выберите **VLAN** и укажите идентификатор VLAN. Чтобы создать плоскую физическую сеть, выберите **Untagged** (Без тега).

e. Нажмите кнопку **Далее**.



3. Если вы включили управление IP-адресами, вы будете перенаправлены на шаг **Управление IP-адресами**, где можно добавить подсети IPv4 и IPv6.

- Как добавить подсеть IPv4

  a. В разделе **Подсети** нажмите **Добавить** и выберите **Подсеть IPv4**.

  b. В окне **Добавить подсеть IPv4** укажите диапазон адресов IPv4 сети, также при необходимости можно указать шлюз. Если оставить поле **Шлюз** пустым, то шлюз будет исключен из сетевых параметров.

  c. Включите или отключите встроенный DHCP-сервер:

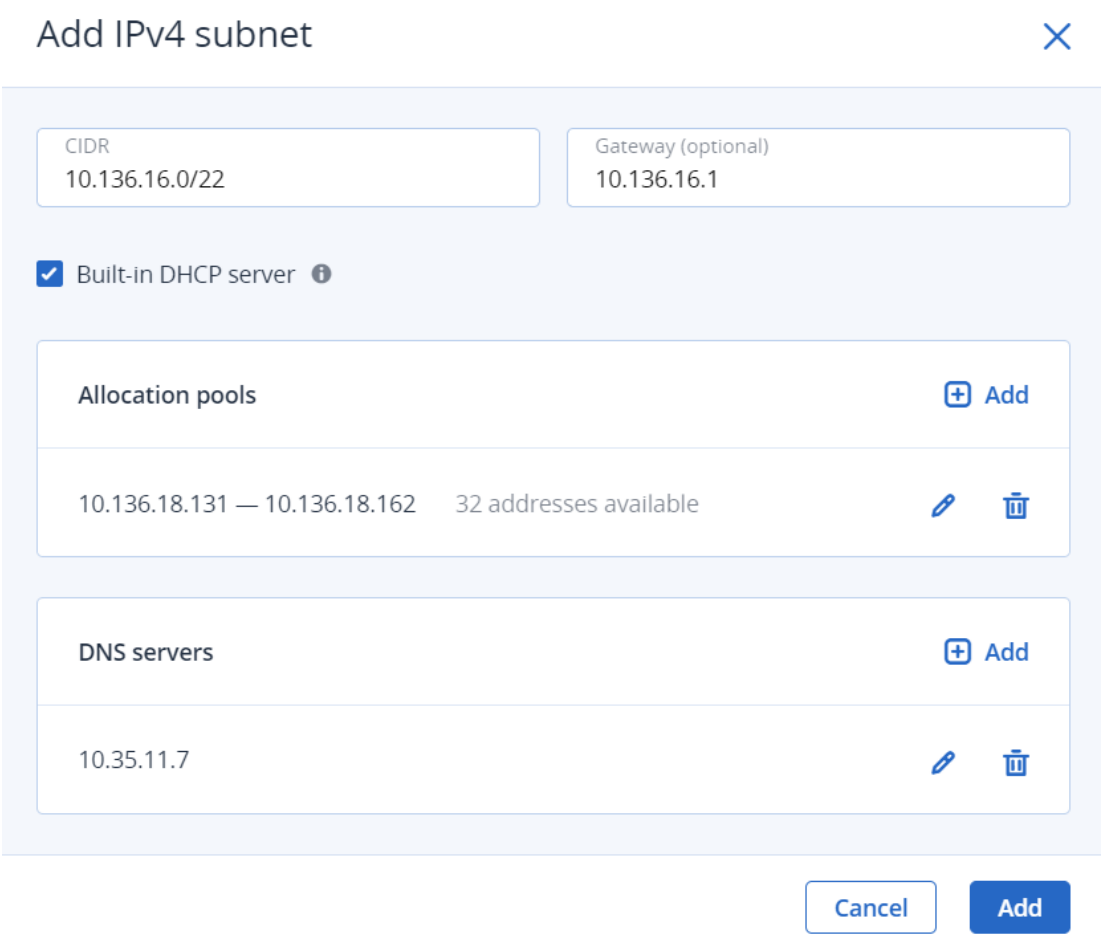
  - Если DHCP-сервер включен, сетевым интерфейсам ВМ будут автоматически назначены IP-адреса: либо из пулов IP-адресов, либо при отсутствии пулов из всего диапазона IP-адресов сети. DHCP-сервер получит первые два IP-адреса из пула IP-адресов. Например:
    - В подсети 192.168.128.0/24 без шлюза DHCP-серверу будут назначены IP-адреса 192.168.128.1 и 192.168.128.2.
    - В подсети 192.168.128.0/24, в которой шлюзу назначен IP-адрес 192.168.128.1, DHCP-серверу будут назначены IP-адреса 192.168.128.2 и 192.168.128.3.
  - Если DHCP-сервер отключен, сетевые интерфейсы ВМ все равно получат IP-адреса, но их нужно будет назначить вручную внутри виртуальных машин.

  Виртуальный DHCP-сервер будет работать только внутри текущей сети и не будет виден из других сетей.

  d. Укажите один или несколько пулов IP-адресов (диапазоны IP-адресов, которые будут автоматически назначаться виртуальным машинам).

e. Укажите DNS-серверы, которые будут использоваться виртуальными машинами. Эти серверы могут предоставляться виртуальным машинам посредством встроенного DHCP-сервера либо с помощью сетевой конфигурации cloud-init (если пакет cloud-init установлен в ВМ).

f. Нажмите **Добавить**.

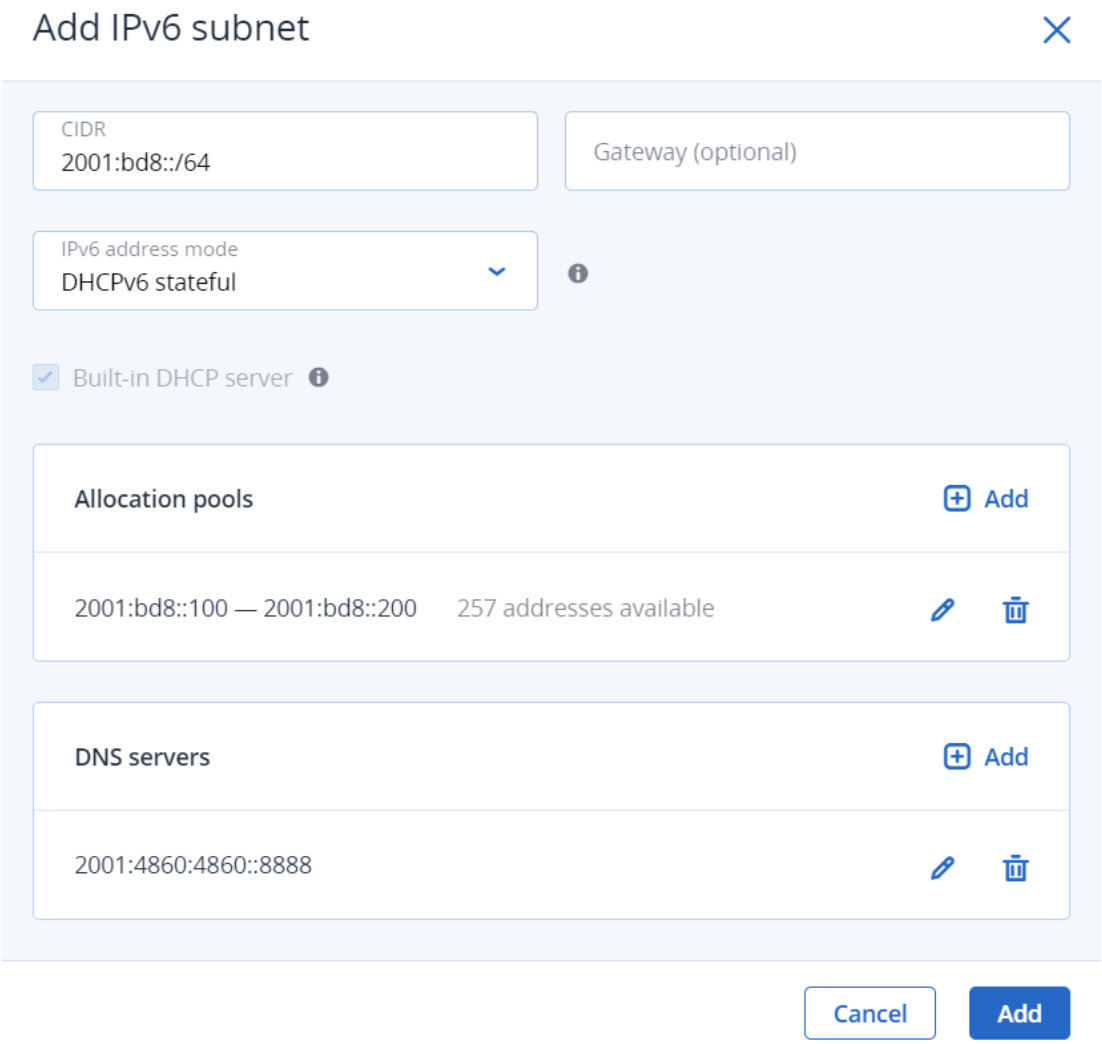


- Как добавить подсеть IPv6
  a. В разделе **Подсети** нажмите **Добавить** и выберите **Подсеть IPv6**.
  b. В окне **Добавить подсеть IPv6** укажите диапазон адресов IPv6 сети, также при необходимости можно указать шлюз. Если оставить поле **Шлюз** пустым, то шлюз будет исключен из сетевых параметров.
  c. Выберите нужный режим адресации IPv6 в соответствии с таблицей выше.
  d. Если вы выбрали для режима адресации IPv6 значение **Нет**, включите или отключите встроенный DHCP-сервер.
     - Если DHCP-сервер включен, ВМ будет получать адрес IPv6 автоматически.
     - Если DHCP-сервер отключен, необходимо будет назначать адрес IPv6 для ВМ вручную.

e. Укажите один или несколько пулов IP-адресов (диапазоны IP-адресов, которые будут автоматически назначаться виртуальным машинам).

f. Если вы выбрали режим адресации IPv6 **DHCPv6 stateless** (без отслеживания состояния) или **DHCPv6 stateful** (с отслеживанием состояния), укажите DNS-серверы, которые будут отправлены виртуальным машинам через встроенный DHCP-сервер.

g. Нажмите **Добавить**.



4. На шаге **Сетевой доступ** можно настроить сетевой доступ следующим образом:

   a. Выберите проекты, для которых нужно обеспечить сетевой доступ:

   - Чтобы сеть была доступна из всех существующих и новых проектов, выберите **Все проекты**.
   - Чтобы сеть была доступна из всех существующих проектов в пределах домена, выберите **Выбрать проекты**, а затем установите флажок напротив нужного домена.
   - Чтобы сеть была доступна из определенного проекта внутри домена, выберите **Выбрать**

проекты, щелкните имя домена, а затем выберите нужный проект.

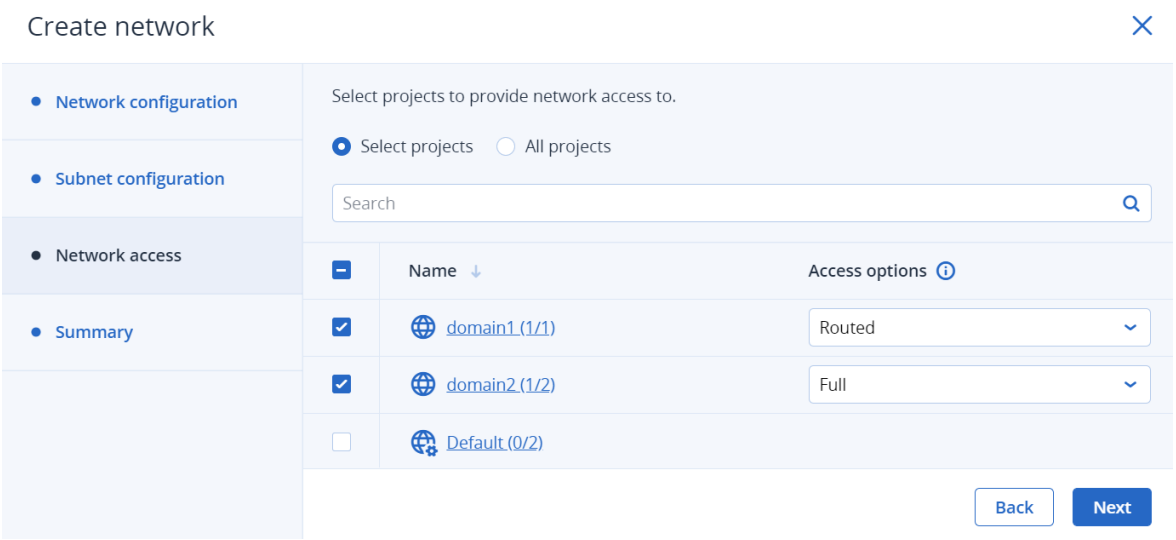
- Если вы не хотите открывать общий доступ к сети, пропустите этот шаг, нажав **Далее**.

b. Выберите тип доступа:

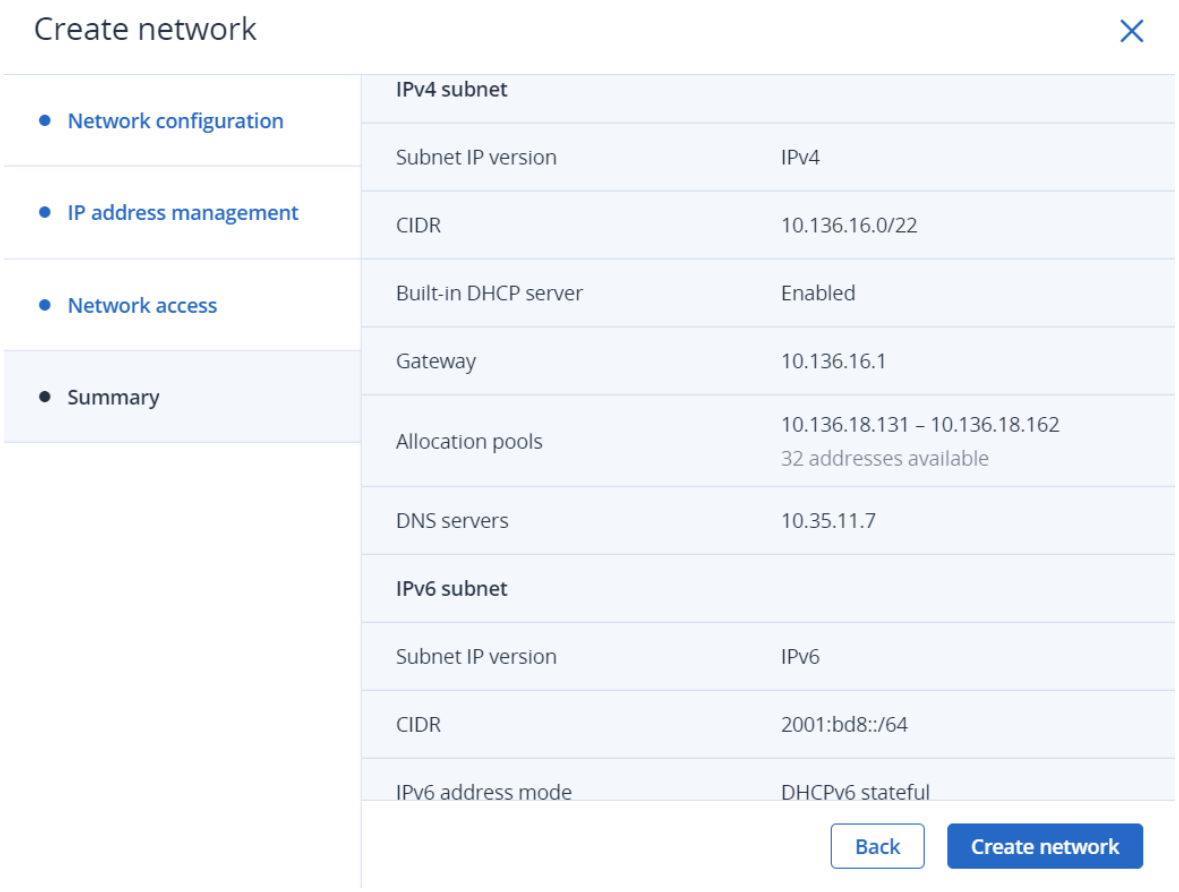
- Предоставляя полный доступ, вы разрешаете виртуальным машинам в выбранных проектах взаимодействовать с этой сетью напрямую либо через виртуальные маршрутизаторы.
- Предоставляя маршрутизируемый доступ, вы разрешаете виртуальным машинам в выбранных проектах взаимодействовать с этой сетью только через виртуальные маршрутизаторы.

Также можно предоставить прямой доступ, который подразумевает прямое подключение виртуальных машин внутри проектов к физической сети. Прямой доступ можно открыть только с помощью инструмента vinfra, указав ключ direct в параметре --rbac-policies. Этот тип доступа нельзя настроить на панели администрирования.

c. Нажмите кнопку **Далее**.



5. На шаге **Сводка** просмотрите конфигурацию и нажмите кнопку **Добавить сеть**.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute network create [--dhcp | --no-dhcp]
                                      [--dns-nameserver <dns-nameserver>]
                                      [--allocation-pool <allocation-pool>]
                                      [--gateway <gateway> | --no-gateway]
                                      [--rbac-policies <rbac-policies>]
                                      [--physical-network <physical-network>]
                                      [--vlan-network <vlan-network>]
                                      [--vlan <vlan>] [--cidr <cidr>]
                                      [--ipv6-address-mode <ipv6-address-mode>]
                                      <network-name>
```

--dhcp

Включение DHCP

--no-dhcp

Отключение DHCP

--dns-nameserver <dns-nameserver>

IP-адрес сервера DNS. Этот параметр можно использовать несколько раз.

--allocation-pool <allocation-pool>

Пул IP-адресов для создания внутри сети в формате: ip_addr_start-ip_addr_end. Этот параметр можно использовать несколько раз.

--gateway <gateway>

IP-адрес шлюза

--no-gateway

Не настраивать шлюз для этой сети.

--rbac-policies <rbac-policies>

Разделенный запятыми список политик RBAC в формате <target>:<target_id>:<action> | none. Допустимые цели: project, domain. Допустимые действия: direct, full, routed. «*» является допустимым значением target_id для всех целей. Передайте none для очистки всех существующих политик.

Пример: domain:default:routed,project:uuid1:full

--physical-network <physical-network>

Инфраструктурная сеть для связи с физической сетью

--vlan-network <vlan-network>

Сеть VLAN для связи

--vlan <vlan>

Идентификатор VLAN виртуальной сети

--cidr <cidr>

Маска подсети в нотации CIDR

--ipv6-address-mode <ipv6-address-mode>

Режим адресации IPv6: dhcpv6-stateful, dhcpv6-stateless, slaac

<network-name>

Имя сети

Пример 1. Чтобы создать нетегированную физическую сеть поверх инфраструктурной сети Public с включенным управлением IP-адресами, заданными сетевыми параметрами и полным сетевым доступом между всеми проектами в пределах указанного домена, выполните:

```
# vinfra service compute network create mypubnet --physical-network Public \
--cidr 10.136.16.0/22 --gateway 10.136.16.1 --dns-nameserver 10.35.11.7 \
--allocation-pool 10.136.18.141-10.136.18.148 \
--rbac-policies domain:cd421db9f3e84e3e8cd2c932c1f7a698:full
```

Пример 2. Чтобы создать физическую сеть на базе VLAN поверх инфраструктурной сети Public с идентификатором VLAN 10, включенным управлением IP-адресами, заданными сетевыми параметрами и прямым (общим) сетевым доступом между всеми проектами в инфраструктуре, выполните:

```
# vinfra service compute network create mypubnet_vlan --vlan 10 \
--physical-network Public --cidr 10.136.16.0/22 --gateway 10.136.16.1 \
--dns-nameserver 10.35.11.7 --allocation-pool 10.136.18.131-10.136.18.138 \
--rbac-policies project:*:direct
```

Новая вычислительная сеть появится в выводе команды vinfra service compute network list:

```
# vinfra service compute network list -c id -c name -c cidr -c allocation_pools
+---------------+--------------+-----------------+-----------------------------+
| id            | name         | cidr            | allocation_pools            |
+---------------+--------------+-----------------+-----------------------------+
| 22674f9d-<...> | mypubnet     | 10.136.16.0/22  | - 10.136.18.141-10.136.18.148  |
| 8f0dc747-<...> | mypubnet_vlan | 10.136.16.0/22  | - 10.136.18.131-10.136.18.138  |
| a0019b43-<...> | myprivnet    | 192.168.128.0/24 | - 192.168.128.2-192.168.128.254 |
+---------------+--------------+-----------------+-----------------------------+
```

Создание виртуальных вычислительных сетей

Ограничения

- Подсети IPv6 недоступны для виртуальных вычислительных сетей.

Предварительные требования

- Четкое понимание архитектуры вычислительных сетей, которая разъясняется в разделе "Архитектура вычислительных сетей" на странице 23.

Как добавить виртуальную вычислительную сеть

Панель администратора

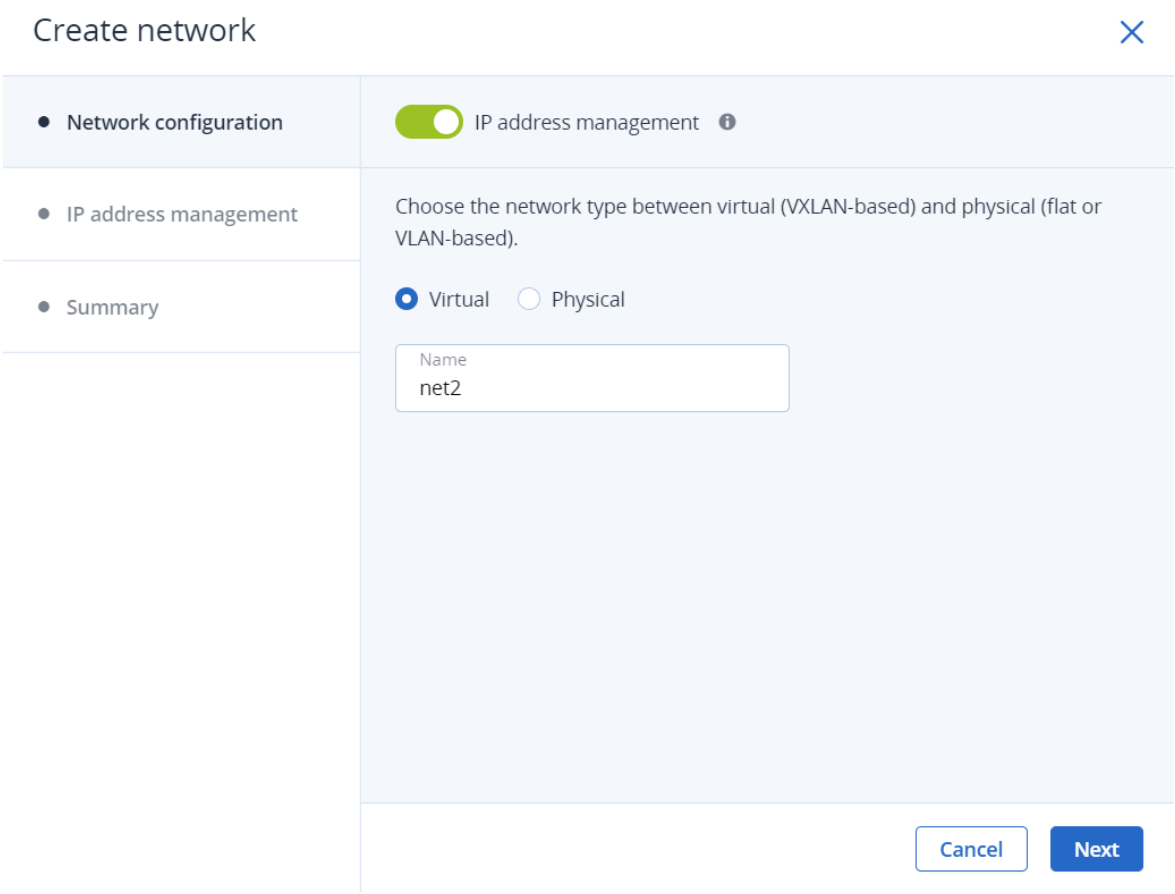
1. На экране **Вычисления** > **Сеть** > **Сети** нажмите **Создать сеть**.
2. На шаге **Конфигурация сети** выполните следующие действия:
   a. Включите или отключите управление IP-адресами:
      - Если управление IP-адресами включено, встроенный DHCP-сервер автоматически назначит ВМ, подключенным к сети, IP-адреса из пулов IP-адресов, а также задаст для ВМ настраиваемые DNS-серверы. Кроме того, по умолчанию для всех сетевых портов ВМ будет включена защита от спуфинга. Каждый сетевой интерфейс ВМ сможет принимать и отправлять IP-пакеты, только если ему назначены IP- и MAC-адреса. При необходимости защиту от спуфинга для интерфейса ВМ можно отключить вручную.
      - Если управление IP-адресами отключено, то ВМ, подключенные к сети, получат IP-адреса от DHCP-серверов в этой сети (при их наличии). Кроме того, защита от спуфинга будет отключена для всех сетевых портов ВМ, и ее нельзя будет включить вручную. Это означает, что каждый сетевой интерфейс ВМ с назначенными IP- и MAC-адресами или без них сможет принимать и отправлять IP-пакеты.

      В любом случае можно будет вручную назначить статические IP-адреса изнутри виртуальных машин.

b. Выберите тип сети **Виртуальная**.

c. Укажите имя сети.

d. Нажмите кнопку **Далее**.



3. Если вы включили управление IP-адресами, вы будете перенаправлены на шаг **Управление IP-адресами**, где можно добавить подсеть IPv4.

   a. В разделе **Подсети** нажмите **Добавить** и выберите **Подсеть IPv4**.

   b. В окне **Добавить подсеть IPv4** укажите диапазон адресов IPv4 сети, также при необходимости можно указать шлюз. Если оставить поле **Шлюз** пустым, то шлюз будет исключен из сетевых параметров.

   c. Включите или отключите встроенный DHCP-сервер:

   - Если DHCP-сервер включен, сетевым интерфейсам ВМ будут автоматически назначены IP-адреса: либо из пулов IP-адресов, либо при отсутствии пулов из всего диапазона IP-адресов сети. DHCP-сервер получит первые два IP-адреса из пула IP-адресов. Например:
     - В подсети 192.168.128.0/24 без шлюза DHCP-серверу будут назначены IP-адреса 192.168.128.1 и 192.168.128.2.
     - В подсети 192.168.128.0/24, в которой шлюзу назначен IP-адрес 192.168.128.1, DHCP-серверу будут назначены IP-адреса 192.168.128.2 и 192.168.128.3.

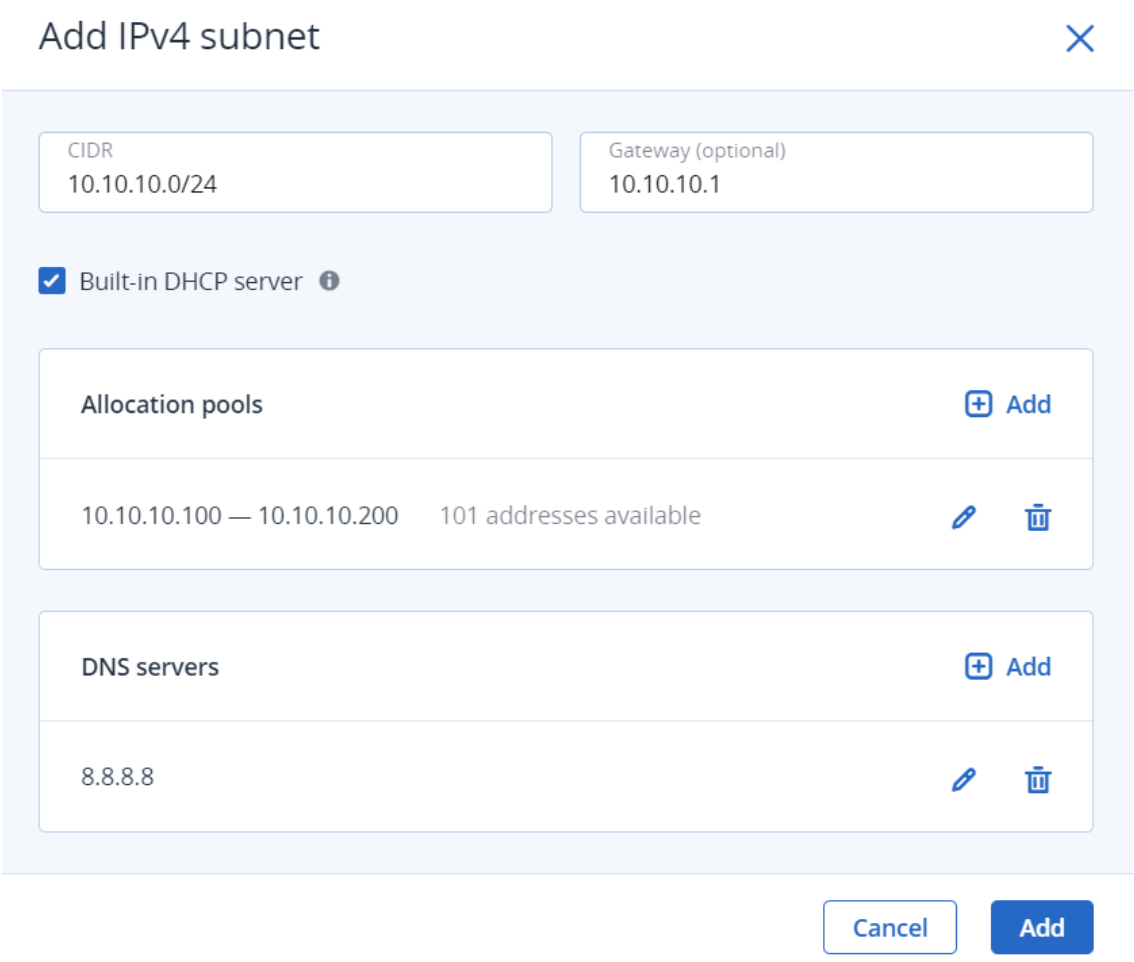
- Если DHCP-сервер отключен, сетевые интерфейсы ВМ все равно получат IP-адреса, но их нужно будет назначить вручную внутри виртуальных машин.

Виртуальный DHCP-сервер будет работать только внутри текущей сети и не будет виден из других сетей.

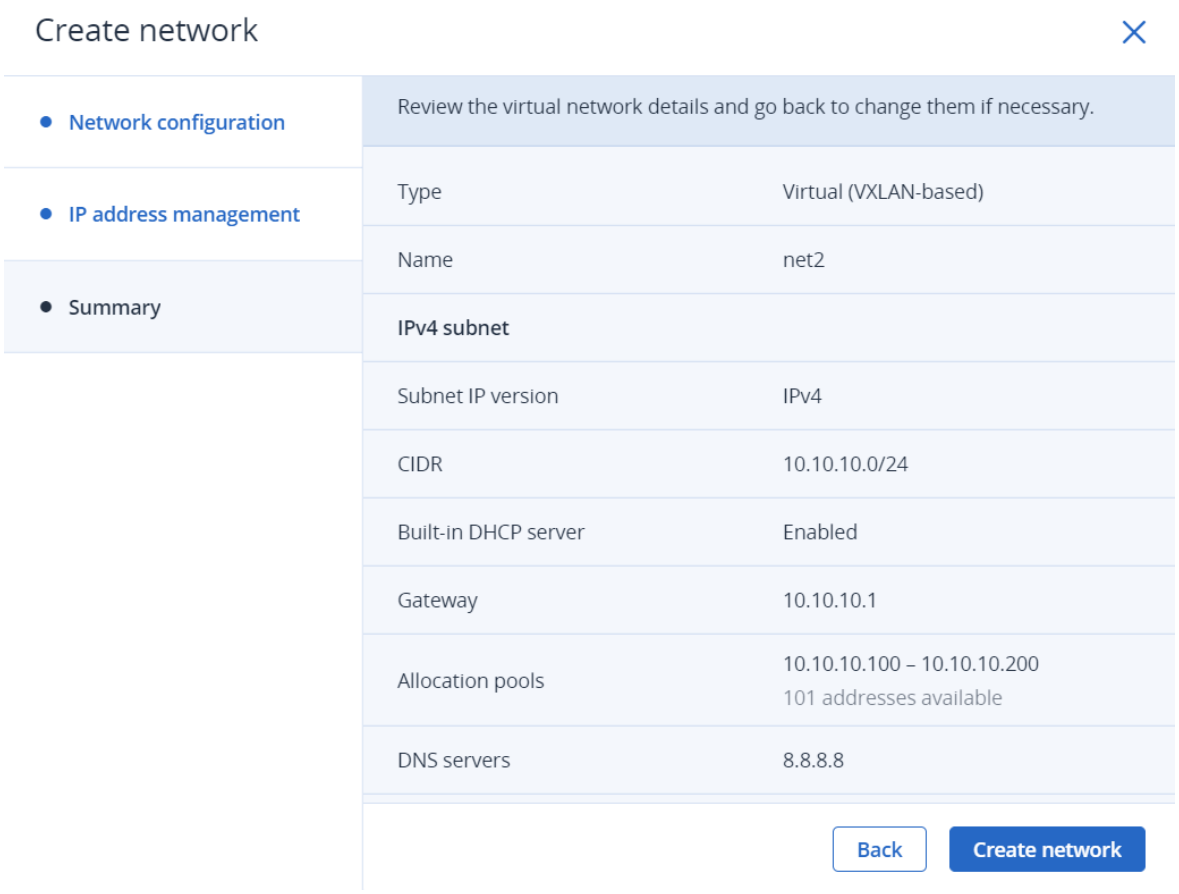
d. Укажите один или несколько пулов IP-адресов (диапазоны IP-адресов, которые будут автоматически назначаться виртуальным машинам).

e. Укажите DNS-серверы, которые будут использоваться виртуальными машинами. Эти серверы могут предоставляться виртуальным машинам посредством встроенного DHCP-сервера либо с помощью сетевой конфигурации cloud-init (если пакет cloud-init установлен в ВМ).

f. Нажмите **Добавить**.



4. На шаге **Сводка** просмотрите конфигурацию и нажмите **Создать сеть**.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute network create [--dhcp | --no-dhcp]
                                      [--dns-nameserver <dns-nameserver>]
                                      [--allocation-pool <allocation-pool>]
                                      [--gateway <gateway> | --no-gateway]
                                      [--rbac-policies <rbac-policies>]
                                      [--physical-network <physical-network>]
                                      [--vlan-network <vlan-network>]
                                      [--vlan <vlan>] [--cidr <cidr>]
                                      [--ipv6-address-mode <ipv6-address-mode>]
                                      <network-name>
```

--dhcp

Включение DHCP

--no-dhcp

Отключение DHCP

--dns-nameserver <dns-nameserver>

IP-адрес сервера DNS. Этот параметр можно использовать несколько раз.

--allocation-pool <allocation-pool>

Пул IP-адресов для создания внутри сети в формате: ip_addr_start-ip_addr_end. Этот параметр можно использовать несколько раз.

--gateway <gateway>

IP-адрес шлюза

--no-gateway

Не настраивать шлюз для этой сети.

--rbac-policies <rbac-policies>

Разделенный запятыми список политик RBAC в формате <target>:<target_id>:<action> | none. Допустимые цели: project, domain. Допустимые действия: direct, full, routed. «*» является допустимым значением target_id для всех целей. Передайте none для очистки всех существующих политик.

Пример: domain:default:routed,project:uuid1:full

--physical-network <physical-network>

Инфраструктурная сеть для связи с физической сетью

--vlan-network <vlan-network>

Сеть VLAN для связи

--vlan <vlan>

Идентификатор VLAN виртуальной сети

--cidr <cidr>

Маска подсети в нотации CIDR

--ipv6-address-mode <ipv6-address-mode>

Режим адресации IPv6: dhcpv6-stateful, dhcpv6-stateless, slaac

<network-name>

Имя сети

Например, чтобы создать виртуальную сеть myprivnet с включенным управлением IP-адресами и заданными сетевыми параметрами, выполните:

```
# vinfra service compute network create myprivnet --cidr 192.168.128.0/24 \
--gateway 192.168.128.1 --dns-nameserver 8.8.8.8
+-------------------+-----------------------------------------------------+
| Field             | Value                                               |
+-------------------+-----------------------------------------------------+
| allocation_pools  | - end: 192.168.128.254                              |
|                   |   start: 192.168.128.2                              |
| cidr              | 192.168.128.0/24                                    |
| dns_nameservers   | - 8.8.8.8                                           |
| enable_dhcp       | True                                                |
| gateway_ip        | 192.168.128.1                                       |
| id                | fa6d0ead-32de-4ce2-b620-5529a15eb52a                |
```

```
| ip_version        | 4                                                    |
| ipam_enabled      | True                                                 |
| name              | myprivnet                                            |
| physical_network  |                                                      |
| project_id        | b906404c55bb44729da99987536ac5bc                     |
| rbac_policies     | []                                                   |
| router_external   | False                                                |
| shared            | False                                                |
| spoofing_protection | True                                               |
| subnet            | allocation_pools:                                    |
|                   | - end: 192.168.128.254                               |
|                   |   start: 192.168.128.2                               |
|                   | cidr: 192.168.128.0/24                               |
|                   | dns_nameservers:                                     |
|                   | - 8.8.8.8                                            |
|                   | enable_dhcp: true                                    |
|                   | gateway_ip: 192.168.128.1                            |
|                   | id: e607dd29-ffe1-46d8-a189-1baf392d1520             |
|                   | ip_version: 4                                        |
|                   | ipv6_address_mode: null                              |
|                   | ipv6_ra_mode: null                                   |
|                   | network_id: fa6d0ead-32de-4ce2-b620-5529a15eb52a     |
| subnets           | - allocation_pools:                                  |
|                   |   - end: 192.168.128.254                             |
|                   |     start: 192.168.128.2                             |
|                   |   cidr: 192.168.128.0/24                             |
|                   |   dns_nameservers:                                   |
|                   |   - 8.8.8.8                                          |
|                   |   enable_dhcp: true                                  |
|                   |   gateway_ip: 192.168.128.1                          |
|                   |   id: e607dd29-ffe1-46d8-a189-1baf392d1520           |
|                   |   ip_version: 4                                      |
|                   |   ipv6_address_mode: null                            |
|                   |   ipv6_ra_mode: null                                 |
|                   |   network_id: fa6d0ead-32de-4ce2-b620-5529a15eb52a   |
| tags              | []                                                   |
| type              | virtual                                              |
| vlan_id           |                                                      |
+-------------------+------------------------------------------------------+
```

Новая вычислительная сеть появится в выводе команды vinfra service compute network list:

```
# vinfra service compute network list -c id -c name -c cidr -c allocation_pools
+---------------+--------------+-----------------+-----------------------------+
| id            | name         | cidr            | allocation_pools            |
+---------------+--------------+-----------------+-----------------------------+
| 22674f9d-<...> | mypubnet     | 10.136.16.0/22  | - 10.136.18.141-10.136.18.148  |
| 8f0dc747-<...> | mypubnet_vlan | 10.136.16.0/22  | - 10.136.18.131-10.136.18.138  |
| a0019b43-<...> | myprivnet    | 192.168.128.0/24 | - 192.168.128.2-192.168.128.254 |
+---------------+--------------+-----------------+-----------------------------+
```

Управление вычислительными подсетями

Можно добавлять и удалять подсети физических сетей. Кроме того, если вы исчерпали все публичные IP-адреса в физической вычислительной сети, можно добавить в эту сеть дополнительные подсети с помощью средства командной строки OpenStack. Новые подсети будут доступны на панели администрирования и самообслуживания для назначения IP-адресов и управления ими.

Ограничения

- Для подсети IPv6 нельзя изменить режим адресации IPv6.
- В вычислительной сети с включенным управлением IP-адресами должна быть как минимум одна подсеть.

Предварительные требования

- Вычислительные сети должны быть созданы автоматически в ходе развертывания вычислительного кластера или вручную, как описано в разделах "Создание физических вычислительных сетей" на странице 532 и "Создание виртуальных вычислительных сетей" на странице 540.
- Для авторизации выполнения приведенных ниже команд настроен клиент командной строки OpenStack, как описано в разделе "Подключение к интерфейсу командной строки OpenStack" на странице 427.

Чтобы добавить подсеть в физическую вычислительную сеть

1. На экране **Вычисления** > **Сеть** > **Сети** щелкните по нужной физической сети.
2. В разделе **Подсети** нажмите **Добавить**, а затем выберите **Подсеть IPv4** или **Подсеть IPv6** в зависимости от доступных вариантов.
3. В новом окне укажите настройки подсети и нажмите **Добавить**.

Чтобы добавить дополнительные подсети в физическую вычислительную сеть

1. Определите нужную сеть, отобразив список всех существующих сетей:

```
# openstack --insecure network list
+----------------------+---------+--------------------------------------+
| ID                   | Name    | Subnets                              |
+----------------------+---------+--------------------------------------+
| a1d8d6ae-c89d-4307<…> | public  | d52aa9f4-6a4b-4268-a71d-1a50f9b60aa9 |
| e31eac69-9ab7-41ad<…> | private | 470526d3-ea5a-48fb-81ac-20273f005f61 |
+----------------------+---------+--------------------------------------+
```

2. Создайте новую подсеть в этой сети с помощью команды openstack subnet create. Например:

```
# openstack --insecure subnet create --ip-version 4 --subnet-range 10.164.132.0/24 \
--gateway 10.164.132.1 --dhcp --dns-nameserver 8.8.8.8 --allocation-pool \
start=10.164.132.201,end=10.164.132.212 --network public newsubnet
```

Чтобы удалить подсеть из физической вычислительной сети

1. На экране **Вычисления** > **Сеть** > **Сети** щелкните по нужной физической сети.
2. В разделе **Подсети** нажмите значок корзины возле подсети, которую следует удалить.

Примечание
Удалить единственную подсеть нельзя.

Просмотр сведений о вычислительных сетях

Предварительные требования

- Вычислительные сети должны быть созданы автоматически в ходе развертывания вычислительного кластера или вручную, как описано в разделах "Создание физических вычислительных сетей" на странице 532 и "Создание виртуальных вычислительных сетей" на странице 540.

Чтобы просмотреть сведения о вычислительной сети

Панель администратора

На экране **Вычисления** > **Сеть** > **Сети** щелкните по сети. На правой панели будут отображены сведения об этой сети.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute network show <network>
```

<network>

Идентификатор или имя сети

Например, чтобы вывести сведения о вычислительной сети mypubnet, выполните:

```
# vinfra service compute network show mypubnet
+-----------------+-------------------------------------------------------+
| Field           | Value                                                 |
+-----------------+-------------------------------------------------------+
| allocation_pools | 10.136.18.141-10.136.18.148                          |
| cidr            | 10.136.16.0/22                                        |
| dns_nameservers  | 10.35.11.7                                           |
| enable_dhcp     | True                                                  |
| gateway_ip      | 10.136.16.1                                           |
| id              | 22674f9d-1c94-4953-b79b-7f6029ee9bd0                  |
| ip_version      | 4                                                     |
| ipam_enabled    | True                                                  |
| name            | mypubnet                                              |
| physical_network | Public                                               |
| project_id      | c22613639b3147e0b22ef057b87698fe                      |
| rbac_policies   | - actions:                                            |
|                 |   - routed                                            |
|                 |   - shared                                            |
```

```
|              |  target_domain: cd421db9f3e84e3e8cd2c932c1f7a698  |
|              |  target_project: f59a0d9a4cd543daa73160575d48611b |
| router_external  | True                                          |
| shared           | False                                         |
| tags             | []                                            |
| type             | physical                                      |
| vlan_id          |                                               |
+------------------+-----------------------------------------------+
```

Изменение и удаление вычислительных сетей

Можно изменить имя сети и настройки сетевого доступа, а также удалить вычислительную сеть, которая не используется виртуальными машинами.

Ограничения

- Изменять управление IP-адресами вычислительной сети невозможно.

Предварительные требования

- Вычислительные сети должны быть созданы автоматически в ходе развертывания вычислительного кластера или вручную, как описано в разделах "Создание физических вычислительных сетей" на странице 532 и "Создание виртуальных вычислительных сетей" на странице 540.
- Чтобы вычислительную сеть можно было удалить, к ней не должна быть подключена ни одна виртуальная машина.

Чтобы изменить параметры вычислительной сети

Панель администратора

1. На экране **Вычисления** > **Сеть** > **Сети** щелкните по сети, которую необходимо изменить.
2. На правой панели сети щелкните по значку карандаша рядом с нужным разделом, затем внесите требуемые изменения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute network set [--rbac-policies <rbac-policies>]
                                   [--name <name>] <network>
```

--rbac-policies <rbac-policies>

Разделенный запятыми список политик RBAC в формате <target>:<target_id>:<action> | none. Допустимые цели: project, domain. Допустимые действия: direct, full, routed. «*» является допустимым значением target_id для всех целей. Передайте none для очистки всех существующих политик.

Пример: domain:default:routed,project:uuid1:full

--name <name>

Новое имя для сети

<network>

Идентификатор или имя сети

Например, чтобы запретить сетевой доступ к вычислительной сети mypubnet, выполните:

```
# vinfra service compute network set mypubnet --rbac-policies none
+-----------------+--------------------------------------+
| Field           | Value                                |
+-----------------+--------------------------------------+
| allocation_pools | 10.136.18.141-10.136.18.148         |
| cidr            | 10.136.16.0/22                       |
| dns_nameservers  | 10.35.11.7                          |
| enable_dhcp     | True                                 |
| gateway_ip      | 10.136.16.1                          |
| id              | 22674f9d-1c94-4953-b79b-7f6029ee9bd0 |
| ip_version      | 4                                    |
| ipam_enabled    | True                                 |
| name            | mypubnet                             |
| physical_network | Public                              |
| project_id      | c22613639b3147e0b22ef057b87698fe     |
| rbac_policies   | []                                   |
| router_external  | False                               |
| shared          | False                                |
| tags            | []                                   |
| type            | physical                             |
| vlan_id         |                                      |
+-----------------+--------------------------------------+
```

Чтобы удалить вычислительную сеть

Панель администратора

1. На экране **Вычисления** > **Сеть** > **Сети** щелкните по сети, которую необходимо удалить.
2. На правой панели сети нажмите **Удалить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute network delete <network>
```

<network>

Идентификатор или имя сети

Например, чтобы удалить вычислительную сеть myprivnet, выполните:

```
# vinfra service compute network delete myprivnet
Operation accepted.
```

7.6.3.2 Управление группами безопасности

Группа безопасности – это набор правил сетевого доступа, которые контролируют входящий и исходящий трафик виртуальных машин, назначенных в эту группу. С помощью правил группы безопасности можно задать тип и направление трафика, которому разрешен доступ к порту виртуального интерфейса. Трафик, не соответствующий ни одному правилу, отбрасывается.

Для каждого проекта в вычислительном кластере автоматически создается группа безопасности **default** (по умолчанию). Эта группа разрешает весь трафик на всех портах для всех протоколов, и удалить ее нельзя. Когда вы присоединяете сетевой интерфейс к ВМ, он привязывается к группе безопасности **default**, если не выбрана пользовательская группа безопасности.

Как новым, так и существующим виртуальным машинам можно назначить одну или несколько групп безопасности. При добавлении или удалении правил из групп безопасности эти изменения принудительно применяются во время выполнения.

Ограничения

- Можно управлять только правилами групп безопасности IPv4.

Создание и удаление групп безопасности

Ограничения

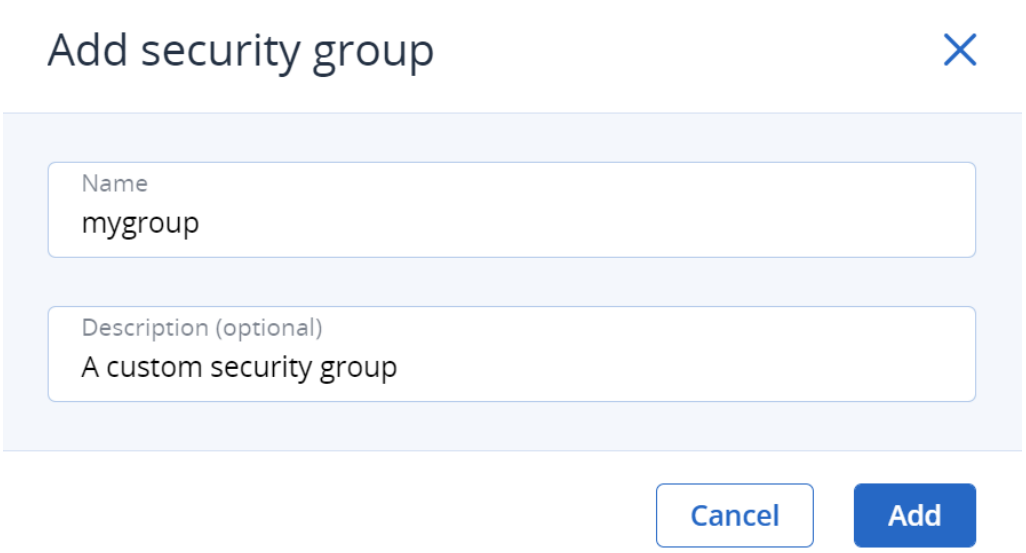
- Нельзя удалить группу безопасности **default**.
- Группу безопасности нельзя удалить, если она назначена виртуальной машине.

Как создать группу безопасности

Панель администратора

1. На экране **Вычисления** > **Сеть** > **Группы безопасности** нажмите **Создать**.
2. В окне **Добавить группу безопасности** введите имя и описание для группы и нажмите

Добавить.



По умолчанию новая группа безопасности будет отклонять весь входящий трафик и разрешать только исходящий трафик для назначенных виртуальных машин.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute security-group create [--description <description>]
                                             <name>
```

--description <description>

Описание группы безопасности

<name>

Имя группы безопасности

Например, чтобы создать группу безопасности mygroup, выполните:

```
# vinfra service compute security-group create mygroup
+---------------------+-----------------------------------------------------+
| Field               | Value                                               |
+---------------------+-----------------------------------------------------+
| description         |                                                     |
| id                  | 12e6b260-0b61-4551-8168-3e59602a2433                |
| name                | mygroup                                             |
| project_id          | e215189c0472482f93e71d10e1245253                    |
| security_group_rules | - description: null                                |
|                     |   direction: egress                                 |
|                     |   ethertype: IPv4                                   |
|                     |   id: ce854e2b-537f-4618-bea9-e9ec3d8616ac          |
|                     |   port_range_max: null                              |
|                     |   port_range_min: null                              |
```

```
|                 |  project_id: e215189c0472482f93e71d10e1245253   |
|                 |  protocol: null                                 |
|                 |  remote_group_id: null                          |
|                 |  remote_ip_prefix: null                         |
|                 |  security_group_id: 12e6b260-0b61-4551-8168<...> |
|                 | - description: null                             |
|                 |  direction: egress                              |
|                 |  ethertype: IPv6                                |
|                 |  id: a7c65861-df3d-47f2-bec3-089747141936       |
|                 |  port_range_max: null                           |
|                 |  port_range_min: null                           |
|                 |  project_id: e215189c0472482f93e71d10e1245253   |
|                 |  protocol: null                                 |
|                 |  remote_group_id: null                          |
|                 |  remote_ip_prefix: null                         |
|                 |  security_group_id: 12e6b260-0b61-4551-8168<...> |
| tags            | []                                              |
+-----------------+-------------------------------------------------+
```

Созданная группа безопасности появится в выводе команды vinfra service compute security-group list:

```
# vinfra service compute security-group list -c id -c name
+--------------------------------------+---------+
| id                                   | name    |
+--------------------------------------+---------+
| 062f75cf-abc0-419d-bb1a-92989ad9383f | default |
| 12e6b260-0b61-4551-8168-3e59602a2433 | mygroup |
+--------------------------------------+---------+
```

Как удалить группу безопасности

Панель администратора

1. На экране **Вычисления** > **Сеть** > **Группы безопасности** щелкните по нужной группе.
2. На правой панели группы нажмите **Удалить**.
3. Нажмите **Удалить** в окне подтверждения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute security-group delete <security-group>
```

<security-group>

Имя или идентификатор группы безопасности

Например, чтобы удалить группу безопасности mygroup, выполните:

```
# vinfra service compute security-group delete mygroup
Operation successful.
```

Управление правилами групп безопасности

Группы безопасности можно изменять путем добавления и удаления правил. Редактирование правил не предусмотрено. Если необходимо изменить существующее правило, удалите его и создайте заново с нужными параметрами.

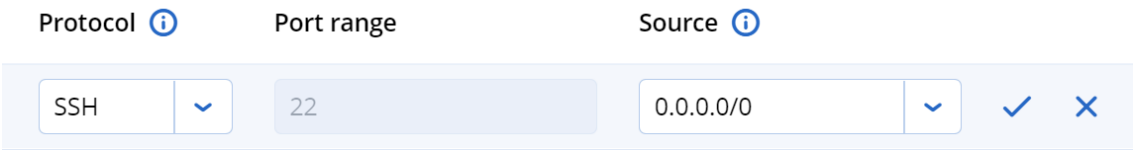
Предварительные требования

- Создана группа безопасности, как описано в разделе "Создание и удаление групп безопасности" на странице 550.

Как добавить правило в группу безопасности

Панель администратора

1. Перейдите на экран **Вычисления** > **Сеть** > **Группы безопасности** и щелкните группу безопасности, в которую нужно добавить правило.
2. На правой панели группы нажмите **Добавить** в разделе **Входящие** или **Исходящие**, чтобы создать правило для входящего или исходящего трафика.
3. Укажите параметры правила.
   a. Выберите протокол из списка или введите число от 0 до 255.
   b. Введите номер порта или диапазон номеров. У некоторых протоколов уже есть стандартный диапазон портов. Например, для SSH используется порт 22.
   c. Выберите готовую маску подсети (CIDR) или существующую группу безопасности.



4. Щелкните по галочке, чтобы сохранить изменения.

Сразу после создания правило применяется ко всем виртуальным машинам, назначенным в эту группу безопасности.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute security-group rule create [--remote-group <remote-group>]
                                                  [--remote-ip <ip-address>]
                                                  [--ethertype <ethertype>]
                                                  [--protocol <protocol>]
                                                  [--port-range-max <port-range-max>]
                                                  [--port-range-min <port-range-min>]
```

```
                              (--ingress | --egress)
                              <security-group>
```

--remote-group <remote-group>

Имя или идентификатор удаленной группы безопасности

--remote-ip <ip-address>

Блок удаленных IP-адресов в нотации CIDR

--ethertype <ethertype>

Тип Ethertype сетевого трафика: IPv4 или IPv6

--protocol <protocol>

IP-протокол: tcp, udp, icmp, vrrp и т. д.

--port-range-max <port-range-max>

Максимальный номер порта в диапазоне портов, который соответствует правилу группы безопасности

--port-range-min <port-range-min>

Минимальный номер порта в диапазоне портов, который соответствует правилу группы безопасности

--ingress

Правило для входящего сетевого трафика

--egress

Правило для исходящего сетевого трафика

<security-group>

Имя или идентификатор группы безопасности, в которой создается правило

Например, чтобы создать правило в группе безопасности mygroup, разрешающее входящий сетевой трафик IPv4 для TCP-порта 22, выполните:

```
# vinfra service compute security-group rule create mygroup \
--ethertype IPv4 --protocol tcp --port-range-max 22 --port-range-min 22 --ingress
+-------------------+--------------------------------------+
| Field             | Value                                |
+-------------------+--------------------------------------+
| description       |                                      |
| direction         | ingress                              |
| ethertype         | IPv4                                 |
| id                | 0f395e2f-a8ab-47f4-b670-64399461393c |
| port_range_max    | 22                                   |
| port_range_min    | 22                                   |
| project_id        | e215189c0472482f93e71d10e1245253     |
| protocol          | tcp                                  |
| remote_group_id   |                                      |
| remote_ip_prefix  |                                      |
```

```
| security_group_id | 12e6b260-0b61-4551-8168-3e59602a2433 |
+-------------------+--------------------------------------+
```

Созданное правило появится в выводе команды vinfra service compute security-group rule list:

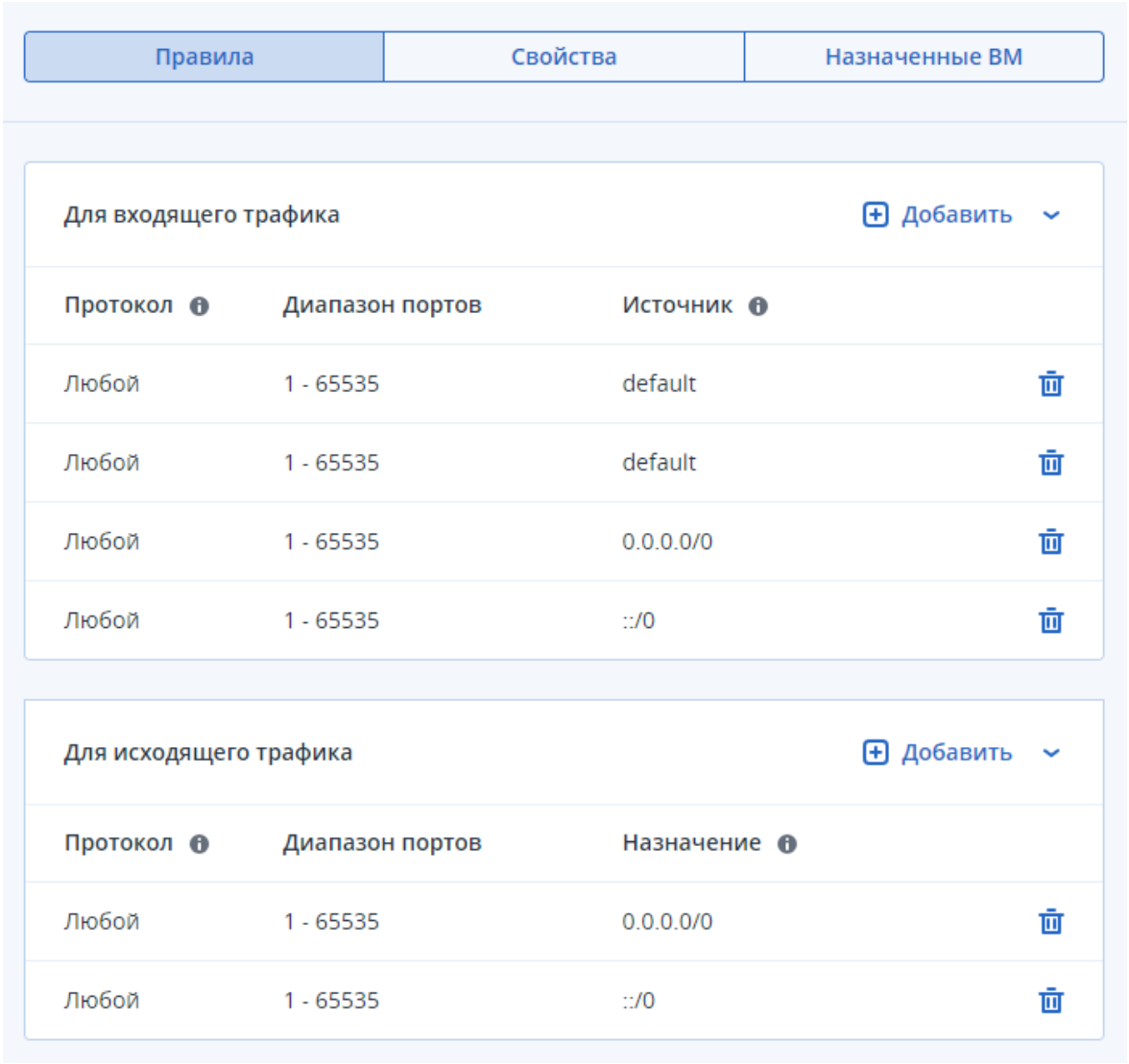
```
# vinfra service compute security-group rule list mygroup -c id -c direction -c protocol
+--------------------------------------+-----------+----------+
| id                                   | direction | protocol |
+--------------------------------------+-----------+----------+
| 0f395e2f-a8ab-47f4-b670-64399461393c | ingress   | tcp      |
| a7c65861-df3d-47f2-bec3-089747141936 | egress    |          |
| ce854e2b-537f-4618-bea9-e9ec3d8616ac | egress    |          |
+--------------------------------------+-----------+----------+
```

Как просмотреть сведения о правиле группы безопасности

Панель администратора

1. Перейдите на экран **Вычисления** > **Сеть** > **Группы безопасности** и щелкните группу безопасности, в которой находится требуемое правило.
2. В правой панели откройте вкладку **Правила**. Будут отображены списки правил для входящего и исходящего трафика. В одном из них вы можете найти и просмотреть сведения об

интересующем вас правиле.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute security-group rule show <security-group-rule>
```

<security-group-rule>

Идентификатор правила группы безопасности

Например, чтобы вывести сведения о правиле группы безопасности с идентификатором 0f395e2f-a8ab-47f4-b670-64399461393c, выполните:

```
# vinfra service compute security-group rule show \
0f395e2f-a8ab-47f4-b670-64399461393c
+-------------------+--------------------------------------+
| Field             | Value                                |
+-------------------+--------------------------------------+
```

```
| description      |                                      |
| direction        | ingress                              |
| ethertype        | IPv4                                 |
| id               | 0f395e2f-a8ab-47f4-b670-64399461393c |
| port_range_max   | 22                                   |
| port_range_min   | 22                                   |
| project_id       | e215189c0472482f93e71d10e1245253     |
| protocol         | tcp                                  |
| remote_group_id  |                                      |
| remote_ip_prefix |                                      |
| security_group_id | 12e6b260-0b61-4551-8168-3e59602a2433 |
+------------------+--------------------------------------+
```

Как удалить правило из группы безопасности

Панель администратора

1. На экране **Группы безопасности** щелкните по нужной группе.
2. На правой панели группы щелкните по значку корзины рядом с правилом, которое следует удалить.

Сразу после удаления правила это изменение применяется ко всем виртуальным машинам, назначенным в эту группу безопасности.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute security-group rule delete <security-group-rule>
```

<security-group-rule>

Идентификатор правила группы безопасности

Например, чтобы удалить правило группы безопасности с идентификатором 0f395e2f-a8ab-47f4-b670-64399461393c, выполните:

```
# vinfra service compute security-group rule delete 0f395e2f-a8ab-47f4-b670-64399461393c
Operation successful.
```

Изменение назначения групп безопасности

При создании ВМ выбираются группы безопасности для сетевых интерфейсов ВМ. Назначенные группы безопасности можно изменить позже.

Ограничения

- Нельзя настроить группы безопасности, если для выбранной сети отключена защита от спуфинга или отключено управление IP-адресами.

Как просмотреть виртуальные машины, назначенные в группу безопасности

1. На экране **Группы безопасности** щелкните по нужной группе.
2. На правой панели группы перейдите на вкладку **Назначенные ВМ**. Отобразятся все назначенные виртуальные машины и их статусы.

Можно щелкнуть по имени ВМ, чтобы открыть панель **Сводка** этой ВМ и изменить назначенную группу безопасности для ее сетевых интерфейсов.

Как назначить группу безопасности виртуальной машине

Панель администратора

1. На экране **Виртуальные машины** щелкните по нужной ВМ.
2. На вкладке **Сводка** щелкните по значку карандаша в разделе **Сети**.
3. Щелкните по значку многоточия рядом с сетевым интерфейсом, которому следует назначить группу безопасности, и выберите **Изменить**.
4. В окне **Изменить сетевой интерфейс** перейдите на вкладку **Группы безопасности**.
5. Выберите одну или несколько групп безопасности из раскрывающегося списка и нажмите **Сохранить**.

Правила из выбранных групп безопасности будут применены во время выполнения.

Интерфейс командной строки

1. Выведите список сетевых интерфейсов виртуальной машины и назначенные им группы безопасности. Например:

```
# vinfra service compute server iface list --server myvm -c id -c security_groups --long
+--------------------------------------+--------------------------------------+
| id                                   | security_groups                      |
+--------------------------------------+--------------------------------------+
| 8c11c29b-9a73-4017-baff-1e872b18b54b | - d3a7d0c3-0f5c-4e77-8add-dafebae4a225 |
+--------------------------------------+--------------------------------------+
```

2. Измените группу безопасности сетевого интерфейса. Например:

```
# vinfra service compute server iface set --server myvm --security-group mygroup \
8c11c29b-9a73-4017-baff-1e872b18b54b
+--------------------+--------------------------------------+
| Field              | Value                                |
+--------------------+--------------------------------------+
| fixed_ips          | - 192.168.128.100                    |
| id                 | 8c11c29b-9a73-4017-baff-1e872b18b54b |
| mac_addr           | fa:16:3e:a6:d4:32                    |
| network_id         | 8774a1a4-f7a0-4729-be9b-d282751434c5 |
| security_groups    | 12e6b260-0b61-4551-8168-3e59602a2433 |
| spoofing_protection | True                                |
+--------------------+--------------------------------------+
```

Просмотр и изменение групп безопасности

Предварительные требования

- Создана группа безопасности, как описано в разделе "Создание и удаление групп безопасности" на странице 550.

Как просмотреть сведения о группе безопасности

Панель администратора

Перейдите на экран **Вычисления** > **Сеть** > **Группы безопасности** и щелкните по имени группы безопасности. На правой панели будут отображены сведения об этой группе.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute security-group show <security-group>
```

<security-group>

Имя или идентификатор группы безопасности

Например, чтобы вывести сведения о группе безопасности mygroup, выполните:

```
# vinfra service compute security-group show mygroup
+---------------------+-----------------------------------------------------+
| Field               | Value                                               |
+---------------------+-----------------------------------------------------+
| description         |                                                     |
| id                  | 12e6b260-0b61-4551-8168-3e59602a2433                |
| name                | mygroup                                             |
| project_id          | e215189c0472482f93e71d10e1245253                    |
| security_group_rules | - description: null                                |
|                     |   direction: egress                                 |
|                     |   ethertype: IPv4                                   |
|                     |   id: ce854e2b-537f-4618-bea9-e9ec3d8616ac          |
|                     |   port_range_max: null                              |
|                     |   port_range_min: null                              |
|                     |   project_id: e215189c0472482f93e71d10e1245253      |
|                     |   protocol: null                                    |
|                     |   remote_group_id: null                             |
|                     |   remote_ip_prefix: null                            |
|                     |   security_group_id: 12e6b260-0b61-4551-8168<...>   |
|                     | - description: null                                 |
|                     |   direction: egress                                 |
|                     |   ethertype: IPv6                                   |
|                     |   id: a7c65861-df3d-47f2-bec3-089747141936          |
|                     |   port_range_max: null                              |
|                     |   port_range_min: null                              |
|                     |   project_id: e215189c0472482f93e71d10e1245253      |
|                     |   protocol: null                                    |
|                     |   remote_group_id: null                             |
|                     |   remote_ip_prefix: null                            |
|                     |   security_group_id: 12e6b260-0b61-4551-8168<...>   |
```

```
| tags                | []                                                  |
+---------------------+-----------------------------------------------------+
```

Как изменить группу безопасности

Панель администратора

1. Перейдите на экран **Вычисления** > **Сеть** > **Группы безопасности** и щелкните по имени группы безопасности.
2. В правой панели перейдите на вкладку **Свойства** и нажмите **Изменить**.
3. В окне **Изменить группу безопасности** укажите новое имя и описание группы безопасности, а затем нажмите **Сохранить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute security-group set [--name <name>]
                                [--description <description>]
                                <security-group>
```

--name <name>

Имя группы безопасности

--description <description>

Описание группы безопасности

<security-group>

Имя или идентификатор группы безопасности

Например, чтобы изменить описание группы безопасности mygroup, выполните:

```
# vinfra service compute security-group set mygroup \
--description "A new security group"
+---------------------+-----------------------------------------------------+
| Field               | Value                                               |
+---------------------+-----------------------------------------------------+
| description         | A new security group                                |
| id                  | 12e6b260-0b61-4551-8168-3e59602a2433                |
| name                | mygroup                                             |
| project_id          | e215189c0472482f93e71d10e1245253                    |
| security_group_rules | - description: null                                |
|                     |   direction: egress                                 |
|                     |   ethertype: IPv4                                   |
|                     |   id: ce854e2b-537f-4618-bea9-e9ec3d8616ac          |
|                     |   port_range_max: null                              |
|                     |   port_range_min: null                              |
|                     |   project_id: e215189c0472482f93e71d10e1245253      |
|                     |   protocol: null                                    |
|                     |   remote_group_id: null                             |
```

```
|                 |  remote_ip_prefix: null                    |
|                 |  security_group_id: 12e6b260-0b61-4551-8168<...> |
|                 | - description: null                        |
|                 |  direction: egress                         |
|                 |  ethertype: IPv6                           |
|                 |  id: a7c65861-df3d-47f2-bec3-089747141936      |
|                 |  port_range_max: null                      |
|                 |  port_range_min: null                      |
|                 |  project_id: e215189c0472482f93e71d10e1245253   |
|                 |  protocol: null                            |
|                 |  remote_group_id: null                     |
|                 |  remote_ip_prefix: null                    |
|                 |  security_group_id: 12e6b260-0b61-4551-8168<...> |
| tags            | []                                         |
+-----------------+--------------------------------------------------+
```

7.6.3.3 Управление виртуальными маршрутизаторами

Виртуальные маршрутизаторы предоставляют сервисы L3, такие как маршрутизация и преобразование исходных сетевых адресов (SNAT), между виртуальными и физическими сетями либо различными виртуальными сетями.

- Виртуальный маршрутизатор между виртуальной и физической сетью обеспечивает доступ к внешним сетям, например к Интернету, для ВМ, подключенных к этой виртуальной сети.
- Виртуальный маршрутизатор между различными виртуальными сетями обеспечивает обмен данными по сети для ВМ, подключенных к этим виртуальным сетям.

У виртуального маршрутизатора есть два типа портов:

- Внешний шлюз, подключенный к физической сети.
- Внутренний порт, подключенный к виртуальной сети.

С виртуальными маршрутизаторами можно выполнить следующие действия.

- Создать виртуальные маршрутизаторы
- Изменить внешние или внутренние интерфейсы маршрутизатора
- Создать, изменить и удалить статические маршруты
- Изменить имя маршрутизатора
- Удалить маршрутизатор

Ограничения

- Маршрутизатор может соединять только сети с включенным управлением IP-адресами.
- Виртуальный маршрутизатор можно удалить, если ни с одной из подключенных к нему сетей не связаны плавающие IP-адреса.

Создание виртуальных маршрутизаторов

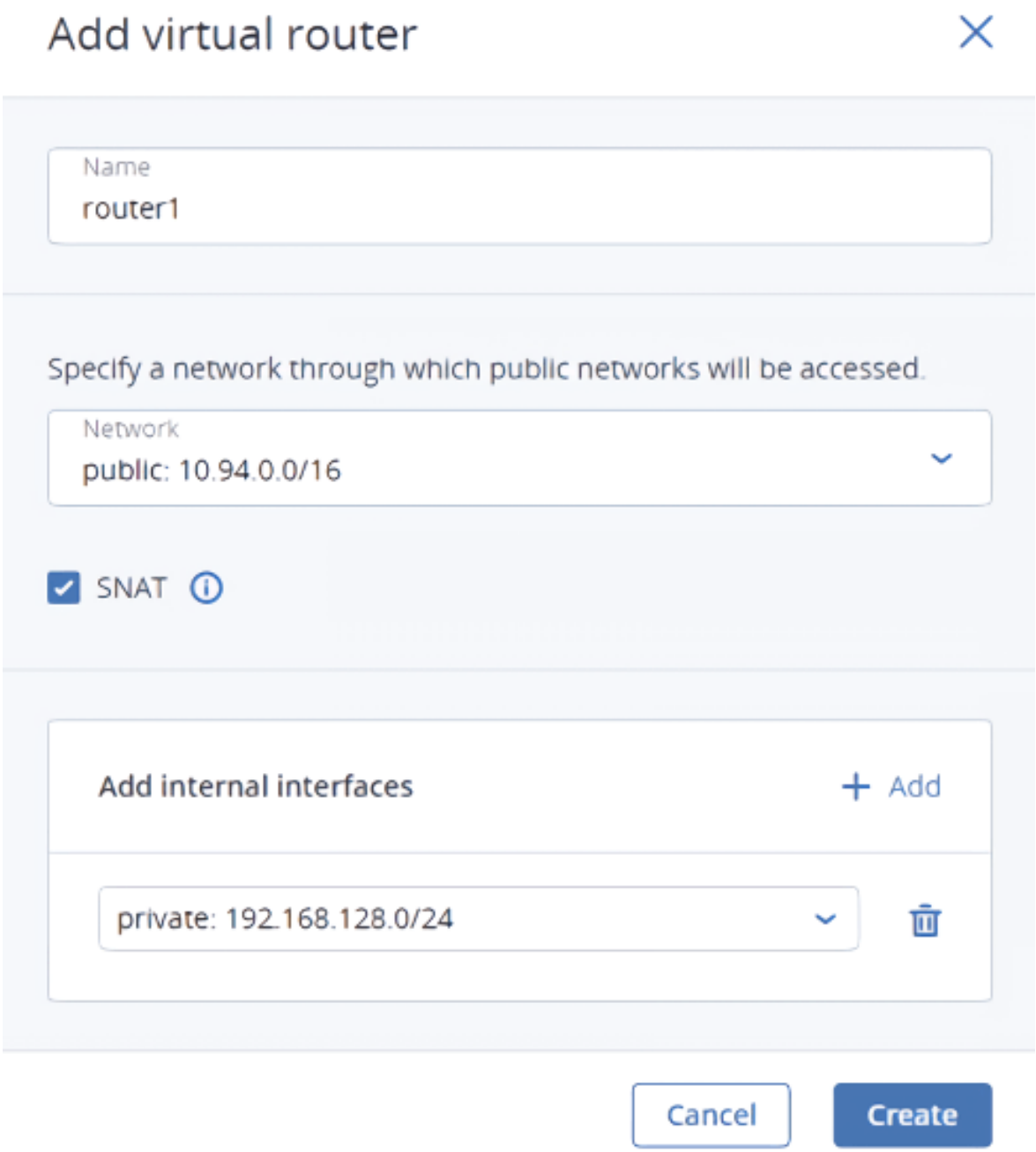
Предварительные требования

- Созданы вычислительные сети, как описано в разделах "Создание физических вычислительных сетей" на странице 532 и "Создание виртуальных вычислительных сетей" на странице 540.
- Для вычислительных сетей, которые будут подключены к маршрутизатору, указан шлюз.

Как создать виртуальный маршрутизатор

Панель администратора

1. Перейдите на экран **Маршрутизаторы** и нажмите **Добавить маршрутизатор**.
2. В окне **Добавить маршрутизатор** выполните следующие действия.
   a. Укажите имя маршрутизатора.
   b. В раскрывающемся списке **Сеть** выберите физическую сеть, через которую будет предоставляться внешний доступ посредством внешнего шлюза. Новый внешний шлюз получит неиспользуемый IP-адрес из выбранной физической сети.
   c. В разделе **Добавить внутренние интерфейсы** выберите одну или несколько виртуальных сетей для подключения к маршрутизатору через внутренние интерфейсы. Новые внутренние интерфейсы по умолчанию будут пытаться использовать IP-адрес шлюза выбранных виртуальных сетей.
   d. [Необязательно] Установите или снимите флажок **SNAT**, чтобы включить или отключить SNAT на внешнем шлюзе маршрутизатора. При включенном преобразовании SNAT маршрутизатор заменяет частные IP-адреса ВМ публичным IP-адресом внешнего шлюза.



3. Нажмите кнопку **Создать**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute router create [--external-gateway <network>]
                                     [--enable-snat | --disable-snat]
                                     [--fixed-ip <fixed-ip>]
                                     [--internal-interface <network=network,ip-addr=ip-addr> |
                                     <network>] <router-name>
```

--external-gateway <network>

Указывает физическую сеть для использования в качестве внешнего шлюза маршрутизатора (имя или идентификатор).

--enable-snat

Включение SNAT на внешнем шлюзе.

--disable-snat

Отключение SNAT на внешнем шлюзе.

--fixed-ip <fixed-ip>

Нужный IP-адрес на внешнем шлюзе.

--internal-interface <network=network,ip-addr=ip-addr>|<network>

Указывает внутренний интерфейс. Этот параметр можно использовать несколько раз.

- network – имя виртуальной сети.
- ip-addr – неиспользуемый IP-адрес из выбранной виртуальной сети для назначения интерфейсу; укажите, если шлюз по умолчанию для выбранной виртуальной сети уже используется.

<router-name>

Имя виртуального маршрутизатора.

Например, чтобы создать маршрутизатор myrouter между физической сетью public и виртуальной сетью private с включенным преобразованием SNAT на внешнем шлюзе, выполните:

```
# vinfra service compute router create myrouter --external-gateway public \
--internal-interface private --enable-snat
+----------------------+-----------------------------------------------------+
| Field                | Value                                               |
+----------------------+-----------------------------------------------------+
| external_gateway_info | enable_snat: true                                  |
|                      | ip_addresses:                                       |
|                      | - 10.94.129.76                                      |
|                      | network_id: 720e45bc-4225-49de-9346-26513d8d1262 |
| id                   | b9d8b000-5d06-4768-9f65-2715250cda53                |
| name                 | myrouter                                            |
| project_id           | 894696133031439f8aaa7e4868dcbd4d                    |
| routes               | []                                                  |
| status               | ACTIVE                                              |
+----------------------+-----------------------------------------------------+
```

Созданный маршрутизатор появится в выводе команды vinfra service compute router list:

```
# vinfra service compute router list -c id -c external_gateway_info -c name
-c status
+--------------------+--------------------------------+----------+--------+
| id                 | external_gateway_info          | name     | status |
+--------------------+--------------------------------+----------+--------+
```

```
| b9d8b000-5d06-<...> | enable_snat: true            | myrouter | ACTIVE |
|                     | ip_addresses:                |          |        |
|                     | - 10.94.129.76               |          |        |
|                     | network_id: 720e45bc-4225-<...> |          |        |
+---------------------+------------------------------+----------+--------+
```

Просмотр сведений о виртуальных маршрутизаторах

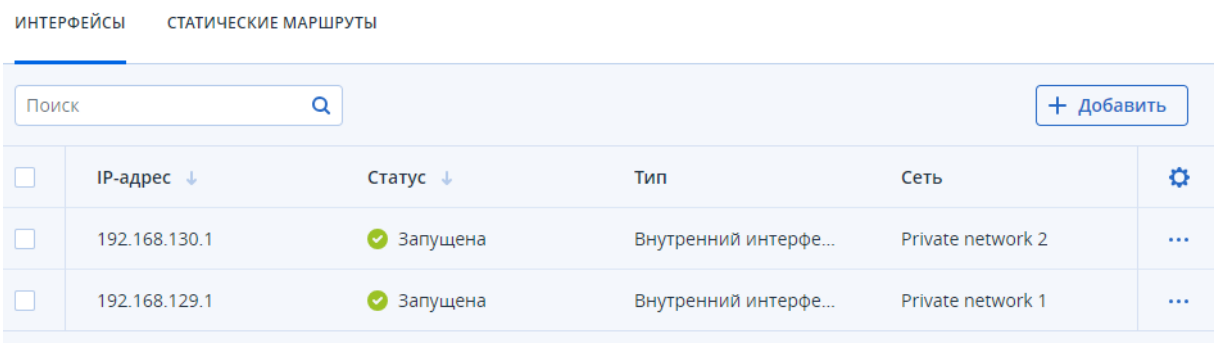
Предварительные требования

- Создан виртуальный маршрутизатор, как описано в разделе "Создание виртуальных маршрутизаторов" на странице 562.

Просмотр сведений о виртуальном маршрутизаторе

Панель администратора

На экране **Вычисления** > **Сеть** > **Маршрутизаторы** щелкните виртуальный маршрутизатор.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute router show <router>
```

<router>

Имя виртуального маршрутизатора.

Например, чтобы вывести сведения о виртуальном маршрутизаторе myrouter, выполните:

```
# vinfra service compute router show myrouter
+----------------------+-----------------------------------------------------+
| Field                | Value                                               |
+----------------------+-----------------------------------------------------+
| external_gateway_info | enable_snat: true                                  |
|                      | ip_addresses:                                       |
|                      | - 10.94.129.76                                      |
|                      | network_id: 720e45bc-4225-49de-9346-26513d8d1262    |
| id                   | b9d8b000-5d06-4768-9f65-2715250cda53                |
| name                 | myrouter                                            |
| project_id           | 894696133031439f8aaa7e4868dcbd4d                    |
```

```
| routes              | []                                                   |
| status              | ACTIVE                                               |
+---------------------+------------------------------------------------------+
```

Управление интерфейсами маршрутизаторов

Предварительные требования

- Создан виртуальный маршрутизатор, как описано в разделе "Создание виртуальных маршрутизаторов" на странице 562.

Как добавить внешний интерфейс маршрутизатора

Панель администратора

1. Если у вас уже есть внешний шлюз, сначала удалите существующий.
2. На странице **Маршрутизаторы** нажмите имя маршрутизатора, чтобы открыть список его интерфейсов.
3. Нажмите **Добавить** на панели инструментов либо нажмите **Добавить интерфейс**, если не отображается ни одного интерфейса.
4. В окне **Добавить интерфейс** выполните следующие действия.
   a. Выберите **Внешний шлюз**.
   b. В раскрывающемся списке **Сеть** выберите физическую сеть для подключения к маршрутизатору. Новый интерфейс получит неиспользуемый IP-адрес из выбранной физической сети. Также можно указать определенный IP-адрес из выбранной сети и назначить его интерфейсу в поле **IP-адрес**.
   c. [Необязательно] Установите или снимите флажок **SNAT**, чтобы включить или отключить SNAT на внешнем шлюзе маршрутизатора. При включенном преобразовании SNAT маршрутизатор заменяет частные IP-адреса ВМ публичным IP-адресом внешнего шлюза.

5. Нажмите **Добавить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute router iface add [--ip-address <ip-address>]
                                        --interface <network> <router>
```

--ip-address <ip-address>

IP-адрес

--interface <network>

Имя или идентификатор сети

<router>

Имя или идентификатор виртуального маршрутизатора

Например, чтобы добавить интерфейс из виртуальной сети public на виртуальный маршрутизатор myrouter с IP-адресом 10.94.129.76, выполните:

```
# vinfra service compute router iface add myrouter --interface public \
--ip-address 10.94.129.76
+--------------------------------------+-------------+-----------------+--------+
| network_id                           | is_external | ip_addresses    | status |
+--------------------------------------+-------------+-----------------+--------+
| 720e45bc-4225-49de-9346-26513d8d1262 | True        | - 10.94.129.76  | ACTIVE |
| e6f146ce-a6d0-48b2-9e4f-64a128ce97ae | False       | - 192.168.128.1 | ACTIVE |
+--------------------------------------+-------------+-----------------+--------+
```

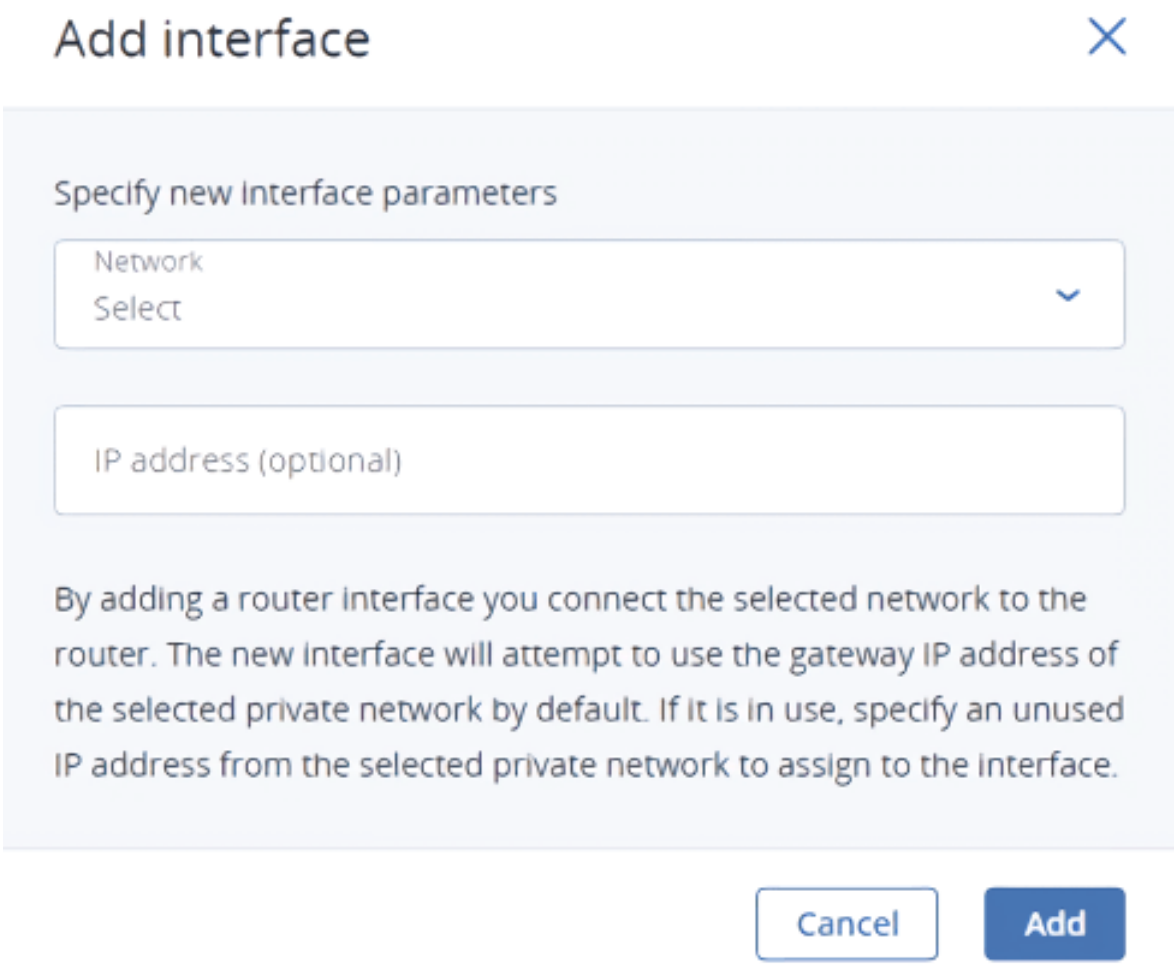
Добавленный интерфейс появится в выводе команды vinfra service compute router iface list:

```
# vinfra service compute router iface list myrouter
+--------------------------------+-------------+-----------------+--------+
| network_id                     | is_external | ip_addresses    | status |
+--------------------------------+-------------+-----------------+--------+
| 720e45bc-4225-<...> (public)   | True        | - 10.94.129.76  | ACTIVE |
| e6f146ce-a6d0-<...> (private)  | False       | - 192.168.128.1 | ACTIVE |
+--------------------------------+-------------+-----------------+--------+
```

Как добавить внутренний интерфейс маршрутизатора

Панель администратора

1. На странице **Маршрутизаторы** нажмите имя маршрутизатора, чтобы открыть список его интерфейсов.
2. Нажмите **Добавить**.
3. В окне **Добавить интерфейс** выберите сеть для подключения к маршрутизатору из раскрывающегося списка **Сеть**. Новый внутренний интерфейс по умолчанию будет пытаться использовать IP-адрес шлюза выбранной виртуальной сети. Если он уже используется, укажите неиспользуемый IP-адрес из выбранной виртуальной сети и назначьте его маршрутизатору в поле **IP-адрес**.



4. Нажмите **Добавить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute router iface add [--ip-address <ip-address>]
                                        --interface <network> <router>
```

--ip-address <ip-address>

IP-адрес

--interface <network>

Имя или идентификатор сети

<router>

Имя или идентификатор виртуального маршрутизатора

Например, чтобы добавить интерфейс из виртуальной сети private2 на виртуальный маршрутизатор myrouter с IP-адресом 192.168.30.3, выполните:

```
# vinfra service compute router iface add myrouter --interface private2 \
--ip-address 192.168.30.3
+--------------------------------------+------------+----------------+--------+
| network_id                           | is_external | ip_addresses    | status |
+--------------------------------------+------------+----------------+--------+
| 720e45bc-4225-49de-9346-26513d8d1262 | True       | - 10.94.129.76  | ACTIVE |
| e6f146ce-a6d0-48b2-9e4f-64a128ce97ae | False      | - 192.168.128.1 | ACTIVE |
| 86803e07-a6d7-4809-9566-1cbe4a89adfd | False      | - 192.168.30.3  | DOWN   |
+--------------------------------------+------------+----------------+--------+
```

Добавленный интерфейс появится в выводе команды vinfra service compute router iface list:

```
# vinfra service compute router iface list myrouter
+------------------------------+------------+----------------+--------+
| network_id                   | is_external | ip_addresses    | status |
+------------------------------+------------+----------------+--------+
| 720e45bc-4225-<...> (public)   | True       | - 10.94.129.76  | ACTIVE |
| e6f146ce-a6d0-<...> (private)  | False      | - 192.168.128.1 | ACTIVE |
| 86803e07-a6d7-<...> (private2) | False      | - 192.168.30.3  | ACTIVE |
+------------------------------+------------+----------------+--------+
```

Как изменить параметры интерфейса маршрутизатора

Панель администратора

1. Щелкните по значку многоточия рядом с интерфейсом и выберите **Изменить**.
2. В окне **Изменить интерфейс** измените IP-адрес.
3. Для внешнего интерфейса включите или отключите SNAT.
4. Нажмите **Сохранить**, чтобы сохранить изменения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute router set [--external-gateway <network> |
                                   --no-external-gateway]
                                   [--fixed-ip <fixed-ip>]
                                   [--enable-snat | --disable-snat]
                                   <router>
```

--external-gateway <network>

Указывает физическую сеть для использования в качестве внешнего шлюза маршрутизатора (имя или идентификатор).

--no-external-gateway

Удаление внешнего шлюза с маршрутизатора.

--enable-snat

Включение SNAT на внешнем шлюзе.

--disable-snat

Отключение SNAT на внешнем шлюзе.

--fixed-ip <fixed-ip>

Нужный IP-адрес на внешнем шлюзе.

<router>

Имя или идентификатор виртуального маршрутизатора.

Например, чтобы отключить SNAT на внешнем шлюзе виртуального маршрутизатора myrouter, выполните:

```
# vinfra service compute router set myrouter --disable-snat --external-gateway public
+----------------------+-----------------------------------------------------+
| Field                | Value                                               |
+----------------------+-----------------------------------------------------+
| external_gateway_info | enable_snat: false                                 |
|                      | ip_addresses:                                       |
|                      | - 10.94.129.76                                      |
|                      | network_id: 720e45bc-4225-49de-9346-26513d8d1262    |
| id                   | b9d8b000-5d06-4768-9f65-2715250cda53                |
| name                 | myrouter                                            |
| project_id           | 894696133031439f8aaa7e4868dcbd4d                    |
| routes               | []                                                  |
| status               | ACTIVE                                              |
+----------------------+-----------------------------------------------------+
```

Как удалить интерфейс маршрутизатора

Панель администратора

1. Выберите интерфейс, который следует удалить.
2. Щелкните рядом с ним по значку многоточия и выберите **Удалить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute router iface remove --interface <network> <router>
```

--interface <network>

Имя или идентификатор сети

<router>

Имя или идентификатор виртуального маршрутизатора

Например, чтобы удалить интерфейс виртуальной сети private2 из виртуального маршрутизатора myrouter, выполните:

```
# vinfra service compute router iface remove myrouter --interface private2
+--------------------------------------+-------------+-----------------+--------+
| network_id                           | is_external | ip_addresses    | status |
+--------------------------------------+-------------+-----------------+--------+
| 720e45bc-4225-49de-9346-26513d8d1262 | True        | - 10.94.129.76  | ACTIVE |
| e6f146ce-a6d0-48b2-9e4f-64a128ce97ae | False       | - 192.168.128.1 | ACTIVE |
+--------------------------------------+-------------+-----------------+--------+
```

Управление статическими маршрутами

Также можно настроить статические маршруты, вручную добавив записи в таблицу маршрутизации. Это может пригодиться, например, если вам не нужно двустороннее соединение между двумя виртуальными сетями, а требуется только доступ к одной виртуальной сети из другой.

Рассмотрим следующий пример:

- Виртуальная машина **VM1** подключена к виртуальной сети **private1** (192.168.128.0/24) через сетевой интерфейс с IP-адресом 192.168.128.10.
- Виртуальная машина **VM2** подключена к виртуальной сети **private2** (192.168.30.0/24) через сетевой интерфейс с IP-адресом 192.168.30.10.
- Маршрутизатор **router1** соединяет сеть **private1** с физической сетью через внешний шлюз с IP-адресом 10.94.129.73.
- Маршрутизатор **router2** соединяет сеть **private2** с физической сетью через внешний шлюз с IP-адресом 10.94.129.74.

Для обеспечения доступа к **VM2** с **VM1** необходимо добавить статический маршрут для **router1**, указав CIDR сети **private2**, то есть 192.168.30.0/24, в качестве целевой подсети и IP-адрес внешнего шлюза **router2**, то есть 10.94.129.74, в качестве IP-адреса следующего транзитного участка. В этом случае, когда IP-пакет для 192.168.30.10 поступает на маршрутизатор **router1**, он перенаправляется на **router2**, а затем на **VM2**.

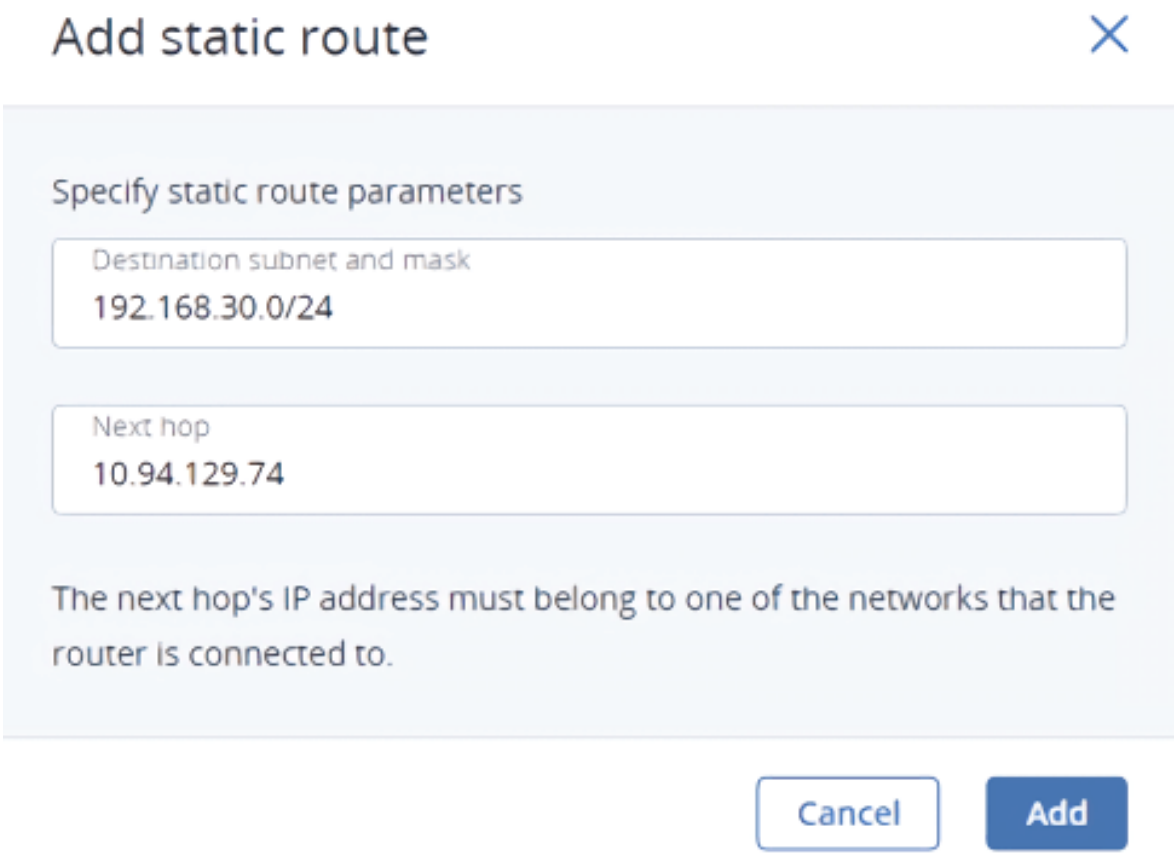
Предварительные требования

- Создан виртуальный маршрутизатор, как описано в разделе "Создание виртуальных маршрутизаторов" на странице 562.

Как создать статический маршрут для маршрутизатора

Панель администратора

1. На странице **Маршрутизаторы** щелкните по имени маршрутизатора. Откройте вкладку **Статические маршруты** и нажмите **Добавить** на панели справа. Если не отображается ни одного маршрута, нажмите **Добавить статический маршрут**.
2. В окне **Добавить статический маршрут** укажите диапазон и маску целевой подсети в нотации CIDR и IP-адрес следующего транзитного участка. IP-адрес следующего транзитного участка должен принадлежать одной из сетей, к которым подключен маршрутизатор.



3. Нажмите **Добавить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute router set --route <destination=destination,
                                  nexthop=nexthop> <router>
```

--route <destination=destination,nexthop=nexthop>

Статический маршрут для маршрутизатора. Этот параметр можно использовать несколько раз.

- destination – целевая подсеть в нотации CIDR.
- nexthop – IP-адрес следующего транзитного участка в одной из сетей, к которым подключен маршрутизатор.

<router>

Имя или идентификатор виртуального маршрутизатора.

Например, чтобы создать статический маршрут для виртуального маршрутизатора myrouter с подсетью назначения 192.128.30.0/24 и IP-адресом следующего транзитного участка 10.94.129.74, выполните:

```
# vinfra service compute router set myrouter --route
destination=192.128.30.0/24,nexthop=10.94.129.74
+----------------------+-------------------------------------------------+
| Field                | Value                                           |
+----------------------+-------------------------------------------------+
| external_gateway_info | enable_snat: false                             |
|                      | ip_addresses:                                   |
|                      | - 10.94.129.76                                  |
|                      | network_id: 720e45bc-4225-49de-9346-26513d8d1262 |
| id                   | b9d8b000-5d06-4768-9f65-2715250cda53            |
| name                 | myrouter                                        |
| project_id           | 894696133031439f8aaa7e4868dcbd4d                |
| routes               | - destination: 192.128.30.0/24                  |
|                      |   nexthop: 10.94.129.74                         |
| status               | ACTIVE                                          |
+----------------------+-------------------------------------------------+
```

Как изменить статический маршрут

Панель администратора

1. Щелкните по значку многоточия рядом с нужным статическим маршрутом и выберите **Изменить**.
2. В окне **Изменить статический маршрут** измените нужные параметры и нажмите **Сохранить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute router set --route <destination=destination,
                        nexthop=nexthop> <router>
```

--route <destination=destination,nexthop=nexthop>

Статический маршрут для маршрутизатора. Этот параметр можно использовать несколько раз.

- destination – целевая подсеть в нотации CIDR.
- nexthop – IP-адрес следующего транзитного участка в одной из сетей, к которым подключен маршрутизатор.

<router>

Имя или идентификатор виртуального маршрутизатора.

Например, чтобы задать статический маршрут для виртуального маршрутизатора myrouter с подсетью назначения 192.168.30.0/24 и IP-адресом следующего транзитного участка 10.94.129.15, выполните:

```
# vinfra service compute router set myrouter --route
destination=192.168.30.0/24,nexthop=10.94.129.15
```

```
+----------------------+-----------------------------------------------------+
| Field                | Value                                               |
+----------------------+-----------------------------------------------------+
| external_gateway_info | enable_snat: false                                 |
|                      | ip_addresses:                                       |
|                      | - 10.94.129.76                                      |
|                      | network_id: 720e45bc-4225-49de-9346-26513d8d1262 |
| id                   | b9d8b000-5d06-4768-9f65-2715250cda53                |
| name                 | myrouter                                            |
| project_id           | 894696133031439f8aaa7e4868dcbd4d                    |
| routes               | - destination: 192.168.30.0/24                      |
|                      |   nexthop: 10.94.129.15                             |
| status               | ACTIVE                                              |
+----------------------+-----------------------------------------------------+
```

Как удалить статический маршрут

Панель администратора

Щелкните по значку многоточия рядом со статическим маршрутом, который следует удалить, и выберите **Удалить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute router set --no-route <router>
```

--no-route

Очистка маршрутов, связанных с маршрутизатором.

<router>

Имя или идентификатор виртуального маршрутизатора.

Например, чтобы удалить все статические маршруты виртуального маршрутизатора myrouter, выполните:

```
# vinfra service compute router set myrouter --no-route
+----------------------+-----------------------------------------------------+
| Field                | Value                                               |
+----------------------+-----------------------------------------------------+
| external_gateway_info | enable_snat: false                                 |
|                      | ip_addresses:                                       |
|                      | - 10.94.129.76                                      |
|                      | network_id: 720e45bc-4225-49de-9346-26513d8d1262 |
| id                   | b9d8b000-5d06-4768-9f65-2715250cda53                |
| name                 | myrouter                                            |
| project_id           | 894696133031439f8aaa7e4868dcbd4d                    |
| routes               | []                                                  |
| status               | ACTIVE                                              |
+----------------------+-----------------------------------------------------+
```

Удаление виртуальных маршрутизаторов

Предварительные требования

- Создан виртуальный маршрутизатор, как описано в разделе "Создание виртуальных маршрутизаторов" на странице 562.

Удаление виртуального маршрутизатора

Панель администратора

1. На экране **Вычисления** > **Сеть** перейдите на вкладку **Маршрутизаторы**.
2. В списке виртуальных маршрутизаторов выберите маршрутизатор, который вы хотите удалить, и нажмите **Удалить**.
3. В окне подтверждения нажмите **Удалить маршрутизатор**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute router delete <router>
```

<router>

Идентификатор или имя виртуального маршрутизатора.

Например, чтобы удалить виртуальный маршрутизатор myrouter, выполните:

```
# vinfra service compute router delete myrouter
Operation successful
```

7.6.3.4 Управление плавающими IP-адресами

Виртуальная машина, подключенная к виртуальной сети, может быть доступна из внешних сетей, таких как Интернет, через плавающий IP-адрес. Такой адрес берется из физической сети и сопоставляется с частным IP-адресом ВМ. Плавающий и частный IP-адреса используются одновременно на сетевом интерфейсе ВМ. Частный IP-адрес предназначен для связи с другими ВМ в виртуальной сети. Плавающий IP-адрес предназначен для доступа к ВМ из внешних сетей. Гостевая операционная система ВМ не имеет сведений о назначенном плавающем IP-адресе.

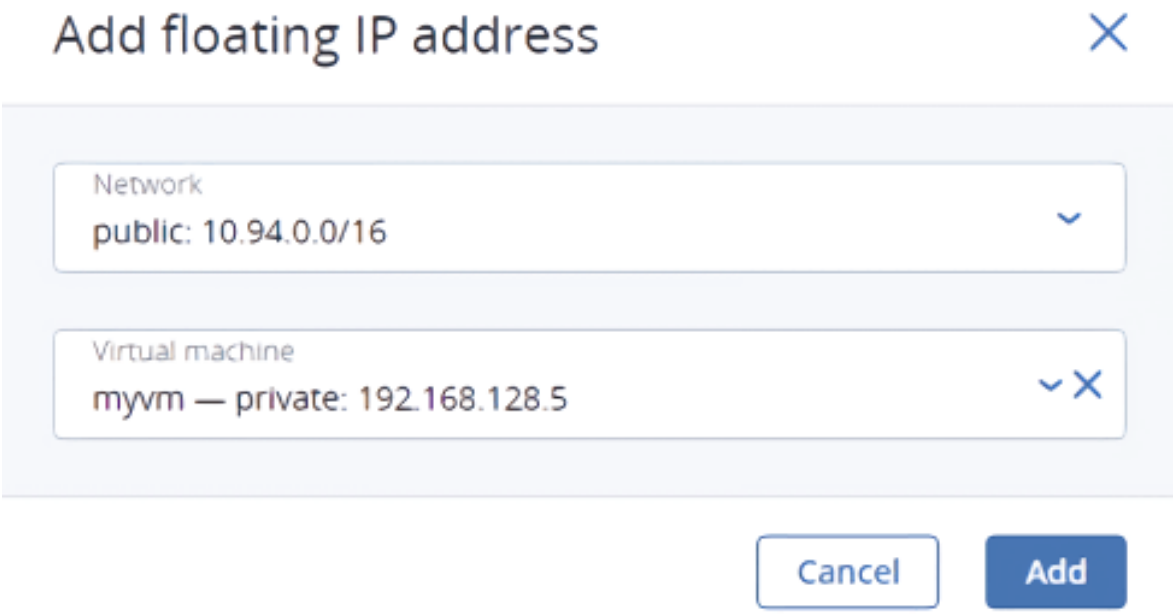
Предварительные требования

- Создан виртуальный маршрутизатор, как описано в разделе "Создание виртуальных маршрутизаторов" на странице 562.
- У виртуальной машины, которой следует назначить плавающий IP-адрес, есть фиксированный частный IP-адрес.
- Виртуальный маршрутизатор соединяет физическую сеть, из которой будет взят плавающий IP-адрес, с виртуальной сетью ВМ.

Как создать плавающий IP-адрес и назначить его виртуальной машине

Панель администратора

1. На экране **Плавающие IP-адреса** нажмите **Добавить плавающий IP-адрес**.
2. В окне **Добавить плавающий IP-адрес** выберите физическую сеть, из которой будет взят плавающий IP, и сетевой интерфейс ВМ с фиксированным частным IP-адресом.



3. Нажмите **Добавить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute floatingip create [--floating-ip <floating-ip>]
                                         [--port-id <port-id>]
                                         [--fixed-ip <fixed-ip>]
                                         [--description <description>]
                                         --network <network>
```

--floating-ip <floating-ip>

Плавающий IP-адрес.

--port-id <port-id>

Идентификатор порта, который будет связан с плавающим IP-адресом. Чтобы узнать идентификатор порта выбранной виртуальной машины, используйте команду vinfra service compute server iface list.

--fixed-ip <fixed-ip>

IP-адрес порта (требуется, только если у порта несколько IP-адресов).

--description <description>

Описание плавающего IP-адреса.

--network <network>

Идентификатор или имя сети, из которой будет выделен плавающий IP-адрес.

Например, чтобы создать плавающий IP-адрес из физической сети public и назначить его виртуальной машине на порт с идентификатором 418c8c9e-aaa5-42f2-8da7-24bfead6f28b и виртуальным IP-адресом 192.168.128.5, выполните:

```
# vinfra service compute floatingip create public --port-id 418c8c9e-aaa5-42f2-8da7-24bfead6f28b \
--fixed-ip-address 192.168.128.5
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| attached_to         | a172cb6a-1c7b-4157-9e86-035f3077646f |
| description         |                                      |
| fixed_ip_address    | 192.168.128.5                        |
| floating_ip_address | 10.94.129.72                         |
| floating_network_id | 720e45bc-4225-49de-9346-26513d8d1262 |
| id                  | a709f884-c43f-4a9a-a243-a340d7682ef8 |
| port_id             | 418c8c9e-aaa5-42f2-8da7-24bfead6f28b |
| project_id          | 894696133031439f8aaa7e4868dcbd4d     |
| router_id           | f7f86029-a553-4d61-b7ec-6f581d9c5f5f |
| status              | DOWN                                 |
+---------------------+--------------------------------------+
```

Созданный плавающий IP-адрес появится в выводе команды vinfra service compute floatingip list:

```
# vinfra service compute floatingip list -c id -c fixed_ip_address -c port_id -c floating_ip_address
+--------------------+---------------------+--------------------+---------------------+
| id                 | fixed_ip_address    | port_id            | floating_ip_address |
+--------------------+---------------------+--------------------+---------------------+
| a709f884-<...>     | 192.168.128.5       | 418c8c9e-<...>     | 10.94.129.72        |
+--------------------+---------------------+--------------------+---------------------+
```

Как получить сведения о плавающем IP-адресе

Используйте следующую команду:

```
vinfra service compute floatingip show <floating-ip>
```

<floating-ip>

Идентификатор плавающего IP-адреса.

Например, чтобы вывести сведения о плавающем IP-адресе с идентификатором a709f884-c43f-4a9a-a243-a340d7682ef8, выполните:

```
# vinfra service compute floatingip show a709f884-c43f-4a9a-a243-a340d7682ef8
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| attached_to         | a172cb6a-1c7b-4157-9e86-035f3077646f |
```

```
| description       |                                      |
| fixed_ip_address  | 192.168.128.5                        |
| floating_ip_address | 10.94.129.72                       |
| floating_network_id | 720e45bc-4225-49de-9346-26513d8d1262 |
| id                | a709f884-c43f-4a9a-a243-a340d7682ef8 |
| port_id           | 418c8c9e-aaa5-42f2-8da7-24bfead6f28b |
| project_id        | 894696133031439f8aaa7e4868dcbd4d     |
| router_id         | f7f86029-a553-4d61-b7ec-6f581d9c5f5f |
| status            | ACTIVE                               |
+-------------------+--------------------------------------+
```

Как переназначить плавающий IP-адрес другой виртуальной машине

Панель администратора

1. Нажмите значок с многоточием напротив плавающего IP-адреса и выберите **Снять назначение**.
2. Когда имя ВМ исчезнет из столбца **Назначен**, снова нажмите значок с многоточием и выберите **Назначить**.
3. В окне **Назначить плавающий IP-адрес** выберите сетевой интерфейс ВМ с фиксированным частным IP-адресом.
4. Нажмите **Назначить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute floatingip set [--port-id <port-id>] [--fixed-ip <fixed-ip>]
                                      [--description <description>] <floating-ip>
```

--port-id <port-id>

Идентификатор порта, который будет связан с плавающим IP-адресом.

--fixed-ip <fixed-ip>

IP-адрес порта (требуется, только если у порта несколько IP-адресов).

--description <description>

Описание плавающего IP-адреса.

<floating-ip>

Идентификатор плавающего IP-адреса.

Например, чтобы назначить плавающий IP-адрес с идентификатором a709f884-c43f-4a9a-a243-a340d7682ef8 виртуальной машине на порт с идентификатором 8c11c29b-9a73-4017-baff-1e872b18b54b и виртуальным IP-адресом 192.128.30.15, выполните:

```
# vinfra service compute floatingip set a709f884-c43f-4a9a-a243-a340d7682ef8 \
--port-id 8c11c29b-9a73-4017-baff-1e872b18b54b --fixed-ip-address 192.128.30.15
+-------------------+--------------------------------------+
```

```
| Field            | Value                                |
+------------------+--------------------------------------+
| attached_to      | 3a092f6f-bbaf-47a9-bcc7-f86223aacb55 |
| description      |                                      |
| fixed_ip_address | 192.128.30.15                        |
| floating_ip_address | 10.94.129.72                      |
| floating_network_id | 720e45bc-4225-49de-9346-26513d8d1262 |
| id               | a709f884-c43f-4a9a-a243-a340d7682ef8 |
| port_id          | 8c11c29b-9a73-4017-baff-1e872b18b54b |
| project_id       | 894696133031439f8aaa7e4868dcbd4d     |
| router_id        | f7f86029-a553-4d61-b7ec-6f581d9c5f5f |
| status           | ACTIVE                               |
+------------------+--------------------------------------+
```

Как удалить плавающий IP-адрес

Панель администратора

1. Отмените его назначение виртуальной машине. Нажмите значок с многоточием напротив плавающего IP-адреса и выберите **Снять назначение**.
2. Снова нажмите значок с многоточием и выберите **Удалить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute floatingip delete <floating-ip>
```

<floating-ip>

Идентификатор плавающего IP-адреса.

Например, чтобы удалить плавающий IP-адрес с идентификатором a709f884-c43f-4a9a-a243-a340d7682ef8, выполните:

```
# vinfra service compute floatingip delete a709f884-c43f-4a9a-a243-a340d7682ef8
Operation successful
```

7.6.3.5 Управление балансировщиками нагрузки

Балансировщики нагрузки создаются и управляются пользователями самообслуживания, как описано в разделе «Управление балансировщиками нагрузки» в Руководстве по самообслуживанию. На панели администрирования можно отслеживать состояние пулов балансировки, управлять ими, а также включать, отключать и удалять балансировщики нагрузки.

Создание и удаление балансировщиков нагрузки

Предварительные требования

- Должен быть создан вычислительный кластер, как описано в разделе "Создание вычислительного кластера" на странице 169.
- Служба балансировщика нагрузки должна быть установлена либо в ходе развертывания вычислительного кластера, либо позже, как описано в разделе "Подготовка к работе балансировщиков нагрузки" на странице 191.

Чтобы создать балансировщик нагрузки

Используйте следующую команду:

```
vinfra service compute load-balancer create [--description <description>]
                                            [--enable | --disable]
                                            [--address <address>]
                                            [--floating-ip <floating-ip>]
                                            [--pools-config <pools>]
                                            <name> <network>
```

--description <description>

Описание балансировщика нагрузки.

--enable

Включение балансировщика нагрузки.

--disable

Отключение балансировщика нагрузки.

--address <address>

IP-адрес, который балансировщик нагрузки попытается выделить в сети.

--floating-ip <floating-ip>

Плавающий IP-адрес, который будет использоваться для подключения к балансировщику нагрузки из внешних сетей.

--pools-config <pools>

Файл конфигурации пулов.

Ниже приведен пример файла конфигурации пулов в формате YAML.

```
- backend_protocol: HTTPS
  backend_protocol_port: 443
  healthmonitor: {delay: 5, max_retries: 3, max_retries_down: 3, timeout: 5,
    type: PING, url_path: /}
  lb_algorithm: ROUND_ROBIN
  members:
  - address: 192.168.30.49
  - address: 192.168.30.15
  name: pool1
  protocol: HTTPS
  protocol_port: 443
  sticky_session: False
```

<name>

Имя балансировщика нагрузки.

<network>

Идентификатор или имя сети, в которой будет работать балансировщик нагрузки.

Например, чтобы создать балансировщик нагрузки mylbaas без пулов балансировки, который будет работать в сети private с плавающим IP-адресом 10.94.129.70, выполните:

```
# vinfra service compute load-balancer create mylbaas private1 \
                --floating-ip 10.94.129.70
+---------------+--------------------------------------+
| Field         | Value                                |
+---------------+--------------------------------------+
| address       | 192.168.30.230                       |
| amphorae      |                                      |
| created_at    | 2019-11-18T12:59:08.243413           |
| description   |                                      |
| enabled       | True                                 |
| floating_ip   | 10.94.129.70                         |
| ha_enabled    |                                      |
| id            | 941bf637-2d55-40f0-92c0-e65d6567b468 |
| members_count | 0                                    |
| name          | mylbaas                              |
| network_id    | 2b821d00-e428-4a76-b1ae-d181c9f5ae7f |
| pools         | []                                   |
| port_id       | 2d8ab88a-847c-4396-857e-11eaa80e1b24 |
| project_id    | e4e059c67dee4736851df14d4519a5a5     |
| status        | CREATING                             |
| updated_at    |                                      |
+---------------+--------------------------------------+
```

Созданный балансировщик нагрузки появится в выводе команды vinfra service compute load-balancer list.

Чтобы удалить балансировщик нагрузки

Панель администратора

1. На вкладке **Вычисления** > **Сеть** > **Балансировщики нагрузки** выберите балансировщик нагрузки.
2. Щелкните по значку многоточия рядом с ним, затем нажмите **Удалить**.
3. Нажмите **Удалить** в окне подтверждения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute load-balancer delete <load-balancer>
```

<load-balancer>

Идентификатор или имя балансировщика нагрузки.

Например, чтобы удалить балансировщик нагрузки mylbaas, выполните:

```
# vinfra service compute load-balancer delete mylbaas
```

Просмотр сведений о балансировщиках нагрузки

Чтобы просмотреть свойства балансировщика нагрузки

Панель администратора

1. На вкладке **Вычисления** > **Сеть** > **Балансировщики нагрузки** выберите нужный балансировщик нагрузки.
2. Откройте вкладку **Свойства**. В поле **Виртуальные машины** можно найти имена экземпляров балансировщика нагрузки.
3. Щелкните по имени нужного экземпляра, чтобы открыть соответствующую панель виртуальной машины.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute load-balancer show <load-balancer>
```

<load-balancer>

Идентификатор или имя балансировщика нагрузки

Например, чтобы просмотреть свойства балансировщика нагрузки mylbaas, выполните:

```
# vinfra service compute load-balancer show mylbaas
+---------------+-------------------------------------------------------+
| Field         | Value                                                 |
+---------------+-------------------------------------------------------+
| address       | 192.168.30.230                                        |
| amphorae      | - active: true                                        |
|               |   compute_id: b0c4793f-e1b1-4251-91c2-94e34787f537 |
|               |   created_at: '2019-11-18T12:59:12.742446'        |
|               |   id: b7b23106-a87b-412d-9ce6-7c69b5594342        |
|               |   image_id: 6d1ba6f9-cf86-4ea4-a32d-f138868a9742  |
|               |   role: STANDALONE                                |
|               |   status: ALLOCATED                               |
|               |   updated_at: '2019-11-18T13:01:07.601184'        |
| created_at    | 2019-11-18T12:59:08.243413                        |
| description   |                                                   |
| enabled       | True                                              |
| floating_ip   | 10.94.129.70                                      |
| ha_enabled    | False                                             |
| id            | 941bf637-2d55-40f0-92c0-e65d6567b468              |
| members_count | 0                                                 |
| name          | mylbaas                                           |
| network_id    | 2b821d00-e428-4a76-b1ae-d181c9f5ae7f              |
```

```
| pools       | []                                   |
| port_id     | 2d8ab88a-847c-4396-857e-11eaa80e1b24           |
| project_id  | e4e059c67dee4736851df14d4519a5a5               |
| status      | ACTIVE                                 |
| updated_at  | 2019-11-18T13:01:10.983144                 |
+-------------+----------------------------------------------------+
```

Включение и выключение балансировщиков нагрузки

Чтобы включить/отключить балансировщик нагрузки

Панель администратора

1. На вкладке **Вычисления** > **Сеть** > **Балансировщики нагрузки** выберите балансировщик нагрузки.
2. Щелкните по значку многоточия рядом с ним, затем нажмите **Включить** или **Отключить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute load-balancer set [--enable | --disable] <load-balancer>
```

--enable

Включение балансировщика нагрузки.

--disable

Отключение балансировщика нагрузки.

<load-balancer>

Идентификатор или имя балансировщика нагрузки.

Например, чтобы отключить балансировщик нагрузки mylbaas, выполните:

```
# vinfra service compute load-balancer set mylbaas --disable \
--description "Disabled load balancer"
+-------------+--------------------------------------+
| Field       | Value                                |
+-------------+--------------------------------------+
| address     | 192.168.30.230                       |
| amphorae    |                                      |
| created_at  | 2019-11-18T12:59:08.243413           |
| description | Disabled load balancer               |
| enabled     | False                                |
| floating_ip |                                      |
| ha_enabled  |                                      |
| id          | 941bf637-2d55-40f0-92c0-e65d6567b468 |
| members_count | 0                                  |
| name        | mylbaas                              |
| network_id  | 2b821d00-e428-4a76-b1ae-d181c9f5ae7f |
```

```
| pools       | []                                   |
| port_id     | 2d8ab88a-847c-4396-857e-11eaa80e1b24 |
| project_id  | e4e059c67dee4736851df14d4519a5a5     |
| status      | DISABLED                             |
| updated_at  | 2019-11-18T13:09:09.151442           |
+-------------+--------------------------------------+
```

Выполнение переключения при сбое балансировщика нагрузки

Чтобы выполнить переключение при сбое балансировщика нагрузки

Используйте следующую команду:

```
vinfra service compute load-balancer failover <load-balancer>
```

<load-balancer>

Идентификатор или имя балансировщика нагрузки

Например, чтобы выполнить переключение на резерв при сбое балансировщика нагрузки mylbaas, выполните:

```
# vinfra service compute load-balancer failover mylbaas
Operation accepted.
```

Управление пулами балансировки

Создание пула балансировщика нагрузки

Используйте следующую команду:

```
vinfra service compute load-balancer pool create --protocol
                                {HTTP,HTTPS,TCP,UDP}
                                 --port <port>
                                 --algorithm <algorithm>
                                 --backend-protocol
                                 {HTTP,HTTPS,TCP,UDP}
                                 --backend-port <backend-port>
                                 [--certificate-file <cert-file>]
                                 [--connection-limit <limit>]
                                 [--description <description>]
                                 [--healthmonitor type=<type>,
                                 url_path=<url>[,key=value,...]]
                                 [--member address=<ip>
                                 [,enabled=<bool>, weight=<int>]]
                                 [--privatekey-file <key>]
                                 [--enable-sticky-session |
                                 --disable-sticky-session]
                                 [--enable | --disable]
                                 [--name <name>] <load-balancer>
```

--protocol

Протокол для входящих подключений (HTTP, HTTPS, TCP или UDP).

--port <port>

Порт для входящих подключений.

--algorithm <algorithm>

Алгоритм балансировки нагрузки (LEAST_CONNECTIONS, ROUND_ROBIN или SOURCE_IP).

--backend-protocol

Протокол для целевых подключений (HTTP, HTTPS, TCP или UDP).

--backend-port <backend-port>

Порт для целевых подключений.

--certificate-file <cert-file>

Файл сертификата x.509 в формате PEM. Требуется для TLS-терминированных балансировщиков нагрузки HTTPS->HTTP.

--connection-limit <limit>

Максимально разрешенное количество подключений для этого пула. Значение по умолчанию – это -1 (неограниченные подключения).

--description <description>

Описание пула.

--healthmonitor type=<type>,url_path=<url>[,key=value,...]

Параметры монитора состояния:

- type: тип монитора состояния (HTTP, HTTPS, PING, TCP или UDP).
- url_path: URL-путь к монитору состояния.
- разделенные запятыми пары key=value с ключами (необязательно):
  - delay: время в секундах между отправками запросов участникам.
  - enabled: указывает, включен монитор состояния или нет (true или false).
  - max_retries: количество успешных проверок, необходимых для смены статуса участника на HEALTHY. Значение в диапазоне от 1 до 10.
  - max_retries_down: количество неуспешных проверок, необходимых для смены статуса участника на UNHEALTHY. Значение в диапазоне от 1 до 10.
  - timeout: максимальное время в секундах, в течение которого монитор ожидает подключения. Это значение должно быть меньше значения delay.

--member address=<ip>[,enabled=<bool>,weight=<int>]

Параметры участника:

- address=<ip>: адрес IPv4 виртуальной машины.
- enabled=<bool> указывает, включен участник или нет. Может иметь значение true или false.

- weight=<int> определяет долю подключений, которые обслуживает участник по сравнению с другими участниками пула. Например, weight 10 означает, что этот участник обрабатывает в пять раз больше подключений, чем участник с weight 2. Значение 0 показывает, что этот участник не получает новых подключений, но продолжает обслуживать существующие. Значение может быть в диапазоне от 0 до 256. Значение по умолчанию – 1.

Этот параметр можно использовать несколько раз.

--privatekey-file <key>

Закрытый TLS-ключ в формате PEM. Требуется для TLS-терминированных балансировщиков нагрузки HTTPS->HTTP.

--enable-sticky-session

Включить сохранение сеанса.

--disable-sticky-session

Отключить сохранение сеанса.

--enable

Включить пул.

--disable

Отключить пул.

--name <name>

Имя пула

<load-balancer>

Идентификатор или имя балансировщика нагрузки.

Например, чтобы создать пул балансировки, выполните:

```
# vinfra service compute load-balancer pool create mylbaas --protocol HTTP \
--port 80 --backend-protocol HTTP --backend-port 80 --name mypool \
--algorithm LEAST_CONNECTIONS --member address=192.168.31.153 \
--member address=192.168.31.22 --enable-sticky-session
+----------------------+--------------------------------------+
| Field                | Value                                |
+----------------------+--------------------------------------+
| backend_protocol     | HTTP                                 |
| backend_protocol_port | 80                                  |
| certificate          |                                      |
| connection_limit     | -1                                   |
| created_at           | 2019-11-18T13:11:27.982129           |
| description          |                                      |
| enabled              | True                                 |
| healthmonitor        |                                      |
| id                   | fa40e282-b29a-465a-afaa-2c702d2bde17 |
| lb_algorithm         | LEAST_CONNECTIONS                    |
```

```
| listener_id         | 66cc714e-af7f-40eb-9db8-67b8b6b6d23c |
| loadbalancer_id     | 941bf637-2d55-40f0-92c0-e65d6567b468 |
| members             | []                                   |
| name                | mypool                               |
| private_key         |                                      |
| project_id          | e4e059c67dee4736851df14d4519a5a5     |
| protocol            | HTTP                                 |
| protocol_port       | 80                                   |
| status              | CREATING                             |
| sticky_session      | True                                 |
| updated_at          |                                      |
+---------------------+--------------------------------------+
```

Эта команда добавляет пул балансировки mypool для балансировщика нагрузки mylbaas со следующими параметрами:

- правило перенаправления «HTTP на порте 80 -> HTTP на порте 80»,
- алгоритм балансировки LEAST_CONNECTIONS,
- два участника в пуле,
- сохранение сеанса включено.

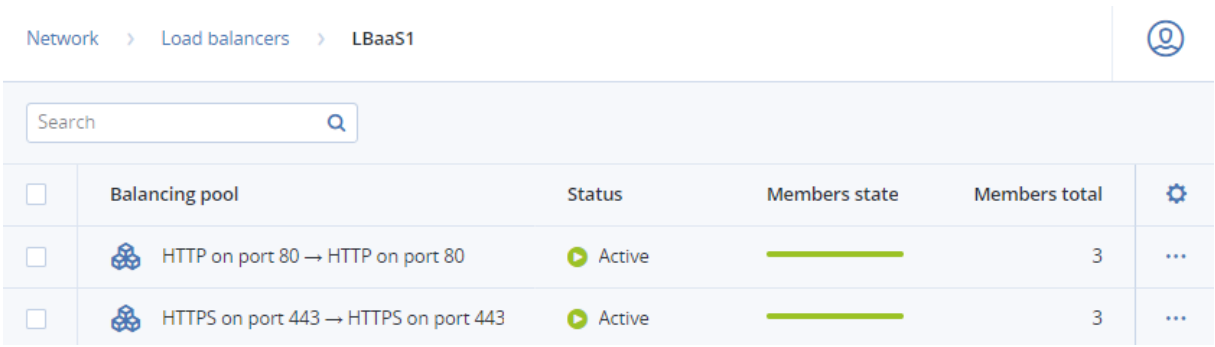
Созданный пул появится в выводе команды vinfra service compute load-balancer pool list:

```
# vinfra service compute load-balancer pool list --load-balancer mylbaas -c id \
-c protocol -c protocol_port -c backend_protocol -c backend_protocol_port -c status
+-----------+----------+---------------+--------------+--------------+--------+
| id        | protocol | protocol_port | backend<...> | backend<...> | status |
+-----------+----------+---------------+--------------+--------------+--------+
| fa40<...> | HTTP     |            80 | HTTP         |           80 | ACTIVE |
+-----------+----------+---------------+--------------+--------------+--------+
```

Просмотр сведений о пуле балансировщика нагрузки

Панель администратора

На вкладке **Вычисления** > **Сеть** > **Балансировщики нагрузки** щелкните по имени балансировщика нагрузки, чтобы отобразить его список пулов балансировки.



Для отслеживания производительности и работоспособности пула откройте панель этого пула на вкладке **Обзор**.

Чтобы просмотреть параметры пула, откройте панель пула и перейдите на вкладку **Свойства**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute load-balancer pool show <pool>
```

<pool>

Идентификатор или имя пула балансировщика нагрузки.

Например, чтобы вывести сведения о пуле балансировщика нагрузки mypool, выполните:

```
# vinfra service compute load-balancer pool show mypool
+----------------------+--------------------------------------------+
| Field                | Value                                      |
+----------------------+--------------------------------------------+
| backend_protocol     | HTTP                                       |
| backend_protocol_port | 80                                        |
| certificate          |                                            |
| connection_limit     | -1                                         |
| created_at           | 2019-11-18T13:11:27.982129                 |
| description          |                                            |
| enabled              | True                                       |
| healthmonitor        |                                            |
| id                   | fa40e282-b29a-465a-afaa-2c702d2bde17       |
| lb_algorithm         | LEAST_CONNECTIONS                          |
| listener_id          | 66cc714e-af7f-40eb-9db8-67b8b6b6d23c       |
| loadbalancer_id      | 941bf637-2d55-40f0-92c0-e65d6567b468       |
| members              | - address: 192.168.31.153                  |
|                      |   compute_server_id: d51c10a7-6187-<...>   |
|                      |   created_at: '2019-11-18T13:11:59.681101' |
|                      |   enabled: true                            |
|                      |   id: 3fd5dcc5-6e2c-4e22-8d0a-8e94e20a122f |
|                      |   name: ''                                 |
|                      |   pool_id: null                            |
|                      |   status: HEALTHY                          |
|                      |   updated_at: '2019-11-18T13:12:01.467306' |
|                      |   weight: 1                                |
|                      | - address: 192.168.31.22                   |
|                      |   compute_server_id: 54603109-8963-<...>   |
|                      |   created_at: '2019-11-18T13:12:10.176853' |
|                      |   enabled: true                            |
|                      |   id: ccb645b3-63c7-44f8-b861-b197c85506d4 |
|                      |   name: ''                                 |
|                      |   pool_id: null                            |
|                      |   status: HEALTHY                          |
|                      |   updated_at: '2019-11-18T13:12:12.281578' |
|                      |   weight: 1                                |
```

```
| name              | mypool                              |
| private_key       |                                     |
| project_id        | e4e059c67dee4736851df14d4519a5a5    |
| protocol          | HTTP                                |
| protocol_port     | 80                                  |
| status            | ACTIVE                              |
| sticky_session    | True                                |
| updated_at        | 2019-11-18T13:12:12.305509          |
+-------------------+-------------------------------------+
```

Изменение параметров пула балансировщика нагрузки

Панель администратора

1. На вкладке **Вычисления** > **Сеть** > **Балансировщики нагрузки** щелкните по имени балансировщика нагрузки, чтобы отобразить его список пулов балансировки.
2. Для управления участниками пула откройте панель пула и перейдите на вкладку **Участники**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute load-balancer pool set [--name <name>
                                --protocol {HTTP,HTTPS,TCP,UDP}]
                                [--port <port>
                                --algorithm <algorithm>]
                                [--backend-protocol
                                {HTTP,HTTPS,TCP,UDP}]
                                [--backend-port <backend-port>]
                                [--certificate-file <cert-file>]
                                [--connection-limit <limit>]
                                [--description <description>]
                                [--healthmonitor type=<type>,
                                url_path=<url>[,key=value,...]]
                                [--member address=<ip>
                                [,enabled=<bool>,weight=<int>]]
                                [--privatekey-file <key>]
                                [--enable-sticky-session |
                                --disable-sticky-session]
                                [--enable | --disable]  <pool>
```

--name <name>

Имя пула.

--protocol

Протокол для входящих подключений (HTTP, HTTPS, TCP или UDP).

--port <port>

Порт для входящих подключений.

--algorithm <algorithm>

Алгоритм балансировки нагрузки (LEAST_CONNECTIONS, ROUND_ROBIN или SOURCE_IP).

--backend-protocol

Протокол для целевых подключений (HTTP, HTTPS, TCP или UDP).

--backend-port <backend-port>

Порт для целевых подключений.

--certificate-file <cert-file>

Файл сертификата x.509 в формате PEM. Требуется для TLS-терминированных балансировщиков нагрузки HTTPS->HTTP.

--connection-limit <limit>

Максимально разрешенное количество подключений для этого пула. Значение по умолчанию – это -1 (неограниченные подключения).

--description <description>

Описание пула.

--healthmonitor type=<type>,url_path=<url>[,key=value,...]

Параметры монитора состояния:

- type: тип монитора состояния (HTTP, HTTPS, PING, TCP или UDP).
- url_path: URL-путь к монитору состояния.
- разделенные запятыми пары key=value с ключами (необязательно):
  - delay: время в секундах между отправками запросов участникам.
  - enabled: указывает, включен монитор состояния или нет (true или false).
  - max_retries: количество успешных проверок, необходимых для смены статуса участника на HEALTHY. Значение в диапазоне от 1 до 10.
  - max_retries_down: количество неуспешных проверок, необходимых для смены статуса участника на UNHEALTHY. Значение в диапазоне от 1 до 10.
  - timeout: максимальное время в секундах, в течение которого монитор ожидает подключения. Это значение должно быть меньше значения delay.

--member address=<ip>[,enabled=<bool>,weight=<int>]

Параметры участника:

- address=<ip>: адрес IPv4 виртуальной машины.
- enabled=<bool> указывает, включен участник или нет. Может иметь значение true или false.
- weight=<int> определяет долю подключений, которые обслуживает участник по сравнению с другими участниками пула. Например, weight 10 означает, что этот участник обрабатывает в пять раз больше подключений, чем участник с weight 2. Значение 0 показывает, что этот участник не получает новых подключений, но продолжает обслуживать существующие. Значение может быть в диапазоне от 0 до 256. Значение по умолчанию – 1.

Этот параметр можно использовать несколько раз.

--privatekey-file <key>

Закрытый TLS-ключ в формате PEM. Требуется для TLS-терминированных балансировщиков нагрузки HTTPS->HTTP.

--enable-sticky-session

Включить сохранение сеанса.

--disable-sticky-session

Отключить сохранение сеанса.

--enable

Включить пул.

--disable

Отключить пул.

<pool>

Идентификатор или имя пула балансировщика нагрузки.

Например, чтобы изменить параметры пула балансировки mypool, выполните:

```
# vinfra service compute load-balancer pool set mypool --algorithm ROUND_ROBIN \
--member address=192.168.31.153 --member address=192.168.31.22 \
--member address=192.168.31.51 --disable-sticky-session
Operation accepted.
```

Эта команда изменяет параметры пула следующим образом:

- Устанавливает алгоритм балансировки ROUND_ROBIN.
- Добавляет третьего участника в пул.
- Отключает сохранение сеанса.

Удаление пула балансировщика нагрузки

Панель администратора

1. На вкладке **Вычисления** > **Сеть** > **Балансировщики нагрузки** щелкните по имени балансировщика нагрузки, чтобы отобразить его список пулов балансировки.
2. Чтобы удалить пул балансировки, нажмите значок с многоточием рядом с ним и выберите **Удалить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute load-balancer pool delete <pool>
```

<pool>

Идентификатор или имя пула балансировщика нагрузки.

Например. чтобы удалить пул балансировщика нагрузки mypool, выполните:

```
# vinfra service compute load-balancer pool delete mypool
Operation successful.
```

Изменение типа ВМ по умолчанию для балансировщика нагрузки

По умолчанию балансировщик нагрузки создается с частным типом ВМ amphora, которым нельзя управлять через vinfra, однако тип ВМ можно изменить с помощью инструмента командной строки OpenStack.

Предварительные требования

- Для авторизации выполнения приведенных ниже команд настроен клиент командной строки OpenStack, как описано в разделе "Подключение к интерфейсу командной строки OpenStack" на странице 427.

Чтобы изменить тип ВМ по умолчанию для балансировщика нагрузки

1. Проверьте, что стандартный тип ВМ amphora существует:

```
# openstack --insecure flavor list --all
+---------+---------+-------+------+-----------+-------+-----------+
| ID      | Name    |   RAM | Disk | Ephemeral | VCPUs | Is Public |
+---------+---------+-------+------+-----------+-------+-----------+
| 100     | tiny    |   512 |    0 |         0 |     1 | True      |
| 101     | small   |  2048 |    0 |         0 |     1 | True      |
| 102     | medium  |  4096 |    0 |         0 |     2 | True      |
| 103     | large   |  8192 |    0 |         0 |     4 | True      |
| 104     | xlarge  | 16384 |    0 |         0 |     8 | True      |
| amphora | amphora |  4096 |   30 |         0 |     2 | False     |
+---------+---------+-------+------+-----------+-------+-----------+
```

2. Удалите этот тип ВМ:

```
# openstack --insecure flavor delete amphora
```

3. Создайте новый тип ВМ amphora с нужными параметрами. Например:

```
# openstack --insecure flavor create amphora --id amphora --ram 8192 \
--vcpus 4 --disk 60 --private
+----------------------------+---------+
| Field                      | Value   |
+----------------------------+---------+
| OS-FLV-DISABLED:disabled   | False   |
| OS-FLV-EXT-DATA:ephemeral  | 0       |
| disk                       | 60      |
| id                         | amphora |
| name                       | amphora |
| os-flavor-access:is_public | False   |
| properties                 |         |
| ram                        | 8192    |
| rxtx_factor                | 1.0     |
```

```
| swap                        |       |
| vcpus                       | 4     |
+-----------------------------+---------+
```

4. Измените тип ВМ балансировщика нагрузки, выполнив переключение на резерв. Например:

```
# openstack --insecure loadbalancer failover mylbaas
```

Балансировщик нагрузки mylbaas будет создан заново с 4 виртуальными ЦП, 8 ГБ ОЗУ и 30 ГБ дискового пространства.

7.6.3.6 Управление соединениями VPN

Виртуальная частная сеть как услуга (VPN as a Service) – это возможность, предоставляемая продуктом Кибер Инфраструктура, с помощью которой пользователи самообслуживания могут соединять виртуальные сети через общедоступные сети, такие как Интернет. Для соединения двух или более конечных точек виртуальные частные сети используют виртуальные соединения, для которых выполнятся туннелирование через физические сети. Для обеспечения безопасности обмена данными при использовании VPN трафик, проходящий между удаленными конечными точками, шифруется. Реализация VPN в продукте Кибер Инфраструктура использует протоколы Internet Key Exchange (IKE) и IP Security (IPsec), чтобы устанавливать безопасные соединения VPN, и основана на IPsec-решении strongSwan.

Кроме того, поддерживается высокая доступность соединений VPN в кластерах с включенной высокой доступностью. Если сервер, на котором размещен виртуальный маршрутизатор, откажет, соединение VPN будет установлено повторно, после того как виртуальный маршрутизатор будет перемещен на работоспособный сервер.

Соединения VPN создаются и управляются пользователями самообслуживания, как описано в разделе «Управление соединениями VPN» руководства по самообслуживанию. В панели администрирования можно просматривать сведения о соединениях VPN, а также удалять их.

Ограничения

- Туннелирование соединений VPN не может быть выполнено через физические сети IPv6 и физические сети с двойным стеком.

Предварительные требования

- Должен быть создан вычислительный кластер, как описано в разделе "Создание вычислительного кластера" на странице 169.

Чтобы просмотреть сведения о соединении VPN

Панель администратора

На экране **Вычисления** > **Сеть** > **VPN** выберите соединение VPN, чтобы открыть его правую панель.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute vpn connection show <connection>
```

<connection>

Идентификатор или имя соединения VPN

Например, чтобы просмотреть сведения о VPN-соединении vpn1, выполните:

```
# vinfra service compute vpn connection show vpn1
+------------------+--------------------------------------+
| Field            | Value                                |
+------------------+--------------------------------------+
| dpd              | action: hold                         |
|                  | interval: 30                         |
|                  | timeout: 120                         |
| id               | 9848fd7c-ac1c-4412-bf8d-7616b13a3d03 |
| ikepolicy_id     | 1d70c833-4a8b-455b-9a1b-a86a61159123 |
| initiator        | bi-directional                       |
| ipsecpolicy_id   | 2e1edf17-2874-41ba-9faa-0cb879d09c97 |
| local_ep_group_id | cc8959d8-7274-44b3-b76c-373b19b1ca32 |
| local_id         |                                      |
| mtu              | 1500                                 |
| name             | vpn1                                 |
| peer_address     | 10.136.18.134                        |
| peer_ep_group_id | deb02fcd-6e24-46e8-b3db-bf41b9ec2564 |
| peer_id          | 10.136.18.134                        |
| project_id       | bba7c2edf544432c9177e2b63b755e10     |
| route_mode       | static                               |
| router_id        | 1da614a7-3fe7-42e0-9494-864d1e890135 |
| status           | ACTIVE                               |
| vpnservice_id    | 01a4ee33-2192-4575-9b01-629144093712 |
+------------------+--------------------------------------+
```

Чтобы удалить соединение VPN

Панель администратора

1. На экране **Вычисления** > **Сеть** > **VPN** выберите соединение VPN.
2. На правой панели нажмите **Удалить**.
3. Нажмите **Удалить** в окне подтверждения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute vpn connection delete <connection>
```

<connection>

Идентификатор или имя соединения VPN

Например, чтобы удалить VPN-соединение vpn1, выполните:

```
# vinfra service compute vpn connection delete vpn1
```

7.6.3.7 Использование сетевых политик качества обслуживания

Политики качества обслуживания можно использовать, чтобы обеспечить или ограничить пропускную способность для исходящего и входящего трафика ВМ в различных проектах. Такие политики можно назначать для отдельных сетевых портов, плавающих IP-адресов или целых сетей. Кроме того, для проекта можно назначить стандартную политику качества обслуживания, чтобы автоматически назначать ее всем новым сетям, созданным в рамках проекта. Стандартная политика качества обслуживания назначается, если во время создания сети явно не назначена другая политика.

При назначении политики сети все порты, подключенные к этой сети, наследуют эту политику, если им не назначены другие политики. Назначенная политика применяется как к существующим, так и новым виртуальным машинам. Сетевые политики не применяются к портам внутренней сети, например DHCP, и портам внутреннего маршрутизатора.

Правила политики качества обслуживания

Для определения политики качества обслуживания можно создавать правила двух типов: ограничение пропускной способности и минимальную пропускную способность.

Ограничение пропускной способности

Вводит ограничение пропускной способности для сетей, портов и плавающих IP-адресов. Любой трафик ВМ, превышающий указанный показатель, будет остановлен.

Чтобы задать ограничение пропускной способности, настройте следующие параметры:

- max_kbps: максимальная пропускная способность отправки данных ВМ, в кбит/с.
- max_burst_kbps: максимальный объем данных в кбит/с, пропускаемый на ВМ через порт, если буфер токенов переполнен. Буфер токенов заполняется со скоростью max_kbps.

  Внимание
  - Если для этого параметра установлено слишком низкое значение, использование сети будет затруднено даже при надлежащей настройке ограничений пропускной способности, что приведет к снижению пропускной способности.
  - Если для этого параметра установлено слишком высокое значение, ограничение пакетов будет недостаточным, что приведет к превышению пропускной способности сети.

  Если не указать значение для этого параметра, будет использовано рекомендуемое значение пакетов для трафика TCP, которое составляет 80% от ограничения пропускной способности.

Например, если ограничение пропускной способности составляет 1000 кбит/с, достаточно установить для ограничения пакетов значение 800 кбит/с.

- ingress или egress: направление трафика, к которому применяется правило. Для BM ingress означает загрузку, а egress — отправку.

Минимальная пропускная способность

Обеспечивает минимальную пропускную способность для сетей, портов и плавающих IP-адресов. Трафик BM будет использовать не меньше указанного значения.

Внимание
Политику качества обслуживания с таким правилом нельзя применить ко всей виртуальной сети.

Чтобы задать минимальную пропускную способность, настройте следующие параметры:

- min-kbps: минимальная пропускная способность, гарантированная BM, в кбит/с.
- ingress или egress: направление трафика, к которому применяется правило. Для BM ingress означает загрузку, а egress — отправку.

В одной политике качества обслуживания можно объединять разные типы правил. Например, можно создать правило, ограничивающее пропускную способность, и правило, устанавливающее минимальную пропускную способность. Кроме того, в политику можно добавлять правила одного типа для различных направлений трафика. Например, можно создать два правила, ограничивающие пропускную способность: одно для входящего трафика, другое для исходящего.

Создание политик качества обслуживания

Предварительные требования

- Четкое понимание правил политик качества обслуживания, которые описаны в разделе "Правила политики качества обслуживания" на предыдущей странице.
- Перед тем как создавать политику качества обслуживания как системный администратор, убедитесь, что для пользователя создан файл переменных среды, как описано в разделе "Подключение к интерфейсу командной строки OpenStack" на странице 427.
- Перед тем как создавать политику качества обслуживания как администратор домена, убедитесь, что для пользователя создан файл переменных среды, как описано в разделе "Создание и назначение роли менеджера квот" на странице 307.

Чтобы создать политику качества обслуживания с правилами

1. Создайте политику качества обслуживания:
   - Если вы создаете политику как системный администратор
     a. Используйте файл переменных среды для системного администратора:

        ```
        # source /etc/kolla/admin-openrc.sh
        ```

     b. Создайте политику качества обслуживания в проекте, в котором она будет применяться. Например:

```
# openstack --insecure network qos policy create --project
3823a2d908ea4dd6909a8f93a6f66018 policy1
```

- Если вы создаете политику как администратор домена
  a. Используйте файл переменных среды для администратора домена. Например:

  ```
  # source domain-admin.sh
  ```

  b. Используйте переменную имени проекта для проекта, где вы хотите создать политику качества обслуживания. Например:

  ```
  # export OS_PROJECT_NAME=testproject
  ```

  c. Создайте политику качества обслуживания. Например:

  ```
  # openstack --insecure network qos policy create policy1
  ```

2. Создайте правило для этой политики качества обслуживания:
   - Чтобы задать предел пропускной способности, укажите значение bandwidth-limit для параметра --type и параметры правила. Например, чтобы ограничить исходящий трафик до 3 Мбит/с, выполните следующую команду:

   ```
   # openstack --insecure network qos rule create --type bandwidth-limit \
   --max-kbps 3000 --max-burst-kbits 2400 --egress policy1
   +----------------+-------------------------------------------------+
   | Field          | Value                                           |
   +----------------+-------------------------------------------------+
   | direction      | egress                                          |
   | id             | 6f036f09-d952-420d-986b-27c7eb14b2da            |
   | location       | Munch({'project': Munch({'domain_name': Default, |
   |                | 'domain_id': None, 'name': admin,               |
   |                | 'id': u'e215189c0472482f93e71d10e1245253'}),    |
   |                | 'cloud': '', 'region_name': '', 'zone': None})  |
   | max_burst_kbps | 2400                                            |
   | max_kbps       | 3000                                            |
   | name           | None                                            |
   | project_id     |                                                 |
   +----------------+-------------------------------------------------+
   ```

   - Чтобы установить минимальную пропускную способность, укажите значение minimum-bandwidth для параметра --type и задайте параметры правила. Например, чтобы обеспечить минимальную пропускную способность для входящего трафика не ниже 1000 кбит/с, выполните следующую команду:

   ```
   # openstack --insecure network qos rule create --type minimum-bandwidth \
   --min-kbps 1000 --ingress policy1
   +------------+-------------------------------------------------+
   | Field      | Value                                           |
   +------------+-------------------------------------------------+
   ```

```
| direction  | ingress                                          |
| id         | 4eb79c67-e2b7-4ee7-845c-4cbe39f095cd             |
| location   | Munch({'project': Munch({'domain_name': Default, |
|            | 'domain_id': None, 'name': admin,                |
|            | 'id': u'e215189c0472482f93e71d10e1245253'}),     |
|            | 'cloud': '', 'region_name': '', 'zone': None})   |
| min_kbps   | 1000                                             |
| name       | None                                             |
| project_id |                                                  |
+------------+--------------------------------------------------+
```

Назначение стандартной политики качества обслуживания

Для проекта можно настроить политику качества обслуживания по умолчанию. Она будет автоматически назначена всем сетям, созданным в рамках проекта. Существующие сети проекта не наследуют политику качества обслуживания по умолчанию, для них ее требуется назначить вручную.

Ограничения

- Для каждого проекта можно назначить только одну стандартную политику качества обслуживания. Чтобы изменить политику, используемую по умолчанию, отмените прежнюю политику.

Предварительные требования

- Создана политика качества обслуживания, как описано в разделе "Создание политик качества обслуживания" на странице 597.

Чтобы назначить проекту политику качества обслуживания в качестве стандартной

Используйте параметр --default при выполнении команды openstack network qos policy set. Например:

```
# openstack --insecure network qos policy set --default policy1
```

Чтобы отменить стандартную политику качества обслуживания для проекта

Используйте параметр --no-default при выполнении команды openstack network qos policy set. Например:

```
# openstack --insecure network qos policy set --no-default policy1
```

Назначение политик качества обслуживания

Помимо политик качества обслуживания по умолчанию, можно назначать политики для отдельных сетевых портов, плавающих IP-адресов и целых сетей.

Предварительные требования

- Создана политика качества обслуживания, как описано в разделе "Создание политик качества обслуживания" на странице 597.

Чтобы назначить политику качества обслуживания порту

Узнайте идентификатор требуемого порта, а затем назначьте политику с помощью команды openstack port set --qos-policy <qos-policy>. Например:

```
# openstack --insecure port list
+--------------------------------------+-----+---------------------------+
| ID                                   | <…> | Fixed IP Addresses        |
+--------------------------------------+-----+---------------------------+
| c0ea690f-4993-4467-afd5-5389016a0658 |     | ip_address='10.136.18.133' |
+--------------------------------------+-----+---------------------------+
# openstack --insecure port set --qos-policy policy1 c0ea690f-4993-4467-afd5-5389016a0658
```

Чтобы назначить политику качества обслуживания плавающему IP-адресу

Узнайте идентификатор требуемого плавающего IP-адреса, а затем назначьте политику с помощью команды openstack floating ip set --qos-policy <qos-policy>. Например:

```
# openstack --insecure floating ip list
+--------------------------------------+---------------------+-----+
| ID                                   | Floating IP Address | <…> |
+--------------------------------------+---------------------+-----+
| 866203a2-4e1c-459f-807f-14ed563409f1 | 10.136.18.135       |     |
+--------------------------------------+---------------------+-----+
# openstack --insecure floating ip set --qos-policy policy1 866203a2-4e1c-459f-807f-14ed563409f1
```

Чтобы назначить политику качества обслуживания всем портам в сети

Узнайте идентификатор или имя требуемой сети, а затем назначьте политику с помощью команды openstack network set --qos-policy <qos-policy>. Например:

```
# openstack --insecure network list
+--------------------------------------+----------+-----+
| ID                                   | Name     | <…> |
+--------------------------------------+----------+-----+
| c6ee561e-9cf7-489b-bbab-7bca557ee7a5 | public   |     |
+--------------------------------------+----------+-----+
# openstack --insecure network set --qos-policy policy1 public
```

Изменение правил политики качества обслуживания

Правила политики качества обслуживания можно изменять во время выполнения. Изменения применяются ко всем портам, на которые распространяется политика.

Предварительные требования

- Создана политика качества обслуживания, как описано в разделе "Создание политик качества обслуживания" на странице 597.

Чтобы изменить правило политики качества обслуживания

Укажите новые значения параметров, имя политики и идентификатор правила при выполнении команды openstack network qos rule set. Например:

```
# openstack --insecure network qos policy show policy1
+-------+--------------------------------------------------------------------+
| Field | Value                                                              |
+-------+--------------------------------------------------------------------+
| <...>  |                                                                    |
| name  | policy1                                                            |
| rules | [{u'max_kbps': 3000, u'direction': u'ingress',                     |
|      |  u'qos_policy_id': u'8e2511c9-7db5-456c-b8ee-939f7729d981',  |
|      |  u'type': u'bandwidth_limit', u'max_burst_kbps': 2400,      |
|      |  u'id': u'6f036f09-d952-420d-986b-27c7eb14b2da'}]          |
| <...>  |                                                                    |
+-------+--------------------------------------------------------------------+
# openstack --insecure network qos rule set --max-kbps 2000 --max-burst-kbits 1600 \
--ingress policy1 6f036f09-d952-420d-986b-27c7eb14b2da
```

Снятие назначенных политик качества обслуживания

Предварительные требования

- Политика качества обслуживания назначена ресурсу, как описано в разделе "Назначение политик качества обслуживания" на странице 599.
- Проверено, что политика качества обслуживания не используется сетями, портами или IP-адресами.

Чтобы снять назначение политики качества обслуживания порту

Отсоедините порт от политики с помощью команды openstack port unset --qos-policy. Например:

```
# openstack --insecure port unset --qos-policy c0ea690f-4993-4467-afd5-5389016a0658
```

Чтобы снять назначение политики качества обслуживания плавающему IP-адресу

Отсоедините плавающий IP-адрес от политики с помощью команды openstack floating ip unset --qos-policy. Например:

```
# openstack --insecure floating ip unset --qos-policy 866203a2-4e1c-459f-807f-14ed563409f1
```

Чтобы снять назначение политики качества обслуживания сети

Отсоедините сеть от политики с помощью команды openstack network set --no-qos-policy. Например:

```
# openstack --insecure network set --no-qos-policy public
```

7.6.4 Управление вычислительным хранилищем

В продукте Кибер Инфраструктура вычислительное хранилище состоит из томов, выделенных виртуальным машинам. Выделенное дисковое пространство может превышать доступное физическое пространство. Правила хранения томов можно задать через политики хранения. Они также позволяют задать разные уровни производительности и режимы избыточности для томов ВМ.

Предварительные требования

- Должен быть создан вычислительный кластер, как описано в разделе "Создание вычислительного кластера" на странице 169.

7.6.4.1 Управление вычислительными томами

Том в продукте Кибер Инфраструктура представляет собой виртуальный дисковый накопитель, который можно присоединить к виртуальной машине. Целостность данных в томах обеспечивается в соответствии с режимом избыточности, указанным в политике хранилища.

Создание и удаление томов

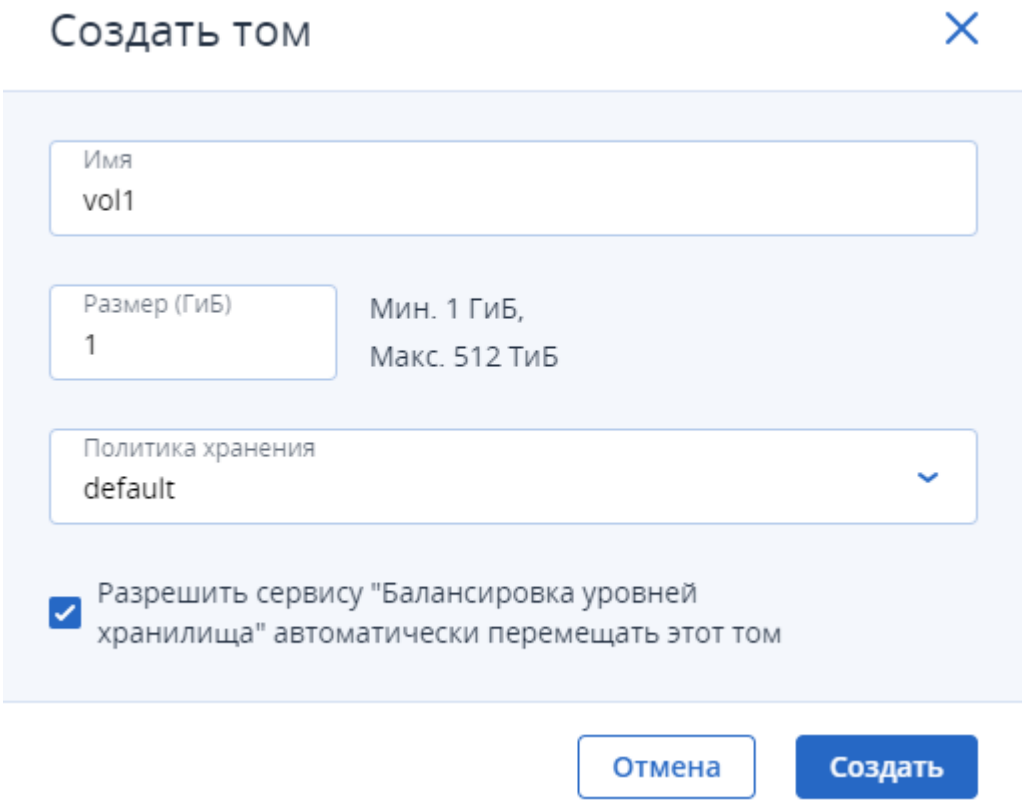
Ограничения

- Том удаляется вместе со всеми своими снимками.

Как создать том

Панель администратора

1. На экране **Тома** нажмите **Создать том**.



2. В окне **Создать том** укажите имя и размер тома в гигабайтах, выберите политику хранилища. При необходимости снимите флажок **Разрешить сервису "Балансировка уровней хранилища" автоматически перемещать этот том**, который установлен по умолчанию.
3. Нажмите **Создать**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute volume create [--description <description>]
                                     [--network-install <network_install>]
                                     [--image <image>]
                                     [--snapshot <snapshot>]
                                     --storage-policy <storage_policy>
                                     --size <size-gb>
                                     [--allow-auto-migration <allow_auto_migration>]
                                     <volume-name>
```

--description <description>

Описание тома.

--network-install <network_install>

Выполнение установки по сети (true – да или false – нет).

--image <image>

Идентификатор или имя исходного образа вычислений.

--snapshot <snapshot>

Идентификатор или имя исходного снимка образа вычислений.

--storage-policy <storage_policy>

Идентификатор или имя политики хранилища.

--size <size-gb>

Размер тома в гигабайтах.

--allow-auto-migration <allow_auto_migration>

Разрешить сервису «Балансировка уровней хранилища» автоматически перемещать том (true – да или false – нет).

<volume-name>

Имя тома.

Например, чтобы создать том myvolume размером в 8 ГБ с политикой хранилища по умолчанию, выполните:

```
# vinfra service compute volume create myvolume --storage-policy default --size 8
+--------------------------------+--------------------------------------+
| Field                          | Value                                |
+--------------------------------+--------------------------------------+
| allow_auto_migration           | True                                 |
| attachments                    | []                                   |
| availability_zone              | nova                                 |
| bootable                       | False                                |
| consistencygroup_id            |                                      |
| created_at                     | 2024-02-27T13:54:08.710602           |
| description                    |                                      |
| encrypted                      | False                                |
| id                             | 98388a00-7c69-4732-8e89-b049d89597a4 |
| imageRef                       |                                      |
| migration_status               |                                      |
| multiattach                    | False                                |
| name                           | myvolume                             |
| network_install                | False                                |
| os-vol-host-attr:host          |                                      |
| os-vol-mig-status-attr:migstat |                                      |
| os-vol-mig-status-attr:name_id |                                      |
| project_id                     | bd020e2a59384a86894ec35167828687     |
| replication_status             |                                      |
| size                           | 8                                    |
| snapshot_id                    |                                      |
| source_volid                   |                                      |
| status                         | creating                             |
| storage_policy_name            | default                              |
| traits                         | []                                   |
| updated_at                     |                                      |
```

```
| user_id                    | b358fae8bce648c4ab33d59cad279178    |
| volume_image_metadata      |                                     |
+----------------------------+-------------------------------------+
```

Новый том появится в выводе команды vinfra service compute volume list:

```
# vinfra service compute volume list -c id -c name -c size -c status
+--------------------------------------+----------+------+-----------+
| id                                   | name     | size | status    |
+--------------------------------------+----------+------+-----------+
| 98388a00-7c69-4732-8e89-b049d89597a4 | myvolume |    8 | available |
+--------------------------------------+----------+------+-----------+
```

Как удалить том

Панель администратора

1. На вкладке **Тома** проверьте статус тома, который планируется удалить.
2. Если статус тома «Используется», щелкните по тому и нажмите **Отсоединить принудительно**.
3. Если статус тома «Доступен», щелкните по тому и нажмите **Удалить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute volume delete <volume>
```

<volume>

Идентификатор или имя тома

Например, чтобы удалить том myvolume2, выполните:

```
# vinfra service compute volume delete myvolume2
Operation successful
```

Присоединение и отсоединение томов

Ограничения

- Присоединять и отсоединять можно только незагрузочные тома.

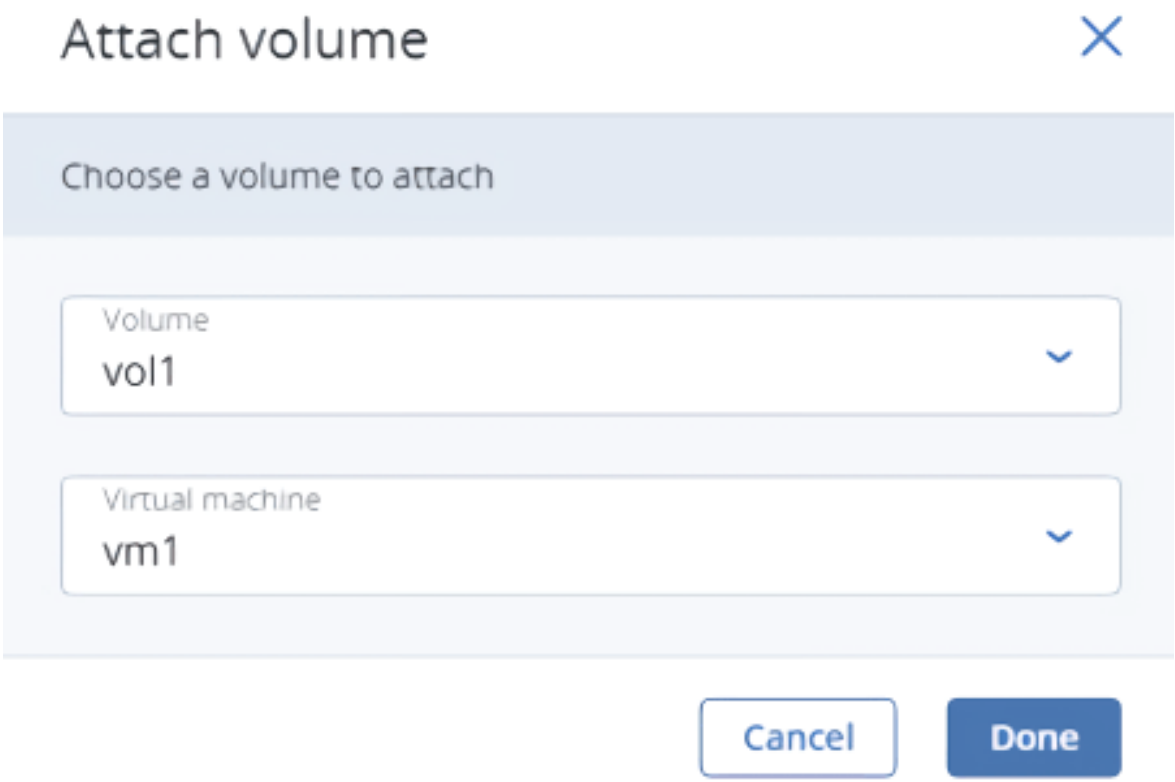
Предварительные требования

- Создан том, как описано в разделе "Создание и удаление томов" на странице 602.
- Чтобы можно было использовать тома, присоединенные к ВМ, они должны быть инициализированы внутри гостевой ОС стандартными средствами.

Как присоединить том к виртуальной машине

Панель администратора

1. На экране **Тома** щелкните по неиспользуемому тому.
2. На правой панели тома нажмите **Присоединить**.
3. В окне **Присоединить том** выберите ВМ из раскрывающегося списка и нажмите **Готово**.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server volume attach --server <server> <volume>
```

--server <server>

Идентификатор или имя виртуальной машины

<volume>

Идентификатор или имя тома

Например, чтобы присоединить доступный том с идентификатором e4cb5363-1fb2-41f5-b24b-18f98a388cba к виртуальной машине myvm, выполните:

```
# vinfra service compute server volume attach e4cb5363-1fb2-41f5-b24b-18f98a388cba --server
myvm
+--------+--------------------------------------+
| Field  | Value                                |
+--------+--------------------------------------+
| device | /dev/vdb                             |
```

```
| id    | e4cb5363-1fb2-41f5-b24b-18f98a388cba |
+-------+--------------------------------------+
```

Имя нового устройства будет отображено в выводе команды. Чтобы посмотреть все тома ВМ, выполните:

```
# vinfra service compute server volume list --server myvm
+--------------------------------------+----------+
| id                                   | device   |
+--------------------------------------+----------+
| e4cb5363-1fb2-41f5-b24b-18f98a388cba | /dev/vdb |
| b325cc6e-8de1-4b6c-9807-5a497e3da7e3 | /dev/vda |
+--------------------------------------+----------+
```

Как отсоединить том от виртуальной машины

Панель администратора

1. На экране **Тома** щелкните по используемому тому.
2. Если ВМ остановлена, нажмите **Отсоединить** на правой панели тома.
3. Если ВМ работает, нажмите **Отсоединить принудительно** на правой панели тома.

Предупреждение
При этом есть риск потери данных.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server volume detach --server <server> <volume>
```

--server <server>

Идентификатор или имя виртуальной машины

<volume>

Идентификатор или имя тома

Например, чтобы отсоединить том с идентификатором e4cb5363-1fb2-41f5-b24b-18f98a388cba от виртуальной машины с идентификатором 871fef54-519b-4111-b18d-d2039e2410a8, выполните:

```
# vinfra service compute server volume detach e4cb5363-1fb2-41f5-b24b-18f98a388cba \
--server 871fef54-519b-4111-b18d-d2039e2410a8
```

Изменение размера томов

Размер томов можно изменять только в сторону увеличения. Тома можно расширять как для работающих (онлайн-режим), так и для остановленных (офлайн-режим) виртуальных машин.

Изменение размера тома в онлайн-режиме позволяет избежать простоев и масштабировать емкость хранилища ВМ на лету без прерывания работы сервиса.

Ограничения

- Уменьшать размер томов нельзя.
- При изменении размера тома файловая система внутри гостевой ОС не расширяется.
- Если вернуть том к моментальному снимку, созданному до расширения, у тома останется новый размер.

Предварительные требования

- Создан том, как описано в разделе "Создание и удаление томов" на странице 602.

Как увеличить размер тома

Панель администратора

1. На экране **Тома** щелкните по тому.
2. Нажмите значок карандаша в поле **Размер**.
3. Введите нужную емкость тома и нажмите значок галочки.

После расширения тома потребуется заново создать разделы на диске внутри гостевой ОС, чтобы распределить добавленное дисковое пространство.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute volume extend --size <size_gb> <volume>
```

--size <size_gb>

Размер тома в гигабайтах

<volume>

Идентификатор или имя тома

Например, чтобы увеличить размер тома myvolume до 16 ГБ, выполните:

```
# vinfra service compute volume extend myvolume --size 16
Operation successful
```

Изменение политики хранилища тома

Управлять избыточностью вычислительного тома можно путем изменения политики хранилища, примененной к этому тому. Политику хранилища можно изменять для томов, присоединенных как к работающим, так и остановленным виртуальным машинам.

Ограничения

- Нельзя изменить тип избыточности тома. Как следствие, можно применить политику хранилища только с тем же самым типом избыточности. Например, политика хранилища с 3 репликами может быть заменена только на политику хранилища с 2 репликами или с 1 репликой (без избыточности).
- Нельзя изменить схему избыточности тома, если используется тип избыточности «помехоустойчивое кодирование». Как следствие, можно применить политику хранилища только с той же самой схемой избыточности. Например, политика с типом избыточности «помехоустойчивое кодирование», схемой избыточности 3+2, уровнем хранения 0 и областью отказа «диск» может быть заменена на политику с типом избыточности «помехоустойчивое кодирование», схемой избыточности 3+2, уровнем хранения 1 и областью отказа «узел».

Предварительные требования

- Четкое понимание концепции "Политики хранения" на странице 37.
- Создан том, как описано в разделе "Создание и удаление томов" на странице 602.

Как изменить политику хранилища для тома

Панель администратора

1. На экране **Тома** щелкните по тому.
2. Нажмите значок карандаша в поле **Политика хранения**.
3. Выберите новую политику хранилища и нажмите значок галочки. Можно выбрать только между политиками хранилища с одинаковым типом избыточности.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute volume set --storage-policy <storage_policy> <volume>
```

--storage-policy <storage_policy>

Идентификатор или имя политики хранилища

<volume>

Идентификатор или имя тома

Например, чтобы изменить политику хранилища тома myvolume на mystorpolicy, выполните:

```
# vinfra service compute volume set myvolume --storage-policy mystorpolicy
+--------------------------------+----------------------------------------+
| Field                          | Value                                  |
+--------------------------------+----------------------------------------+
| attachments                    | []                                     |
| availability_zone              | nova                                   |
| bootable                       | False                                  |
| consistencygroup_id            |                                        |
| created_at                     | 2018-09-12T12:30:12.665916             |
| description                    |                                        |
```

```
| encrypted                  | False                                |
| id                         | c9c0e9e7-ce7a-4566-99d5-d7e40f2987ab |
| imageRef                   |                                      |
| migration_status           |                                      |
| multiattach                | False                                |
| name                       | myvolume                             |
| network_install            | False                                |
| os-vol-host-attr:host      | node001.vstoragedomain@vstorage#vstorage |
| os-vol-mig-status-attr:migstat |                                  |
| os-vol-mig-status-attr:name_id |                                  |
| project_id                 | 72a5db3a033c403a86756021e601ef34     |
| replication_status         |                                      |
| size                       | 8                                    |
| snapshot_id                |                                      |
| source_volid               |                                      |
| status                     | available                            |
| storage_policy_name        | mystorpolicy                         |
| updated_at                 | 2018-09-12T12:55:29.298717           |
| user_id                    | 98bf389983c24c07af9677b931783143     |
| volume_image_metadata      |                                      |
+----------------------------+--------------------------------------+
```

Клонирование томов

Ограничения

- Можно клонировать тома, которые не присоединены к ВМ или присоединены к остановленным ВМ.

Предварительные требования

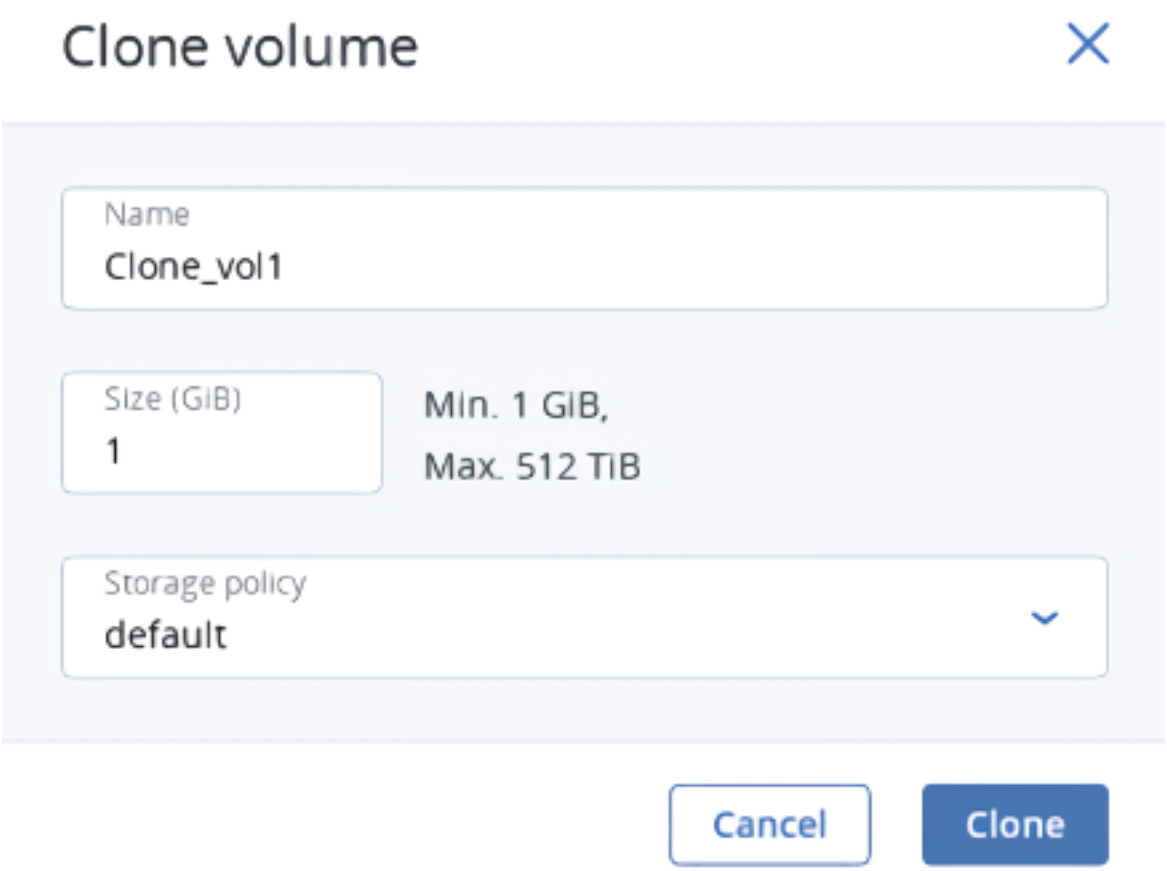
- Создан том, как описано в разделе "Создание и удаление томов" на странице 602.

Как клонировать том

Панель администратора

1. На экране **Тома** щелкните по тому.
2. На правой панели тома нажмите **Клонировать**.
3. В окне **Клонировать том** укажите имя тома, размер и политику хранилища. Нажмите

Клонировать.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute volume clone --name <name> [--size <size-gb>]
                                    [--storage-policy <storage_policy>] <volume>
```

--name <name>

Имя нового тома

--size <size-gb>

Размер тома в гигабайтах

--storage-policy <storage_policy>

Идентификатор или имя политики хранилища

<volume>

Идентификатор или имя тома

Например, чтобы создать копию тома myvolume и назвать ее myvolume2, выполните:

```
# vinfra service compute volume clone myvolume --name myvolume2
+-------------------------------+----------------------------------------+
| Field                         | Value                                  |
+-------------------------------+----------------------------------------+
| attachments                   | []                                     |
| availability_zone             | nova                                   |
| bootable                      | True                                   |
| consistencygroup_id           |                                        |
| created_at                    | 2021-10-18T16:36:39.937068             |
| description                   |                                        |
| encrypted                     | False                                  |
| id                            | 22eb7529-0a2c-44ce-a73c-24f3152bdb54   |
| imageRef                      |                                        |
| migration_status              |                                        |
| multiattach                   | False                                  |
| name                          | myvolume2                              |
| network_install               | False                                  |
| os-vol-host-attr:host         | node003.vstoragedomain@vstorage#vstorage |
| os-vol-mig-status-attr:migstat |                                        |
| os-vol-mig-status-attr:name_id |                                        |
| project_id                    | b906404c55bb44729da99987536ac5bc       |
| replication_status            |                                        |
| size                          | 64                                     |
| snapshot_id                   |                                        |
| source_volid                  | c80f58c9-c52e-41c4-ad5f-d5b5ed072d4a   |
| status                        | creating                               |
| storage_policy_name           | default                                |
| traits                        | []                                     |
| updated_at                    | 2021-10-18T16:36:40.133516             |
| user_id                       | c727a901a6444ee1a8ad31e3d5b53b3a       |
| volume_image_metadata         |                                        |
+-------------------------------+----------------------------------------+
```

Просмотр сведений о томах

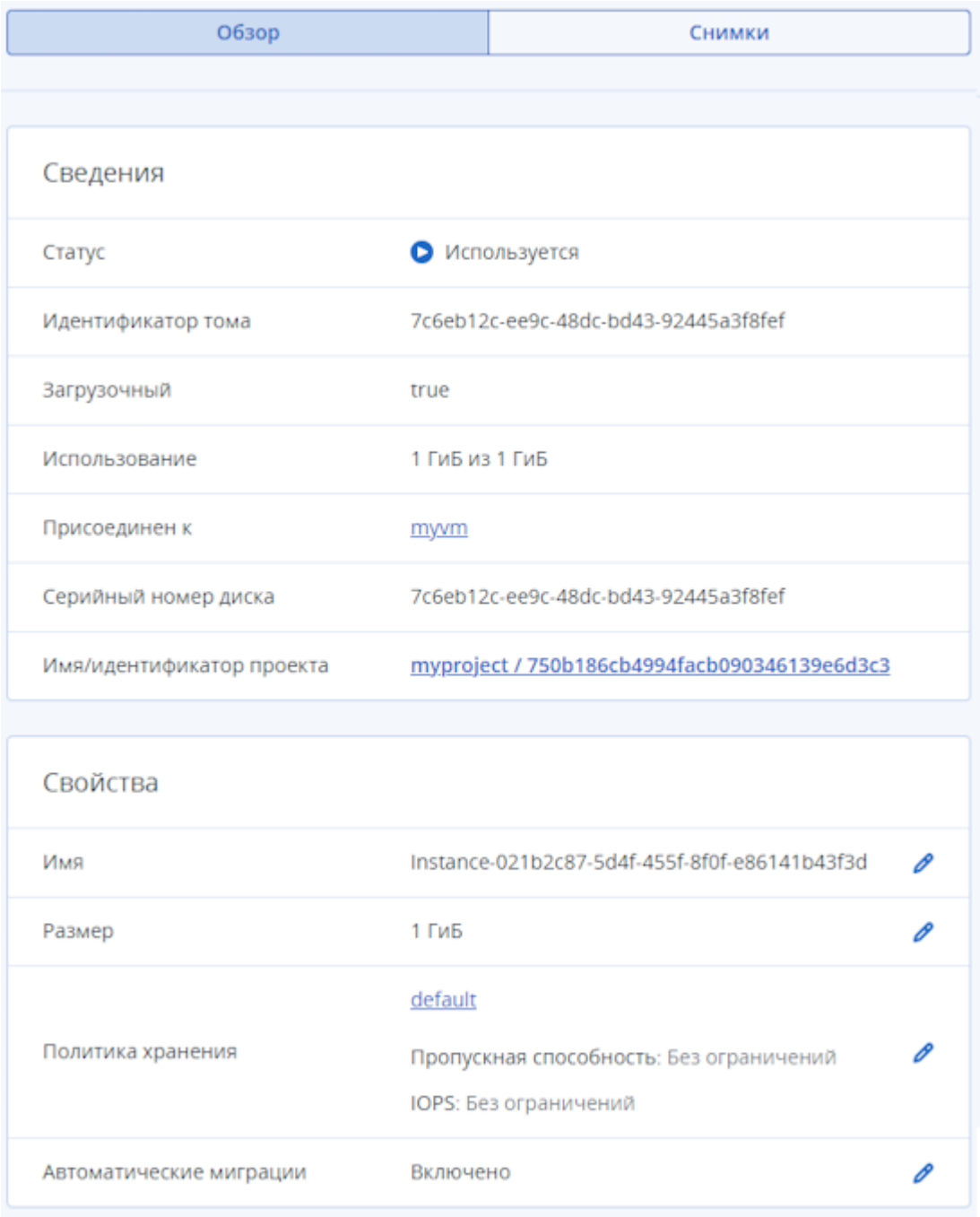
Предварительные требования

- Создан том, как описано в разделе "Создание и удаление томов" на странице 602.

Как просмотреть общие сведения о вычислительном томе

Панель администратора

На экране **Вычисления** > **Хранилище** > **Тома** щелкните по имени тома. На правой панели будут отображены сведения об этом томе.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute volume show <volume>
```

<volume>

Идентификатор или имя тома

Например, чтобы вывести сведения о томе myvolume, выполните:

```
# vinfra service compute volume show myvolume
+------------------------------+--------------------------------------+
| Field                        | Value                                |
+------------------------------+--------------------------------------+
| allow_auto_migration         | True                                 |
| attachments                  | []                                   |
| availability_zone            | nova                                 |
| bootable                     | False                                |
| consistencygroup_id          |                                      |
| created_at                   | 2024-02-27T13:56:32.678021           |
| description                  |                                      |
| encrypted                    | False                                |
| id                           | e85fad66-7c49-486b-9dbb-6c6384af9603 |
| imageRef                     |                                      |
| migration_status             |                                      |
| multiattach                  | False                                |
| name                         | myvolume                             |
| network_install              | False                                |
| os-vol-host-attr:host        | amd8.vstoragedomain@vstorage#vstorage |
| os-vol-mig-status-attr:migstat |                                    |
| os-vol-mig-status-attr:name_id |                                    |
| project_id                   | bd020e2a59384a86894ec35167828687     |
| replication_status           |                                      |
| size                         | 8                                    |
| snapshot_id                  |                                      |
| source_volid                 |                                      |
| status                       | available                            |
| storage_policy_name          | default                              |
| traits                       | []                                   |
| updated_at                   | 2024-02-27T13:56:33.789959           |
| user_id                      | b358fae8bce648c4ab33d59cad279178     |
| volume_image_metadata        |                                      |
+------------------------------+--------------------------------------+
```

Как просмотреть сведения о томе ВМ

Панель администратора

1. На экране **Вычисления** > **Виртуальные машины** щелкните по имени виртуальной машины.
2. В правой панели перейдите на вкладку **Обзор**.
3. В разделе **Свойства** щелкните по имени тома, сведения о котором вы хотите просмотреть.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server volume show --server <server> <volume>
```

--server <server>

Идентификатор или имя виртуальной машины

<volume>

Идентификатор или имя тома

Например, чтобы вывести сведения о томе с идентификатором e4cb5363-1fb2-41f5-b24b-18f98a388cba, присоединенном к виртуальной машине myvm, выполните:

```
# vinfra service compute server volume show --server myvm \
e4cb5363-1fb2-41f5-b24b-18f98a388cba
+--------+--------------------------------------+
| Field  | Value                                |
+--------+--------------------------------------+
| device | /dev/vdb                             |
| id     | e4cb5363-1fb2-41f5-b24b-18f98a388cba |
+--------+--------------------------------------+
```

Управление моментальными снимками томов

Можно сохранить текущее состояние файловой системы ВМ или пользовательских данных, создав моментальный снимок тома. Создание снимка загрузочного тома может оказаться полезным, например, перед обновлением ПО виртуальной машины. Если что-то пойдет не так, можно будет в любой момент вернуть ВМ в рабочее состояние. Снимок тома данных можно использовать для резервного копирования пользовательских данных или для тестирования.

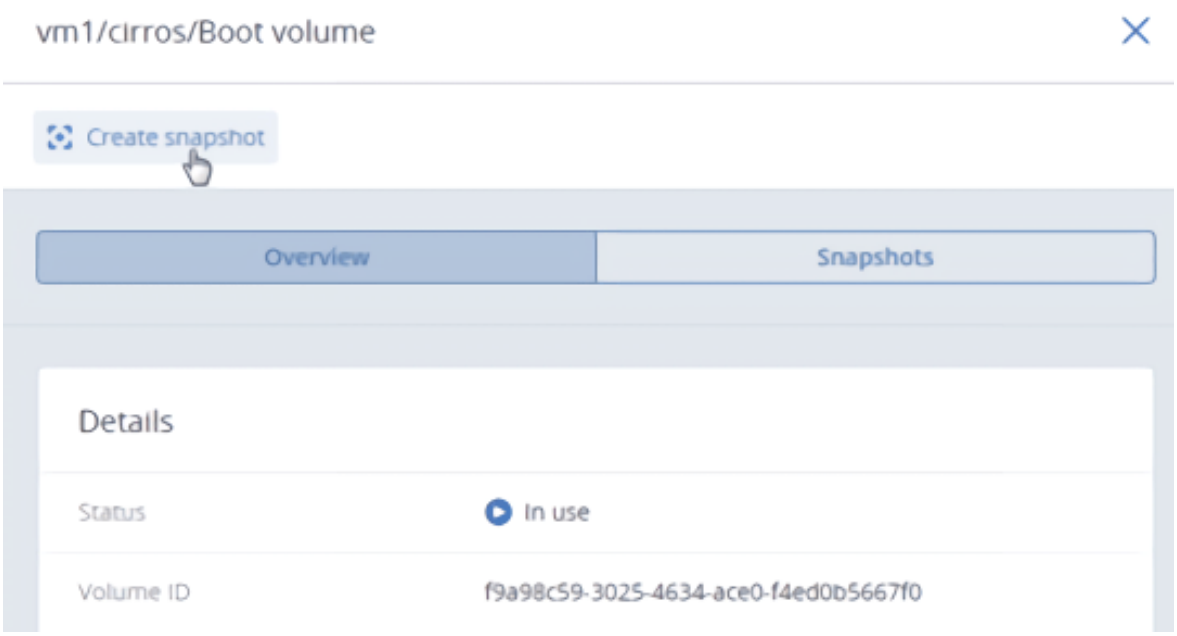
Предварительные требования

- Чтобы создать согласованный снимок тома работающей ВМ, необходимо, чтобы в ВМ были установлены дополнения гостевой ОС, как описано в разделе "Установка дополнений гостевой ОС" на странице 471. Гостевой агент QEMU, который входит в образ дополнений гостевой ОС, автоматически замораживает файловую систему во время создания снимка.

Как создать моментальный снимок тома

Панель администратора

1. На экране **Тома** щелкните по тому.
2. На правой панели тома перейдите на вкладку **Снимки** и нажмите **Создать снимок**.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute volume snapshot create [--description <description>]
                                              --volume <volume> <volume-snapshot-name>
```

--description <description>

Описание снимка тома

--volume <volume>

Идентификатор или имя тома

<volume-snapshot-name>

Имя снимка тома

Например, чтобы создать моментальный снимок mysnapshot тома myvolume, выполните:

```
# vinfra service compute volume snapshot create mysnapshot --volume myvolume
+-------------+--------------------------------------+
| Field       | Value                                |
+-------------+--------------------------------------+
| created_at  | 2019-04-30T13:12:54.297629+00:00     |
| description |                                      |
| id          | 3fdfe5d6-8bd2-4bf5-8599-a9cef50e5b71 |
| metadata    | {}                                   |
| name        | mysnapshot                           |
| project_id  | fd0ae61496d04ef6bb637bc3167b7eaf     |
| size        | 8                                    |
| status      | creating                             |
| volume_id   | 92dc3bd7-713d-42bf-83cd-4de40c24fed9 |
+-------------+--------------------------------------+
```

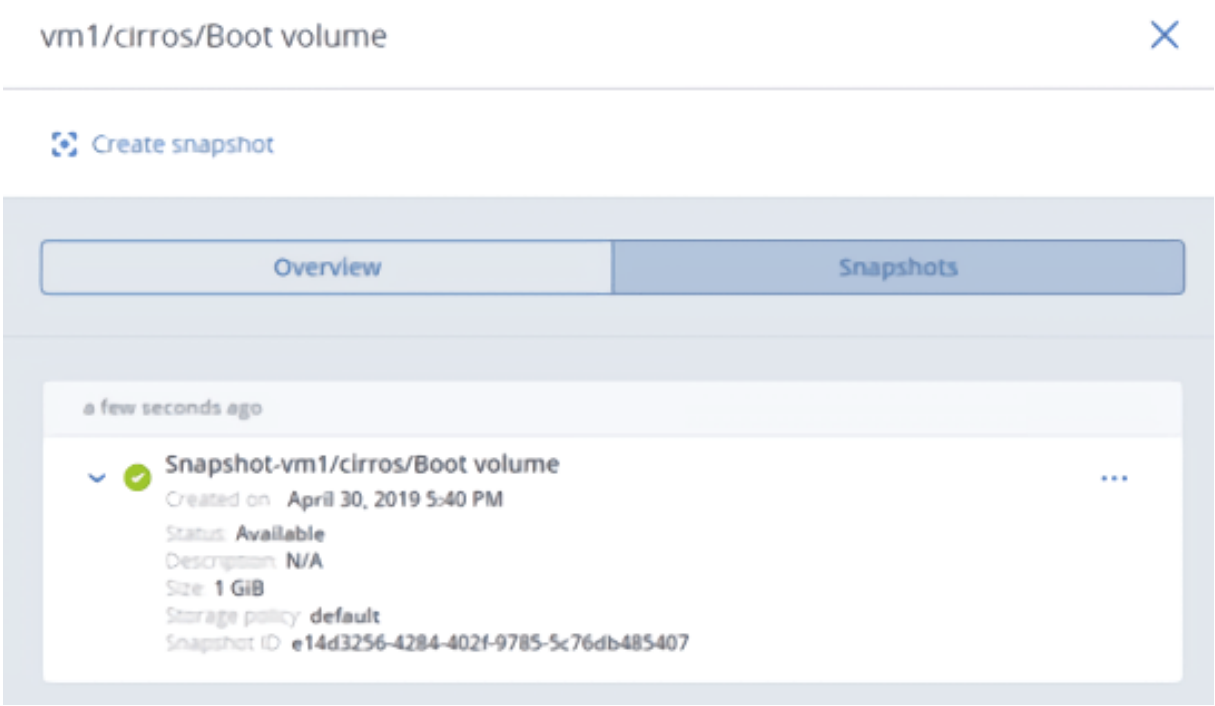
Новый моментальный снимок появится в выводе команды vinfra service compute volume snapshot list:

```
# vinfra service compute volume snapshot list -c id -c name -c size -c status
+--------------------------------------+------------+-----------+
| id                                   | name       | status    |
+--------------------------------------+------------+-----------+
| 3fdfe5d6-8bd2-4bf5-8599-a9cef50e5b71 | mysnapshot | available |
+--------------------------------------+------------+-----------+
```

Как управлять моментальным снимком тома

Панель администратора

Выберите том и откройте вкладку **Снимки** на его правой панели.



Можно выполнить следующие действия.

- Создать новый том из моментального снимка.
- Создать шаблон из моментального снимка.
- Отменить все изменения, внесенные в том с момента создания снимка. Это действие доступно только для виртуальных машин со статусами «Выключена» или «Ресурсы высвобождены».

Предупреждение
Поскольку для каждого тома существует только одна ветвь снимков, то все снимки, созданные после того снимка, к которому вы возвращаете состояние тома, будут удалены. Если вы хотите сохранить какой-либо последующий снимок перед возвратом, сначала создайте из него том или образ.

- Изменить имя или описание моментального снимка.
- Сбросить снимок, зависший в состоянии «Ошибка» или в переходном состоянии, в состояние «Доступно».
- Удалить моментальный снимок.

Чтобы выполнить эти действия, нажмите кнопку с многоточием рядом с моментальным снимком и выберите нужное действие.

Интерфейс командной строки

Используйте следующие команды:

- Чтобы отменить все изменения, внесенные в том с момента создания снимка, используйте команду vinfra service compute volume snapshot revert. Например:

  ```
  # vinfra service compute volume snapshot revert mynewsnapshot
  ```

- Чтобы создать шаблон из моментального снимка, используйте команду vinfra service compute volume snapshot upload-to-image. Например:

  ```
  # vinfra service compute volume snapshot upload-to-image --name myvm-image mysnapshot
  ```

- Чтобы создать новый том из моментального снимка, используйте команду vinfra service compute volume create. Например:

  ```
  # vinfra service compute volume create myvolume2 --snapshot mysnapshot --storage-policy
  default --size 8
  ```

- Чтобы изменить имя или описание моментального снимка, используйте команду vinfra service compute volume snapshot set. Например:

  ```
  # vinfra service compute volume snapshot set mysnapshot --name mynewsnapshot \
  --description "My new snapshot"
  ```

- Чтобы сбросить снимок, зависший в состоянии «Ошибка» или в переходном состоянии, в состояние «Доступно», используйте команду vinfra service compute volume snapshot reset-state. Например:

  ```
  # vinfra service compute volume snapshot reset-state mysnapshot
  ```

- Чтобы вывести сведения о моментальном снимке, используйте команду vinfra service compute volume snapshot show. Например:

  ```
  # vinfra service compute volume snapshot show mysnapshot
  ```

- Чтобы удалить моментальный снимок, используйте команду vinfra service compute volume snapshot delete. Например:

  ```
  # vinfra service compute volume snapshot delete mynewsnapshot
  ```

7.6.4.2 Управление политиками хранения

Политика хранения представляет собой группу параметров, которые определяют, как следует хранить тома ВМ: их уровень, область отказа и режим избыточности. Политика хранения также может ограничивать пропускную способность и количество операций ввода-вывода в секунду (IOPS) для тома. Эти ограничения помогают настроить распределение ресурсов кластера между виртуальными машинами. Они также необходимы, чтобы обеспечить прогнозируемые уровни производительности для дисков виртуальных машин.

При развертывании вычислительного кластера создается политика хранения по умолчанию, которая принудительно применяет наилучшую схему репликации, которую допускает количество узлов в кластере хранилища. Политику по умолчанию нельзя удалить или переименовать. По умолчанию она применяется к передаваемым образам и базовым томам, созданным из этих образов.

О базовых томах
Базовый том создается на основе исходного образа при развертывании виртуальной машины. Он не используется виртуальной машиной напрямую, но все тома, которые она фактически использует (перечисленные на вкладке **Тома**), по сути, представляют собой дельты (разности) от базового тома. Важно поддерживать доступность базовых томов, так как от них зависят тома ВМ. Для этого потребуется задать множественные реплики в политике хранения по умолчанию.

Если в кластере хранилища недостаточно узлов для обеспечения множественных реплик (такая конфигурация не рекомендуется), можно будет скорректировать политику хранения по умолчанию после того, как в кластер хранилища будут добавлены дополнительные узлы. Она будет применена к образам и базовым томам, которые были созданы с политикой по умолчанию.

Чтобы применить пользовательские схемы избыточности к томам ВМ, можно создать, изменить или клонировать для них политики хранения.

Ограничения

- Изменить тип избыточности существующей политики хранения невозможно.
- Политику хранения нельзя удалить, если она управляет существующими томами. Если вы все равно хотите удалить такую политику хранения, сначала удалите эти тома или выберите для них другую политику.

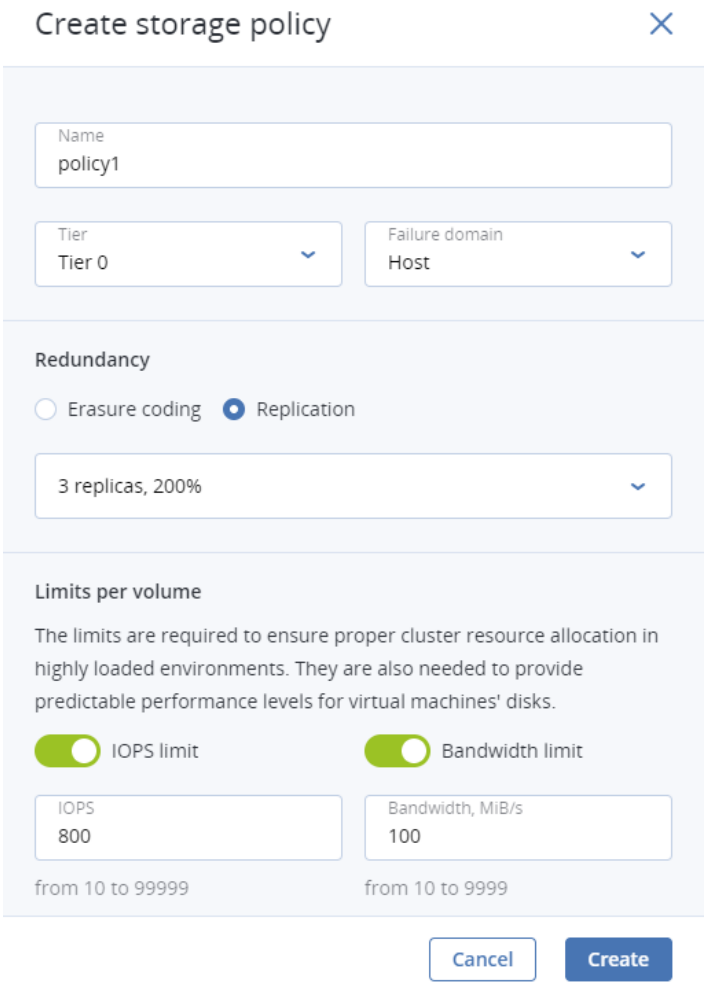
Предварительные требования

- Четкое понимание следующих понятий: "Политики хранения" на странице 37, "Избыточность данных" на странице 29, "Области отказа" на странице 35 и "Уровни хранения данных" на странице 36.

Чтобы создать политику хранения

Панель администратора

1. На экране **Вычисления** > **Хранилище** > **Политики хранения** нажмите **Создать политику хранения**.
2. В окне **Создать политику хранения** укажите имя политики и выберите параметры избыточности.



3. [Необязательно] Укажите **Предел IOPS** или **Предел пропускной способности**, чтобы задать соответствующие ограничения для тома.
4. Нажмите кнопку **Создать**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute storage-policy create --tier {0,1,2,3} (--replicas <norm>[:<min>] | --encoding
<M>+<N>)
                                    --failure-domain {0,1,2,3,4}
                                    [--write-bytes-sec <limit>] [--read-bytes-sec <limit>]
                                    [--read-iops-sec <limit>] [--write-iops-sec <limit>]
                                    [--total-bytes-sec <limit>] [--total-iops-sec <limit>]
                                    <name>
```

--tier {0,1,2,3}

Уровень хранилища

--encoding <M>+<N>

Схема помехоустойчивого кодирования хранилища в формате:

- M: число блоков данных
- N: число паритетных блоков

--failure-domain {0,1,2,3,4}

Область отказа хранилища

--replicas <norm>[:<min>]

Схема репликации хранилища в формате:

- norm: количество сохраняемых реплик
- min: минимально требуемое количество реплик (необязательно)

--write-bytes-sec <limit>

Количество байтов, записываемых в секунду

--read-bytes-sec <limit>

Количество байтов, считываемых в секунду

--read-iops-sec <limit>

Количество операций чтения в секунду

--write-iops-sec <limit>

Количество операций записи в секунду

--total-bytes-sec <bytes>

Общее количество байтов, считываемых и записываемых в секунду

--total-iops-sec <iops>

Общее количество операций чтения и записи

<name>

Имя политики хранилища

Например, чтобы создать политику хранилища mystorpolicy, в которой уровень хранилища – 3, схема избыточности – избыточное кодирование 3+2, область отказа – хост, общее количество операций чтения и записи в секунду – 100, общее количество байтов, считываемых и записываемых в секунду – 104 857 600, выполните:

```
# vinfra service compute storage-policy create mystorpolicy --tier 3 \
--encoding 3+2 --failure-domain 1 --total-bytes-sec 104857600 --total-iops-sec 100
```

Созданная политика хранилища появится в выводе команды vinfra service compute storage-policy list:

```
# vinfra service compute storage-policy list
+-------------+--------------+------+-------------+---------------+-------------------------------+
| id          | name         | tier | redundancy  | failure_domain | qos                           |
+-------------+--------------+------+-------------+---------------+-------------------------------+
| 97b55811<…> | mystorpolicy | 3    | encoding=3+2 | 1             | read_bytes_sec: -1            |
|             |              |      |             |               | read_bytes_sec_per_gb: -1     |
|             |              |      |             |               | read_bytes_sec_per_gb_min: -1 |
|             |              |      |             |               | read_iops_sec: -1             |
|             |              |      |             |               | read_iops_sec_per_gb: -1      |
|             |              |      |             |               | read_iops_sec_per_gb_min: -1  |
|             |              |      |             |               | total_bytes_sec: 104857600    |
|             |              |      |             |               | total_bytes_sec_per_gb: -1    |
|             |              |      |             |               | total_bytes_sec_per_gb_min: -1|
|             |              |      |             |               | total_iops_sec: 100           |
|             |              |      |             |               | total_iops_sec_per_gb: -1     |
|             |              |      |             |               | total_iops_sec_per_gb_min: -1 |
|             |              |      |             |               | write_bytes_sec: -1           |
|             |              |      |             |               | write_bytes_sec_per_gb: -1    |
|             |              |      |             |               | write_bytes_sec_per_gb_min: -1|
|             |              |      |             |               | write_iops_sec: -1            |
|             |              |      |             |               | write_iops_sec_per_gb: -1     |
|             |              |      |             |               | write_iops_sec_per_gb_min: -1 |
| 603bd56b<…> | default      | 0    | replicas=3  | 1             | read_bytes_sec: -1            |
|             |              |      |             |               | read_bytes_sec_per_gb: -1     |
|             |              |      |             |               | read_bytes_sec_per_gb_min: -1 |
|             |              |      |             |               | read_iops_sec: -1             |
|             |              |      |             |               | read_iops_sec_per_gb: -1      |
|             |              |      |             |               | read_iops_sec_per_gb_min: -1  |
|             |              |      |             |               | total_bytes_sec: -1           |
|             |              |      |             |               | total_bytes_sec_per_gb: -1    |
|             |              |      |             |               | total_bytes_sec_per_gb_min: -1|
|             |              |      |             |               | total_iops_sec: -1            |
|             |              |      |             |               | total_iops_sec_per_gb: -1     |
|             |              |      |             |               | total_iops_sec_per_gb_min: -1 |
|             |              |      |             |               | write_bytes_sec: -1           |
|             |              |      |             |               | write_bytes_sec_per_gb: -1    |
|             |              |      |             |               | write_bytes_sec_per_gb_min: -1|
|             |              |      |             |               | write_iops_sec: -1            |
|             |              |      |             |               | write_iops_sec_per_gb: -1     |
|             |              |      |             |               | write_iops_sec_per_gb_min: -1 |
+-------------+--------------+------+-------------+---------------+-------------------------------+
```

Чтобы изменить политику хранения

Панель администратора

1. На экране **Вычисления** > **Хранилище** > **Политики хранения** выберите политику из списка.
2. На правой панели политики нажмите **Изменить**.
3. Измените нужные параметры и нажмите кнопку **Сохранить**.

Не забывайте, что внесенные в политику изменения затронут избыточность и производительность всех томов, на которые распространяется эта политика.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute storage-policy set [--name <name>] [--tier {0,1,2,3}]
                                          [--replicas <norm>[:<min>] |
                                          --encoding <M>+<N>]
                                          [--failure-domain {0,1,2,3,4}]
                                          [--write-bytes-sec <limit>] [--read-bytes-sec <limit>]
                                          [--read-iops-sec <limit>] [--write-iops-sec <limit>]
                                          [--total-bytes-sec <limit>] [--total-iops-sec <limit>]
                                          <storage-policy>
```

--name <name>

Новое имя для политики хранилища

--tier {0,1,2,3}

Уровень хранилища

--encoding <M>+<N>

Схема помехоустойчивого кодирования хранилища в формате:

- M: число блоков данных
- N: число паритетных блоков

--failure-domain {0,1,2,3,4}

Область отказа хранилища

--replicas <norm>[:<min>]

Схема репликации хранилища в формате:

- norm: количество сохраняемых реплик
- min: минимально требуемое количество реплик (необязательно)

--write-bytes-sec <limit>

Количество байтов, записываемых в секунду

--read-bytes-sec <limit>

Количество байтов, считываемых в секунду

--read-iops-sec <limit>

Количество операций чтения в секунду

--write-iops-sec <limit>

Количество операций записи в секунду

--total-bytes-sec <bytes>

Общее количество байтов, считываемых и записываемых в секунду

--total-iops-sec <iops>

Общее количество операций чтения и записи

<storage-policy>

Идентификатор или имя политики хранилища

Например, чтобы изменить тип избыточности для политики mystorpolicy с избыточного кодирования 3+2 на 5+2, выполните:

```
# vinfra service compute storage-policy set mystorpolicy --encoding 5+2
```

Чтобы клонировать политику хранения

1. На экране **Вычисления** > **Хранилище** > **Политики хранения** выберите политику из списка.
2. На правой панели политики нажмите **Клонировать**.
3. [Необязательно] Внесите изменения в существующие параметры (или оставьте их без изменений), а затем нажмите **Клонировать**.

Чтобы просмотреть сведения о политике хранения

Панель администратора

На экране **Вычисления** > **Хранилище** > **Политики хранения** выберите политику из списка. На правой панели будут отображены сведения об этой политике.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute storage-policy show <storage-policy>
```

<storage-policy>

Идентификатор или имя политики хранения

Например, чтобы вывести подробные данные о политике хранения mystorpolicy, выполните:

```
# vinfra service compute storage-policy show mystorpolicy
+----------------+--------------------------------------+
| Field          | Value                                |
+----------------+--------------------------------------+
| available      | False                                |
| failure_domain | host                                 |
| id             | 2199e71e-ce8a-4ba9-81cd-75502f0344ca |
| name           | mystorpolicy                         |
| qos            | total_bytes_sec: 104857600           |
|                | total_iops_sec: 100                  |
| redundancy     | encoding=3+2                         |
| tier           | 3                                    |
+----------------+--------------------------------------+
```

Чтобы удалить политику хранения

Панель администратора

1. На экране **Вычисления** > **Хранилище** > **Политики хранения** выберите политику из списка.
2. На правой панели политики нажмите **Удалить**.
3. В окне подтверждения нажмите **Удалить политику**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute storage-policy delete <storage-policy>
```

<storage-policy>

Идентификатор или имя политики хранилища

Например, чтобы удалить политику хранилища mystorpolicy, выполните:

```
# vinfra service compute storage-policy delete mystorpolicy
```

7.6.4.3 Использование политик качества обслуживания для томов

Можно использовать политики качества обслуживания, основанные на емкости, чтобы задавать динамические ограничения для вычислительных томов. Погигабайтные политики качества обслуживания позволяют настроить производительность и пропускную способность томов в зависимости от их размера. Например, если ограничения составляют 5 IOPS на ГБ и 1 МБ/с на ГБ, том на 100 ГБ будет обладать производительностью 500 IOPS и пропускной способностью 100 МБ/с, тогда как том на 1 ТБ – 5 000 IOPS и 1 000 МБ/с. После увеличения размера тома, для которого заданы погигабайтные ограничения, его пропускная способность и производительность будут увеличены пропорционально размеру.

Для динамической конфигурации производительности и пропускной способности можно ограничивать следующие параметры томов:

- Количество операций чтения в секунду на ГБ
- Количество операций записи в секунду на ГБ
- Общее количество операций чтения и записи в секунду на ГБ
- Количество считываемых байтов в секунду на ГБ
- Количество записываемых байтов в секунду на ГБ
- Общее количество считываемых и записываемых байтов в секунду на ГБ

Кроме того, можно контролировать минимальные значения производительности и пропускной способности, чтобы гарантировать высокую производительность для томов маленького размера.

Погигабайтные политики качества обслуживания можно задавать для вычислительных томов посредством политик хранения. Можно либо создать новую политику хранения с погигабайтными ограничениями, либо можно добавить такие ограничения к существующей политике хранения.

Ограничения

- Погигабайтные ограничения не применяются к существующим томам на лету. Чтобы применить их к существующему тому, остановите и запустите ВМ, к которой присоединен этот том.
- В одной политике качества обслуживания можно ограничить либо общую производительность и общую пропускную способность, либо производительность и пропускную способность отдельно для чтения и отдельно для записи. Например, нельзя указать параметр total-bytes-sec-per-gb вместе с параметром write-bytes-sec-per-gb или read-bytes-sec-per-gb.

Чтобы создать погигабайтную политику качества обслуживания

Используйте следующую команду:

```
vinfra service compute storage-policy create --tier {0,1,2,3} (--replicas <norm> | --encoding
<M>+<N>)
                --failure-domain {0,1,2,3,4}
                [--write-bytes-sec-per-gb <limit>] [--write-bytes-sec-per-gb-min <limit>]
                [--read-bytes-sec-per-gb <limit>] [--read-bytes-sec-per-gb-min <limit>]
                [--write-iops-sec-per-gb <limit>] [--write-iops-sec-per-gb-min <limit>]
                [--read-iops-sec-per-gb <limit>] [--read-iops-sec-per-gb-min <limit>]
                [--total-bytes-sec-per-gb <limit>] [--total-bytes-sec-per-gb-min <limit>]
                [--total-iops-sec-per-gb <limit>] [--total-iops-sec-per-gb-min <limit>]
                <name>
```

--tier {0,1,2,3}

Уровень хранилища

--encoding <M>+<N>

Схема помехоустойчивого кодирования хранилища в формате:

- M: число блоков данных
- N: число паритетных блоков

--failure-domain {0,1,2,3,4}

Область отказа хранилища

--replicas <norm>[:<min>]

Схема репликации хранилища в формате:

- norm: количество сохраняемых реплик
- min: минимально требуемое количество реплик (необязательно)

--write-bytes-sec-per-gb <limit>

Количество записываемых в секунду байтов на ГБ

--write-bytes-sec-per-gb-min <limit>

Минимальное количество записываемых в секунду байтов на ГБ

--read-bytes-sec-per-gb <limit>

Количество считываемых в секунду байтов на ГБ

--read-bytes-sec-per-gb-min <limit>

Минимальное количество считываемых в секунду байтов на ГБ

--write-iops-sec-per-gb <limit>

Количество операций записи в секунду на ГБ

--write-iops-sec-per-gb-min <limit>

Минимальное количество операций записи в секунду на ГБ

--read-iops-sec-per-gb <limit>

Количество операций чтения в секунду на ГБ

--read-iops-sec-per-gb-min <limit>

Минимальное количество операций чтения в секунду на ГБ

--total-bytes-sec-per-gb <limit>

Общее количество считываемых и записываемых в секунду байтов на ГБ

--total-bytes-sec-per-gb-min <limit>

Минимальное общее количество считываемых и записываемых в секунду байтов на ГБ

--total-iops-sec-per-gb <limit>

Общее количество операций чтения и записи в секунду на ГБ

--total-iops-sec-per-gb-min <limit>

Минимальное общее количество операций чтения и записи в секунду на ГБ

<name>

Имя политики хранения

Например, чтобы создать политику хранения myqospolicy, в которой общее количество операций чтения и записи в секунду на ГБ — 100, минимальное общее количество операций чтения и записи в секунду на ГБ — 50, выполните:

```
# vinfra service compute storage-policy create myqospolicy --tier 1 --failure-domain 1 --replicas 3 \
        --total-iops-sec-per-gb 100 --total-iops-sec-per-gb-min 50
```

Чтобы добавить погигабайтные ограничения к существующей политике хранения

Используйте команду vinfra service compute storage-policy set, указав необходимое значение для параметра, который требуется ограничить. Например, чтобы добавить к политике хранения myqospolicy погигабайтное ограничение пропускной способности в 104 857 600 байт, считываемых и записываемых в секунду, выполните:

```
# vinfra service compute storage-policy set myqospolicy --total-bytes-sec-per-gb 104857600
```

Чтобы удалить погигабайтные ограничения из существующей политики хранения

Используйте команду vinfra service compute storage-policy set, указав -1 как значение для параметра, для которого необходимо отменить погигабайтное ограничение. Например, чтобы

удалить погигабайтное ограничение общей пропускной способности из политики хранения myqospolicy, выполните:

```
# vinfra service compute storage-policy set myqospolicy --total-bytes-sec-per-gb -1
```

7.6.5 Управление кластерами Kubernetes

Кластеры Kubernetes создаются и управляются пользователями панели самообслуживания, как описано в разделе «Управление кластерами Kubernetes» в руководстве по самообслуживанию. На панели администрирования можно просматривать подробные сведения о кластерах Kubernetes, просматривать группы мастер-серверов и рабочих серверов, изменять сервисные параметры, обновлять версию Kubernetes, а также удалять кластеры Kubernetes.

Кибер Инфраструктура использует мягкую политику противодействия сближению для узлов кластера Kubernetes. В соответствии с этой политикой узлы Kubernetes распределяются между узлами вычислений по группам: мастер-серверы распределяются отдельно от рабочих серверов. В данном случае на одном вычислительном узле могут размещаться и мастер-сервер, и рабочий сервер. Однако если количество вычислительных узлов будет недостаточным для равномерного распределения по ним узлов Kubernetes из одной группы, некоторые из этих узлов могут быть помещены совместно на один вычислительный узел.

7.6.5.1 Создание и удаление кластеров Kubernetes

Ограничения

- Версии Kubernetes 1.15.x, 1.18.x и 1.19.x больше не поддерживаются. Кластеры Kubernetes, созданные в этих версиях, имеют метку **Устаревший**.
- Сертификаты кластеров Kubernetes выпускаются со сроком действия, составляющим пять лет. Чтобы продлить сертификаты, используйте команду vinfra service compute k8saas rotate-ca (см. раздел "Обновление сертификатов кластеров Kubernetes" на странице 639). Как вариант, можно использовать команду openstack coe ca rotate (см. документацию OpenStack).

Предварительные требования

- Должен быть создан вычислительный кластер, как описано в разделе "Создание вычислительного кластера" на странице 169.
- Служба Kubernetes должна быть установлена либо в ходе развертывания вычислительного кластера, либо позже, как описано в разделе "Подготовка к работе кластеров Kubernetes" на странице 192.
- Создана виртуальная сеть, которая будет соединять серверы Kubernetes. Для нее должны быть указаны шлюз и DNS-сервер.
- Создан SSH-ключ, который будет установлен на рабочих и мастер-серверах.
- Достаточно ресурсов для всех серверов Kubernetes с учетом их типов.

Чтобы создать кластер Kubernetes

Используйте следующую команду:

```
vinfra service compute k8saas create [--master-node-count <count>]
                                     [--node-count <count>]
                                     [--volume-storage-policy <policy>]
                                     [--kubernetes-version <version>]
                                     --master-flavor <flavor>
                                     --flavor <flavor>
                                     [--volume-size <size>]
                                     --external-network <network>
                                     [--network <network>]
                                     --key-name <key-name>
                                     [--use-floating-ip <use-floating-ip>]
                                     [--enable-public-access]
                                     [--containers-network-cidr <cidr>]
                                     [--containers-network-node-subnet-prefix-length <prefix_length>]
                                     [--service-network-cidr <cidr>]
                                     [--dns-service-ip <ip>] <name>
```

<name>

Имя кластера Kubernetes.

--master-node-count <count>

Количество мастер-серверов в кластере Kubernetes.

--node-count <count>

Количество рабочих серверов в кластере Kubernetes.

--volume-storage-policy <policy>

Имя политики хранилища для тома, на котором будут расположены контейнеры.

--kubernetes-version <version>

Версия Kubernetes (v1.21.3, v1.20.7 и v1.19.9).

--master-flavor <flavor>

Тип ВМ, который следует использовать для мастер-серверов Kubernetes.

--flavor <flavor>

Тип ВМ, который следует использовать для рабочих серверов Kubernetes.

--volume-size <size>

Размер тома хранилища на каждом сервере Kubernetes.

--external-network <network>

Идентификатор или имя физической сети, обеспечивающей доступ в Интернет для серверов Kubernetes.

--network <network>

Идентификатор или имя виртуальной сети, обеспечивающей взаимодействие между серверами Kubernetes.

--key-name <key-name>

Пара ключей, которую следует использовать для доступа к серверам Kubernetes.

--use-floating-ip <use-floating-ip>

Использование плавающих IP-адресов для всех серверов Kubernetes (true или false).

--enable-public-access

Использование плавающего IP-адреса для API Kubernetes (true или false).

--containers-network-cidr <cidr>

Диапазон сети контейнеров в нотации CIDR.

--containers-network-node-subnet-prefix-length <prefix_length>

Длина префикса для подсети контейнеров, выделенной каждому серверу Kubernetes.

--service-network-cidr <cidr>

Диапазон сети сервиса Kubernetes в нотации CIDR.

--dns-service-ip <ip>

IP-адрес сервиса DNS.

Например, чтобы создать кластер Kubernetes, выполните:

```
# vinfra service compute k8saas create k8s1 --kubernetes-version v1.20.7 \
--master-node-count 1 --node-count 3 --volume-storage-policy default \
--master-flavor medium --volume-size 10 --external-network public \
--network private1 --flavor small --key-name key1 --use-floating-ip true \
--vinfra-username user1 --vinfra-password password --vinfra-domain domain1 \
--vinfra-project project1
+---------------------------------+-----------------------------------------+
| Field                           | Value                                   |
+---------------------------------+-----------------------------------------+
| action_status                   | CREATE_IN_PROGRESS                      |
| boot_volume_size                | 10                                      |
| boot_volume_storage_policy      | default                                 |
| containers_volume_size          | 10                                      |
| containers_volume_storage_policy | default                                |
| create_timeout                  | 60                                      |
| external_network_id             | 10cc4d59-adac-4ec1-8e0a-df5015b82c64    |
| id                              | 749737ae-2452-4a98-a057-b59b1c579a85    |
| key_name                        | key1                                    |
| master_flavor                   | medium                                  |
| master_node_count               | 1                                       |
| name                            | k8s1                                    |
| network_id                      | d037623b-0db7-40c2-b38a-9ac34fbd1cc5    |
| nodegroups                      | - action_status: CREATE_IN_PROGRESS     |
|                                 |   flavor: medium                        |
|                                 |   id: c3b4ec41-b8c1-4dae-9e1c-aa586b99a62c |
|                                 |   is_default: true                      |
|                                 |   name: default-master                  |
|                                 |   node_count: 1                         |
```

```
|                      |  role: master                      |
|                      |  status: CREATING                  |
|                      |  version: v1.20.7                  |
|                      | - action_status: CREATE_IN_PROGRESS      |
|                      |  flavor: small                     |
|                      |  id: 65b80f19-0920-48b7-84e0-d0c63c46e99f |
|                      |  is_default: true                  |
|                      |  name: default-worker              |
|                      |  node_count: 3                     |
|                      |  role: worker                      |
|                      |  status: CREATING                  |
|                      |  version: v1.20.7                  |
| project_id           | d8a72d59539c431381989af6cb48b05d         |
| status               | CREATING                           |
| user_id              | 5846f988280f42199ed030a22970d48e         |
| worker_pools         | - flavor: small                    |
|                      |  node_count: 3                     |
+----------------------+--------------------------------------+
```

Эта команда, выполняемая от имени пользователя user1 из domain1 > project1, запускает создание кластера Kubernetes k8s1 с этими параметрами:

- версия Kubernetes 1.20.7;
- 1 мастер-сервер на базе типа BM medium и 3 рабочих узла на базе типа BM small;
- тома хранилища размером 10 ГБ с применением политики хранилища по умолчанию;
- виртуальная сеть private1, которая будет подключаться к Интернету через физическую сеть public;
- плавающие IP-адреса для каждого сервера, взятые из указанной физической сети;
- открытый SSH-ключ key1.

Созданный кластер Kubernetes появится в выводе команды vinfra service compute k8saas list.

Чтобы удалить кластер Kubernetes

Панель администратора

1. На экране **Вычисления** > **Kubernetes** щелкните по кластеру Kubernetes.
2. На правой панели кластера нажмите кнопку **Удалить**.
3. Нажмите кнопку **Удалить** в окне подтверждения.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute k8saas delete <cluster>
```

<cluster>

Идентификатор или имя кластера.

Например, чтобы удалить Kubernetes-кластер k8s1, выполните:

```
# vinfra service compute k8saas delete k8s1
```

7.6.5.2 Получение файла kubeconfig

Для получения параметров доступа для кластера Kubernetes, используйте следующую команду:

```
vinfra service compute k8saas config <cluster>
```

Эта команды должна выполняться от имени пользователя, создавшего указанный кластер Kubernetes.

<cluster>

Идентификатор или имя кластера.

Например, чтобы вывести параметры доступа для кластера Kubernetes k8s1 в файл kubeconfig, выполните:

```
# vinfra service compute k8saas config k8s1 --vinfra-domain domain1 \
--vinfra-project project1 --vinfra-username user1 --vinfra-password password \
> kubeconfig
```

7.6.5.3 Просмотр сведений о кластерах Kubernetes

Чтобы просмотреть подробные данные о кластере Kubernetes

Панель администратора

На экране **Вычисления** > **Kubernetes** щелкните по кластеру Kubernetes, чтобы открыть его правую панель.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute k8saas show <cluster>
```

<cluster>

Идентификатор или имя кластера

Например, чтобы просмотреть сведения о Kubernetes-кластере k8s1, выполните:

```
# vinfra service compute k8saas show k8s1
+--------------------------------+----------------------------------------+
| Field                          | Value                                  |
+--------------------------------+----------------------------------------+
| action_status                  | CREATE_COMPLETE                        |
| boot_volume_size               | 10                                     |
```

```
| boot_volume_storage_policy      | default                                  |
| containers_volume_size          | 10                                       |
| containers_volume_storage_policy | default                                 |
| create_timeout                  | 60                                       |
| external_network_id             | 10cc4d59-adac-4ec1-8e0a-df5015b82c64     |
| id                              | 749737ae-2452-4a98-a057-b59b1c579a85     |
| key_name                        | key1                                     |
| master_flavor                   | medium                                   |
| master_node_count               | 1                                        |
| name                            | k8s1                                     |
| network_id                      | d037623b-0db7-40c2-b38a-9ac34fbd1cc5     |
| nodegroups                      | - action_status: CREATE_COMPLETE         |
|                                 |   flavor: medium                         |
|                                 |   id: c3b4ec41-b8c1-4dae-9e1c-aa586b99a62c |
|                                 |   is_default: true                       |
|                                 |   name: default-master                   |
|                                 |   node_count: 1                          |
|                                 |   role: master                           |
|                                 |   status: ACTIVE                         |
|                                 |   version: v1.22.2                       |
|                                 | - action_status: CREATE_COMPLETE         |
|                                 |   flavor: small                          |
|                                 |   id: 65b80f19-0920-48b7-84e0-d0c63c46e99f |
|                                 |   is_default: true                       |
|                                 |   name: default-worker                   |
|                                 |   node_count: 3                          |
|                                 |   role: worker                           |
|                                 |   status: ACTIVE                         |
|                                 |   version: v1.22.2                       |
| project_id                      | d8a72d59539c431381989af6cb48b05d         |
| status                          | ACTIVE                                   |
| user_id                         | 5846f988280f42199ed030a22970d48e         |
| worker_pools                    | - flavor: small                          |
|                                 |   node_count: 3                          |
+---------------------------------+------------------------------------------+
```

Чтобы просмотреть группы мастер-серверов и рабочих серверов

1. На экране **Вычисления** > **Kubernetes** щелкните по кластеру Kubernetes.
2. На правой панели кластера перейдите на вкладку **Группы**.
3. Чтобы просмотреть все узлы в группе, щелкните по значку стрелки рядом с нужной группой узлов.

7.6.5.4 Изменение параметров кластеров Kubernetes

Чтобы изменить параметры кластера Kubernetes, используйте следующую команду:

```
vinfra service compute k8saas set [--node-count <count>]
                                  <cluster>
```

<cluster>

Идентификатор или имя кластера.

--node-count <count>

Количество рабочих серверов в кластере Kubernetes.

Эта команда должна выполняться от имени пользователя, создавшего указанный кластер Kubernetes.

Например, чтобы в кластере Kubernetes k8s1 количество рабочих серверов равнялось 5, выполните:

```
# vinfra service compute k8saas set --node-count 5 k8s1 \
--vinfra-domain domain1 --vinfra-project project1 \
--vinfra-username user1 --vinfra-password password
+---------------------------------+------------------------------------------+
| Field                           | Value                                    |
+---------------------------------+------------------------------------------+
| action_status                   | UPDATE_COMPLETE                          |
| boot_volume_size                | 10                                       |
| boot_volume_storage_policy      | default                                  |
| containers_volume_size          | 10                                       |
| containers_volume_storage_policy | default                                |
| create_timeout                  | 60                                       |
| external_network_id             | 10cc4d59-adac-4ec1-8e0a-df5015b82c64     |
| id                              | 749737ae-2452-4a98-a057-b59b1c579a85     |
| key_name                        | key1                                     |
| master_flavor                   | medium                                   |
| master_node_count               | 1                                        |
| name                            | k8s1                                     |
| network_id                      | d037623b-0db7-40c2-b38a-9ac34fbd1cc5     |
| nodegroups                      | - action_status: UPDATE_COMPLETE         |
|                                 |   flavor: medium                         |
|                                 |   id: c3b4ec41-b8c1-4dae-9e1c-aa586b99a62c |
|                                 |   is_default: true                       |
|                                 |   name: default-master                   |
|                                 |   node_count: 1                          |
|                                 |   role: master                           |
|                                 |   status: ACTIVE                         |
|                                 |   version: v1.20.7                       |
|                                 | - action_status: UPDATE_COMPLETE         |
|                                 |   flavor: small                          |
|                                 |   id: 65b80f19-0920-48b7-84e0-d0c63c46e99f |
|                                 |   is_default: true                       |
|                                 |   name: default-worker                   |
|                                 |   node_count: 5                          |
|                                 |   role: worker                           |
|                                 |   status: ACTIVE                         |
|                                 |   version: v1.20.7                       |
| project_id                      | d8a72d59539c431381989af6cb48b05d         |
| status                          | ACTIVE                                   |
| user_id                         | 5846f988280f42199ed030a22970d48e         |
```

```
| worker_pools                  | - flavor: small                          |
|                               |   node_count: 5                          |
+-------------------------------+------------------------------------------+
```

7.6.5.5 Управление группами рабочих серверов

Чтобы создать группу рабочих серверов Kubernetes

Выполните следующую команду:

```
vinfra service compute k8saas workergroup create --flavor <flavor>
                                  [--node-count <count>]
                                  <cluster> <name>
```

<cluster>

Идентификатор или имя кластера.

<name>

Имя группы рабочих серверов Kubernetes.

--flavor <flavor>

Тип BM, который используется для группы рабочих серверов Kubernetes.

--node-count <count>

Количество рабочих серверов в группе Kubernetes.

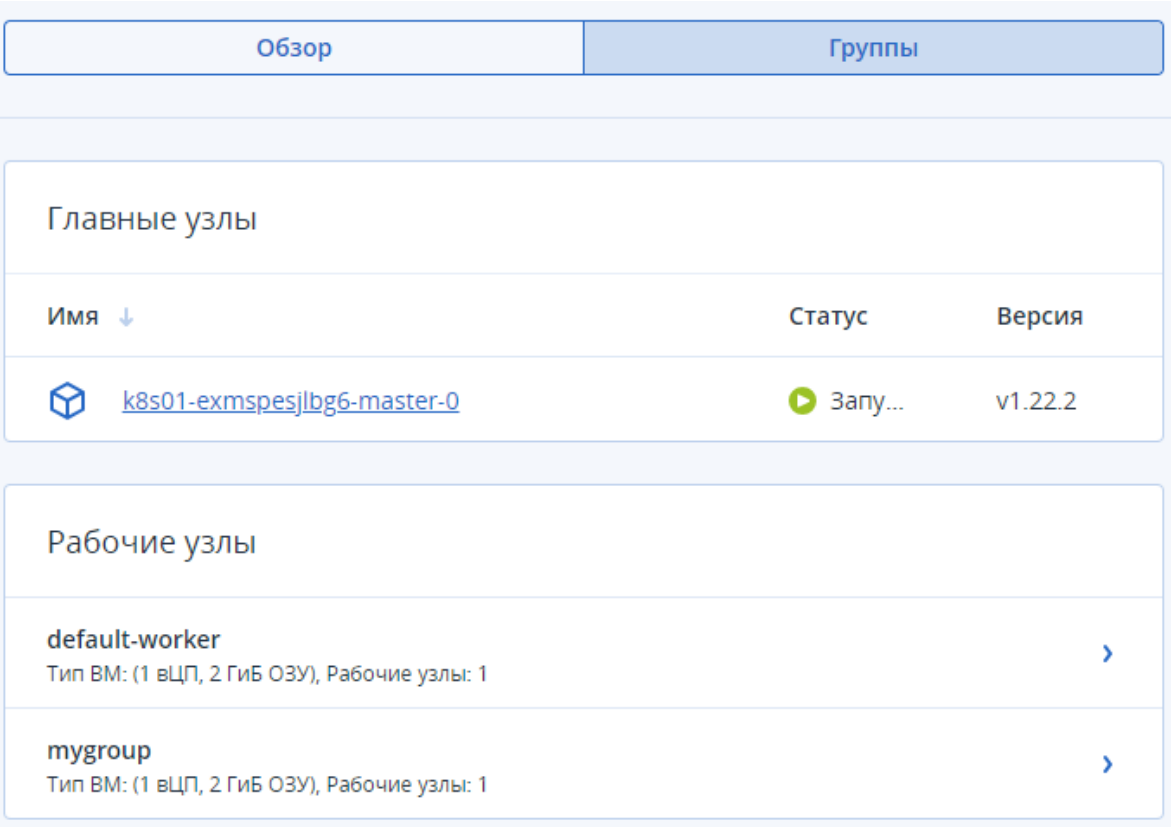
Например, чтобы запустить создание группы рабочих серверов mygroup, которая включает в себя 3 узла для кластера Kubernetes k8s1, выполните:

```
# vinfra service compute k8saas workergroup create k8s1 mygroup \
--flavor small --node-count 3 --vinfra-domain domain1 \
--vinfra-project project1 --vinfra-username user1 \
--vinfra-password password
+------------+--------------------------------------+
| Field      | Value                                |
+------------+--------------------------------------+
| flavor     | small                                |
| id         | 70d071eb-7a81-471f-ae50-99758ae27678 |
| is_default | False                                |
| name       | mygroup                              |
| node_count | 3                                    |
| role       | worker                               |
| status     | CREATING                             |
+------------+--------------------------------------+
```

Чтобы просмотреть список групп рабочих серверов Kubernetes

Панель администратора

1. На экране **Вычисления** > **Kubernetes** щелкните по кластеру Kubernetes.
2. На правой панели кластера выберите вкладку **Группы**. В разделе **Рабочие узлы** будут отображены группы рабочих серверов кластера Kubernetes.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute k8saas workergroup list [--long] <cluster>
```

cluster

Идентификатор или имя кластера.

--long

Включение доступа и перечисления для всех полей объектов.

Например, чтобы вывести все группы серверов для кластера Kubernetes k8s1, выполните:

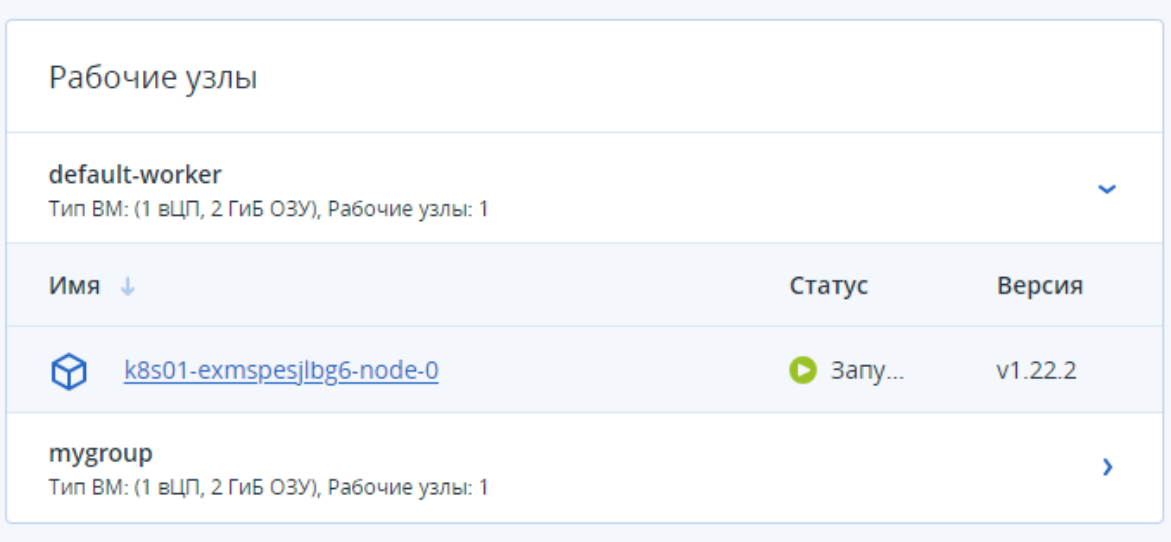
```
# vinfra service compute k8saas workergroup list k8s1 \
--vinfra-domain domain1 --vinfra-project project1 \
--vinfra-username user1 --vinfra-password password
+--------------------------------------+---------------+----------+
| id                                   | name          | status   |
+--------------------------------------+---------------+----------+
| efa32b7d-55d7-4a16-a765-68950404ec45 | default-master | ACTIVE   |
| 54242833-3416-474e-9651-a266d62e0962 | default-worker | ACTIVE   |
```

```
| 70d071eb-7a81-471f-ae50-99758ae27678 | mygroup       | CREATING |
+--------------------------------------+---------------+----------+
```

Чтобы просмотреть сведения о группе рабочих серверов Kubernetes

Панель администратора

1. На экране **Вычисления** > **Kubernetes** щелкните по кластеру Kubernetes.
2. На правой панели кластера выберите вкладку **Группы**, а затем в разделе **Рабочие узлы** щелкните по имени рабочей группы серверов Kubernetes.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute k8saas workergroup show <cluster> <worker-group>
```

<cluster>

Идентификатор или имя кластера.

<worker-group>

Идентификатор или имя группы рабочих серверов.

Например, чтобы вывести сведения о группе рабочих серверов mygroup для кластера Kubernetes k8s1, выполните:

```
# vinfra service compute k8saas workergroup show k8s1 mygroup \
--vinfra-domain domain1 --vinfra-project project1 \
--vinfra-username user1 --vinfra-password password
+----------------+--------------------------------------+
| Field          | Value                                |
+----------------+--------------------------------------+
| flavor         | small                                |
| id             | 70d071eb-7a81-471f-ae50-99758ae27678 |
```

```
| is_default     | False                                |
| name           | mygroup                              |
| node_count     | 3                                    |
| role           | worker                               |
| server_group_id | 50f4ae08-4e44-4132-a40b-7043a2c3e739 |
| status         | ACTIVE                               |
+----------------+--------------------------------------+
```

Чтобы измененить параметры группы рабочих серверов Kubernetes

Используйте следующую команду:

```
vinfra service compute k8saas workergroup set [--node-count <count>]
                                <cluster> <worker-group>
```

<cluster>

Идентификатор или имя кластера.

<worker-group>

Идентификатор или имя группы рабочих серверов.

--node-count <count>

Количество рабочих серверов в группе Kubernetes.

Например, чтобы количество рабочих серверов установить равным 5 для группы рабочих серверов mygroup кластера Kubernetes k8s1, выполните:

```
# vinfra service compute k8saas workergroup set k8s1 mygroup \
--node-count 5 --vinfra-domain domain1 --vinfra-project project1 \
--vinfra-username user1 --vinfra-password password
+----------------+--------------------------------------+
| Field          | Value                                |
+----------------+--------------------------------------+
| flavor         | small                                |
| id             | 70d071eb-7a81-471f-ae50-99758ae27678 |
| is_default     | False                                |
| name           | mygroup                              |
| node_count     | 3                                    |
| role           | worker                               |
| server_group_id | 50f4ae08-4e44-4132-a40b-7043a2c3e739 |
| status         | ACTIVE                               |
+----------------+--------------------------------------+
```

Чтобы удалить группу рабочих серверов Kubernetes

Используйте следующую команду:

```
vinfra service compute k8saas workergroup delete <cluster> <worker-group>
```

<cluster>

Идентификатор или имя кластера.

<worker-group>

Идентификатор или имя группы рабочих серверов.

Например, чтобы удалить группу рабочих серверов mygroup кластера Kubernetes k8s1, выполните:

```
# vinfra service compute k8saas workergroup delete k8s1 mygroup \
--vinfra-domain domain1 --vinfra-project project1 \
--vinfra-username user1 --vinfra-password password
Operation accepted.
```

7.6.5.6 Обновление сертификатов кластеров Kubernetes

Чтобы обновить сертификаты кластера Kubernetes

Используйте следующую команду:

```
vinfra service compute k8saas rotate-ca <cluster>
```

<cluster>

Идентификатор или имя кластера

Например, чтобы обновить сертификаты ЦС Kubernetes-кластера k8s1, выполните:

```
# vinfra service compute k8saas rotate-ca k8s1
```

7.6.5.7 Обновление кластеров Kubernetes

Когда новая версия Kubernetes становится доступной, можно обновить до нее Kubernetes-кластер. Серверы Kubernetes будут обновляться по очереди с сохранением доступности данных. Если для мастер-сервера включена высокая доступность, API-интерфейс Kubernetes останется доступен во время обновления.

Ограничения

- Нельзя обновить кластеры Kubernetes версии 1.15.x. до более новых версий.
- Во время обновления нельзя управлять кластерами Kubernetes на панели администрирования.

Чтобы обновить кластер Kubernetes

Панель администратора

1. Щелкните по кластеру Kubernetes с отметкой **Доступно обновление**.
2. На панели кластера Kubernetes нажмите **Обновить** в поле **Версия Kubernetes**.
3. В окне **Обновить** выберите версию Kubernetes, до которой следует выполнить обновление, и перейдите по предоставленной ссылке, чтобы прочитать сведения о ресурсах API, которые устарели или больше не поддерживаются в выбранной версии. Затем нажмите **Обновить**.
4. В окне подтверждения нажмите **Подтвердить**. Начнется обновление без перерыва в работе.

Предупреждение
Не выполняйте управление виртуальными машинами Kubernetes во время обновления, поскольку это может привести к прерыванию процесса обновления и неработоспособности кластера.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute k8saas upgrade <cluster> <version>
```

<cluster>

Идентификатор или имя кластера

<version>

Версия Kubernetes (v1.22.2, v1.21.3 или v1.20.7)

Например, чтобы обновить Kubernetes-кластер k8s1 до версии 1.22.2, выполните:

```
# vinfra service compute k8saas upgrade k8s1 v1.22.2
```

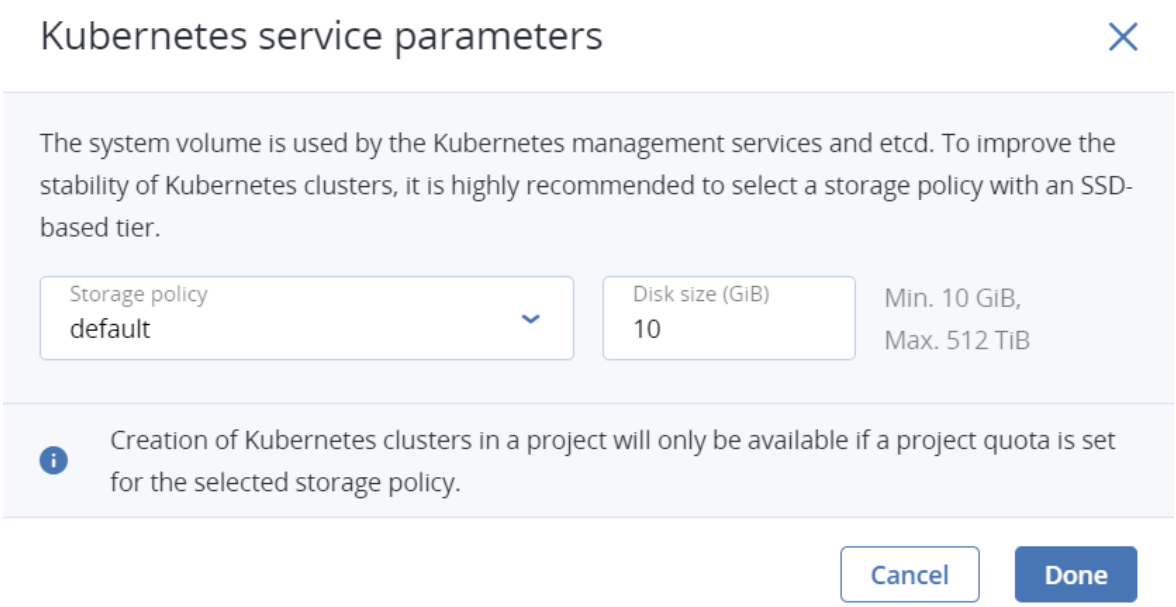
7.6.5.8 Изменение параметров сервиса Kubernetes

Можно изменять параметры Kubernetes, такие как размер и политика хранения для системного тома на мастер-серверах. Системный том используется сервисами управления Kubernetes и etcd. Новые параметры будут применены только в новых кластерах Kubernetes. Системные тома в существующих кластерах Kubernetes сохранят свои прежние параметры. Чтобы повысить стабильность кластеров Kubernetes, настоятельно рекомендуется выбирать политику хранения с уровнем на базе твердотельных накопителей (SSD).

Чтобы изменить параметры сервиса Kubernetes

1. Нажмите **Параметры** на экране **Кластеры Kubernetes**.
2. Установите требуемые политику хранения и размер для системного тома, затем нажмите

кнопку **Готово**.



7.6.6 Управление вычислительными серверами

На вычислительных узлах выполняются сервисы вычислений и виртуальные машины. Вычислительный кластер можно развернуть поверх кластера хранилища, создав тем самым гиперконвергентную инфраструктуру. Вместо этого также можно отделить вычислительные сервисы от основных сервисов хранилища данных, запуская вычислительные сервисы на других узлах инфраструктуры. Следует учитывать, что сервисы вычислений повышают потребление ресурсов и могут отрицательно повлиять на производительность кластера хранилища данных.

Предварительные требования

- Должен быть создан вычислительный кластер, как описано в разделе "Создание вычислительного кластера" на странице 169.

7.6.6.1 Добавление узлов в вычислительный кластер

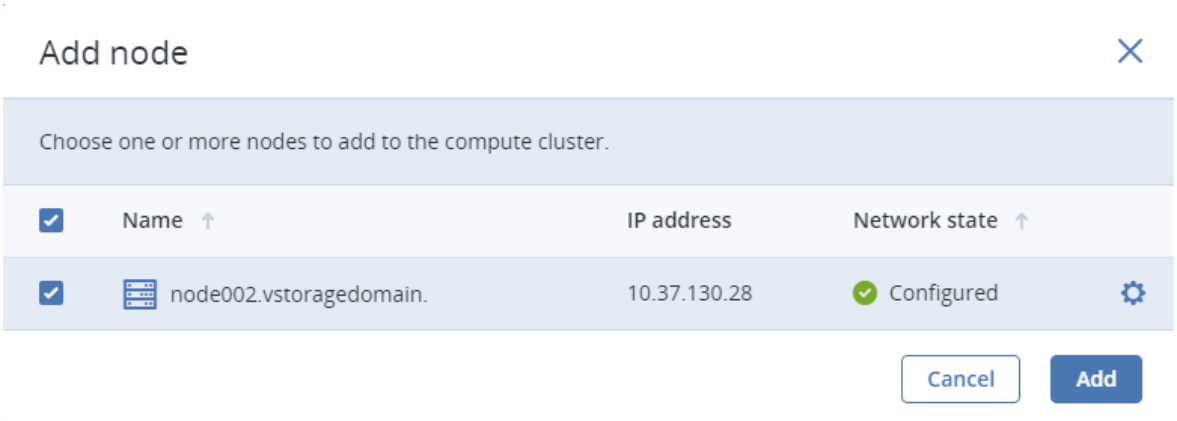
Предварительные требования

- Четкое понимание ограничений, перечисленных в разделе "Высокая доступность и вычислительный кластер" на странице 29.
- Убедитесь, что на узле, который будет добавлен в вычислительный кластер, синхронизировано время. Для автоматической синхронизации времени узел должен быть подключен к Интернету и на нем должна выполняться служба chronyd. Чтобы синхронизировать время немедленно, перезапустите службу вручную, выполнив команду systemctl restart chronyd.

Чтобы добавить узлы в вычислительный кластер

Панель администратора

1. Перейдите на экран **Вычисления** > **Серверы** и нажмите **Добавить сервер**. Откроется окно **Добавить сервер**.
2. Если сеть на каждом узле не отмечена зеленым цветом, настройте ее. Для этого щелкните по значку шестерни, назначьте сетевым адаптерам узла сети с типами трафика, связанными с вычислениями, и нажмите кнопку **Применить**.
3. Выберите узлы и нажмите **Добавить**.



Добавленные узлы появятся на экране **Серверы**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute node add [--compute] [--controller] [--force] <node>
```

--compute
: Роль вычислительного сервера

--controller
: Роль вычислительного сервера контроллера

--force
: Пропустить проверки на соответствие минимальным аппаратным требованиям

<node>
: Идентификатор сервера или имя хоста

Например, чтобы добавить сервер node005.vstoragedomain в вычислительный кластер с ролью compute, выполните:

```
# vinfra service compute node add node005.vstoragedomain --compute
```

Добавленный сервер появится в выводе команды vinfra service compute node list:

```
# vinfra service compute node list
+----------------+----------------------+--------------+--------------+
| id             | host                 | state        | roles        |
+----------------+----------------------+--------------+--------------+
| 7ffa9540-5a20<…> | node001.vstoragedomain | healthy      | - controller |
|                |                      |              | - compute    |
| 6e8afc28-7f71<…> | node002.vstoragedomain | healthy      | - compute    |
| 02ff64ae-5800<…> | node003.vstoragedomain | healthy      | - compute    |
| 827a1f4e-56e5<…> | node004.vstoragedomain | healthy      | - compute    |
| 37c70bfb-c289<…> | node005.vstoragedomain | reconfiguring | - compute    |
+----------------+----------------------+--------------+--------------+
```

7.6.6.2 Управление размещениями для вычислительных узлов

Размещение – это группа вычислительных узлов с общим отличительным признаком. Это может быть специальная лицензия на ПО для запуска в виртуальных машинах или усовершенствованная модель ЦП. После группировки узлов в размещение для него можно назначить образ или тип ВМ. В таком случае все ВМ, созданные из этого образа или с применением этого типа ВМ, будут размещены на узлах, включенных в назначенное размещение. Таким образом, можно создавать размещения, чтобы ВМ, которым необходима определенная функция, назначались на узлы, где она имеется.

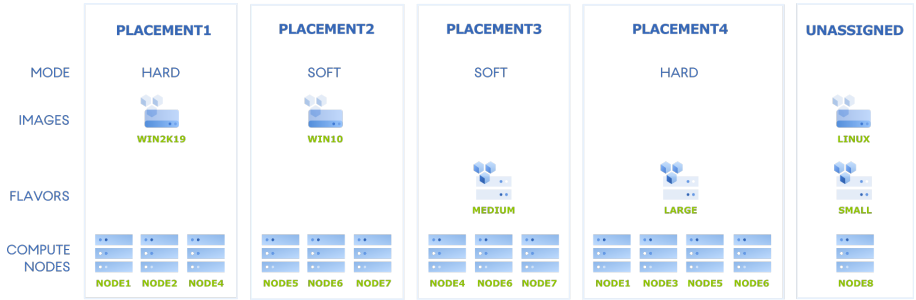
Внимание

При использовании размещений помните, что кластеры Kubernetes и балансировщики нагрузки создаются из готовых образов ОС, которые следуют тем же правилам размещения, что и все остальные вычислительные образы. Необходимо назначить правильное размещение для следующих образов:

- Для кластеров Kubernetes – **fedora-coreos-x64-k8saas**
- Для балансировщиков нагрузки – **amphora-x64-haproxy**

Режимы размещения

У размещения вычислительных узлов может быть два режима: строгое соответствие (hard) и нестрогое соответствие (soft). По умолчанию задается режим строгого соответствия. Чтобы лучше понять, как работают эти режимы, рассмотрим пример, в котором администратор системы создает размещения и назначает их образам, типам ВМ и узлам, как показано ниже.



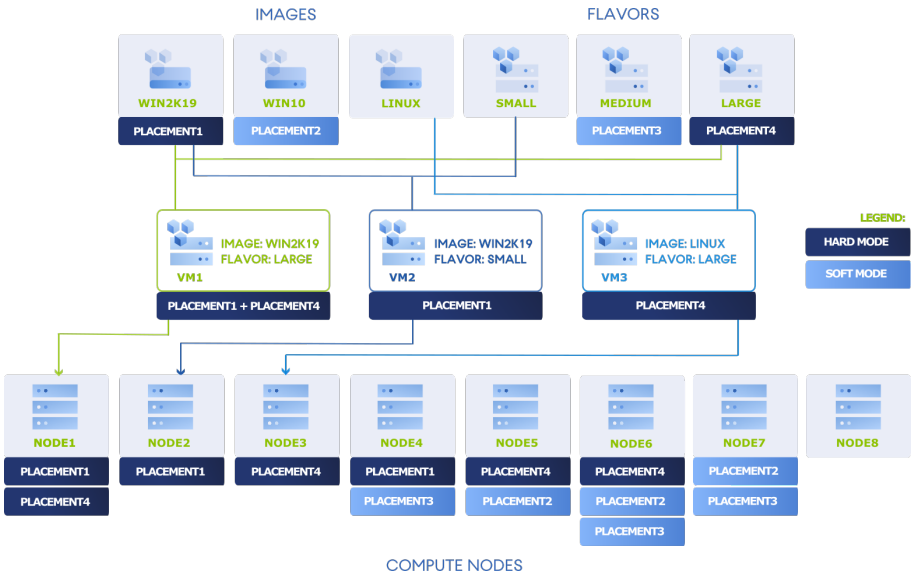
На рисунке выше:

- **Placement1**, для которого задан режим строгого соответствия, назначается образу **Win2k19** и узлам **Node1**, **Node2** и **Node4**.
- **Placement2**, для которого задан режим нестрогого соответствия, назначается образу **Win10** и узлам **Node5**, **Node6** и **Node7**.
- **Placement3**, для которого задан режим нестрогого соответствия, назначается типу ВМ **Medium** и узлам **Node4**, **Node6** и **Node7**.
- **Placement4**, для которого задан режим строгого соответствия, назначается типу ВМ **Large** и узлам **Node1**, **Node3**, **Node5** и **Node6**.
- Образу **Linux**, типу ВМ **Small**, а также узлу **Node8** размещения не назначены.

Когда пользователь начнет создавать виртуальные машины, они будут наследовать размещения от выбранных им образов и типов ВМ. В зависимости от своего режима размещения виртуальная машина может размещаться на различных узлах.

Виртуальные машины с размещениями, для которых задан режим строгого соответствия

При режиме строгого соответствия виртуальная машина размещается на узле, размещения которого в точности совпадают с размещениями этой виртуальной машины.



На рисунке выше:

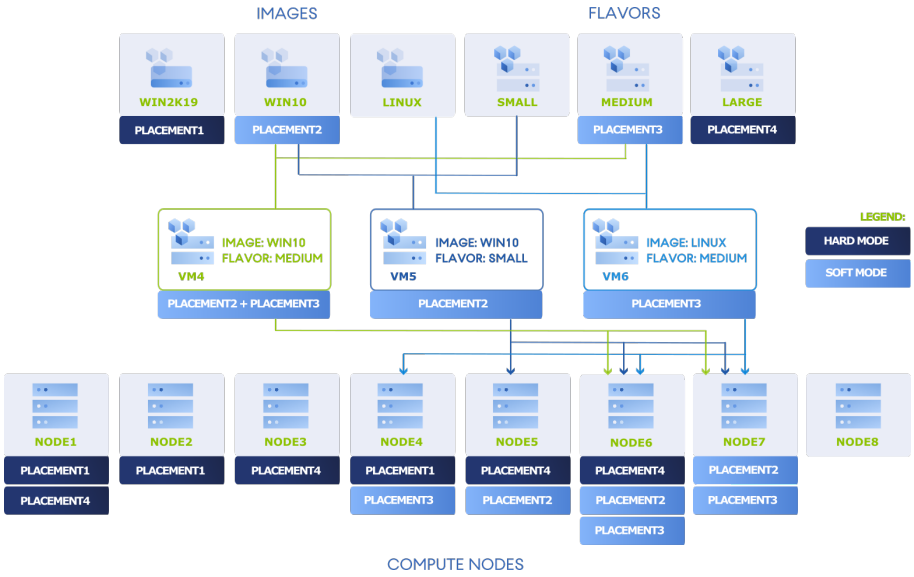
- **VM1** создана на основе образа **Win2k19** с размещением **Placement1** и с типом ВМ **Large** с размещением **Placement4**. Эта виртуальная машина наследует размещения **Placement1** и **Placement4**, для которых задан режим строгого соответствия. Машину **VM1** можно разместить только на узле **Node1**, потому что только этому узлу назначены оба размещения: **Placement1** и **Placement4**.
- **VM2** создана на основе образа **Win2k19** с размещением **Placement1** и с типом ВМ **Small** без размещений. Эта виртуальная машина наследует размещение **Placement1**, для которого задан

режим строгого соответствия. **VM2** может размещаться только на узле **Node2**, потому что лишь этому узлу присвоено только одно размещение **Placement1**.

- **VM3** создана на основе образа **Linux** без размещений и с типом **Large** с размещением **Placement4**. Эта виртуальная машина наследует размещение **Placement4**, для которого задан режим строгого соответствия. **VM3** может размещаться только на узле **Node3**, поскольку лишь этому узлу присвоено только одно размещение **Placement4**.

Виртуальные машины с размещениями, для которых задан режим нестрогого соответствия

При режиме нестрогого соответствия виртуальная машина размещается на узле, размещения которого как минимум включают все размещения этой виртуальной машины (на узле также могут быть другие размещения).



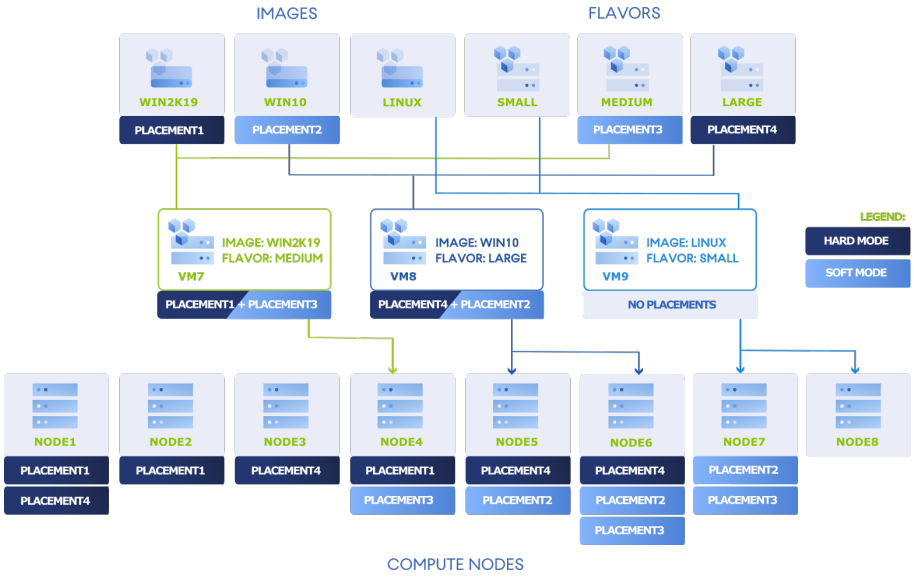
На рисунке выше:

- **VM4** создана на основе образа **Win10** с размещением **Placement2** и с типом ВМ **Medium** с размещением **Placement3**. Эта виртуальная машина наследует размещения **Placement2** и **Placement3**, для которых задан режим нестрогого соответствия. Машину **VM4** можно разместить на узле **Node6** или **Node7**, поскольку у этих узлов имеются оба назначенных размещения: **Placement2** и **Placement3**.
- **VM5** создана на основе образа **Win10** с размещением **Placement2** и с типом ВМ **Small** без размещений. Эта виртуальная машина наследует размещение **Placement2**, для которого задан режим нестрогого соответствия. Машину **VM5** можно поместить на узлах **Node5**, **Node6** или **Node7**, поскольку всем этим узлам присвоено размещение **Placement2**.
- **VM6** создана на основе образа **Linux** без размещений и с типом ВМ **Medium** с размещением **Placement3**. Эта виртуальная машина наследует размещение **Placement3**, для которого задан режим нестрогого соответствия. Машину **VM6** можно поместить на узлах **Node4**, **Node6** или **Node7**, поскольку всем этим узлам присвоено размещение **Placement3**.

Виртуальные машины с обоими режимами размещения и без размещений

У виртуальной машины могут быть размещения, для которых заданы режимы строгого и нестрогого соответствия. В таком случае размещения ВМ обрабатываются в режиме нестрогого соответствия, то есть виртуальная машина размещается на узле, у которого имеется по меньшей мере тот же набор размещений, что и у самой виртуальной машины.

Если у виртуальной машины нет размещений, она может быть помещена либо на узел с размещениями, для которых задан режим нестрогого соответствия, либо на узел, который не добавлен ни в одно размещение.



На рисунке выше:

- **VM7** создана на основе образа **Win2k19** с размещением **Placement1** и с типом ВМ **Medium** с размещением **Placement3**. Эта виртуальная машина наследует размещение **Placement1**, для которого задан режим строгого соответствия, и размещение **Placement3**, для которого задан режим нестрогого соответствия. Машину **VM7** можно поместить только на узле **Node4**, поскольку лишь этому узлу одновременно назначены оба размещения: **Placement1** и **Placement3**.
- **VM8** создана на основе образа **Win10** с размещением **Placement2** и с типом ВМ **Large** с размещением **Placement4**. Эта виртуальная машина наследует размещение **Placement4**, для которого задан режим строгого соответствия, и размещение **Placement2**, для которого задан режим нестрогого соответствия. Машину **VM8** можно разместить на узлах **Node5** и **Node6**, поскольку обоим этим узлам назначены и размещение **Placement2**, и размещение **Placement4**.
- **VM9** создана на основе образа **Linux** без размещений и с типом ВМ **Small** без размещений. Эта виртуальная машина не наследует ни одного размещения. Машину **VM9** можно поместить на узле **Node7**, потому что у этого узла размещения, для которых задан режим нестрогого соответствия. Также машину **VM9** можно поместить на узел **Node8**, поскольку этому узлу не назначены размещения.

Создание размещений

Хотя создавать и настраивать размещения можно только на панели администрирования, их применение возможно и с панели самообслуживания. Пользователи панели самообслуживания могут использовать размещения, создавая ВМ из образов и типов ВМ с назначенными размещениями. После загрузки образа на панель самообслуживания пользователь не может назначать ему какие-либо размещения. ВМ, созданная на основе такого образа, можно поместить лишь на узлы, на которых размещения работают в режиме нестрогого соответствия или на которых вообще нет размещений. При создании размещений убедитесь, что либо размещения работают в режиме нестрогого соответствия, либо имеются неназначенные узлы. В противном случае пользователи панели самообслуживания не смогут создавать ВМ на основе своих пользовательских образов.

Ограничения

- После добавления узла в размещение тем ВМ, которые уже размещены на этом узле, данное размещение не назначается автоматически.
- Виртуальную машину, которая назначена размещению, можно переносить только между узлами в этом размещении. При добавлении узлов в размещения не забудьте указать параметры миграции для различных сценариев, включая высокую доступность и обслуживание. Избегайте ситуаций, в которых ВМ невозможно перенести из-за ограничений, налагаемых размещениями. В таком случае можно изменить размещение ВМ, как описано в разделе "Управление виртуальными машинами в размещениях" на странице 490.
- Если создать размещение после создания проекта, то это размещение не включается автоматически в квотах проекта.

Предварительные требования

- Четкое понимание понятий, связанных с режимами размещения, которые описываются в разделе "Режимы размещения" на странице 643.

Чтобы создать размещение

Панель администратора

1. Откройте вкладку **Вычисления** > **Серверы** > **Размещения** и нажмите кнопку **Создать размещение**.
2. Выберите режим размещения.
   - В режиме **Нестрогое соответствие** ВМ может быть размещена на узле, которому назначены по меньшей мере те же размещения, что и у ВМ. Этот режим позволяет располагать ВМ без назначенных размещений на любом узле.
   - В режиме **Строгое соответствие** ВМ может размещаться только на узле, которому назначены в точности те же размещения, что и этой ВМ.
3. Укажите имя для нового размещения. Имя должно ясно отражать отличительный признак узлов в этом размещении, например **лицензия Microsoft Windows Server**.

4. В разделе **Серверы** нажмите кнопку **Добавить** и выберите узлы, которым необходимо назначить создаваемое размещение. Один и тот же узел может быть добавлен в несколько размещений.
5. [Необязательно] В разделах **Образы** и **Типы ВМ** нажмите кнопку **Добавить** и выберите образы и типы ВМ, которым нужно назначить размещение. Виртуальным машинам, созданным из таких образов и с такими типами ВМ, будет автоматически назначаться это размещение.
6. Нажмите кнопку **Создать**.

Новое размещение появится в списке. Чтобы разрешить пользователям панели самообслуживания создавать виртуальные машины из образов и с типами ВМ, которым назначено это размещение, добавьте данное размещение в квоты проекта.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute placement create [--isolated | --non-isolated] [--description <description>]
                                        [--nodes <nodes>] [--images <images>] [--flavors <flavors>]
                                        <placement-name>
```

--isolated
: Создание размещения, для которого будет задан режим строгого соответствия (используется по умолчанию)

--non-isolated
: Создание размещения, для которого будет задан режим нестрогого соответствия

--description <description>
: Описание размещения

--nodes <nodes>
: Разделенный запятыми список идентификаторов или имен хостов вычислительных серверов для назначения в размещение

--images <images>
: Разделенный запятыми список идентификаторов или имен образов для назначения в вычислительное размещение

--flavors <flavors>
: Разделенный запятыми список идентификаторов или имен типов ВМ для назначения в вычислительное размещение

<placement-name>
: Имя размещения

Например, чтобы создать размещение с именем placement1, задать для него режим строгого соответствия и назначить его узлам node001, node002, node003, а также типу ВМ с идентификатором 101, выполните:

```
# vinfra service compute placement create placement1 --nodes node001,node002,node003 --flavors
101
+-------------+--------------------------------------+
| Field       | Value                                |
+-------------+--------------------------------------+
| description |                                      |
| flavors     | 1                                    |
| id          | e4230b75-a858-404c-be3b-4b3f2dedb057 |
| images      | 0                                    |
| name        | placement1                           |
| nodes       | 3                                    |
| servers     | 0                                    |
+-------------+--------------------------------------+
```

Новое расположение появится в выводе команды vinfra service compute placement list:

```
# vinfra service compute placement list -c id -c name -c nodes -c images -c flavors -c isolated
+--------------------+------------+-------------+-------+--------+---------+---------+----------+
| id                 | name       | description | nodes | images | servers | flavors | isolated |
+--------------------+------------+-------------+-------+--------+---------+---------+----------+
| e4230b75-a858-<...> | placement1 |             | 3     | 0      | 0       | 1       | True     |
+--------------------+------------+-------------+-------+--------+---------+---------+----------+
```

Назначение и отмена назначения расположений

Ограничения

- После добавления узла в размещение тем ВМ, которые уже размещены на этом узле, данное размещение не назначается автоматически.
- Виртуальную машину, которая назначена размещению, можно переносить только между узлами в этом размещении. При добавлении узлов в размещения не забудьте указать параметры миграции для различных сценариев, включая высокую доступность и обслуживание. Избегайте ситуаций, в которых ВМ невозможно перенести из-за ограничений, налагаемых размещениями. В таком случае можно изменить размещение ВМ, как описано в разделе "Управление виртуальными машинами в размещениях" на странице 490.

Предварительные требования

- Должны быть созданы размещения для вычислительных узлов, как описано в разделе "Создание размещений" на странице 647.

Чтобы назначить размещение узлу

Панель администратора

1. На вкладке **Вычисления** > **Серверы** > **Размещения** щелкните по нужному размещению.
2. Перейдите на вкладку **Серверы** и нажмите **Добавить**.
3. Выберите узлы, которым следует назначить это размещение, и нажмите **Добавить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute placement assign --nodes <nodes> <placement>
```

--nodes <nodes>

Разделенный запятыми список идентификаторов или имен хостов вычислительных серверов для назначения в размещение

<placement>

Идентификатор или имя размещения

Например, чтобы назначить размещение placement1 вычислительному серверу node005.vstoragedomain, выполните:

```
# vinfra service compute placement assign --nodes node005 placement1
```

Чтобы назначить размещение образу

Панель администратора

1. Откройте вкладку **Вычисления** > **Серверы** > **Размещения** и щелкните по нужному размещению.
2. На вкладке **Свойства** нажмите **Добавить** в разделе **Образы**.
3. Выберите один или несколько образов, которым следует назначить это размещение, и нажмите **Добавить**.

При выборе этого образа в процессе создания ВМ соответствующее размещение будет выбрано автоматически.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute placement assign --images <images> <placement>
```

--images <images>

Разделенный запятыми список идентификаторов или имен образов для назначения в вычислительное размещение

<placement>

Идентификатор или имя размещения

Например, чтобы назначить размещение placement1 образу cirros, выполните:

```
# vinfra service compute placement assign --images cirros placement1
```

Чтобы назначить размещение типу ВМ

Панель администратора

1. Откройте вкладку **Вычисления** > **Серверы** > **Размещения** и щелкните по нужному размещению.
2. На вкладке **Свойства** нажмите **Добавить** в разделе **Типы ВМ**.
3. Выберите один или несколько типов ВМ, которым следует назначить это размещение, и нажмите **Добавить**.

При выборе этого типа ВМ в процессе создания ВМ соответствующее размещение будет выбрано автоматически.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute placement assign --flavors <images> <placement>
```

--flavors <flavors>

Разделенный запятыми список идентификаторов или имен типов ВМ для назначения в вычислительное размещение

<placement>

Идентификатор или имя размещения

Например, чтобы назначить размещение placement1 типу ВМ с идентификатором 102, выполните:

```
# vinfra service compute placement assign --flavors 102 placement1
```

Чтобы отменить назначения размещения

Панель администратора

1. Откройте вкладку **Вычисления** > **Серверы** > **Размещения** и щелкните по нужному размещению.
2. На вкладке **Свойства** нажмите на значок корзины рядом с образом или типом ВМ, чтобы отменить назначение.
3. Перейдите на вкладку **Серверы** и нажмите на значок корзины рядом с узлом, чтобы отменить назначение.
4. В окне подтверждения нажмите **Удалить**.

Интерфейс командной строки

1. Получите сведения о размещении, чтобы узнать, назначено ли оно каким-либо образам, типам ВМ или вычислительным серверам. Например:

```
# vinfra service compute placement show placement1
+-------------+--------------------------------------+
| Field       | Value                                |
+-------------+--------------------------------------+
| description |                                      |
```

```
| flavors    | 0                                    |
| id         | e4230b75-a858-404c-be3b-4b3f2dedb057 |
| images     | 1                                    |
| name       | placement1                           |
| nodes      | 3                                    |
| servers    | 0                                    |
+------------+--------------------------------------+
```

2. Получите список объектов, которым это размещение назначено. Если такие объекты есть, узнайте их имена. Например:

```
# vinfra service compute node list --long -c id -c placements
+-----------------------+--------------------------------------+
| host                  | placements                           |
+-----------------------+--------------------------------------+
| node001.vstoragedomain | - e4230b75-a858-404c-be3b-4b3f2dedb057 |
| node002.vstoragedomain | - e4230b75-a858-404c-be3b-4b3f2dedb057 |
| node003.vstoragedomain | - e4230b75-a858-404c-be3b-4b3f2dedb057 |
| node004.vstoragedomain | []                                   |
| node005.vstoragedomain | []                                   |
+-----------------------+--------------------------------------+
# vinfra service compute image list --long -c name -c placements
+--------------------------+--------------------------------------+
| name                     | placements                           |
+--------------------------+--------------------------------------+
| fedora-coreos-x64-k8saas | []                                   |
| amphora-x64-haproxy      | []                                   |
| cirros                   | - e4230b75-a858-404c-be3b-4b3f2dedb057 |
+--------------------------+--------------------------------------+
```

3. Отмените все назначения размещения. Например:

```
# vinfra service compute placement delete-assign --node node001 placement1
# vinfra service compute placement delete-assign --node node002 placement1
# vinfra service compute placement delete-assign --node node003 placement1
# vinfra service compute placement delete-assign --image cirros placement1
```

Изменение и удаление размещений

Ограничения

- Размещение, которое содержит узлы, образы или типы ВМ, удалить нельзя.
- После удаления размещения его назначение виртуальным машинам и томам не отменяется автоматически. Чтобы очистить назначения, присвоенные виртуальным машинам и томам, используйте параметр --no-placements в командах vinfra service compute server set и vinfra service compute volume set.

Предварительные требования

- Должны быть созданы размещения для вычислительных узлов, как описано в разделе "Создание размещений" на странице 647.
- Перед удалением размещения все его назначения должны быть отменены, как описано в разделе "Назначение и отмена назначения расположений" на странице 649.

Чтобы переименовать размещение

Панель администратора

1. На вкладке **Вычисления** > **Серверы** > **Размещения** выберите нужное размещение и нажмите **Изменить** на его правой панели.
2. Введите новое имя и нажмите **Сохранить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute placement update [--name <placement-name>] <placement>
```

--name <placement-name>

Новое имя размещения

<placement>

Имя размещения

Например, чтобы переименовать размещение placement1 в placement2, выполните:

```
# vinfra service compute placement update --name placement2 placement1
```

Чтобы удалить размещение

Панель администратора

1. На вкладке **Вычисления** > **Серверы** > **Размещения** выберите нужное размещение.
2. На вкладке **Свойства** удалите все назначенные размещению образы и типы ВМ, если они имеются.
3. Перейдите на вкладку **Серверы** и удалите все назначенные размещению узлы, если они имеются.
4. На правой панели размещения нажмите кнопку **Удалить**.
5. В окне подтверждения нажмите **Удалить размещение**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute placement delete <placement>
```

<placement>

Имя размещения

Например, чтобы удалить размещение placement1, выполните:

```
# vinfra service compute placement delete placement1
```

7.6.6.3 Возвращение огражденных узлов к работе

На вычислительном узле может произойти отказ, вызванный сбоем ядра, отключением питания, или он может оказаться недоступен для сетевого подключения. Когда отказавший узел снова становится доступен, он ограждается и на нем не планируется размещение новых виртуальных машин, но из этого состояния его можно вернуть к работе вручную.

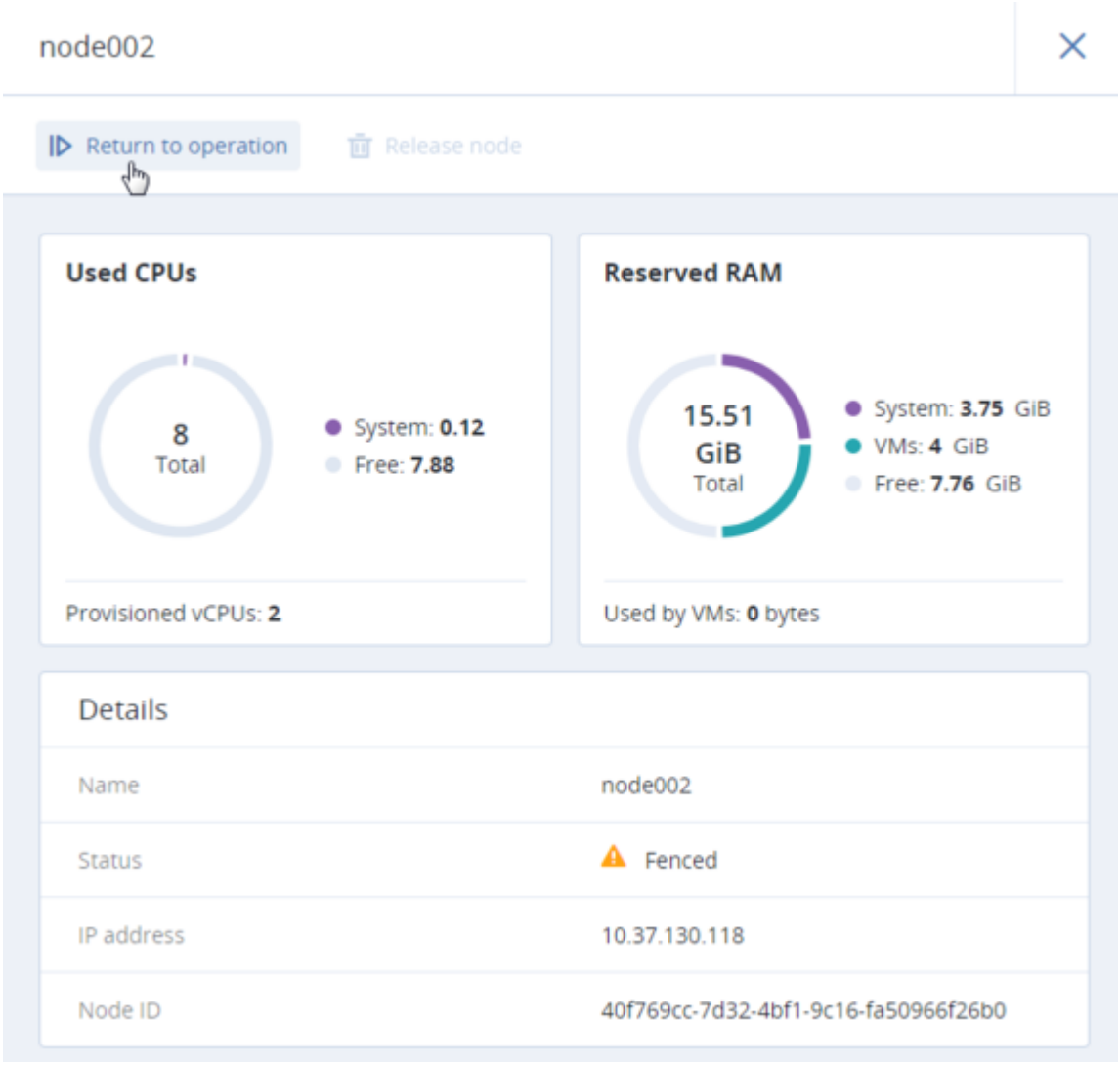
Ограничения

- Вычислительный кластер может выдержать выход из строя только одного узла.

Чтобы вернуть огражденный узел к работе

Панель администратора

Откройте панель огражденного узла и щелкните **Вернуть к работе**.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute node unfence <node>
```

<node>

Идентификатор или имя хоста узла

Например, чтобы вернуть к работе узел node005.vstoragedomain, выполните:

```
# vinfra service compute node unfence node005.vstoragedomain
```

При необходимости можно вернуть узел в огражденное состояние с помощью команды vinfra service compute node fence.

7.6.6.4 Освобождение узлов из вычислительного кластера

Если вам понадобится высвободить вычислительные узлы из кластера, можно начать с обычных узлов (то есть не узлов управления). Когда будут высвобождены все обычные вычислительные узлы, можно начинать исключение узлов управления. Узлы управления можно высвободить только все одновременно. Их освобождение уничтожает вычислительный кластер.

Ограничения

- В вычислительном кластере должно быть как минимум три сервера, чтобы пользователи в режиме самообслуживания могли включить высокую доступность для мастер-серверов Kubernetes.

Предварительные требования

- Четкое понимание ограничений, перечисленных в разделе "Высокая доступность и вычислительный кластер" на странице 29.
- Если на узле размещаются виртуальные машины, их следует перенести на другие узлы, как описано в разделе "Миграция виртуальных машин" на странице 491.
- Чтобы уничтожить вычислительный кластер, необходимо удалить все виртуальные машины на нем.

Чтобы освободить узлы из вычислительного кластера

Панель администратора

1. На экране **Вычисления** > **Серверы** выполните одно из следующих действий.
   - Выберите узлы и нажмите кнопку **Освободить** над списком.
   - Щелкните по значку многоточия рядом с нужным узлом и выберите **Освободить**.
   - Щелкните по узлу, чтобы открыть подробные сведения о нем, затем щелкните **Освободить узел** на правой панели узла.
2. В окне **Освободить узел** подтвердите действие, нажав кнопку **Освободить**.

Выбранные узлы исчезнут с экрана **Серверы**. Если были выбраны все вычислительные узлы, то вычислительный кластер также будет уничтожен.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute node release [--compute] [--controller] <node>
```

--compute

Роль вычислительного сервера

--controller

Роль вычислительного сервера контроллера

<node>

Идентификатор сервера или имя хоста

Например, чтобы освободить узел node005.vstoragedomain из вычислительного кластера, выполните:

```
# vinfra service compute node release node005.vstoragedomain
```

Освобожденный узел исчезнет из вывода команды vinfra service compute node list:

```
# vinfra service compute node list
+------------------+------------------------+---------+--------------+
| id               | host                   | state   | roles        |
+------------------+------------------------+---------+--------------+
| 7ffa9540-5a20<...> | node001.vstoragedomain | healthy | - controller |
|                  |                        |         | - compute    |
| 6e8afc28-7f71<...> | node002.vstoragedomain | healthy | - compute    |
| 02ff64ae-5800<...> | node003.vstoragedomain | healthy | - compute    |
| 827a1f4e-56e5<...> | node004.vstoragedomain | healthy | - compute    |
+------------------+------------------------+---------+--------------+
```

Чтобы освободить все узлы из вычислительного кластера, используйте следующую команду:

```
vinfra service compute delete
```

7.6.7 Использование учета для вычислительных ресурсов

Можно собирать данные об использовании вычислительных ресурсов с помощью Gnocchi. Эта база данных временных рядов обрабатывает и хранит данные измерений вычислительных ресурсов и предоставляет доступ к ним через REST API или программу командной строки.

Выборка измерений может производиться из таких вычислительных ресурсов, как виртуальные машины, диски и интерфейсы BM, вычислительные сети, тома и т. д. Все ресурсы постоянно пересматриваются, и, если изменяется какой-либо атрибут ресурса, это изменение записывается

в историю ресурса. Например, для ВМ можно измерить объем выделенной памяти и количество виртуальных ЦП, а также потребление памяти и ресурсов ЦП.

Сущность, в которой хранятся агрегированные показатели, состоящие из метки времени и значения, называется метрикой. Метрика прикрепляется к определенному ресурсу и связывается с политикой архивирования. Политика определяет, как долго агрегированные показатели хранятся в метрике и как они вычисляются (минимум, максимум, среднее и т. д.).

Для хранения метрик используются две стандартные политики архивирования low и ceilometer-low-rate. Эти политики подразумевают, что все полученные агрегированные результаты хранятся один месяц с точностью до 5 минут. Разница между ними состоит в следующем:

- ceilometer-low-rate используется для накопительных метрик и сохраняет только средние значения, а также среднее изменение значений на интервал.
- low используется для измерительных метрик и сохраняет минимальные, максимальные и средние значения, среднеквадратичное отклонение, а также сумму и количество измерений.

Следующие метрики доступны для агрегирования:

Метрики вычислительных ресурсов

Метрика	Тип	Тип ресурса	Описание
memory	gauge	instance	Объем ОЗУ, выделенный для ВМ, в мегабайтах
memory.usage	gauge	instance	Процент использования ОЗУ виртуальной машиной
vcpus	gauge	instance	Количество виртуальных ЦП, выделенных для ВМ
cpu	cumulative	instance	Процессорное время, использованное виртуальной машиной, в наносекундах
disk.device.read.requests	cumulative	instance_disk	Количество запросов на чтение
disk.device.write.requests	cumulative	instance_disk	Количество запросов на запись
disk.device.read.bytes	cumulative	instance_disk	Объем прочитанных данных в байтах
disk.device.write.bytes	cumulative	instance_disk	Объем записанных данных в байтах
network.incoming.bytes	cumulative	instance_ network_ interface	Входящий сетевой трафик в байтах
network.outgoing.bytes	cumulative	instance_ network_ interface	Исходящий сетевой трафик в байтах
network.incoming.packets	cumulative	instance_ network_	Входящий сетевой трафик в пакетах

Метрика	Тип	Тип ресурса	Описание
		interface	
network.outgoing.packets	cumulative	instance_ network_ interface	Исходящий сетевой трафик в пакетах
image.size	gauge	image	Размер отправленного образа в байтах
volume.size	gauge	volume	Размер тома в гигабайтах
snapshot.size	gauge	volume	Размер моментального снимка тома в гигабайтах
magnum.cluster	gauge	coe_cluster	Количество кластеров системы оркестрации контейнеров (COE), то есть Kubernetes
bandwidth	delta	network	Входящий и исходящий сетевой трафик для физической вычислительной сети в байтах

Накопительные метрики опрашиваются каждые пять минут и увеличиваются с течением времени, а измерительные метрики обновляются при каждом событии и показывают переменные значения.

Предварительные требования

- Установлен сервис учета и биллинга, как описано в разделе "Подготовка к работе учета и биллинга" на странице 193.
- Для авторизации выполнения приведенных ниже команд настроен клиент командной строки OpenStack, как описано в разделе "Подключение к интерфейсу командной строки OpenStack" на странице 427.

7.6.7.1 Просмотр ресурсов, метрик и измерений

После подключения к интерфейсу командной строки OpenStack можно получить доступ к метрикам вычислительных ресурсов с помощью инструмента командной строки Gnocchi. Посмотреть полный список команд утилиты gnocchi можно в документации OpenStack.

Чтобы просмотреть существующие ресурсы

Используйте команду gnocchi resource list. Например:

```
# gnocchi --insecure resource list -c id -c type -c project_id
+--------------+---------------------------+------------+
| id           | type                      | project_id |
+--------------+---------------------------+------------+
| 238597c7<...> | volume                    | c1bf1<...> |
| 3c78558f<...> | instance                  | c1bf1<...> |
| 44f1896f<...> | instance_network_interface | c1bf1<...> |
```

```
| 880e9efc<...> | instance_disk            | c1bf1<...> |
+--------------+--------------------------+------------+
```

Выходные данные показывают, что в вычислительном кластере размещена одна виртуальная машина с одним сетевым адаптером и одним диском, который также присутствует как том.

Чтобы просмотреть доступные метрики ресурсов

Используйте команду gnocchi metric list. Например:

```
# gnocchi --insecure metric list
+-------------+-------+------------------------------+---------+-------------+
| id          | <...> | name                         | unit    | resource_id |
+-------------+-------+------------------------------+---------+-------------+
| 243c7a<...> | <...> | disk.root.size               | GB      | 3c7855<...> |
| 365e45<...> | <...> | network.outgoing.packets     | packet  | 44f189<...> |
| 4fbd3e<...> | <...> | disk.device.read.requests    | request | 880e9e<...> |
| 54519f<...> | <...> | compute.instance.booting.time | sec     | 3c7855<...> |
| 5e1406<...> | <...> | disk.device.write.bytes      | B       | 880e9e<...> |
| 66a96c<...> | <...> | vcpus                        | vcpu    | 3c7855<...> |
| 722ea9<...> | <...> | memory                       | MB      | 3c7855<...> |
| 7c961a<...> | <...> | disk.device.write.requests   | request | 880e9e<...> |
| 87e9fb<...> | <...> | network.incoming.packets     | packet  | 44f189<...> |
| 9d5632<...> | <...> | disk.device.read.bytes       | B       | 880e9e<...> |
| b8be8f<...> | <...> | cpu                          | ns      | 3c7855<...> |
| c1961b<...> | <...> | disk.ephemeral.size          | GB      | 3c7855<...> |
| c9b61e<...> | <...> | volume.size                  | GB      | 238597<...> |
| d06a58<...> | <...> | network.outgoing.bytes       | B       | 44f189<...> |
| e2d998<...> | <...> | network.incoming.bytes       | B       | 44f189<...> |
| eaac2b<...> | <...> | memory.usage                 | MB      | 3c7855<...> |
+-------------+-------+------------------------------+---------+-------------+
```

Чтобы просмотреть измерения для метрики

Используйте команду gnocchi measures show. Например:

```
# gnocchi --insecure measures show cpu \
--resource-id 3c78558f-08bf-47e2-ba3e-bdb13e7b25bb
+---------------------------+-------------+-------------+
| timestamp                 | granularity |       value |
+---------------------------+-------------+-------------+
| 2019-12-11T17:05:00+03:00 |       300.0 |  2.2756e+11 |
| 2019-12-11T17:10:00+03:00 |       300.0 |  2.8897e+11 |
| 2019-12-11T17:15:00+03:00 |       300.0 |  3.7367e+11 |
| 2019-12-11T17:20:00+03:00 |       300.0 |    4.64e+11 |
| 2019-12-11T17:25:00+03:00 |       300.0 |  7.6104e+11 |
+---------------------------+-------------+-------------+
```

По умолчанию используется метод агрегирования mean. Чтобы получить данные о потреблении процессорного времени на каждый интервал, используйте параметр --aggregation rate:mean:

```
# gnocchi --insecure measures show cpu --aggregation rate:mean \
--resource-id 3c78558f-08bf-47e2-ba3e-bdb13e7b25bb
+---------------------------+-------------+---------------+
| timestamp                 | granularity |         value |
+---------------------------+-------------+---------------+
| 2019-12-11T17:10:00+03:00 |       300.0 | 61410000000.0 |
| 2019-12-11T17:15:00+03:00 |       300.0 | 84700000000.0 |
| 2019-12-11T17:20:00+03:00 |       300.0 | 90330000000.0 |
| 2019-12-11T17:25:00+03:00 |       300.0 |     2.9704e+11 |
| 2019-12-11T17:30:00+03:00 |       300.0 |      3.64e+11 |
+---------------------------+-------------+---------------+
```

7.6.7.2 Изменение срока хранения метрик

Примечание
Увеличение срока хранения ведет к значительному увеличению размера базы данных Gnocchi по сравнению со стандартным значением.

Срок хранения метрик можно изменить с помощью политики архивирования. По умолчанию для хранения метрик используются политики ceilometer-low-rate и low. Обратите внимание на то, что для этих политик нельзя изменить точность измерения.

Чтобы просмотреть сведения о политике метрики

Используйте команду gnocchi archive-policy show. Например:

```
# gnocchi --insecure archive-policy show ceilometer-low-rate
+--------------------+---------------------------------------+
| Field              | Value                                 |
+--------------------+---------------------------------------+
| aggregation_methods | rate:mean, mean                      |
| back_window        | 0                                     |
| definition         | - points: 8640, granularity: 0:05:00, |
|                    |   timespan: 30 days, 0:00:00          |
| name               | ceilometer-low-rate                   |
+--------------------+---------------------------------------+
```

В выходных данных:

- «8640 точек» означает количество агрегированных результатов, которые будут сохранены;
- «точность 5 минут» определяет промежуток времени между агрегированными результатами;
- «интервал 30 дней» означает период хранения результатов.

Иначе говоря, метрики, к которым применяется политика ceilometer-low-rate, в течение месяца будут хранить 8640 рассчитанных агрегированных результатов с точностью 5 минут.

Чтобы изменить определение политики

Используйте команду gnocchi archive-policy update. Для расчета правильного количества точек, необходимых для желаемого интервала, используйте следующую формулу:

```
количество точек = интервал \ точность
```

Например, чтобы обеспечить хранение агрегированных результатов в течение 2 месяцев с точностью 5 минут, укажите 17 280 точек:

```
# gnocchi --insecure archive-policy update ceilometer-low-rate \
-d points:17280,granularity:0:05:00,timespan:60d
+--------------------+---------------------------------------+
| Field              | Value                                 |
+--------------------+---------------------------------------+
| aggregation_methods | rate:mean, mean                      |
| back_window        | 0                                     |
| definition         | - points: 17280, granularity: 0:05:00, |
|                    |   timespan: 60 days, 0:00:00          |
| name               | ceilometer-low-rate                   |
+--------------------+---------------------------------------+
```

7.6.7.3 Просмотр использования исходящего трафика

Метрика bandwidth, которая может показывать использование исходящего трафика, по умолчанию недоступна. Чтобы использовать эту метрику, сначала необходимо ее настроить.

Чтобы настроить метрику для исходящего трафика

1. Создайте счетчик с помощью команды openstack network meter create. Например, чтобы создать счетчик outgoing_traffic в проекте project1 внутри домена domain1, выполните следующую команду:

   ```
   # openstack --insecure network meter create outgoing_traffic --share \
   --project project1 --project-domain domain1
   ```

2. Создайте правило, которое включает весь исходящий сетевой трафик, указав CIDR 0.0.0.0/0 и направление выходного трафика. Например:

   ```
   # openstack --insecure network meter rule create outgoing_traffic --egress \
   --include --remote-ip-prefix 0.0.0.0/0
   ```

3. Создайте правило, которое исключает исходящий сетевой трафик вашей физической вычислительной сети, указав ее CIDR. Например, для физической вычислительной сети с CIDR 10.10.10.0/24 выполните следующую команду:

   ```
   # openstack --insecure network meter rule create outgoing_traffic --egress \
   --exclude --remote-ip-prefix 10.10.10.0/24
   ```

Теперь можно приступать к созданию виртуальных маршрутизаторов и назначению плавающих IP-адресов виртуальным машинам на панели самообслуживания. Метрика bandwidth будет учитывать только исходящий трафик ВМ через виртуальные маршрутизаторы.

Чтобы просмотреть измерения для метрики исходящего трафика

1. Найдите resource_id для метрики bandwidth. Например:

```
# gnocchi --insecure metric list | grep bandwidth
| dce6d500-37c9<…> | low | bandwidth | B | cfc0cbb3-ff05-4b25-be7c-ab7f872e4180 |
```

2. Просмотрите измерения для этого ресурса. Например:

```
# gnocchi --insecure measures show --resource-id cfc0cbb3-ff05-4b25-be7c-ab7f872e4180
bandwidth
+---------------------------+-------------+---------+
| timestamp                 | granularity |   value |
+---------------------------+-------------+---------+
| 2021-10-03T02:40:00+03:00 |       300.0 |  1045.0 |
| 2021-10-03T02:50:00+03:00 |       300.0 |  1907.0 |
| 2021-10-03T02:55:00+03:00 |       300.0 | 15932.0 |
+---------------------------+-------------+---------+
```

7.6.7.4 Просмотр использования ресурсов на уровне проекта

Чтобы получить данные об использовании вычислительных ресурсов, выделенных всем виртуальным машинам, принадлежащим к определенному проекту, используйте либо команду vinfra, либо утилиту gnocchi. Утилита собирает данные об использовании ресурсов за определенный период времени.

Чтобы просмотреть использование ресурсов на уровне проекта с помощью команды vinfra

Используйте команду vinfra service compute quotas show --usage <project_id>. Например:

```
# vinfra service compute quotas show 6ef6f48f01b640ccb8ff53117b830fa3 --usage
+---------------------------------+-------+
| Field                           | Value |
+---------------------------------+-------+
| compute.cores.limit             | 20    |
| compute.cores.used              | 2     |
| compute.ram.limit               | 40960 |
| compute.ram.used                | 4096  |
| k8saas.cluster.limit            | 10    |
| k8saas.cluster.used             | 0     |
| lbaas.loadbalancer.limit        | 10    |
| lbaas.loadbalancer.used         | 0     |
| network.floatingip.limit        | 10    |
| network.floatingip.used         | 0     |
| storage.gigabytes.default.limit | 1024  |
| storage.gigabytes.default.used  | 66    |
+---------------------------------+-------+
```

Выходные данные показывают, что для ВМ, включенных в проект с идентификатором 6ef6f48f01b640ccb8ff53117b830fa3, было выделено 2 виртуальных ЦП, 4 ГБ ОЗУ и 66 ГБ дискового пространства.

Чтобы просмотреть использование ресурсов на уровне проекта с помощью утилиты gnocchi

Используйте команды, приведенные ниже. Например, чтобы получить агрегированные данные об использовании ресурсов для проекта с идентификатором 75521ab61d1f4e9090aac5836c219492 с 12:00 18 июля 2021 г. по 12:00 19 июля 2021 г., выполните следующие команды:

- Для агрегирования количества выделенных виртуальных ЦП:

```
# gnocchi --insecure aggregates --resource-type instance --needed-overlap 0 "(aggregate sum
(metric vcpus mean))" \
"project_id=75521ab61d1f4e9090aac5836c219492" --start 2021-07-18T12:00:00 --stop 2021-07-
19T12:00:00
```

- Для агрегирования объема выделенной оперативной памяти:

```
# gnocchi --insecure aggregates --resource-type instance --needed-overlap 0 "(aggregate sum
(metric memory mean))" \
"project_id=75521ab61d1f4e9090aac5836c219492" --start 2021-07-18T12:00:00 --stop 2021-07-
19T12:00:00
```

- Для агрегирования общего размера выделенного дискового пространства:

```
# gnocchi --insecure aggregates --resource-type volume --needed-overlap 0 "(aggregate sum
(metric volume.size mean))" \
"project_id=75521ab61d1f4e9090aac5836c219492" --start 2021-07-18T12:00:00 --stop 2021-07-
19T12:00:00
```

- Для агрегирования размера выделенного дискового пространства с политикой хранилища с идентификатором 10056d2e-6fc9-4f2e-92c2-dbebb1714778:

```
# gnocchi --insecure aggregates --resource-type volume --needed-overlap 0 \
"(aggregate sum (metric volume.size.10056d2e-6fc9-4f2e-92c2-dbebb1714778 mean))" \
"project_id=75521ab61d1f4e9090aac5836c219492" --start 2021-07-18T12:00:00 --stop 2021-07-
19T12:00:00
```

- Для агрегирования количества используемых плавающих IP-адресов:

```
# gnocchi --insecure aggregates --resource-type network --needed-overlap 0 "(aggregate sum
(metric ip.floating mean))" \
"project_id=75521ab61d1f4e9090aac5836c219492" --start 2021-07-18T12:00:00 --stop 2021-07-
19T12:00:00
```

- Для агрегирования объема исходящего сетевого трафика:

```
# gnocchi --insecure aggregates --resource-type network --needed-overlap 0 "(aggregate sum
(metric bandwidth mean))" \
```

```
"project_id=75521ab61d1f4e9090aac5836c219492" --start 2021-07-18T12:00:00 --stop 2021-07-19T12:00:00
```

- Для агрегирования количества балансировщиков нагрузки:

```
# gnocchi --insecure aggregates --resource-type loadbalancer --needed-overlap 0 \
"(aggregate sum (metric network.services.lb.loadbalancer mean))" \
"project_id=75521ab61d1f4e9090aac5836c219492" --start 2021-07-18T12:00:00 --stop 2021-07-19T12:00:00
```

- Для агрегирования количества кластеров Kubernetes:

Внимание
Кластеры Kubernetes могут создаваться с пустым идентификатором проекта. В этом случае укажите None для атрибута project_id.

```
# gnocchi --insecure aggregates --resource-type coe_cluster --needed-overlap 0 "(aggregate sum (metric magnum.cluster mean))" \
"project_id=75521ab61d1f4e9090aac5836c219492" --start 2021-07-18T12:00:00 --stop 2021-07-19T12:00:00
```

7.6.8 Управление автоматической балансировкой нагрузки на вычислительные серверы

Автоматическая балансировка нагрузки на вычислительные серверы (DRS) – это функция, которая позволяет отслеживать нагрузку на серверы, создаваемую размещенными на них виртуальными машинами, определять недостаточно или чрезмерно нагруженные серверы и выполнять балансировку нагрузки таким образом, чтобы она равномерно распределялась между всеми серверами. Балансировка нагрузки осуществляется путем перемещения виртуальных машин между серверами без остановки перемещаемых виртуальных машин. При балансировке учитываются размещения, коэффициенты перераспределения виртуальных ЦП и ОЗУ, а также ресурсы, выделенные службам хранилища и вычислений.

Эта функция снимает с администраторов инфраструктуры необходимость выполнения ручных действий, а также позволяет увеличить общую производительность виртуальных машин за счет их оптимального распределения по серверам вычислительного кластера.

Включение автоматической балансировки нагрузки

1. На экране **Настройки** > **Системные настройки** > **DRS** установите флажок **Включить DRS**.
2. Задайте параметры балансировки.
   - **Степень агрессивности**. Степень «агрессивности» балансировки. Чем больше значение этого параметра, тем меньшая несбалансированность нагрузки может привести к перемещениям виртуальных машин. При достаточно малых значениях возможно полное отсутствие перемещений, а при достаточно больших значениях – большое количество

малоэффективных перемещений.

- **Периодичность принятия решений**. Интервал времени между запусками балансировки. Между запусками балансировки собираются данные об использовании виртуальных ЦП и ОЗУ вычислительных серверов виртуальными машинами. При запуске балансировки происходит принятие решений о перемещениях на основании собранных данных и осуществляются перемещения. Чем больше значение этого параметра, тем реже будут выполняться перемещения виртуальных машин.
- **Ресурсы для балансировки**. Типы ресурсов для расчета показателя несбалансированности нагрузки на вычислительные серверы.
  - **Фактически используемые ресурсы**. Количество виртуальных ЦП и объем ОЗУ, используемые виртуальными машинами на серверах.
  - **Выделенные ресурсы**. Количество виртуальных ЦП и объем ОЗУ, выделенные виртуальным машинам на серверах.

3. [Необязательно] По умолчанию балансировка нагрузки всегда включена и выполняется с заданной периодичностью в течение дня. Можно ограничить ее время работы частью дня, установив флажок **Задать график работы** и указав время начала и конца работы в полях **Начало** и **Конец**. Вне зависимости от того, задан график работы или нет, будет осуществляться сбор данных об использовании виртуальными машинами ресурсов вычислительных серверов.
4. [Необязательно] Задайте расширенные параметры балансировки.
   - **Максимальное количество перемещений ВМ за 1 цикл**. Максимальное количество перемещений виртуальных машин между вычислительными серверами за один запуск балансировки нагрузки. Чем выше значение этого параметра, тем больше виртуальных машин может быть перемещено за один запуск.
   - **Перемещать одну ВМ не чаще <N единиц времени>**. Минимальная продолжительность промежутка времени между перемещениями одной и той же виртуальной машины между вычислительными серверами. Этот параметр позволяет предотвратить слишком частые перемещения виртуальных машин.
   - **Не перемещать ВМ с ОЗУ более, ГБ**. Максимальный объем ОЗУ, выделенный виртуальной машине. Виртуальная машина, объем ОЗУ которой больше максимального, не перемещается. Этот параметр можно использовать для предотвращения перемещений больших виртуальных машин, при перемещении которых возможны задержки или перебои в их работе.
   - **Режим вычислений**. Точность и скорость вычислений показателя несбалансированности нагрузки.
     - **Вычислять точнее**. Выполнять вычисления показателя несбалансированности нагрузки с большей точностью, но с меньшей скоростью.
     - **Вычислять быстрее**. Выполнять вычисления показателя несбалансированности нагрузки с большей скоростью, но с меньшей точностью.
   - **Формула расчета ресурсов для балансировки**. Ресурсы и способ расчета для вычислений показателя несбалансированности нагрузки.
     - **Взвешенная сумма ресурсов ЦП и ОЗУ**. Показатель несбалансированности нагрузки основан на количестве виртуальных ЦП и объеме ОЗУ вычислительных серверов,

количестве виртуальных ЦП и объеме ОЗУ виртуальных машин.

- **Взвешенная сумма выделенных и используемых ресурсов ЦП**. Показатель несбалансированности нагрузки основан на количестве виртуальных ЦП вычислительных серверов, количестве виртуальных ЦП, используемых виртуальными машинами, количестве виртуальных ЦП, выделенных виртуальным машинам.
- **Ресурсы ЦП**. Показатель несбалансированности нагрузки основан на количестве виртуальных ЦП вычислительных серверов, количестве виртуальных ЦП виртуальных машин.

- **Интервал наблюдения**. Период усреднения собранных данных об использовании виртуальных ЦП и ОЗУ вычислительных серверов виртуальными машинами. Чем больше значение этого параметра, тем меньше при балансировке будут учитываться краткосрочные изменения нагрузки (выбросы).

5. Нажмите **Сохранить**.

Примечание
Перемещение отдельной виртуальной машины можно запретить, сняв установленный по умолчанию флажок **Разрешить миграции DRS** в разделе сведений о виртуальной машине.

Выключение автоматической балансировки нагрузки

На экране **Настройки** > **Системные настройки** > **DRS** снимите флажок **Включить DRS**.

8 Мониторинг

Кибер Инфраструктура использует систему мониторинга Prometheus для отслеживания производительности и доступности кластера хранилища, узлов инфраструктуры и развернутых сервисов. Кроме того, система формирует оповещения, которые можно настроить для отправки в виде уведомлений по электронной почте.

8.1 Просмотр оповещений

Оповещение создается и регистрируется каждый раз, когда выполняется одно из следующих условий или происходит соответствующее событие.

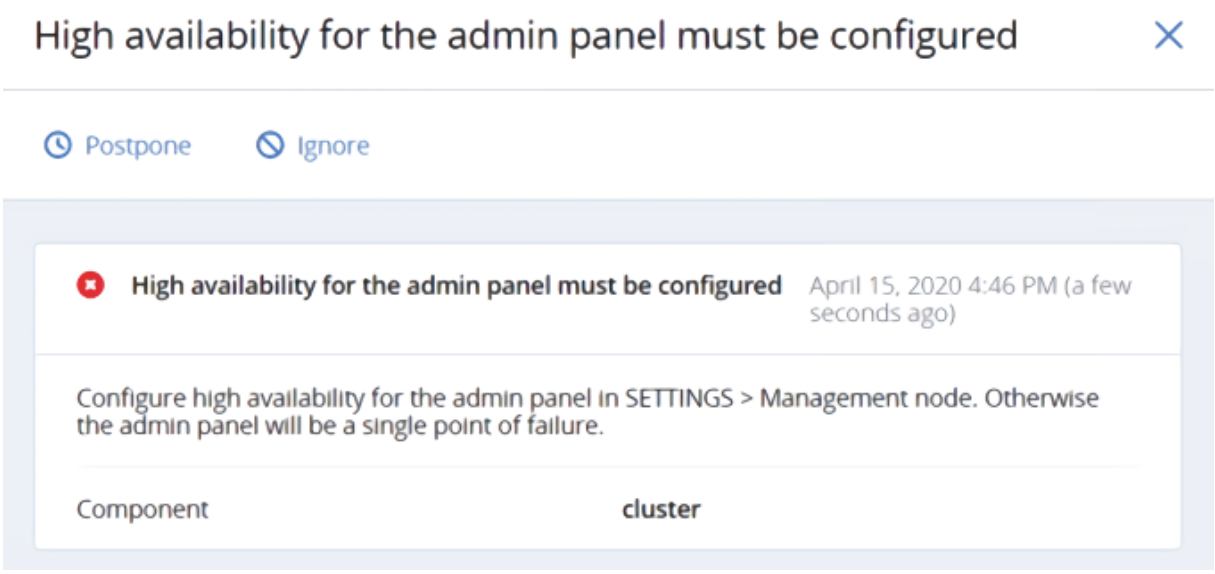
- Возникла критическая проблема с кластером, его компонентами (CS, MDS), дисками, узлами или сервисами.
- Кластеру требуются настройка или дополнительные ресурсы для построения или восстановления работоспособности.
- Сети требуется настройка, или в ней происходят неполадки, которые могут повлиять на производительность.
- Истек срок действия лицензии.
- В кластере скоро закончится или закончилось доступное пространство.

Оповещения можно проигнорировать (удалить из списка оповещений) или отложить на несколько часов. Отложенные оповещения повторно появляются в списке через некоторое время.

Чтобы просмотреть оповещение

Панель администратора

1. Перейдите на экран **Мониторинг** > **Оповещения**, на котором отображается список всех оповещений, зарегистрированных в Кибер Инфраструктура.
2. Щелкните по нужному оповещению в списке, чтобы открыть подробные сведения о нем.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster alert show <alert>
```

<alert>

Идентификатор оповещения, который можно получить с помощью команды vinfra cluster alert list

Например, чтобы просмотреть оповещение про лицензию, выполните:

```
# vinfra cluster alert list
+----+-----------------------------------------------------------+---------------------+----------+---------+
| id | type                                      | datetime          | severity | enabled |
+----+-----------------------------------------------------------+---------------------+----------+---------+
| 8  | High availability for the admin panel must be configured | 2021-09-07T18:38:55 | error    | True    |
| 6  | Network warning                                | 2021-09-07T18:38:55 | warning  | True    |
| 4  | Network warning                                | 2021-09-07T18:38:55 | warning  | True    |
| 23 | Disk cache settings are not optimal                 | 2021-09-30T23:46:28 | warning  | True    |
| 1  | License is not loaded                           | 2021-09-07T18:38:55 | warning  | True    |
| 22 | Configuration warning                           | 2021-09-30T23:21:32 | warning  | True    |
| 3  | Network warning                                | 2021-09-07T18:38:55 | warning  | True    |
| 7  | Network warning                                | 2021-09-07T18:38:55 | warning  | True    |
+----+-----------------------------------------------------------+---------------------+----------+---------+
# vinfra cluster alert show 1
+--------------+----------------------+
| Field        | Value                |
+--------------+----------------------+
| _type        | license_isnot_loaded |
| cluster_id   | 1                    |
| cluster_name | cluster1             |
```

```
| datetime     | 2021-09-07T18:38:55  |
| details      | {}                   |
| enabled      | True                 |
| group        | cluster              |
| host         |                      |
| id           | 1                    |
| message      | License is not loaded |
| node_id      |                      |
| object_id    | None                 |
| orig_hostname |                     |
| severity     | warning              |
| suspended    |                      |
| type         | License is not loaded |
+--------------+----------------------+
```

Чтобы проигнорировать оповещение

1. Перейдите на экран **Мониторинг** > **Оповещения** и щелкните в списке по нужному оповещению.
2. На правой панели оповещений нажмите **Игнорировать**.

Чтобы отложить оповещение

Панель администратора

1. Перейдите на экран **Мониторинг** > **Оповещения** и щелкните в списке по нужному оповещению.
2. На правой панели оповещений нажмите **Отложить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster alert delete <alert>
```

<alert>

Идентификатор оповещения

Например, чтобы удалить оповещение с идентификатором 1 из списка оповещений, выполните:

```
# vinfra cluster alert delete 1
```

8.1.1 Оповещения инфраструктуры

На панели администрирования формируются и отображаются следующие оповещения:

Заголовок	Сообщение	Серьезность
Оповещения о лицензии		
Лицензия не загружена	Лицензия не установлена.	предупреждение

Заголовок	Сообщение	Серьезность
Срок лицензии истек	Срок лицензии кластера <cluster_name> истек. Обратитесь к своему реселлеру, чтобы срочно обновить лицензию!	критическое
Не удается применить лицензию SPLA	Не удается применить лицензию SPLA для кластера <cluster_name>. Обратитесь к своему реселлеру, чтобы решить проблему!	критическое
Не удается передать статистику использования пространства	Не удается передать статистику использования пространства для кластера <cluster_name>. Убедитесь, что узел управления подключен к Интернету.	предупреждение
Не удается получить статистику использования пространства	Не удается получить статистику использования пространства для кластера <cluster_name>.	предупреждение
Оповещения о кластере		
Недостаточно места в кластере	В кластере осталось всего <free_space> TB (<free_space_in_percent> %) физического дискового пространства. Можно освободить часть пространства или увеличить емкость хранилища.	предупреждение
	В кластере <cluster_name> закончилось дисковое пространство, разрешенное лицензией. Дальнейшая запись данных невозможна. Обратитесь к своему реселлеру, чтобы срочно обновить лицензию!	предупреждение
Осталось мало лицензированного свободного места	Кластер достиг 80 % от лицензированного объёма хранилища.	предупреждение
Осталось критически мало лицензированного свободного места	Кластер достиг 90 % от лицензированного объёма хранилища.	критическое
Недостаточно узлов в кластере	В кластере <cluster_name> всего {1,2} узел (узла) вместо рекомендуемого минимума в 3 узла. Добавьте в кластер {2,1} или более узлов.	предупреждение
Необходимо настроить высокую доступность для панели администрирования	Настройте высокую доступность для панели администрирования в разделе «Настройки > Узел управления». Иначе панель администрирования будет единой точкой отказа.	критическое
Резервная копия узла	Резервная копия узла управления старше <number_of_	критическое

Заголовок	Сообщение	Серьезность
управления не существует	days> дн.	
	Последнее резервное копирование узла управления завершилось ошибкой, резервная его копия не существует или устарела.	критическое
Изменения в базе данных управления не реплицируются	Изменения в базе данных управления не реплицируются на узел <hostname>, так как он недоступен. Проверьте состояние узла и его подключение к сети.	критическое
	Изменения в базе данных управления не реплицируются на узел <hostname>. Обратитесь в службу технической поддержки.	
Оповещения о подключении кластера		
Проблема с сетевым подключением кластера	Проблемы с сетевым подключением всех узлов: нестабильное подключение по сети "<network_name>" вследствие потери пакетов.	критическое
	Проблемы с сетевым подключением всех узлов: отсутствует подключение по сети "<network_name>".	критическое
Проблема с сетевым подключением узла	Проблемы с сетевым подключением узла "<hostname>": нестабильное подключение по сети "<network_name>" вследствие потери всех пакетов размера MTU.	критическое
	Проблемы с сетевым подключением узла "<hostname>": нестабильное подключение по сети "<network_name>" вследствие потери некоторых пакетов размера MTU.	критическое
	Проблемы с сетевым подключением узла "<hostname>": нестабильное подключение по сети "<network_name>" вследствие потери пакетов.	критическое
	Проблемы с сетевым подключением узла "<hostname>": отсутствует подключение к узлу "<hostname>" с интерфейсом "<iface>" через интерфейс "<iface>".	критическое
	Проблемы с сетевым подключением узла "<hostname>": нестабильное подключение к узлу "<hostname>" с интерфейсом "<iface>" через интерфейс "<iface>" вследствие потери всех пакетов размера MTU.	критическое
	Проблемы с сетевым подключением узла "<hostname>": нестабильное подключение к узлу "<hostname>" с интерфейсом "<iface>" через интерфейс "<iface>" вследствие потери пакетов.	критическое
	Проблемы с сетевым подключением узла "<hostname>":	критическое

Заголовок	Сообщение	Серьезность
	нестабильное подключение к узлу "<hostname>" с интерфейсом "<iface>" через интерфейс "<iface>" вследствие потери некоторых пакетов размера MTU.	
Несовпадение MTU	У некоторых интерфейсов значение MTU отличается от других интерфейсов в той же сети: сеть "<network_name>" интерфейс на хосте "<iface>@<hostname>".	критическое
Оповещения об узлах		
Узел не в сети	Узел <hostname> не в сети.	предупреждение
Узел слишком много раз оказывался недоступен по сети	Узел <hostname> слишком много раз оказывался недоступен по сети за последний час.	предупреждение
Ядро устарело	На узле <hostname> выполняется не последняя версия ядра.	предупреждение
Сработал механизм OOM Killer	На узле <hostname> сработал механизм OOM Killer.	предупреждение
Время не синхронизировано	Время на узле <hostname> отличается от времени на узле внутреннего хранилища более чем на 5 секунд.	предупреждение
Нет подключения к Интернету	Узел кластера <hostname> не может связаться с репозиторием. Убедитесь, что у всех узлов в кластере есть доступ к Интернету.	предупреждение
Обнаружено несовместимое оборудование	На узле <hostname> обнаружено несовместимое оборудование: <hardware_list>. При использовании аппаратного обеспечения Mellanox или AMD может произойти потеря данных. Проверьте еще раз, правильно ли включена технология SR-IOV.	критическое
Место в файле подкачки заканчивается	<swap_proportion> % файла подкачки использовано на сервере "<hostname>".	критическое
Высокий показатель использования ЦП	Сервер <hostname> имеет показатель использования ЦП выше 90 %. Текущее значение: <value> %.	предупреждение
Высокий показатель использования памяти	Сервер <hostname> имеет показатель использования памяти выше 95 %. Текущее значение: <value> %.	предупреждение
Сервер имеет высокий показатель загрузки диска	Диск /dev/<disk_name> на сервере <hostname> имеет показатель I/O выше 85 %. Текущее значение: <value> %.	предупреждение
Сервер имеет высокий	Высокий показатель (<value>) потерянных пакетов при	предупреждение

Заголовок	Сообщение	Серьезность
показатель потерь сетевых пакетов при приёме	приёме на сервере <hostname>. Пожалуйста, проверьте настройки сети.	
Сервер имеет высокий показатель потерянных пакетов при передаче	Высокий показатель (<value>) потерянных пакетов при передаче на сервере <hostname>. Пожалуйста, проверьте настройки сети.	предупреждение
Сервер имеет высокий показатель ошибок в сетевых пакетах при приёме	Высокий показатель (<value>) ошибок в сетевых пакетах при приёме на сервере <hostname>. Пожалуйста, проверьте настройки сети.	предупреждение
Сервер имеет высокий показатель ошибок в сетевых пакетах при передаче	Высокий показатель (<value>) ошибок в сетевых пакетах при передаче на сервере <hostname>. Пожалуйста, проверьте настройки сети.	предупреждение
Оповещения о диске		
Предупреждение S.M.A.R.T.	Диск <disk_name> (<serial>) на узле <hostname> не прошел проверку S.M.A.R.T.	критическое
Ошибка диска	Произошел сбой диска <disk_name> (<serial>) на узле <hostname>.	критическое
Недостаточно места на диске	Заканчивается место на корневом разделе узла <hostname>.	предупреждение
Кэширование записи на диск включено	Кэширование записи на диск включено для диска <disk_name> на узле <hostname>. Отключите его, чтобы избежать вероятной потери данных в случае отключения питания.	предупреждение
Неизвестный статус кэширования записи на диск	Не удается определить статус кэширования записи для диска <disk_name> на узле <hostname>.	предупреждение
Программный RAID не синхронизирован	Программный RAID <disk_name> на сервере <hostname> синхронизирован на <value> %.	предупреждение
Сервис часто меняет статус	Сервис systemd <service_name> на сервере <hostname> изменил свой статус чаще, чем 5 раз в 5 минут или 15 раз в час.	критическое
Оповещения о сети		
Предупреждение о сети	На сетевом интерфейсе <iface_name> неправильные настройки: режим дуплекса <duplex> и скорость <speed>.	предупреждение

Заголовок	Сообщение	Серьезность
	На сетевом интерфейсе <iface_name> на узле <hostname> отсутствуют (или отключены) важные функции: <feature_name>.	предупреждение
	Сетевой интерфейс <iface_name> на узле <hostname> работает не в полнодуплексном режиме.	предупреждение
	Скорость работы сетевого интерфейса <iface_name> на узле <hostname> ниже минимально требуемой в 1 Гбит/с.	предупреждение
	Скорость сетевого интерфейса <iface_name> на узле <hostname> не определена.	предупреждение
Сетевой интерфейс часто меняет своё состояние	Сетевой интерфейс <iface_name> на сервере <hostname> часто меняет своё состояние.	предупреждение
Нарушена отказоустойчивость агрегации сетевых интерфейсов	У агрегации <iface_name> на сервере <hostname> отсутствуют подчиненные интерфейсы: <number_of_ifaces>.	критическое
Оповещения об обновлениях		
Доступны обновления системы	Доступны обновления для сервера <hostname>. Текущая версия: <current_version>. Доступна версия: <available_version>.	информация
Не удалось проверить наличие обновлений	Не удалось проверить наличие обновлений для сервера <hostname>. Пожалуйста, проверьте доступ к репозиторию.	предупреждение
Не удалось проверить наличие обновлений несколько раз подряд	Не удалось проверить наличие обновлений несколько раз подряд. Пожалуйста, проверьте доступ к репозиторию.	критическое
Не удалось загрузить обновление	Не удалось загрузить обновление на сервер <hostname>.	критическое
Ошибка обновления сервера	Не удалось загрузить обновление на сервер <hostname>.	критическое
Ошибка обновления	Не удалось завершить обновление для панели управления и вычислительного API-интерфейса.	критическое
Ошибка обновления кластера	Ошибка обновления кластера.	критическое
Не удалось перевести	Не удалось перевести сервер <hostname> в режим	критическое

Заголовок	Сообщение	Серьезность
сервер в режим обслуживания для обновления	обслуживания для обновления.	
Оповещения о службах		
Произошел сбой вычислительного кластера	Произошел отказ вычислительного кластера. Управление виртуальными машинами невозможно.	критическое
Срок действия сертификата	Срок действия сертификата Cyber Backup Gateway истек. Все операции резервного копирования остановлены. Обновите сертификат на экране Backup Gateway.	критическое
	Срок действия сертификата Cyber Backup Gateway вскоре истечет. Обновите сертификат на экране Backup Gateway.	предупреждение
	Срок действия сертификата Cyber Backup Gateway истекает <expiration_date>. Обновите сертификат на экране Backup Gateway.	
Предупреждение о избыточности	Для iSCSI LUN <lun_id> из группы целевых устройств <target_group> установлена область отказа «диск», хотя доступное количество узлов – <number_of_nodes>. Рекомендуется установить область отказа «хост», чтобы идентификатор LUN мог выдерживать сбои хостов в дополнение к сбоям дисков.	предупреждение
Сбой крупного обновления iSCSI	Сбой крупного обновления iSCSI. Будет выполнена повторная попытка...	критическое
NFS имеет недоступные файловые сервисы	Некоторые файловые сервисы не запущены на сервере <node>. Проверьте статус сервисов в интерфейсе командной строки.	предупреждение

8.1.2 Оповещения основного хранилища

На основе метрик, перечисленных в разделе "Метрики основного хранилища" на странице 757, формируются и отображаются на панели администрирования следующие оповещения для основного хранилища:

Заголовок	Сообщение	Серьезность
Оповещения о сервисе метаданных		
Недостаточно дисков метаданных	В кластере <cluster_name> имеется только один MDS. В настоящий момент есть только один диск	критическое

Заголовок	Сообщение	Серьезность
	с ролью метаданных. Потеря этого диска полностью уничтожит все данные кластера, независимо от схемы избыточности.	
	Кластеру <cluster_name> требуется больше дисков с ролью метаданных. Потеря еще одного MDS остановит работу кластера.	предупреждение
Предупреждение о конфигурации	На узле <hostname> размещено больше одного сервиса метаданных. Рекомендуется размещать только один сервис метаданных на узел. Удалите дополнительные сервисы метаданных с этого узла и создайте их на других узлах.	предупреждение
	В кластере “<cluster_name>” четыре сервиса метаданных. Эта конфигурация замедляет работу кластера и не повышает его доступность. Для кластера из четырех узлов достаточно настроить три сервиса MDS. Удалите лишний сервис MDS с одного из узлов кластера.	
	В кластере “<cluster_name>” больше пяти сервисов метаданных. Эта конфигурация замедляет работу кластера и не повышает его доступность. Для большого кластера достаточно настроить пять сервисов MDS. Удалите лишние сервисы MDS с узлов кластера.	
Сбой сервиса	Сервис метаданных #<id> находится в состоянии «<status>». Узел: <hostname>. Диск: <disk_name>. Серийный номер диска: <disk_serial>.	предупреждение
Недостаточно места на диске метаданных	Заканчивается место на диске метаданных узла <hostname>.	предупреждение
У сервиса метаданных высокий уровень использования ЦП	У сервиса метаданных на узле <node> использование ЦП выше 80 %. Возможно, сервис перегружен.	предупреждение
Высокий показатель времени ожидания операции commit у сервиса метаданных	У сервиса метаданных на узле <node> 95-й процентиль задержки превышает 1 секунду.	предупреждение
Критический показатель времени ожидания операции commit у сервиса метаданных	У сервиса метаданных на узле <node> 95-й процентиль задержки превышает 5 секунд.	критическое
В кластере есть недоступные сервисы метаданных	Некоторые сервисы метаданных недоступны, или в них произошел сбой. Проверьте	предупреждение

Заголовок	Сообщение	Серьезность
	и перезапустите их.	
Главный сервис метаданных меняется слишком часто	Главный сервис метаданных изменился более одного раза за 5 минут.	предупреждение
Оповещения о сервисе фрагментов		
Недостаточно дисков с ролью хранилища	В кластере <cluster_name> нет дисков с ролью хранилища.	предупреждение
	В кластере <cluster_name> слишком мало доступных CS.	предупреждение
Сбой сервиса	Сервис хранения данных #<id> находится в состоянии «<status>». Узел: <hostname>. Диск: <disk_name>. Серийный номер диска: <disk_serial>.	предупреждение
Неоптимальная конфигурация CS	CS#<cs_id> на уровне <tier> имеет неверные настройки журналирования.	предупреждение
	Шифрование отключено для CS#<cs_id> на уровне <tier>, но включено для других CS на том же уровне.	предупреждение
Диск хранилища работает медленно	Диск <disk_name> (CS#<cs_id>) на узле <hostname> работает медленно, его необходимо заменить.	предупреждение
Настройки кэша диска неоптимальны	У диска <disk_name> (CS#<cs_id>) на узле <hostname> настройки кэша отличаются от других дисков на том же уровне.	предупреждение
В кластере есть медленные сервисы фрагментов данных	Некоторые сервисы фрагментов данных работают замедленно и ухудшают производительность кластера.	предупреждение
В кластере есть выключенные CS сервисы	Некоторые CS сервисы отключены. Проверьте и перезапустите их.	предупреждение
В кластере есть отказавшие сервисы фрагментов данных	Некоторые сервисы фрагментов данных отказали. Возможно, это вызвано физическим отказом накопителя.	предупреждение
Оповещения о кластере хранилища		
В кластере заканчивается физическое пространство	На всех уровнях хранилища осталось мало свободного физического пространства.	предупреждение
В кластере закончилось физическое пространство	На всех уровнях хранилища недостаточно свободного физического пространства.	критическое

Заголовок	Сообщение	Серьезность
На узле имеются зависшие запросы ввода-вывода	Некоторые запросы ввода-вывода зависли на узле <node>.	критическое
Репликация в кластере заблокирована или замедлена	Репликация фрагментов заблокирована или идет слишком медленно.	критическое
На узле имеются сбойные запросы сопоставления	Некоторые из запросов сопоставления на узле <node> завершились сбоем.	критическое
В кластере очень много фрагментов данных	В кластере слишком много фрагментов данных, что замедляет службу метаданных.	предупреждение
В кластере критически много фрагментов данных	В кластере слишком много фрагментов данных, что замедляет службу метаданных.	критическое
В кластере очень много файлов	В кластере слишком много файлов, что замедляет службу метаданных.	предупреждение
В кластере критически много файлов	В кластере слишком много файлов, что замедляет службу метаданных.	критическое
В кластере имеются отказавшие точки подключения	Некоторые точки подключения перестали работать, и их необходимо восстановить.	критическое
В кластере имеются невыровненные операции записи при вводе-выводе	Операции записи при вводе-выводе выполняются без выравнивания по границам кластеров. Это может быть вызвано тем, что диск неправильно отформатирован в виртуальной машине.	информация
В кластере имеются невыровненные операции чтения при вводе-выводе	Операции чтения при вводе-выводе выполняются без выравнивания по границам кластеров. Это может быть вызвано тем, что диск неправильно отформатирован в виртуальной машине.	информация
В журнале CS заканчивается пространство	В журнале CS осталось менее 20 % свободного пространства.	предупреждение

8.1.3 Оповещения хранилища объектов

На основе метрик, перечисленных в разделе "Метрики хранилища объектов" на странице 758, формируются и отображаются на панели администрирования следующие оповещения для хранилища объектов:

Заголовок	Сообщение	Серьезность
Оповещения о сервисе шлюза S3		

Заголовок	Сообщение	Серьезность
В кластере S3 есть недоступные сервисы шлюза S3	Некоторые сервисы шлюза S3 не выполняются на узле <node>. Проверьте статус сервисов в интерфейсе командной строки.	предупреждение
Высокий показатель времени ожидания GET запроса от сервиса "S3 шлюз"	У сервиса шлюза S3 (<service_id>) на узле <node> медианная задержка запросов GET превышает 1 секунду.	предупреждение
	У сервиса шлюза S3 (<service_id>) на узле <node> медианная задержка запросов GET превышает 5 секунд.	критическое
Высокий показатель отмененных запросов у сервиса "S3 шлюз"	У сервиса шлюза S3 (<service_id>) на узле <node> частота отмены запросов превышает 5 %. Это может быть вызвано проблемами с подключением, истечением времени ожидания запросов или малым предельным размером очереди ожидающих запросов.	предупреждение
Критический показатель отмененных запросов у сервиса "S3 шлюз"	У сервиса шлюза S3 (<service_id>) на узле <node> частота отмены запросов превышает 30 %. Это может быть вызвано проблемами с подключением, истечением времени ожидания запросов или малым предельным размером очереди ожидающих запросов.	критическое
Высокий показатель использования ЦП сервисом "S3 шлюз"	У сервиса шлюза S3 (<service_id>) на узле <node> использование ЦП выше 75 %. Возможно, сервис перегружен.	предупреждение
Критический показатель использования ЦП сервисом "S3 шлюз"	У сервиса шлюза S3 (<service_id>) на узле <node> использование ЦП выше 90 %. Возможно, сервис перегружен.	критическое
Слишком много завершившихся сбоем запросов в сервисе шлюза S3	У сервиса шлюза S3 (<service_id>) на узле <node> много завершившихся сбоем запросов с ошибкой сервера (код статуса 5XX).	критическое
Оповещения о сервисе объектов		
В кластере S3 есть недоступные сервисы объектов	Некоторые сервисы объектов не выполняются на узле <node>. Проверьте статус сервисов в интерфейсе командной строки.	предупреждение
Высокий показатель времени ожидания запроса от сервиса объектов	У сервиса объектов (<service_id>) на узле <node> медианная задержка запросов превышает 1 секунду.	предупреждение
Критический показатель времени	У сервиса объектов (<service_id>) на узле <node> медианная задержка запросов превышает 5 секунд.	критическое

Заголовок	Сообщение	Серьезность
ожидания запроса от сервиса объектов		
Высокий показатель времени ожидания операции commit у сервиса объектов	У сервиса объектов (<service_id>) на узле <node> медианная задержка фиксации превышает 1 секунду. Проверьте производительность хранилища.	предупреждение
Критический показатель времени ожидания операции commit у сервиса объектов	У сервиса объектов (<service_id>) на узле <node> медианная задержка фиксации превышает 10 секунд. Проверьте производительность хранилища.	критическое
Оповещения о сервисе имен		
В кластере S3 есть недоступные сервисы имен	Некоторые сервисы имен не выполняются на узле <node>. Проверьте статус сервисов в интерфейсе командной строки.	предупреждение
Высокий показатель времени ожидания запроса от сервиса имён	У сервиса имен (<service_id>) на узле <node> медианная задержка запросов превышает 1 секунду.	предупреждение
Критический показатель времени ожидания запроса от сервиса имён	У сервиса имен (<service_id>) на узле <node> медианная задержка запросов превышает 5 секунд.	критическое
Высокий показатель времени ожидания операции commit у сервиса метаданных	У сервиса имен (<service_id>) на узле <node> медианная задержка фиксации превышает 1 секунду. Проверьте производительность хранилища.	предупреждение
Критический показатель времени ожидания операции commit у сервиса имён	У сервиса имен (<service_id>) на узле <node> медианная задержка фиксации превышает 10 секунд. Проверьте производительность хранилища.	критическое
Оповещения об агенте хранилища объектов		
Агент хранилища объектов заморожен в течение длительного времени	У агента хранилища объектов на узле <node> цикл событий неактивен уже дольше 1 минуты.	критическое
Агент хранилища	Агент хранилища объектов недоступен на узле <node>.	предупреждение

Заголовок	Сообщение	Серьезность
объектов недоступен		
Агент хранилища объектов не подключен к сервису конфигурации	Агент хранилища объектов не смог подключиться к сервису конфигурации на узле <node>.	предупреждение
Оповещения о кластере S3		
Проблема в настройке S3 кластера	Конфигурация кластера S3 не является высокодоступной. Отказ одного сервера S3 может привести к неработоспособности всего кластера S3.	предупреждение
Предупреждение избыточности данных	Для S3 задана область отказа "диск", хотя числов доступных серверов - <number_of_nodes>. Рекомендуется задать область отказа "хост", чтобы S3 мог выдержать как сбой диска, так и сервера.	предупреждение
Сервис S3 заморожен в течение длительного времени	У сервиса S3 (<service_name>, <service_id>) на узле <node> цикл событий неактивен уже дольше 1 минуты.	критическое
Не удалось запустить сервис S3	Агент хранилища объектов не смог запустить сервис <service_name>(<service_id>) на узле <node>.	критическое
В кластере S3 есть недоступные сервисы георепликации	Некоторые сервисы георепликации не выполняются на узле <node>. Проверьте статус сервисов в интерфейсе командной строки.	предупреждение
Другие оповещения		
У сервиса NFS есть недоступные сервисы файловой системы	Некоторые сервисы файловой системы не выполняются на узле <node>. Проверьте статус сервисов в интерфейсе командной строки.	предупреждение
Не удалось запустить сервис файлов	Агент хранилища объектов не смог запустить сервис файлов на узле <node>.	критическое

8.2 Просмотр журнала аудита

В журнале аудита можно просматривать все операции управления, выполненные пользователями, и события их активности.

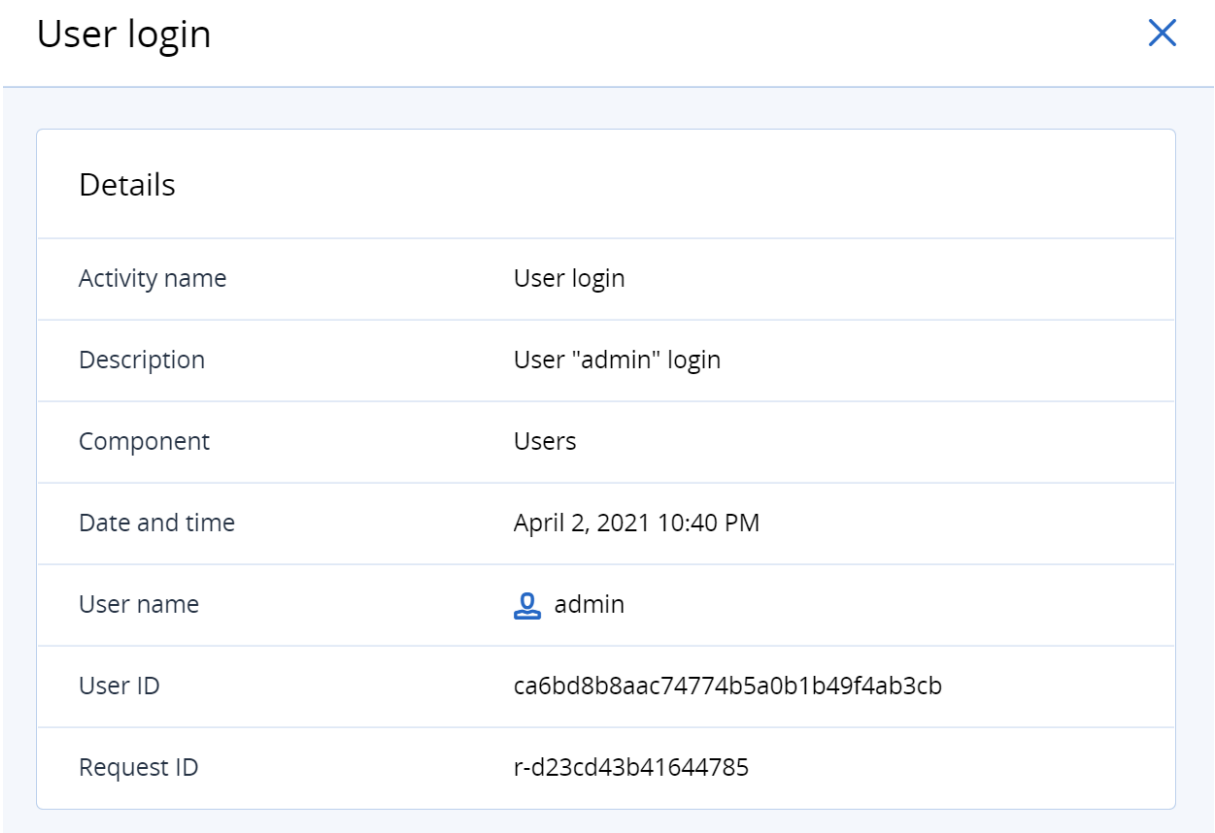
Ограничения

- Записи хранятся в течение 1 года. Когда срок хранения записи превышает 1 год, она удаляется.
- Максимальное количество записей в журнале составляет 100 000. При привышении этого значения старые записи удаляются.

Чтобы просмотреть запись в журнале

Панель администратора

1. Перейдите на экран **Мониторинг** > **Журнал аудита**, чтобы просмотреть список записей журнала аудита.
2. Щелкните по нужной записи журнала в списке, чтобы открыть подробные сведения о ней.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster auditlog show <auditlog>
```

<auditlog>

Идентификатор записи журнала аудита

Например, чтобы получить подробные сведения из записи журнала аудита про создание кластера хранилища, выполните:

```
# vinfra cluster auditlog list
+----+----------+----------------------+------------------------+--------------------+
| id | username | type                 | activity               | timestamp          |
+----+----------+----------------------+------------------------+--------------------+
```

```
| 8  | admin     | CreateCluster         | Create cluster          | 2021-09-07T17:39:16 |
| 7  | anonymous | RegisterNewNode       | Register new node       | 2021-09-07T17:39:14 |
| 6  | anonymous | RegisterNewNode       | Register new node       | 2021-09-07T17:39:10 |
| 5  | admin     | GetRegistrationToken  | Get registration token  | 2021-09-07T17:39:08 |
| 4  | admin     | GetRegistrationToken  | Get registration token  | 2021-09-07T17:39:04 |
| 3  | admin     | LoginUser             | User login              | 2021-09-07T17:39:04 |
| 2  | anonymous | UpdateNodeRegistration | Update node registration | 2021-09-07T17:39:02 |
| 1  | anonymous | RegisterNewNode       | Register new node       | 2021-09-07T17:38:54 |
+----+-----------+-----------------------+-------------------------+---------------------+
# vinfra cluster auditlog show 8
+--------------+-------------------------------------+
| Field        | Value                               |
+--------------+-------------------------------------+
| activity     | Create cluster                      |
| cluster_id   |                                     |
| cluster_name |                                     |
| component    | Cluster                             |
| details      | - id: node                          |
|              |   name: Node                        |
|              |   value: node001.vstoragedomain     |
| id           | 8                                   |
| message      | Create cluster "cluster1"           |
| node_id      | c3b2321a-7c12-8456-42ce-8005ff937e12 |
| result       | success                             |
| task_id      | r-38c61bb2c7144cef                  |
| timestamp    | 2021-09-07T17:39:16                 |
| type         | CreateCluster                       |
| user_id      | c727a901a6444ee1a8ad31e3d5b53b3a    |
| username     | admin                               |
+--------------+-------------------------------------+
```

8.3 Просмотр журналов кластера

При возникновении проблемы в продукте Кибер Инфраструктура можно отправить отчет о проблеме, как описано в разделе "Получение технической поддержки" на странице 830. В отчет будут включены все журналы, необходимые для диагностики и устранения проблемы, которые затем будут отправлены в службу технической поддержки.

Как вариант, можно попытаться определить основную причину проблемы с помощью журналов, перечисленных в таблице ниже.

Папка журнала кластера

Сервис	Папка журнала	Описание
Метаданные	/vstorage/mds/logs/mds.log.zst на узле хранения, где размещен сервис MDS	События сервиса метаданных хранилища
Хранилище	/vstorage/<id>/cs/logs/cs.log.zst на узле хранения, где размещен сервис CS	События сервиса фрагментов

Сервис	Папка журнала	Описание
	Примечание Чтобы найти папку журнала для определенного CS на узле, выполните команду vstorage -c <cluster_ name> list-services -C.	
Точка подключения хранилища	/var/log/vstorage/<cluster_name>/vstorage-mount.*.blog на любом узле хранения	Программно определяемое хранилище, подключенное ко всем узлам
Сервер управления	/var/log/vstorage-ui-backend/messages.log и /var/log/vstorage-ui-backend/celery*.log на сервере управления	События сервера управления и панели администрирования
	/var/log/vstorage-ui-agent/* на любом узле хранения	События компонентов контроллера агента
Backup Gateway	/var/log/vstorage/abgw.log*zst на любом узле в кластере Backup Gateway **Примечание** Последний журнал имеет имя abgw.log.zst, старые журналы получают имена abgw.log.0.zst, abgw.log.1.zst и т. д.	Развертывание кластера Backup Gateway и управление им
iSCSI	/var/log/vstorage/iscsi/vstorage-target.log на любом узле в целевой группе iSCSI	Управление целевой группой iSCSI
	/var/log/vstorage/iscsi/vstorage-target-monitor.log на любом узле в целевой группе iSCSI	Мониторинг целевой группы iSCSI
	/var/log/vstorage/iscsi/scst.log.zst на любом узле в целевой группе iSCSI	Журналы сервиса SCST
S3	/var/log/ostor/NS-* на узле S3 с сервисами NS	События сервера имен S3
	/var/log/ostor/OS-* на узле S3 с сервисами OS	События сервера объектов S3
	/var/log/ostor/S3GW-* на узле S3 с сервисами GW	Событие шлюза S3
	/var/log/nginx/* на любом узле в кластере S3	Журналы сервиса nginx
	/var/log/ostor/GR-* на узле S3 с сервисами GR	События службы георепликатора S3
NFS	/var/log/ganesha/ganesha.log и /var/log/ostor/ostorfs.log.gz на любом узле кластера NFS	События сервера NFS
	/var/log/vstorage/vstorage-nfsd.log на любом узле в кластере NFS	События сервиса NFS

Сервис	Папка журнала	Описание
	/var/log/ostor/FS-* на узле, где размещен том NFS	События сервиса FS
	/var/log/ostor/OS-* на узле, где размещен том NFS	События сервиса OS
Вычисления	/var/log/vstorage-ui-backend/ansible.log на узле контроллера	Развертывание вычислительного кластера и дополнительных сервисов
	/var/log/hci/beholder/beholder.log на узле контроллера	Уведомления обо всех событиях, связанных с вычислениями, включая размещение ВМ
	/var/log/hci/nova/* на вычислительном узле, где размещена ВМ **Примечание** При возникновении проблем во время миграции ВМ проверьте журнал /var/log/hci/nova/nova-compute.log на исходном и целевом вычислительных узлах.	Управление виртуальной машиной
	/var/log/hci/neutron/neutron-l3-agent.log на любом вычислительном узле	События виртуальной маршрутизации
	/var/log/hci/neutron/neutron-openvswitch-agent.log на вычислительных узлах, где размещена ВМ	Управление сетевым интерфейсом ВМ
	/var/log/hci/cinder/* на узле контроллера	Управление вычислительными томами
	/var/log/hci/glance/glance-api.log на узле контроллера	Запросы API сервиса образов
	/var/log/hci/octavia/octavia-worker.log и /var/log/hci/octavia/octavia-api.log на узле контроллера	Управление сервисом балансировщика нагрузки
	/var/log/hci/magnum/magnum-conductor.log, /var/log/hci/magnum/magnum-api.log и /var/log/hci/heat/heat-engine.log на узле контроллера	Развертывание сервиса Kubernetes и стека ВМ и управление ими
	/var/log/hci/gnocchi/* и /var/log/hci/ceilometer/* на любом вычислительном узле	Управление сервисом учета и биллинга
Высокая доступность	/var/log/vstorage-ui-backend/ansible.log на всех узлах управления	Управление высокой доступностью
Обновления	/var/log/vstorage-ui-backend/software-updates.log на узле управления	Оркестрация обновлений ПО
	/var/log/vstorage-ui-agent/software-updates.log	Загрузка и установка

Сервис	Папка журнала	Описание
	на любом узле хранения	обновлений ПО для каждого узла

Чтобы открыть файлы журналов

Используйте следующие команды:

- для файлов LOG:

```
# less <log_file>.log
```

- для файлов BLOG:

```
# blogcat <log_file>.blog | less
```

- для файлов GZ:

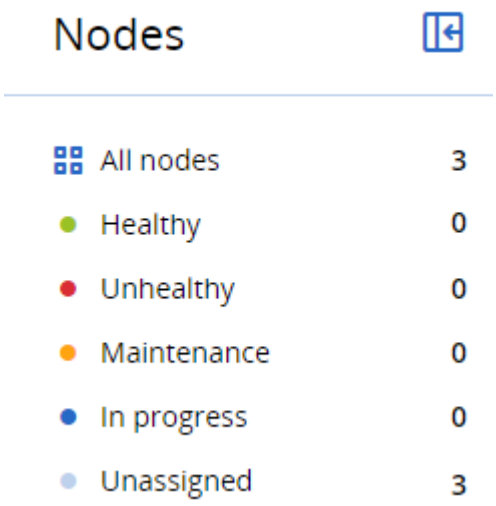
```
# zless <log_file>.gz
```

- для файлов ZST:

```
# zstdless <log_file>.zst
```

8.4 Мониторинг серверов инфраструктуры

Серверы, добавленные в инфраструктуру, перечислены на экране **Инфраструктура** > **Серверы**. Если кластер хранилища данных еще не создан, серверы будут отображаться только в списке **Не назначен**.



Сервер может иметь один из следующих статусов:

Исправен

Все сервисы хранилища на сервере работают.

Неисправен

На сервере произошел отказ одного или нескольких сервисов хранилища.

Обслуживание

Сервер находится в режиме обслуживания. Он не участвует в распределении новых фрагментов данных.

Выполняется

Сервер находится в состоянии развертывания, входит в режим обслуживания или выходит из него. В это время сервером нельзя управлять.

Не назначен

Сервер не назначен кластеру хранилища.

Чтобы просмотреть сведения о сервере

Панель администратора

На экране **Инфраструктура** > **Серверы** щелкните по строке нужного сервера. На вкладке **Обзор** на правой панели отображаются сведения о сервере, такие как идентификатор сервера и имя хоста, его статус и расположение, назначенные IP-адреса, установленные службы и количество дисков и сетевых интерфейсов.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node show <node>
```

<node>

Имя хоста или идентификатор сервера

Например, чтобы просмотреть сведения о сервере node003, выполните:

```
# vinfra node show node003
+--------------+--------------------------------------+
| Field        | Value                                |
+--------------+--------------------------------------+
| has_kvm      | True                                 |
| host         | node003.vstoragedomain               |
| id           | c4d14337-0863-4a67-9dbd-f19c3e49e114 |
| is_assigned  | True                                 |
| is_in_ha     | False                                |
| is_installing | False                               |
| is_online    | True                                 |
| is_primary   | False                                |
| is_virt      | False                                |
| maintenance  |                                      |
```

```
| orig_hostname | node003                          |
| roles         | cses:                            |
|               |   active: 4                      |
|               |   being_released: 0              |
|               | mdses:                           |
|               |   avail: 1                       |
|               |   being_released: 0              |
|               |   is_master: true                |
| tasks         |                                  |
+---------------+----------------------------------+
```

В выводе команды сведения включают в себя идентификатор сервера, имя хоста, количество и состояние служб хранилища. Также можно проверить, добавлен ли сервер в кластер хранилища, включен ли режим высокой доступности, находится ли сервер в рабочем состоянии или в режиме обслуживания.

8.4.1 Мониторинг производительности сервера

Чтобы проверить состояние сервера инфраструктуры

На экране **Инфраструктура** > **Серверы** щелкните по строке нужного сервера. На вкладке **Мониторинг** на правой панели отображается статистика производительности.

- **ЦП/ОЗУ**: загрузка ЦП в процентах по времени и использование ОЗУ в ГиБ по времени
- **Сеть**: показатели переданного (TX) и полученного (RX) трафика по времени
- **Операций чтения**: активность чтения на сервере по времени
- **Операций записи**: активность записи на сервере по времени
- **Физическое пространство**: текущее использование физического пространства в кластере

Интервал времени для диаграмм по умолчанию составляет двенадцать часов. Чтобы рассмотреть определенный интервал времени в большем масштабе, выделите его мышью; чтобы восстановить прежний масштаб, дважды щелкните по любой диаграмме.

Для получения дополнительных сведений мониторинга щелкните **Панель Grafana**.

8.4.2 Мониторинг дисков сервера

Ограничения

- Нельзя отслеживать производительность дисков с черепичной магнитной записью (SMR).

Для отслеживания производительности диска сервера

1. На экране **Инфраструктура** > **Серверы** щелкните по имени нужного сервера.
2. На вкладке **Диски** щелкните по диску сервера и ознакомьтесь с диаграммами на вкладке **Мониторинг**.

На диаграммах отображаются текущие показатели использования диска, средний показатель задержки и действия записи/чтения. Для получения дополнительных сведений щелкните **Панель Grafana**.

Интервал времени для диаграмм по умолчанию составляет двенадцать часов. Чтобы рассмотреть определенный интервал времени в большем масштабе, выделите его мышью; чтобы восстановить прежний масштаб, дважды щелкните по любой диаграмме.

Как просмотреть сведения о сервисах

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по имени нужного сервера.
2. На вкладке **Диски** щелкните по диску сервера и перейдите на вкладку **Сервис**.

Свойства сервиса различаются в зависимости от роли диска.

Свойства сервиса	Хранилище	Метаданные	Метаданные+Кэш	Кэш
Статус	Статус сервиса хранилища: **Активный** Сервис запущен и работает. **Медленный** Работа сервиса замедлена, что ведет к снижению производительности кластера. Диск изолирован от потока операций ввода-вывода кластера. **Неактивный** Сервис временно недоступен. Сервис хранилища помечается как неактивный в течение первых 5 минут неактивности. **Офлайн** Сервис неактивен более 5 минут. Когда сервис хранилища оказывается недоступен, кластер начинает репликацию данных, чтобы восстановить те фрагменты, которые хранились на затронутом диске хранилища.	Статус сервиса метаданных: **Доступен** Сервис находится в состоянии онлайн. **Синхронизация** Сервис выполняет синхронизацию метаданных кластера. **Недоступен** Сервис находится в состоянии офлайн.		–

Свойства сервиса	Хранилище	Метаданные	Метаданные+Кэш	Кэш
	Недостаточно места На диске, где работает сервис, заканчивается место. **Освобождается** Сервис находится в процессе высвобождения. **Отказ** Сервис запущен, но возникла проблема с диском хранилища. **Сбой освобождения** Не удалось высвободить сервис. **Обслуживание** Сервер, на котором размещен сервис, находится в режиме обслуживания. **Неизвестно** Состояние сервиса неизвестно.			
Systemd	Показывает состояние сервиса vstorage-csd.<cluster_name>.<CS_ID>.service	Показывает состояние сервиса vstorage-mdsd.<cluster_name>.<MDS_ID>.service		–
Уровень	Показывает назначенный уровень хранилища	–	Показывает кэшируемые уровни	
Идентификатор сервиса	Идентификатор сервиса хранилища	Идентификатор сервиса метаданных		–
Использование	Использование пространства на диске			
Кэширование	Включено/отключено	–	–	–
Расположение кэша	Показывает твердотельный накопитель, на который сохраняется кэш записи этого диска.	–	–	–

Свойства сервиса	Хранилище	Метаданные	Метаданные+Кэш	Кэш
	Примечание Отображается, если кэширование включено.			
Проверка контрольных сумм	Включено/отключено	–	–	–
Шифрование	Включено/отключено	–	–	–

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node disk show [--node <node>] <disk>
```

--node <node>

Идентификатор сервера или имя хоста

<disk>

Идентификатор или имя устройства диска (по умолчанию node001.vstoragedomain)

Например, чтобы просмотреть сведения о диске nvme0n1, подключенном к серверу node003, выполните:

```
# vinfra node disk show nvme0n1 --node node003
+------------------+-----------------------------------------------------------------------------------------+
| Field            | Value                                                                                   |
+------------------+-----------------------------------------------------------------------------------------+
| being_assigned   | False                                                                                   |
| being_released   | False                                                                                   |
| device           | nvme0n1                                                                                 |
| disk_status      | ok                                                                                      |
| encryption       |                                                                                         |
| form_factor      |                                                                                         |
| id               | B9F2C34F-19CF-4133-A3AF-A1440BE837AD                                                    |
| is_blink_available | False                                                                                 |
| is_blinking      | False                                                                                   |
| issues           | []                                                                                      |
| lun_id           |                                                                                         |
| model            | INTEL SSDPE2KX020T8                                                                     |
| node_id          | e40195d1-64b8-4117-85f3-00bb5d7a1db6                                                    |
| nvme             | True                                                                                    |
| physical_size    | 2000398934016                                                                           |
| protocol         | name: NVMe                                                                              |
|                  | speed: null                                                                             |
| role             | cs                                                                                      |
| rpm              |                                                                                         |
| serial_number    | PHLJ950101C02P0BGN                                                                      |
```

```
| service_id       | 1091                                              |
| service_params    | fail_messages: null                                        |
|                 | journal_data_size: 270532608                               |
|                 | journal_disk_id: B9F2C34F-19CF-4133-A3AF-A1440BE837AD                     |
|                 | journal_path: /vstorage/dc7aea32/journal/journal-cs-6aa56a11-70e6-4fd3-be4c-
bf7fcd65e5d6 |
|                 | journal_type: inner_cache                                  |
|                 | repo_dir: /vstorage/dc7aea32/cs                             |
|                 | systemd: active                                            |
|                 | tier: 0                                                   |
| service_status    | active                                                 |
| smart_status      | passed                                                 |
| space            | size: 1968848437248                                      |
|                 | used: 1540324716544                                      |
| tasks            |                                                       |
| temperature       | 36.0                                                   |
| type             | ssd                                                    |
| zoned            |                                                       |
+-------------------+-------------------------------------------------------------------------------------------+
```

В выводе команды свойства сервиса различаются в зависимости от роли диска.

<table>
<tr><th>Свойства сервиса</th><th>cs</th><th>mds</th><th>mds-journal</th><th>journal</th></tr>
<tr><td>service_id</td><td>Идентификатор сервиса хранилища</td><td colspan="2">Идентификатор сервиса метаданных</td><td>–</td></tr>
<tr><td>service_ params</td><td>journal_data_size
Объем данных в кэше для этого сервиса хранилища
journal_disk_id
Идентификатор диска кэша
journal_path
Путь к директории кэша записи
journal_type
Тип кэша, используемого для этого сервиса хранилища:
• no_cache
• inner_cache
• external_cache
repo_dir
Путь к репозиторию сервиса хранилища
systemd
Показывает состояние сервиса vstorage-csd.<cluster_name>.<CS_ID>.service</td><td colspan="2">repo_dir
Путь к репозиторию сервиса метаданных
systemd
Показывает состояние сервиса vstorage-mdsd.<cluster_ name>.<MDS_ ID>.service</td><td>–</td></tr>
</table>

Свойства сервиса	cs	mds	mds-journal	journal
	tier Показывает назначенный уровень хранилища			
service_status	Статус сервиса хранилища: active Сервис запущен и работает. ill Работа сервиса замедлена, что ведет к снижению производительности кластера. Диск изолирован от потока операций ввода-вывода кластера. inactive Сервис временно недоступен. Сервис хранилища помечается как неактивный в течение первых 5 минут неактивности. offline Сервис неактивен более 5 минут. Когда сервис хранилища оказывается недоступен, кластер начинает репликацию данных, чтобы восстановить те фрагменты, которые хранились на затронутом диске хранилища. no space На диске, где работает сервис, заканчивается место. releasing Сервис находится в процессе высвобождения. failed Сервис запущен, но возникла проблема с диском хранилища. failed rel Не удалось высвободить сервис. maintenance Сервер, на котором размещен сервис, находится в режиме обслуживания. unknown Состояние сервиса неизвестно.	Статус сервиса метаданных: avail Сервис находится в состоянии онлайн. stale Сервис выполняет синхронизацию метаданных кластера. unavail Сервис находится в состоянии офлайн.		–

Как просмотреть сведения о дисках

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по имени нужного сервера.
2. На вкладке **Диски** щелкните по диску сервера и перейдите на вкладку **Диск**.

Свойства диска включают имя накопителя, состояние, тип, физическую емкость, протокол диска, модель, серийный номер, статус S.M.A.R.T. и температуру. Диск может быть в следующих состояниях:

Исправен

Диск работает нормально.

Недоступен

Диск отключен от питания или сервера.

Отказ

Произошел отказ диска, или мониторинг S.M.A.R.T. сообщил об ошибке. Необходимо заменить диск.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node disk show [--node <node>] <disk>
```

--node <node>

Идентификатор сервера или имя хоста

<disk>

Идентификатор или имя устройства диска (по умолчанию node001.vstoragedomain)

Например, чтобы просмотреть сведения о диске nvme0n1, подключенном к серверу node003, выполните:

```
# vinfra node disk show nvme0n1 --node node003
+------------------+--------------------------------------------------------------------------------------------+
| Field            | Value                                                                                      |
+------------------+--------------------------------------------------------------------------------------------+
| being_assigned   | False                                                                                      |
| being_released   | False                                                                                      |
| device           | nvme0n1                                                                                    |
| disk_status      | ok                                                                                         |
| encryption       |                                                                                            |
| form_factor      |                                                                                            |
| id               | B9F2C34F-19CF-4133-A3AF-A1440BE837AD                                                       |
| is_blink_available | False                                                                                    |
| is_blinking      | False                                                                                      |
| issues           | []                                                                                         |
| lun_id           |                                                                                            |
| model            | INTEL SSDPE2KX020T8                                                                        |
| node_id          | e40195d1-64b8-4117-85f3-00bb5d7a1db6                                                       |
| nvme             | True                                                                                       |
```

```
| physical_size     | 2000398934016                                                                                  |
| protocol          | name: NVMe                                                                                     |
|                   | speed: null                                                                                    |
| role              | cs                                                                                             |
| rpm               |                                                                                                |
| serial_number     | PHLJ950101C02P0BGN                                                                             |
| service_id        | 1091                                                                                           |
| service_params    | fail_messages: null                                                                            |
|                   | journal_data_size: 270532608                                                                   |
|                   | journal_disk_id: B9F2C34F-19CF-4133-A3AF-A1440BE837AD                                          |
|                   | journal_path: /vstorage/dc7aea32/journal/journal-cs-6aa56a11-70e6-4fd3-be4c-
bf7fcd65e5d6 |
|                   | journal_type: inner_cache                                                                      |
|                   | repo_dir: /vstorage/dc7aea32/cs                                                                |
|                   | systemd: active                                                                                |
|                   | tier: 0                                                                                        |
| service_status    | active                                                                                         |
| smart_status      | passed                                                                                         |
| space             | size: 1968848437248                                                                            |
|                   | used: 1540324716544                                                                            |
| tasks             |                                                                                                |
| temperature       | 36.0                                                                                           |
| type              | ssd                                                                                            |
| zoned             |                                                                                                |
+-------------------+------------------------------------------------------------------------------------------------+
```

В выводе команды свойства диска включают имя накопителя, состояние, тип, физическую емкость, протокол диска, модель, серийный номер, статус S.M.A.R.T., температуру и т. д. Для дисков iSCSI также отображается LUN ID.

Как проверить диски хранилища с включенным кэшированием

1. На экране **Инфраструктура** > **Серверы** щелкните по имени нужного сервера.
2. На вкладке **Диски** щелкните по диску сервера с ролью **Кэш** и перейдите на вкладку **Кэш для дисков**.

На этой вкладке перечислены все диски хранилища, которые кэшируются на текущий диск.

Чтобы включить мигание светодиодного индикатора активности диска

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по имени нужного сервера.
2. На вкладке **Диски** выберите диск сервера.
3. На правой панели диска нажмите **Включить мигание**.

Чтобы остановить мигание индикатора диска, нажмите **Выключить мигание**.

Интерфейс командной строки

Используйте следующие команды:

- Чтобы включить мигание индикатора указанного диска:

  ```
  vinfra node disk blink on [--node <node>] <disk>
  ```

  --node <node>

  Идентификатор сервера или имя хоста

  <disk>

  Идентификатор или имя устройства диска (по умолчанию node001.vstoragedomain)

  Например, чтобы включить мигание индикатора диска sda сервера node005, выполните:

  ```
  # vinfra node disk blink on sda --node node005
  ```

- Чтобы остановить мигание индикатора указанного диска:

  ```
  vinfra node disk blink off [--node <node>] <disk>
  ```

  --node <node>

  Идентификатор сервера или имя хоста

  <disk>

  Идентификатор или имя устройства диска (по умолчанию node001.vstoragedomain)

  Например, чтобы остановить мигание индикатора диска sda сервера node005, выполните:

  ```
  # vinfra node disk blink off sda --node node005
  ```

8.4.2.1 Расчет состояния диска

Для мониторинга дисков сервера можно использовать службу vstorage-disks-monitor. Она запускается на всех серверах управления и запрашивает метрики сервера фрагментов (CS) у службы Prometheus для дальнейшего анализа. Команда vstorage-disks-monitor служит для выявления медленно работающих CS и помечает их как поврежденные (медленные). Чтобы предотвратить ухудшение производительности кластера, медленные CS исключаются из операций ввода-вывода кластера.

Служба также рассчитывает состояние диска в процентах с учетом веса каждой метрики. Вес метрик можно настроить в файле конфигурации /etc/disks-monitor/analyzers.yml. Журналы службы хранятся в файле /var/log/disks-monitor/disks-monitor.log.

Служба может работать в двух режимах:

- как демон при использовании команды vstorage-disks-monitor sidecar;
- как средство для отображения статусов диска или предупреждений при использовании команд vstorage-disks-monitor health и vstorage-disks-monitor alerts.

Можно отключить ограждение поврежденных CS с помощью команды vstorage-disks-monitor sidecar --fencing.enable.

Ограничения

- Отслеживание медленных дисков отключено для кластеров, развернутых на виртуальных машинах.

Анализаторы состояния диска

Ключевую роль в расчете состояния диска играют анализаторы. Каждый анализатор рассчитывает состояние диска с учетом собственных алгоритмов. Общее состояние диска представляет собой произведение значений, полученных от всех анализаторов.

Пример:

- Согласно атрибутам S.M.A.R.T., состояние диска – 0,9.
- Согласно данным анализатора медленного диска, состояние диска – 0,4.
- Согласно данным анализатора медленного CS, состояние диска – 0,5.
- Судя по показателю ошибок SCSI, состояние диска – 1.0.

Общее состояние диска рассчитывается следующим образом: 0,9*0,4*0,5*1. Равняется 0,18 или 18 %.

Атрибуты S.M.A.R.T.

Представленная ниже таблица содержит атрибуты S.M.A.R.T., которые влияют на показатели состояния диска.

Код	Атрибут S.M.A.R.T.	Вес[1]	Ограничение[2], в процентах
05	Reallocated Sector Count (Количество переназначенных секторов)	2	70
187	Reported Uncorrectable Errors (Сообщенные неисправимые ошибки)	1	70
188	Command Timeout (Время ожидания команды)	1	20
197	Current Pending Sector Count (Текущее количество ожидающих секторов)	2	70
198	Offline uncorrectable Sectors Count (Текущее количество неактивных секторов без возможности исправления)	2	70

---

[1]Определяет, на сколько процентов значение атрибута снижает общий показатель состояния диска.

[2]Определяет максимальное влияние, которое атрибут имеет на общий показатель состояния диска.

Код	Атрибут S.M.A.R.T.	Вес[1]	Ограничение[2], в процентах
233	Media Wearout Indicator (Индикатор износа носителя)	1	100

Показатель состояния диска рассчитывается по следующей формуле:

```
Disk health (%) = K * П (100% - D)
```

где:

- K – коэффициент уменьшения. Состояние диска считается менее исправным, если имеются сообщения о нескольких типах ошибок S.M.A.R.T. Формула коэффициента имеет следующий вид: 0.8^({количество атрибутов S.M.A.R.T. с ошибкой} - 1). Возможные значения: 0-1.
- П – произведение минимальных расчетных значений для каждого атрибута S.M.A.R.T.
- 100 % – исходное состояние диска.
- D – минимальное значение, получаемое в результате умножения предельного значения, значения атрибута и веса. Формула расчета: (min(limit, attribute_value * weight)).
- limit – предельное значение каждого критически важного атрибута S.M.A.R.T.
- attribute_value – текущее значение атрибута.
- weight – вес каждого критически важного атрибута S.M.A.R.T.

Пример:

- Количество перераспределенных секторов: значение атрибута = 30, вес = 2, предел = 70
- Время ожидания команды: значение атрибута = 23, вес = 1, предел = 20
- K = 0,8 * (2-1) = 0,8

Показатель состояния диска S.M.A.R.T. рассчитывается следующим образом: 0,8 * (100 % - (мин. (30*2, 70))) * (100 % - мин.(23*1, 20)) = 0,8 * 0,4 * 0,8 = 0,256 (26 %).

Анализаторы медленных дисков и CS

Анализаторы медленных дисков и CS служат для расчета состояния диска с учетом средней задержки при выполнении операций ввода-вывода с течением времени (15 минут).

Представленная ниже таблица содержит пороговые значения по умолчанию.

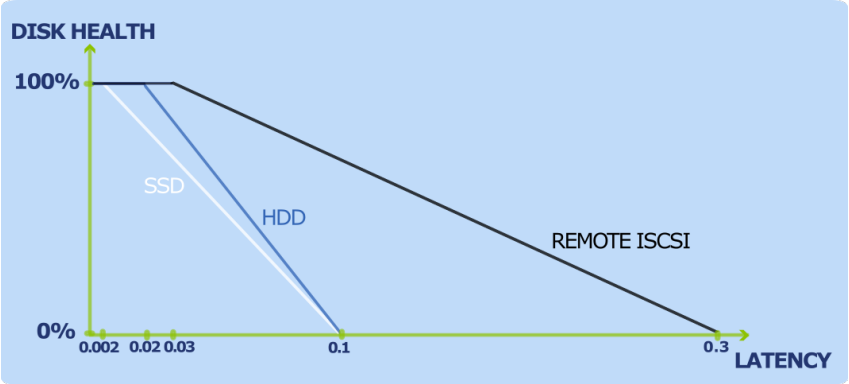
---

[1]Определяет, на сколько процентов значение атрибута снижает общий показатель состояния диска.

[2]Определяет максимальное влияние, которое атрибут имеет на общий показатель состояния диска.

Анализатор	OK latency (Нормальная задержка)[1], в секундах	FATAL latency (Критическая задержка)[2], в секундах
Медленный CS	0,03	0,3
Медленный диск HDD	0,02	0,1
Медленный диск SSD	0,002	0,1

Если показатель задержки диска меньше **OK latency**, состояние диска оценивается как 100 %. Если показатель задержки диска превышает **FATAL latency**, состояние диска оценивается как 0 %. Показатель задержки диска может линейно варьироваться между этими двумя пороговыми значениями от 100 до 0 %.



Когда показатель состояния диска снижается до 0 %, служба создает оповещение и помечает CS как поврежденный. Для такого CS больше не запускается автоматическая репликация, и он больше не доступен для распределения фрагментов данных.

Ошибки SCSI

По умолчанию каждый сбой SCSI снижает показатель состояния диска на 4 %. Максимальный показатель воздействия составляет 70.

Метрики дисков в Prometheus

Сервис Prometheus хранит следующие метрики дисков:

Метрики CS	
csd_io_op_time_seconds	Среднее время на запрос ввода-вывода
master:mdsd_	Статус CS в главном MDS

[1]Максимальное значение задержки для состояния диска 100 %.
[2]Значение задержки для состояния диска 0 %.

cs_status	
Метрики диска из /proc/diskstats	
node_disk_read_time_seconds	Общее время в секундах, затраченное на запросы чтения
node_disk_reads_completed	Общее количество завершенных запросов на чтение
node_disk_write_time_seconds	Общее время в секундах, затраченное на запросы на запись
node_disk_writes_completed	Общее количество завершенных запросов на запись
Метрики S.M.A.R.T.	
smart_device_smart_healthy	Показывает, работоспособен ли диск согласно данным S.M.A.R.T.
smart_reallocated_sector_ct	Общее количество переназначенных секторов (05)
smart_reported_uncorrect	Общее количество ошибок, которые нельзя исправить средствами ECC (187)
smart_command_timeout	Общее количество операций, отмененных из-за превышения времени ожидания (188)
smart_current_pending_sector	Общее количество нестабильных секторов (197)
smart_offline_uncorrectable	Общее количество неисправляемых ошибок при чтении/записи сектора (198)
smart_media_wearout_indicator	Индикатор износа диска SSD (233)
smart_nvme_intel_wear_leveling	Индикатор износа диска Intel NVME (233)
smart_scsi_read_errors_uncorrected	Общее количество неисправляемых ошибок при чтении сектора
smart_scsi_reallocated_sector_ct	Общее количество переназначенных секторов диска

smart_scsi_ verify_errors_ uncorrected	Общее количество неисправляемых ошибок при проверке сектора
smart_scsi_ write_errors_ uncorrected	Общее количество неисправляемых ошибок при записи сектора
Ошибки SCSI согласно данным ядра ОС	
kernel_scsi_ failures_total	Общее количество сбоев SCSI согласно полученным от ядра ОС данным
Метрики состояния диска от vstorage-disks-monitor	
diskmon_cs_ disk_health	Состояние диска согласно данным, полученным от службы vstorage-disks-monitor. Возможные значения – 0.0-1.0. Значение 1.0 означает, что диск полностью работоспособен.

8.4.2.2 Устранение неполадок дисков сервера

Статус S.M.A.R.T. всех дисков отслеживается инструментом smartctl, который устанавливается вместе с продуктом Кибер Инфраструктура. Запускаемый каждые 10 минут инструмент опрашивает все диски, присоединенные к серверам, включая твердотельные накопители журналирования и системные диски, и передает результаты на сервер управления. Инструмент проверяет состояние диска с учетом атрибутов S.M.A.R.T. Если диск близок к отказу, отображается оповещение. Состояние на грани отказа означает, что как минимум один из следующих атрибутов S.M.A.R.T. отличается от нуля:

- Reallocated Sector Count (Количество перераспределенных секторов)
- Reallocated Event Count (Количество событий перераспределения)
- Current Pending Sector Count (Текущее количество ожидающих секторов)
- Uncorrectable Sector Count (Количество не подлежащих исправлению секторов)

Анализаторы медленных дисков и CS служат для расчета состояния диска с учетом средней задержки при выполнении операций ввода-вывода с течением времени. Когда показатель задержки достигает установленного порога, считается, что состояние диска равно 0 %. В этом случае создается предупреждение и диск помечается как медленный.

Ограничения

- Чтобы инструмент работал, функциональность S.M.A.R.T. должна быть включена в параметрах BIOS сервера.

Предварительные требования

- Четкое понимание процедуры расчета состояния диска, описанной в разделе "Расчет состояния диска" на странице 696.

Как выполнить диагностику медленно работающего диска

1. Перейдите на экран **Инфраструктура** > **Серверы** и щелкните по имени сервера, на котором размещен медленный диск хранилища.
2. На вкладке **Диски** щелкните по этому диску хранилища и перейдите на вкладку **Сервис**, чтобы просмотреть предупреждающее сообщение.
3. Проверьте подключение диска, статус S.M.A.R.T. и выходные данные dmesg для этого сервера.

Исправив проблему, нажмите **Пометить как исправный**, чтобы изменить статус диска на **Исправен**. Если устранить проблему не удалось, рекомендуется заменить диск до его отказа. Если восстановить такой диск, он может снизить производительность кластера и увеличить задержку ввода-вывода.

Как выполнить диагностику отказавшего диска

Панель администратора

1. Перейдите на экран **Инфраструктура** > **Серверы** и щелкните по имени сервера, на котором размещен отказавший сервис.
2. На вкладке **Диски** щелкните по отказавшему диску и перейдите на вкладку **Сервис**, чтобы просмотреть сообщение об ошибке.
3. Нажмите **Получить диагностическую информацию**, чтобы проверить выходные данные smartctl и dmesg.
4. Если для ошибки сервиса есть соответствующая статья базы знаний, нажмите **Перейти в базу знаний**, чтобы узнать подробные сведения о проблеме.

Если не удается исправить проблему, обратитесь в службу технической поддержки, как описано в разделе "Получение технической поддержки" на странице 830.

Интерфейс командной строки

1. Узнайте имя устройства отказавшего диска сервера из вывода команды vinfra node disk list:

```
# vinfra node disk list --node node003
+-------------+---------+------+--------+-------------+----------+----------+---------------+------------+-------------
--+
| id          | device  | type | role   | disk_status | used     | size     | physical_size | service_id | service_
status |
+-------------+---------+------+--------+-------------+----------+----------+---------------+------------+-------------
--+
| 36972905<…> | nvme1n1 | ssd  | cs     | ok          | 1.5TiB   | 1.8TiB   | 1.8TiB        | 1090       | failed
   |
| B9F2C34F<…> | nvme0n1 | ssd  | cs     | ok          | 1.5TiB   | 1.8TiB   | 1.8TiB        | 1091       | active
     |
| A8E05CCA<…> | nvme2n1 | ssd  | cs     | ok          | 1.5TiB   | 1.8TiB   | 1.8TiB        | 1086       | active
     |
| D6E421E0<…> | nvme3n1 | ssd  | cs     | ok          | 1.5TiB   | 1.8TiB   | 1.8TiB        | 1087       | active
     |
| md126       | md126   | ssd  | system | ok          | 364.2MiB | 989.9MiB | 1022.0MiB     |            |
|
| md127       | md127   | ssd  | system | ok          | 104.4GiB | 187.1GiB | 190.2GiB      |            |            |
```

```
+-------------+---------+------+--------+-------------+----------+----------+---------------+------------+-------------
--+
```

Диск nvme1n1 сервера node003 отмечен как отказавший.

2. Проверьте выходные данные smartctl и dmesg для отказавшего диска. Например:

```
# vinfra node disk show diagnostic-info --node node003 nvme1n1 -f yaml
- command: smartctl --all /dev/nvme1n1
  stdout: 'smartctl 7.1 2020-06-20 r5066 [x86_64-linux-3.10.0-1160.41.1.vz7.183.5]
    (local build)
  Copyright (C) 2002-19, Bruce Allen, Christian Franke, www.smartmontools.org

  === START OF INFORMATION SECTION ===
  Model Number:                       INTEL SSDPE2KX020T8
  Serial Number:                      PHLJ9500032H2P0BGN
  Firmware Version:                   VDV10131
  PCI Vendor/Subsystem ID:            0x8086
  IEEE OUI Identifier:                0x5cd2e4
  Total NVM Capacity:                 2,000,398,934,016 [2.00 TB]
  Unallocated NVM Capacity:           0
  Controller ID:                      0
  Number of Namespaces:               1
  Namespace 1 Size/Capacity:          2,000,398,934,016 [2.00 TB]
  Namespace 1 Formatted LBA Size:     512
  Namespace 1 IEEE EUI-64:            5cd2e4 75b0070100
  Local Time is:                      Fri Nov 26 13:32:44 2021 EET
  Firmware Updates (0x02):            1 Slot
  Optional Admin Commands (0x000e):   Format Frmw_DL NS_Mngmt
  Optional NVM Commands (0x0006):     Wr_Unc DS_Mngmt
  Maximum Data Transfer Size:         32 Pages
  Warning  Comp. Temp. Threshold:     70 Celsius
  Critical Comp. Temp. Threshold:     80 Celsius

  Supported Power States
  St Op     Max   Active     Idle   RL RT WL WT  Ent_Lat  Ex_Lat
   0 +   25.00W      -        -   0  0  0  0       0       0

  Supported LBA Sizes (NSID 0x1)
  Id Fmt  Data  Metadt  Rel_Perf
   0 +     512      0       2
   1 -    4096      0       0

  === START OF SMART DATA SECTION ===
  SMART overall-health self-assessment test result: PASSED

  SMART/Health Information (NVMe Log 0x02)
  Critical Warning:                   0x00
  Temperature:                        34 Celsius
  Available Spare:                    99%
  Available Spare Threshold:          10%
  Percentage Used:                    5%
```

```
  Data Units Read:                    550,835,698 [282 TB]
  Data Units Written:                 720,479,182 [368 TB]
  Host Read Commands:                 10,050,305,459
  Host Write Commands:                20,760,365,218
  Controller Busy Time:               1,968
  Power Cycles:                       20
  Power On Hours:                     13,405
  Unsafe Shutdowns:                   16
  Media and Data Integrity Errors:    0
  Error Information Log Entries:      0
  Warning  Comp. Temperature Time:    0
  Critical Comp. Temperature Time:    0

  Error Information (NVMe Log 0x01, max 64 entries)
  No Errors Logged
  '
- command: dmesg --ctime --kernel --level=emerg,alert,crit,err,warn --facility=kern
    | grep 'nvme1n1'
  stdout: ''
```

Если не удается исправить проблему, обратитесь в службу технической поддержки, как описано в разделе "Получение технической поддержки" на странице 830.

8.4.3 Мониторинг сетевых интерфейсов сервера

Чтобы проверить статус сетевого интерфейса

Перейдите на экран **Инфраструктура** > **Серверы** и щелкните по имени сервера. На вкладке **Сетевые интерфейсы** будет показан список всех сетевых интерфейсов на сервере с указанием их статусов.

Сетевой интерфейс может иметь один из следующих статусов:

Подключен

Сетевой адаптер подключен к серверу и включен.

Отключен

Сетевой адаптер отключен.

Выключен

Сетевой адаптер отключен от сервера.

Предупреждения

Сетевой адаптер находится не в полнодуплексном режиме, медленно работает или неправильно настроен.

Для отображения сведений о сетевом интерфейсе

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по имени нужного сервера.
2. На вкладке **Сетевые интерфейсы** щелкните по сетевому интерфейсу и перейдите на вкладку **Обзор**.

Информация о сетевом интерфейсе включает следующие сведения: состояние интерфейса, его тип, назначенную сеть, MTU, MAC-адрес и IP-адреса. Также указана скорость передачи (TX) и получения (RX) в пакетах в секунду.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node iface show [--node <node>] <iface>
```

--node <node>

Идентификатор или имя хоста сервера (по умолчанию node001.vstoragedomain)

<iface>

Имя сетевого интерфейса

Например, чтобы посмотреть подробные сведения о сетевом интерфейсе bond0.362 сервера node003, выполните:

```
# vinfra node iface show bond0.362 --node node003
+----------------------+--------------------------------------+
| Field                | Value                                |
+----------------------+--------------------------------------+
| built_on             | bond0                                |
| dhcp4                |                                      |
| dhcp4_enabled        | False                                |
| dhcp6                |                                      |
| dhcp6_enabled        | False                                |
| duplex               | full                                 |
| gw4                  |                                      |
| gw6                  |                                      |
| ignore_auto_routes_v4 | True                                |
| ignore_auto_routes_v6 | True                                |
| ipv4                 | - 192.168.0.15/24                    |
| ipv6                 | []                                   |
| mac_addr             | 0c:42:a1:0d:f4:ac                    |
| mtu                  | 9000                                 |
| multicast            | True                                 |
| name                 | bond0.362                            |
| network              | e4347c48-2a93-4495-9221-0036d4b7fd2c |
| node_id              | c4d14337-0863-4a67-9dbd-f19c3e49e114 |
| plugged              | True                                 |
| rx_bytes             | 132795090298899                      |
| rx_dropped           | 0                                    |
| rx_errors            | 0                                    |
| rx_overruns          | 0                                    |
| rx_packets           | 11992910723                          |
```

```
| speeds              | current: 50000                  |
|                   | max: 50000                        |
| state               | up                              |
| tag                 | 362                             |
| tx_bytes            | 97570120705648                  |
| tx_dropped          | 0                               |
| tx_errors           | 0                               |
| tx_overruns         | 0                               |
| tx_packets          | 10744028252                     |
| type                | vlan                            |
+---------------------+---------------------------------+
```

Информация о сетевом интерфейсе включает следующие сведения: состояние интерфейса, его тип, назначенную сеть, MTU, MAC-адрес и IP-адреса. Также указана скорость передачи (TX) и получения (RX) в пакетах в секунду.

Чтобы проверить производительность сетевого интерфейса

1. На экране **Инфраструктура** > **Серверы** щелкните по имени нужного сервера.
2. На вкладке **Сетевые интерфейсы** щелкните по сетевому интерфейсу и ознакомьтесь с диаграммами на вкладке **Мониторинг**.

Отслеживая производительность сети, помните, что, если диаграммы **Ошибки** не пусты, в сети имеют место неполадки и требуется вмешательство. Для получения дополнительных сведений мониторинга щелкните **Панель Grafana**.

Интервал времени для диаграмм по умолчанию составляет двенадцать часов. Чтобы рассмотреть определенный интервал времени в большем масштабе, выделите его мышью; чтобы восстановить прежний масштаб, дважды щелкните по любой диаграмме.

8.5 Мониторинг кластера хранилища данных

Чтобы просмотреть статус кластера хранилища

Панель администратора

Щелкните по имени кластера в нижней части левого меню. Статус может иметь следующие значения:

Исправен

Все компоненты кластера активны и нормально работают.

Недоступен

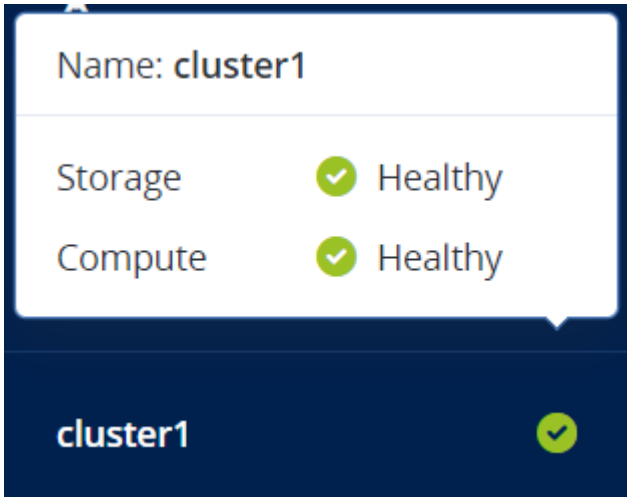
Недостаточно информации о состоянии кластера (например, из-за отсутствия доступа к кластеру).

Деградировал

Некоторые из компонентов кластера неактивны или недоступны. Кластер пытается исправить свое состояние, репликация данных запланирована или выполняется.

Ошибка

В кластере слишком много неактивных сервисов, и автоматическая репликация отключена. Если кластер окажется в этом состоянии, устраните неполадки на серверах или обратитесь в службу поддержки.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster overview
```

Например, чтобы просмотреть статус кластера cluster1, взгляните на эту строку в выводе команды:

```
+------------------+------------------------+
| Field            | Value                  |
+------------------+------------------------+
| ...              | ...                    |
| status           | healthy                |
| ...              | ...                    |
+------------------+------------------------+
```

Чтобы просмотреть статистику кластера хранилища

Панель администратора

Перейдите на экран **Мониторинг** > **Обзор**.

- Чтобы просмотреть статистику кластера хранилища во весь экран, нажмите **Полноэкранный режим**.
- Для выхода из полноэкранного режима нажмите клавишу **Esc** или кнопку **Выйти из полноэкранного режима**.

Интервал времени для диаграмм по умолчанию составляет двенадцать часов. Чтобы рассмотреть определенный интервал времени в большем масштабе, выделите его мышью; чтобы восстановить прежний масштаб, дважды щелкните по любой диаграмме.

Интерфейс командной строки

Используйте следующую команду:

```
vstorage -c <cluster_name> top
```

Например, чтобы просмотреть общую информацию о кластере cluster1, взгляните на эту секцию в выводе команды:

```
Cluster 'cluster1': healthy
Space: [OK] allocatable 11.9TB of 57.3TB, free 13.0TB of 57.3TB
MDS nodes: 3 of 3, epoch uptime: 13d  3h
CS nodes:  32 of 32 (32 avail, 0 inactive, 0 offline)
License: ACTIVE (expiration: 01/01/2100, capacity: 500TB, used: 21.2TB)
Replication:  1 norm,  1 limit
IO:      read 26.2MB/s (1.9Kop/s), write  426MB/s (11Kops/s)
```

Cluster

Общее состояние кластера:

healthy

Все серверы фрагментов данных в этом кластере активны.

unknown

Недостаточно информации о состоянии этого кластера (например, потому, что главный сервер метаданных был выбран только некоторое время назад).

degraded

Часть серверов фрагментов данных в кластере неактивна.

failure

В кластере слишком много неактивных серверов фрагментов данных; автоматическая репликация отключена.

SMART warning

У одного или нескольких физических дисков, подключенных к серверам кластера, близится аппаратный отказ.

Space

Количество дискового пространства в кластере:

free

Свободное дисковое пространство в кластере.

allocatable

Объем логического дискового пространства, доступного для клиентов. Доступное для выделения дисковое пространство рассчитывается на основе текущих параметров репликации и объема свободного дискового пространства на серверах фрагментов данных. Он также может ограничиваться лицензией.

MDS nodes

Количество активных серверов метаданных по сравнению с общим числом серверов метаданных, настроенных для кластера.

epoch uptime

Время, прошедшее с момента выбора главного сервера метаданных.

CS nodes

Количество активных серверов фрагментов данных по сравнению с общим числом серверов фрагментов данных, настроенных для кластера. В скобках отображается дополнительная информация об этих серверах фрагментов данных.

avail

Активные серверы фрагментов данных, которые в настоящее время запущены и работают в кластере.

inactive

Неактивные серверы фрагментов данных, которые в настоящее время недоступны. Сервер фрагментов данных помечается как неактивный в течение первых 5 минут его неактивности.

offline

Отключенные серверы фрагментов данных, которые были неактивны в течение более 5 минут. Сервер фрагментов данных меняет свое состояние на отключенный, если он неактивен больше 5 минут. После изменения состояния сервера на отключенный кластер начинает репликацию данных, чтобы восстановить фрагменты, которые хранились на отключенном сервере фрагментов данных.

License

Номер ключа, под которым лицензия зарегистрирована на сервере аутентификации с ключом, и состояние лицензии.

Replication

Параметры репликации. Нормальное количество реплик фрагментов и предельное число, ниже которого фрагмент блокируется до момента, когда он будет восстановлен.

IO

Активность дискового ввода-вывода в кластере:

- Скорость операций ввода-вывода при чтении и записи в байтах в секунду.
- Количество операций ввода-вывода (чтения и записи) в секунду.

Чтобы просмотреть дополнительные сведения о кластере хранилища

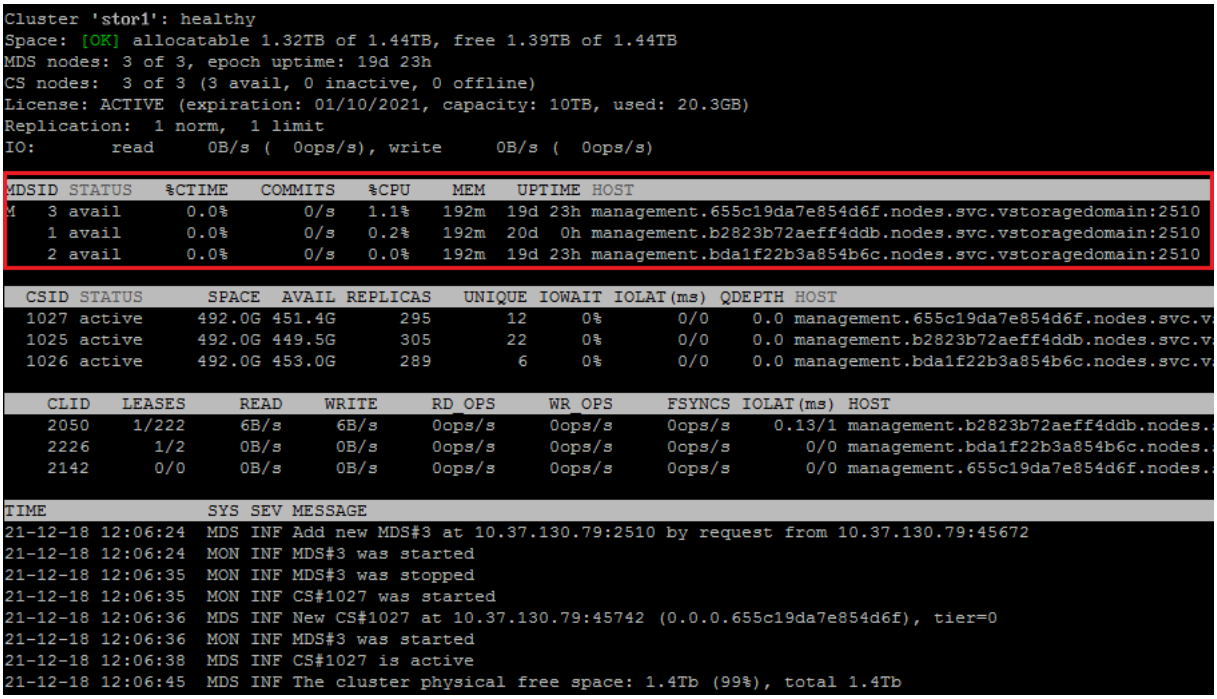
Перейдите на экран **Мониторинг** > **Обзор** и щелкните **Панель Grafana**.

Откроется отдельная вкладка браузера с предварительно настроенными панелями Grafana, где можно управлять существующими панелями мониторинга, создавать новые, предоставлять доступ к ним другим пользователям, настраивать оповещения и т. д. На панелях используется источник

данных Prometheus, метрики которого хранятся в течение семи дней. Если вы хотите увеличить срок хранения, его можно настроить вручную. Дополнительные сведения см. в документации Grafana.

8.5.1 Мониторинг серверов метаданных

Серверы метаданных (MDS) являются критически важным компонентом любого кластера хранения данных, поэтому контроль состояния и работоспособности серверов метаданных – это крайне важная задача. Для мониторинга серверов метаданных используйте команду vstorage -c <cluster_name> top, например:



Приведенная выше команда выводит подробную информацию о кластере stor1. Параметры мониторинга для серверов метаданных (выделены красным) следующие:

MDSID

: Идентификатор сервера метаданных.

  Если перед идентификатором добавлена буква M, она указывает, что этот сервер является главным (master) сервером метаданных.

STATUS

: Статус сервера метаданных.

%CTIME

: Суммарное время, в течение которого сервер метаданных осуществлял запись в локальный журнал.

COMMITS

: Интенсивность фиксаций в локальный журнал.

%CPU

Время активности сервера метаданных.

MEM

Объем физической памяти, используемой сервером метаданных.

UPTIME

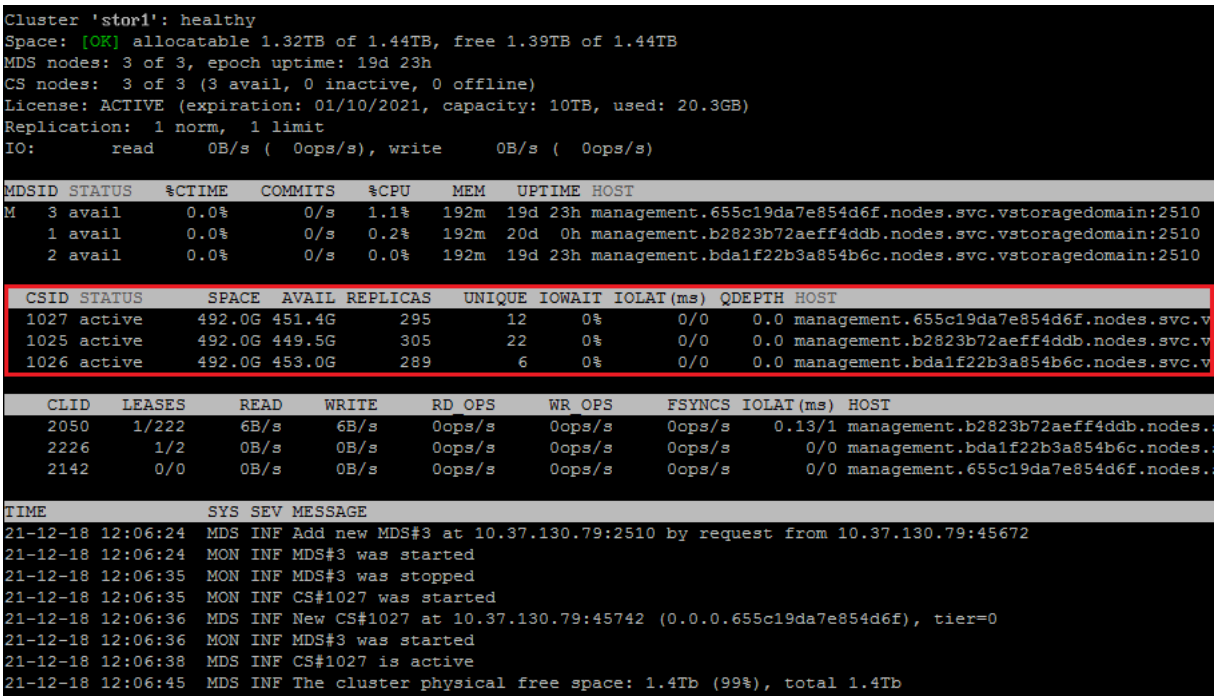
Время, прошедшее с момента последнего запуска сервера метаданных.

HOST

Имя хоста или IP-адрес сервера метаданных.

8.5.2 Мониторинг серверов фрагментов данных

Отслеживая серверы фрагментов данных (CS), можно контролировать объем доступного в кластере хранения данных пространства. Для отслеживания серверов фрагментов данных используйте команду vstorage -c <cluster_name> top, например:



Приведенная выше команда выводит подробную информацию о кластере stor1. Параметры мониторинга для серверов фрагментов данных (выделены красным) следующие:

CSID

Идентификатор сервера фрагментов данных.

STATUS

Статус сервера фрагментов данных.

active

Сервер фрагментов данных запущен и работает.

failed

Процесс сервера фрагментов данных запущен, но возникла проблема с его диском.

inactive

Сервер фрагментов данных временно недоступен. Сервер фрагментов данных помечается как неактивный (inactive) в течение первых 5 минут неактивности.

offline

Сервер фрагментов данных неактивен в течение более чем 5 минут. Когда сервер фрагментов данных оказывается недоступен (offline), кластер начинает репликацию данных, чтобы восстановить те фрагменты, которые хранились на затронутом сервере фрагментов данных.

dropped

Сервер фрагментов данных удален администратором.

maintenance

Производится обслуживание сервера, на котором размещен сервер фрагментов данных.

ill

Работа сервера фрагментов замедлена, что ведет к снижению производительности кластера. Сервер фрагментов изолирован от потока операций ввода-вывода кластера.

SPACE

Общий объем дискового пространства на сервере фрагментов данных.

AVAIL

Объем доступного дискового пространства на сервере фрагментов данных.

REPLICAS

Количество реплик, сохраненных на сервере фрагментов данных.

UNIQUE

Количество фрагментов, у которых нет реплик.

IOWAIT

Процент времени, затраченный на ожидание выполнения операций ввода-вывода.

IOLAT

Среднее/максимальное время в миллисекундах, которое требовалось клиенту для выполнения одной операции ввода-вывода за последние 20 секунд.

QDEPTH

Средняя глубина очереди ввода-вывода на сервере фрагментов данных.

HOST

Имя хоста или IP-адрес сервера фрагментов данных.

FLAGS

Для активных серверов фрагментов данных могут отображаться следующие флаги:

J

Сервер фрагментов данных использует журнал записи.

C

На сервере фрагментов данных включено вычисление контрольной суммы. Расчет контрольных сумм позволяет вам получать уведомление, если третья сторона изменит данные на диске.

D

Прямой ввод-вывод – нормальное состояние сервера фрагментов данных без журнала записи.

c

Журнал записи сервера фрагментов данных пуст: нет никаких данных, ожидающих фиксации с твердотельного накопителя журналирования записи на жесткий диск в месте расположения сервера фрагментов данных.

8.5.2.1 Общие сведения об использовании дискового пространства

Обычно сведения о том, как используется дисковое пространство в вашем кластере, можно получить с помощью команды vstorage top. Эта команда выдает следующую информацию о дисках: общий объем, свободный объем и подлежащий выделению объем, например:

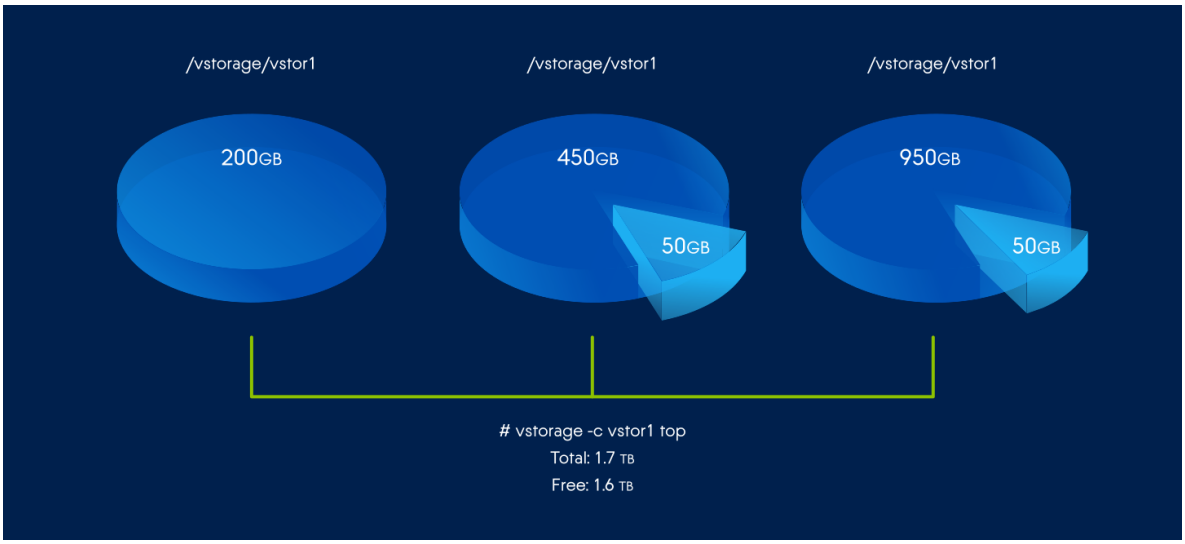
```
# vstorage -c stor1 top
connected to MDS#1
Cluster 'stor1': healthy
Space: [OK] allocatable 180GB of 200GB, free 1.6TB of 1.7TB
<...>
```

В выходных данных этой команды:

- 1,7TB – это общий объем дисков в кластере stor1. Общий объем дисков рассчитывается на основе всего используемого и свободного пространства на всех разделах в кластере. Используемое дисковое пространство включает пространство, занятое всеми фрагментами данных и их репликами, а также пространство, занятое любыми другими файлами, которые хранятся на разделах кластера.

  Допустим, что имеется раздел объемом в 100 ГБ и 20 ГБ на этом разделе занято теми или иными файлами. В случае если настроить на этом разделе сервер фрагментов данных, к кластеру будет добавлено 100 ГБ общего дискового пространства, хотя лишь 80 ГБ из этого пространства будет свободно и доступно для сохранения фрагментов данных.
- 1,6TB – это свободное дисковое пространство в кластере stor1. Свободное дисковое пространство рассчитывается посредством вычета объема дискового пространства, занятого фрагментами данных и любыми другими файлами на разделах кластера, из объема общего дискового пространства.

Например, если объем свободного пространства составляет 1,6 ТБ, а общий объем дискового пространства равен 1,7 ТБ, это означает, что около 100 ГБ на разделах кластера уже занято теми или иными файлами.



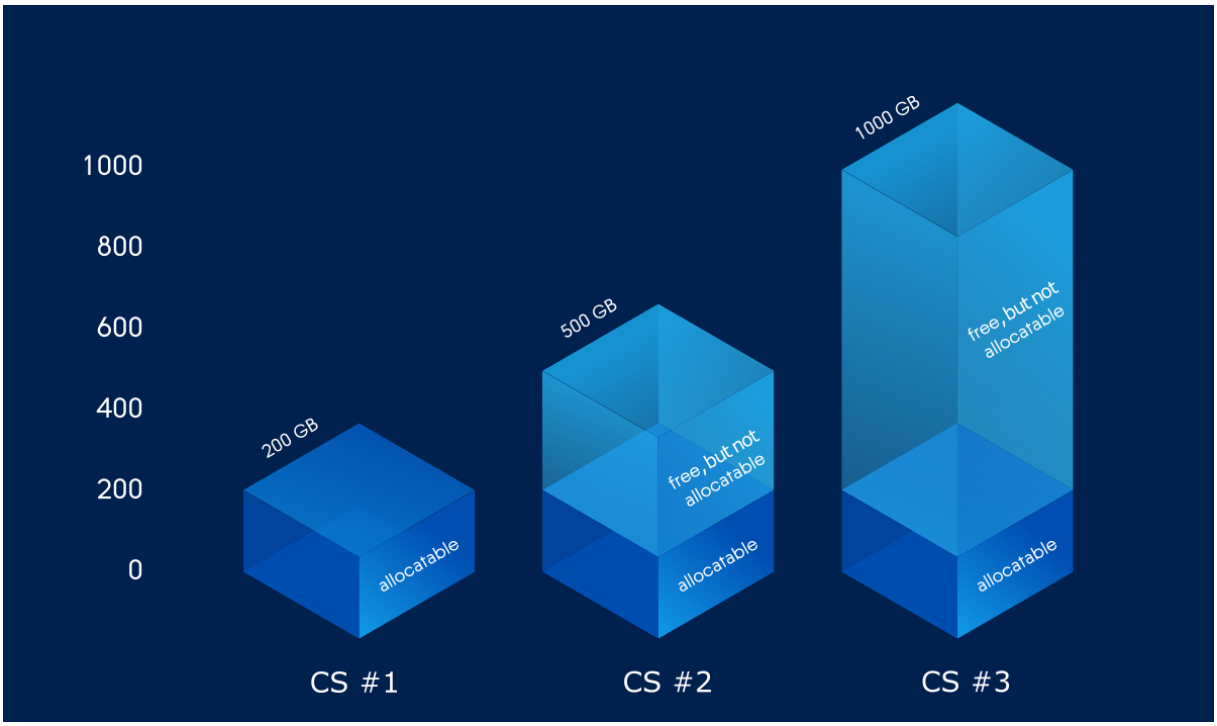
- allocatable 180GB of 200GB (подлежат выделению 180 ГБ из 200 ГБ) – это объем свободного дискового пространства, который может использоваться для сохранения фрагментов данных. Более подробные данные см. в разделе "Общие сведения о распределяемом дисковом пространстве" ниже.

Общие сведения о распределяемом дисковом пространстве

Контролируя данные о дисковом пространстве в кластере, следует также обращать внимание на пространство, о котором утилита vstorage top сообщает как о подлежащем выделению (*allocatable*). Подлежащее выделению пространство – это объем дискового пространства, которое свободно и может использоваться для сохранения пользовательских данных. Когда это пространство закончится, записывать в кластер данные станет невозможно.

Расчет подлежащего выделению дискового пространства показан в следующем примере.

- Кластер содержит три сервера фрагментов данных. На первом сервере имеется 200 ГБ дискового пространства, на втором – 500 ГБ, а на третьем – 1 ТБ.
- В кластере используется коэффициент репликации по умолчанию 3, а это означает, что у каждого фрагмента данных должно быть три реплики, которые должны храниться на трех различных серверах фрагментов данных.



В этом примере доступное дисковое пространство составляет 200 ГБ, то есть равно объему дискового пространства наименьшего из серверов фрагментов данных.

```
# vstorage -c stor1 top
connected to MDS#1
Cluster 'stor1': healthy
Space: [OK] allocatable 180GB of 200GB, free 1.6TB of 1.7TB
<...>
```

В этой конфигурации кластера одна реплика каждого из фрагментов данных должна сохраняться на каждом из серверов. Таким образом, когда доступное дисковое пространство на наименьшем сервере фрагментов данных (200 ГБ) исчерпается, в кластере нельзя будет создавать новые фрагменты, пока в кластер не будет добавлен новый сервер фрагментов данных или не будет уменьшен коэффициент репликации.

Если изменить коэффициент репликации на 2, то команда vstorage top сообщит о доступном дисковом пространстве в 700 ГБ.

```
# vstorage set-attr -R /mnt/vstorage replicas=2:1
# vstorage -c stor1 top
connected to MDS#1
Cluster 'stor1': healthy
Space: [OK] allocatable 680GB of 700GB, free 1.6TB of 1.7TB
<...>
```

Доступное дисковое пространство увеличилось, поскольку теперь для каждого фрагмента данных создаются только две реплики и можно создавать новые фрагменты, даже когда на наименьшем

из серверов фрагментов данных закончится место (в этом случае реплики будут сохраняться на одном из больших серверов фрагментов данных).

Доступное для выделения дисковое пространство также может ограничиваться лицензией.

Просмотр пространства, занятого фрагментами данных

Чтобы просмотреть общий объем дискового пространства, занятого всеми пользовательскими данными в кластере, запустите команду vstorage top и нажмите клавишу **V** на клавиатуре. После этого вывод команды должен выглядеть подобно следующему.

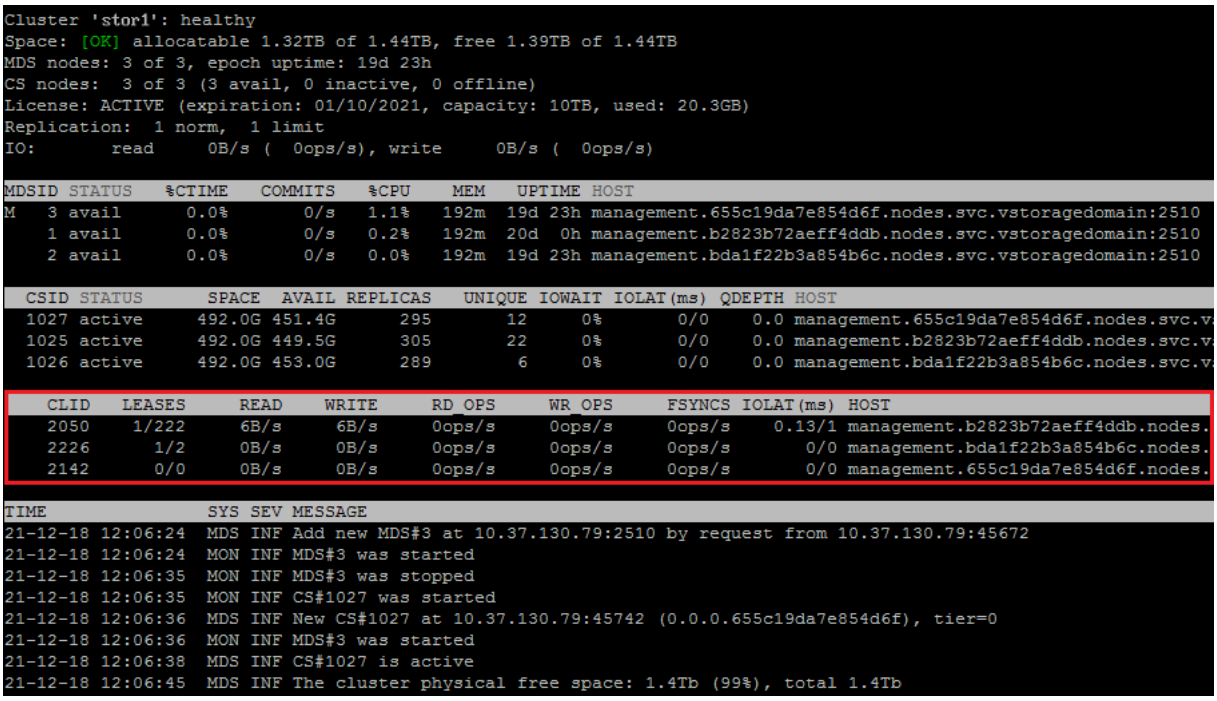
```
# vstorage -c stor1 top
Cluster 'stor1': healthy
Space: [OK] allocatable 1.32TB of 1.44TB, free 1.39TB of 1.44TB
MDS nodes: 3 of 3, epoch uptime: 19d 23h, cluster version: 128
CS nodes:  3 of 3 (3 avail, 0 inactive, 0 offline), storage version: 128
License: ACTIVE (expiration: 01/10/2021, capacity: 10TB, used: 20.3GB)
Replication:  1 norm,  1 limit
Chunks: [OK] 323 (100%) healthy,  0 (0%) standby,  0 (0%) degraded,  0 (0%) urgent,
         0 (0%) blocked,  0 (0%) pending,  0 (0%) offline,  0 (0%) replicating,
         0 (0%) overcommitted,  0 (0%) deleting,  0 (0%) void
FS:  20.3GB in 757 files, 757 inodes,  244 file maps,  323 chunks,  889 chunk replicas
IO:      read     0B/s (  0ops/s), write     0B/s (  0ops/s)
IO total: read   37.1GB ( 473Kops), write  133.7GB ( 4.7Mops)
Repl IO:  read     0B/s, write:     0B/s
Sync rate:   0ops/s, datasync rate:   0ops/s
IO QDEPTH: 0.0 aver, 0.0 max
<...>
```

В поле **FS** отображается размер всех пользовательских данных в кластере без учета реплик.

Описание состояний фрагментов см. в разделе "Диаграмма «Фрагменты данных»" на странице 727.

8.5.3 Мониторинг клиентов

Посредством мониторинга клиентов можно контролировать состояние и работоспособность серверов, используемых для доступа к виртуальным машинам. Для мониторинга клиентов используйте команду vstorage -c <cluster_name> top, например:



Приведенная выше команда выводит подробную информацию о кластере stor1. Параметры мониторинга для клиентов (выделены красным) следующие:

CLID

Идентификатор клиента.

LEASES

Среднее количество файлов, открытых клиентом на чтение/запись и все еще не закрытых, за последние 20 секунд.

READ

Средняя скорость в байтах в секунду, с которой клиент считывает данные, за последние 20 секунд.

WRITE

Средняя скорость в байтах в секунду, с которой клиент записывает данные, за последние 20 секунд.

RD_OPS

Среднее число операций чтения, выполняемых клиентом за секунду, в течение последних 20 секунд.

WR_OPS

Среднее число операций записи, выполняемых клиентом за секунду, в течение последних 20 секунд.

FSYNCS

Среднее число операций синхронизации, выполняемых клиентом за секунду, в течение последних 20 секунд.

IOLAT

Среднее/максимальное время в миллисекундах, которое требовалось клиенту для выполнения одной операции ввода-вывода, за последние 20 секунд.

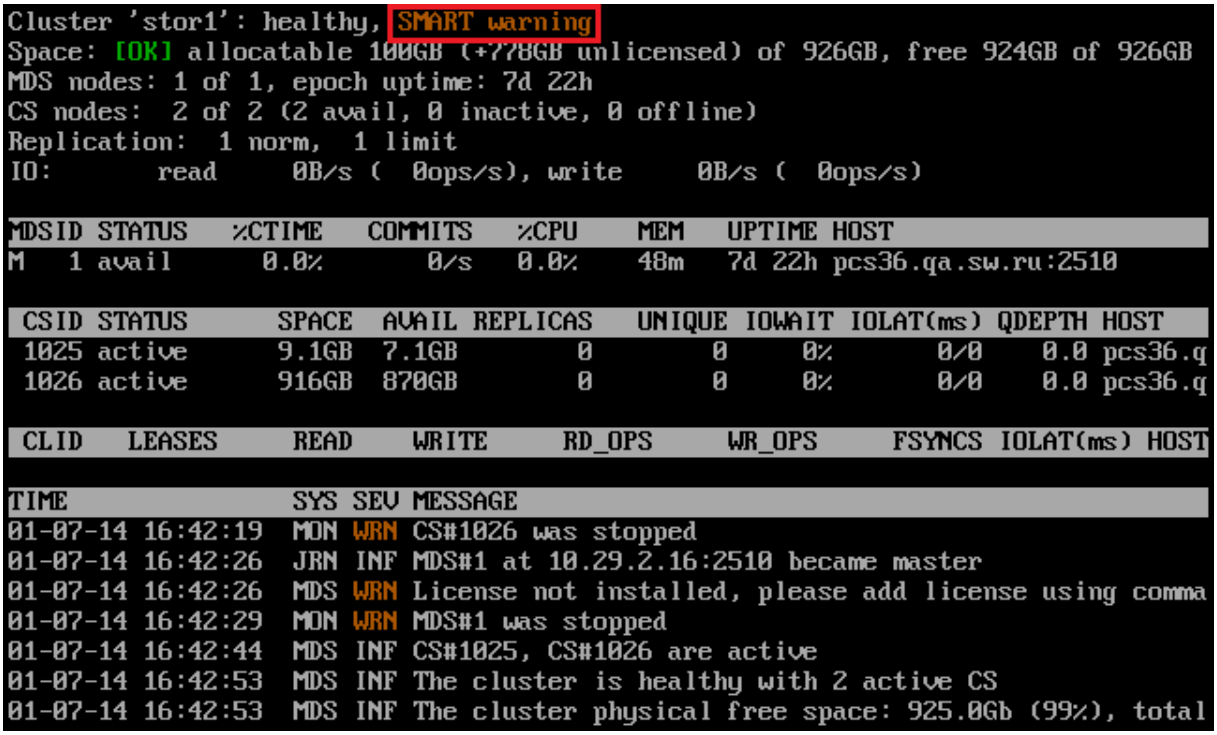
HOST

Имя хоста или IP-адрес клиента.

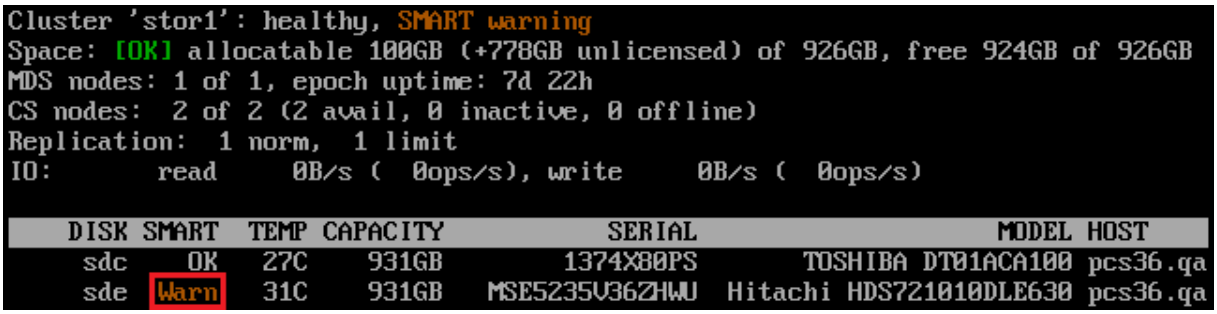
8.5.4 Мониторинг физических дисков

Состояние S.M.A.R.T. физических дисков отслеживается с помощью инструмента smartctl, устанавливаемого вместе с продуктом Кибер Инфраструктура. Чтобы он работал, необходимо включить поддержку S.M.A.R.T. в BIOS соответствующего сервера. Инструмент запускается каждые 10 минут по заданию cron, которое также добавляется в ходе установки. Инструмент smartctl опрашивает все физические диски, подсоединенные к серверам в кластере, в том числе твердотельные накопители кэширования и журналирования, и передает полученные результаты на сервер метаданных.

Результаты опроса накопителей за последние 10 минут можно просмотреть в выходных данных команды vstorage top, например:



Если в главной таблице отображается сообщение SMART warning (Предупреждение SMART), это означает, что для одного из физических дисков близок аппаратный отказ по данным S.M.A.R.T. Нажмите клавишу **d**, чтобы переключиться на таблицу дисков и просмотреть более подробные сведения, например:



В таблице дисков отображаются следующие параметры:

DISK

Имя диска, присвоенное операционной системой.

SMART

Состояние S.M.A.R.T. диска:

OK

Диск исправен.

Warn (Предупреждение)

Диск в состоянии, близком к аппаратному отказу. Близость к аппаратному отказу означает, что по меньшей мере один из следующих счетчиков S.M.A.R.T. не равен нулю:

- Reallocated Sector Count (Количество переназначенных секторов),
- Reallocated Event Count (Количество событий переназначения),
- Current Pending Sector Count (Текущее количество ожидающих секторов),
- Offline Uncorrectable (Отключено без возможности исправления).

TEMP

Температура диска в градусах Цельсия.

CAPACITY

Емкость диска.

SERIAL

Серийный номер диска.

MODEL

Модель диска.

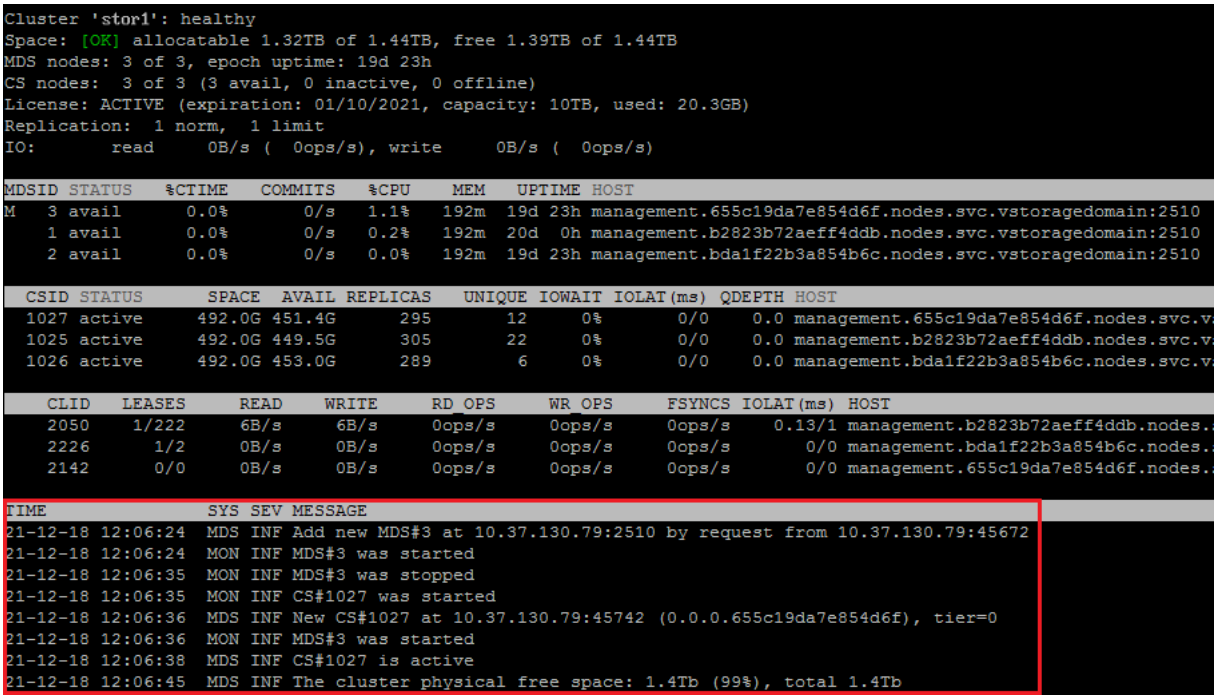
HOST

Имя хоста диска.

Чтобы отключить мониторинг S.M.A.R.T. дисков, удалите соответствующее задание cron.

8.5.5 Мониторинг журналов событий

С помощью утилиты vstorage -c <cluster_name> top можно вести мониторинг важных событий, происходящих в кластере хранения данных, например:



Приведенная выше команда отображает последние события, которые произошли в кластере stor1. Сведения о событиях (выделены красным) отображаются в таблице со следующими столбцами:

TIME

Время события.

SYS

Компонент кластера, в котором произошло событие (например, MDS для сервера метаданных или JRN для локального журнала).

SEV

Уровень серьезности события.

MESSAGE

Описание события.

В следующей таблице перечислены основные события, отображаемые при запуске утилиты vstorage top.

Основные события

Событие	Серьезность	Описание
MDS#<N> (<addr>:<port>) lags behind for more than 1000	JRN err (Ошибка журнала)	Создается главным сервером MDS, когда тот обнаруживает

Событие	Серьезность	Описание
rounds (Сервер MDS № <N> отстает в течение более 1000 циклов)		устаревание/отставание сервера MDS № <N>. Это сообщение может указывать на то, что какой-то сервер MDS работает очень медленно и не успевает обрабатывать операции.
MDS#<N> (<addr>:<port>) didn't accept commits for *M* sec (Сервер MDS № <N> не принимал фиксации в течение M сек.)	JRN err (Ошибка журнала)	Создается главным сервером MDS, если сервер MDS № <N> не принимал фиксаций в течение *M* сек. Такой сервер MDS № <N> помечается как устаревший. Это сообщение может указывать, что на сервере MDS № <N> возникли проблемы со службой MDS. Такая проблема может быть критической, и ее следует решить как можно скорее.
MDS#<N> (<addr>:<port>) state is outdated and will do a full resync (Состояние сервера MDS № <N> устарело, будет произведена полная повторная синхронизация)	JRN err (Ошибка журнала)	Создается главным сервером MDS, если на сервере MDS № <N> будет проведена полная повторная синхронизация. Такой сервер MDS № <N> помечается как устаревший. Это сообщение может указывать, что определенный сервер MDS работал слишком медленно или соединение с ним нарушилось на такое продолжительное время, что он уже не поддерживает актуального состояния метаданных и его необходимо синхронизировать повторно. Такая проблема может быть критической, и ее следует решить как можно скорее.
MDS#<N> at <addr>:<port> became master (Сервер MDS № <N> стал главным сервером)	JRN info (Информация в журнале)	Создается каждый раз, когда в кластере выбирается новый главный сервер MDS. Частые изменения главного сервера MDS могут указывать на проблемы с сетевыми подключениями и негативно влиять на работу

Событие	Серьезность	Описание
		кластеров.
The cluster is healthy with *N* active CS (Кластер работоспособен с N активных CS)	MDS info (Информация MDS)	Создается в случае, если состояние кластера меняется на работоспособное, и при выборе нового главного сервера MDS. Это сообщение указывает, что все серверы фрагментов в кластере активны и количество реплик соответствует установленным в кластере требованиям.
The cluster is degraded with *N* active, *M* inactive, *K* offline CS (Кластер деградировал: N активных серверов фрагментов, M неактивных, K отключены)	MDS warn (Предупреждение MDS)	Создается, когда состояние кластера меняется на деградировавшее, а также при выборе нового главного сервера MDS. Это сообщение указывает, что некоторые серверы фрагментов в кластере либо неактивны, то есть не посылают каких-либо сообщений о регистрации, либо отключены, то есть были неактивны дольше, чем задано в параметре mds.wd.offline_tout (по умолчанию 5 минут).
The cluster failed with *N* active, *M* inactive, *K* offline CS (mds.wd.max_offline_cs=<n>) (Произошел отказ кластера: N активных серверов фрагментов данных, M неактивных, K отключены)	MDS err (Ошибка MDS)	Создается, когда состояние кластера меняется на отказ кластера, а также при выборе нового главного сервера MDS. Это сообщение указывает, что количество отключенных серверов фрагментов данных превышает число, заданное в параметре mds.wd.max_offline_cs (по умолчанию равно 2). В случае отказа кластера планирование автоматической репликации прекращается. Поэтому администратору кластера необходимо принять меры: либо восстановить отказавшие серверы кластера, либо увеличить значение mds.wd.max_offline_cs. При установке значения 0 этого

Событие	Серьезность	Описание
		параметра перехода в режим отказа не происходит никогда.
The cluster is filled up to <N>% (Кластер заполнен на <N> %)	MDS info/warn (Информация/предупреждение MDS)	Уведомляет о текущем использовании пространства в кластере. Если израсходовано 80 % и более дискового пространства, формируется предупреждение. Важно иметь некоторый резервный объем дискового пространства для реплик данных на случай отказа одного из серверов фрагментов данных.
Replication started, N chunks are queued (Репликация начата, в очередь помещено N фрагментов)	MDS info (Информация MDS)	Создается, когда кластер начинает автоматическую репликацию данных для восстановления отсутствующих реплик.
Replication completed (Репликация завершена)	MDS info (Информация MDS)	Создается, когда кластер завершает автоматическую репликацию данных.
CS#<N> has reported hard error on *path* (CS № <N> сообщил об аппаратной ошибке по пути *path*)	MDS warn (Предупреждение MDS)	Создается, когда CS № <N> обнаруживает повреждение данных на диске. Рекомендуется проверить оборудование на предмет ошибок и заменить диски с поврежденными данными как можно скорее.
CS#<N> has not registered during the last *T* sec and is marked as inactive/offline (CS № <N> не проходил регистрацию в течение последних T секунд и помечен как неактивный/отключенный)	MDS warn (Предупреждение MDS)	Создается, когда CS № <N> был недоступен в течение некоторого времени. Через 5 минут его состояние меняется на отключенный (offline), при этом запускается автоматическая репликация данных для восстановления реплик, хранившихся на сервере фрагментов данных, который оказался отключен.
Failed to allocate *N* replicas for '*path*' by request from <addr>:<port> - *K* out of *M*	MDS warn (Предупреждение MDS)	Создается, когда кластер не может выделить пространство для реплик фрагментов, например в случае,

Событие	Серьезность	Описание
chunks servers are available (Не удалось распределить N реплик для пути 'path' по запросу от <addr>:<port> – K из M серверов фрагментов данных недоступны)		если на нем исчерпалось дисковое пространство.
Failed to allocate *N* replicas for '*path*' by request from <addr>:<port> since only *K* chunk servers are registered (Не удалось распределить N реплик для пути 'path' по запросу от <addr>:<port>, поскольку зарегистрировано лишь K серверов фрагментов данных)	MDS warn (Предупреждение MDS)	Создается, когда кластер не может выделить пространство для реплик фрагментов, потому что в кластере зарегистрировано слишком мало серверов фрагментов данных.

8.5.6 Мониторинг параметров репликации

Настраивая параметры репликации, учитывайте, что новые параметры не вступают в силу немедленно. Например, при увеличении параметра количества реплик по умолчанию для фрагментов данных его отработка может занять некоторое время в зависимости от нового значения параметра и числа фрагментов данных в кластере.

Чтобы убедиться, что новые параметры репликации были успешно применены в кластере, выполните следующие действия:

1. Выполните команду vstorage -c <cluster_name> top.
2. Нажмите клавишу **V**, чтобы отобразить дополнительные сведения о кластере. Типичный вывод этой команды может выглядеть следующим образом:

```
# vstorage -c stor1 top
Cluster 'stor1': healthy
Space: [OK] allocatable 448.6GB of 492.0GB, free 1.39TB of 1.44TB
MDS nodes: 3 of 3, epoch uptime: 20d  0h
CS nodes:  3 of 3 (3 avail, 0 inactive, 0 offline)
License: ACTIVE (expiration: 01/10/2021, capacity: 10TB, used: 20.3GB)
Replication:  3 norm,  2 limit
Chunks: [Warning] 187 (57%) healthy,  0 (0%) standby,  0 (0%) degraded,  135 (41%) urgent,
        0 (0%) blocked,  0 (0%) pending,  0 (0%) offline,  1 (0%) replicating,
        0 (0%) overcommitted,  0 (0%) deleting,  0 (0%) void
IO:     read     0B/s (  0ops/s), write  106KB/s (  7ops/s)
<...>
```

3. Проверьте значение в поле Chunks (Фрагменты), учитывая следующие моменты:

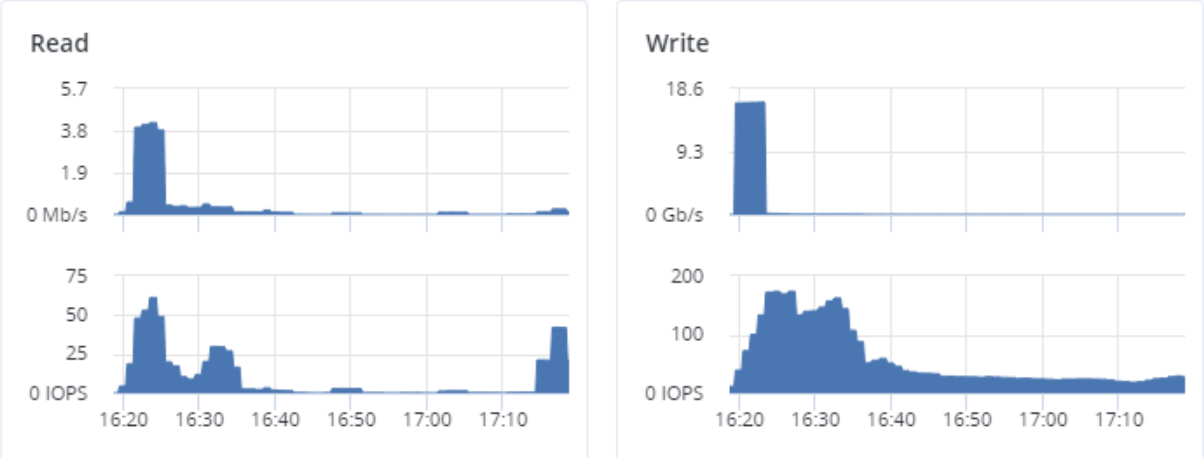
- При уменьшении параметров числа реплик обращайте внимание на фрагменты в состоянии фиксации с избытком (overcommitted) и в состоянии удаления (deleting). После завершения процесса репликации в выходных данных команды не должны отображаться фрагменты ни в одном из этих состояний.
- При увеличении параметров количества реплик обращайте внимание на фрагменты в заблокированном состоянии (blocked) и подлежащие срочной обработке (urgent). После завершения процесса репликации в выходных данных команды не должны отображаться фрагменты ни в одном из этих состояний. Кроме того, пока процесс продолжает выполняться, значение параметра работоспособности (healthy) будет ниже 100 %.

Дополнительные сведения о возможных состояниях фрагментов см. в разделе "Диаграмма «Фрагменты данных»" на странице 727.

8.5.7 Диаграммы активности ввода-вывода

Панель администратора

На диаграммах **Чтение** и **Запись** отображается история активности ввода-вывода кластера в виде скорости операций чтения и записи в мегабайтах в секунду, а также количества операций чтения и записи в секунду (IOPS), например:



Интерфейс командной строки

Используйте следующую команду:

```
vstorage -c <cluster_name> top
```

Например, чтобы просмотреть показатели активности дискового ввода-вывода в кластере cluster1, взгляните на эту строку в выводе команды:

```
IO:     read 30.5MB/s (523ops/s), write  108MB/s (5.9Kop/s)
```

IO

Активность дискового ввода-вывода в кластере:

- Скорость операций ввода-вывода при чтении и записи в байтах в секунду.
- Количество операций ввода-вывода (чтения и записи) в секунду.

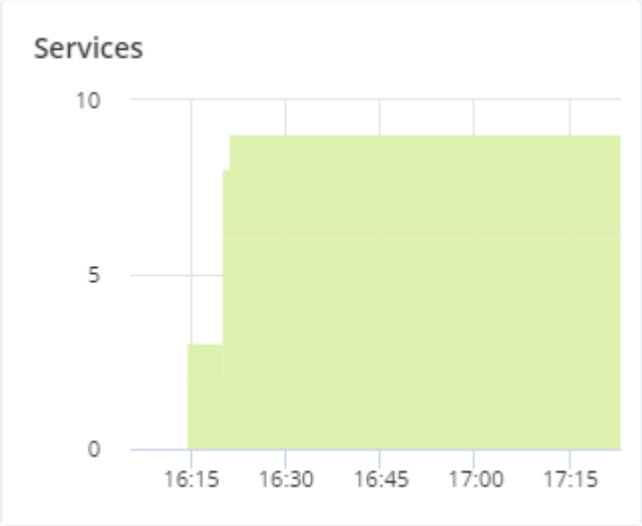
8.5.8 Диаграмма «Сервисы»

Панель администратора

На диаграмме **Сервисы** можно отслеживать два типа сервисов:

- Сервисы метаданных (MDS). Количество всех дисков с ролью метаданных. Убедитесь, что постоянно работают как минимум три сервиса MDS.
- Сервисы фрагментов данных (CS). Количество всех дисков с ролью хранилища.

Типичная статистика может выглядеть следующим образом:



Если некоторые из сервисов фрагментов данных какое-то время работали медленно или находились в режиме обслуживания, соответствующие периоды времени будут выделены на диаграмме оранжевым цветом. Сервисы метаданных и фрагментов данных в состоянии отказа выделены красным.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster overview
```

Например, чтобы просмотреть сведения о сервисах хранилища в кластере cluster1, взгляните на следующие строки в выводе команды:

```
+------------------+-------------------------+
| Field            | Value                   |
+------------------+-------------------------+
| ...              | ...                     |
| cs               | failed: 0               |
|                  | slow: 0                 |
|                  | total: 5                |
| ...              | ...                     |
| mds              | failed: 0               |
|                  | total: 3                |
+------------------+-------------------------+
```

8.5.9 Диаграмма «Фрагменты данных»

Панель администратора

Состояние всех фрагментов данных в кластере можно отслеживать на диаграмме **Фрагменты данных**. Фрагменты данных могут находиться в следующих состояниях:

Исправен

Количество и процент фрагментов данных, у которых достаточно активных реплик. Это нормальное состояние фрагментов данных.

Офлайн

Количество и процент фрагментов данных, все реплики которых находятся в отключенном состоянии. Такие фрагменты данных полностью недоступны для кластера, невозможно их реплицировать, считывать или записывать в них данные. Все запросы к фрагменту данных, находящемуся в состоянии «Офлайн», замораживаются до тех пор, пока сервис CS, хранящий реплику соответствующего фрагмента, не станет активным.

Во избежание потери данных следует как можно быстрее вернуть серверы фрагментов данных, находящиеся в состоянии «Офлайн», в подключенное состояние.

Заблокировано

Количество и процент фрагментов данных, у которых число активных реплик меньше заданного минимального количества. Запросы на запись к заблокированному фрагменту данных замораживаются до тех пор, пока у него не будет по крайней мере заданного минимального количества реплик. В то же время запросы на чтение к заблокированным фрагментам выполняются, поскольку у них еще есть активные реплики. Заблокированные фрагменты имеют более высокий приоритет репликации, чем деградировавшие.

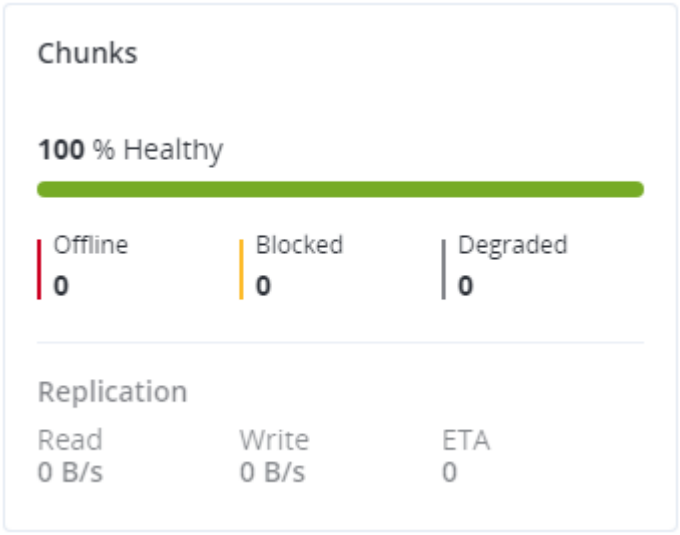
Наличие заблокированных фрагментов данных в кластере повышает риск потери данных, поэтому следует отложить все техническое обслуживание на рабочих серверах кластера и как можно быстрее вернуть недоступные серверы фрагментов данных в рабочее состояние.

Деградировал

Количество и процент фрагментов данных с небольшим количеством активных реплик, но не меньше установленного минимума. Для таких фрагментов данных возможны и чтение

и запись в них. Однако в последнем случае деградировавший фрагмент данных становится срочным.

Исправные фрагменты данных выделяются на шкале зеленым цветом, отключенные – красным, заблокированные – желтым, а деградировавшие – серым, например:



В разделе **Репликация** отображаются сведения об активности репликации в кластере.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster overview
```

Например, чтобы получить сведения о фргаментах данных в кластере cluster1, взгляните на следующие строки в выводе команды:

```
+------------------+-------------------------+
| Field            | Value                   |
+------------------+-------------------------+
| ...              | ...                     |
| chunks           | blocked: 0              |
|                  | degraded: 0             |
|                  | deleting: 0             |
|                  | healthy: 153            |
|                  | offline: 0              |
|                  | overcommitted: 0        |
|                  | pending: null           |
|                  | replicating: 0          |
|                  | standby: null           |
|                  | total: 153              |
|                  | unique: 0               |
|                  | urgent: 0               |
|                  | void: 0                 |
```

```
| ...              | ...                    |
+------------------+------------------------+
```

blocked

Количество фрагментов данных, у которых число активных реплик меньше заданного минимального количества. Запросы на запись к заблокированному фрагменту данных замораживаются до тех пор, пока у него не будет по крайней мере заданного минимального количества реплик. В то же время запросы на чтение к заблокированным фрагментам выполняются, поскольку у них еще есть активные реплики. Заблокированные фрагменты имеют более высокий приоритет репликации, чем деградировавшие.

Наличие заблокированных фрагментов данных в кластере повышает риск потери данных, поэтому следует отложить все техническое обслуживание на рабочих серверах кластера и как можно быстрее вернуть недоступные серверы фрагментов данных в рабочее состояние.

degraded

Количество фрагментов данных с небольшим числом активных реплик, но не меньше установленного минимума. Для таких фрагментов данных возможны и чтение и запись в них. Однако в последнем случае деградировавший фрагмент данных становится срочным.

deleting

Количество фрагментов, поставленных в очередь на удаление.

healthy

Количество фрагментов данных, у которых достаточно активных реплик. Это нормальное состояние фрагментов данных.

offline

Количество фрагментов данных, все реплики которых находятся в отключенном состоянии. Такие фрагменты данных полностью недоступны для кластера, невозможно их реплицировать, считывать или записывать в них данные. Все запросы к фрагменту данных, находящемуся в состоянии «Офлайн», замораживаются до тех пор, пока сервис CS, хранящий реплику соответствующего фрагмента, не станет активным.

Во избежание потери данных следует как можно быстрее вернуть серверы фрагментов данных, находящиеся в состоянии «Офлайн», в подключенное состояние.

overcommitted

Количество фрагментов, у которых количество реплик больше нормального. Обычно такие фрагменты возникают после снижения нормального числа реплик или удаления большого объема данных. Со временем излишние реплики удаляются, однако во время репликации этот процесс может происходить медленнее.

pending

Количество фрагментов, которые необходимо реплицировать немедленно. Для выполнения запроса на запись от клиента во фрагмент у этого фрагмента должно быть не менее заданного минимального числа реплик. Если их меньше, фрагмент блокируется и выполнить

запрос невозможно. Поскольку заблокированные фрагменты необходимо реплицировать как можно быстрее, кластер помещает их в отдельную, высокоприоритетную очередь репликации и сообщает о них как об ожидающих репликации.

replicating

Количество фрагментов, для которых осуществляется репликация. Операции записи в эти фрагменты заморожены до момента окончания репликации.

standby

Количество фрагментов, у которых одна или более реплик находятся в резервном состоянии. Реплика отмечается как резервная, если она была неактивна не более 5 минут.

total

Общее количество всех фрагментов в кластере хранилища.

unique

Количество фрагментов, у которых нет реплик.

urgent

Количество фрагментов, которые деградировали и имеют неидентичные реплики. Реплики деградировавшего фрагмента могут оказаться неидентичными, если некоторые из них окажутся недоступными во время операции записи. В таком случае часть реплик будет содержать новые данные, в то время как в других будут по-прежнему содержаться старые данные. Такие реплики удаляются кластером как можно быстрее. Срочные фрагменты не влияют на целостность информации, так как актуальные данные все равно хранятся не менее чем в заданном минимальном числе реплик.

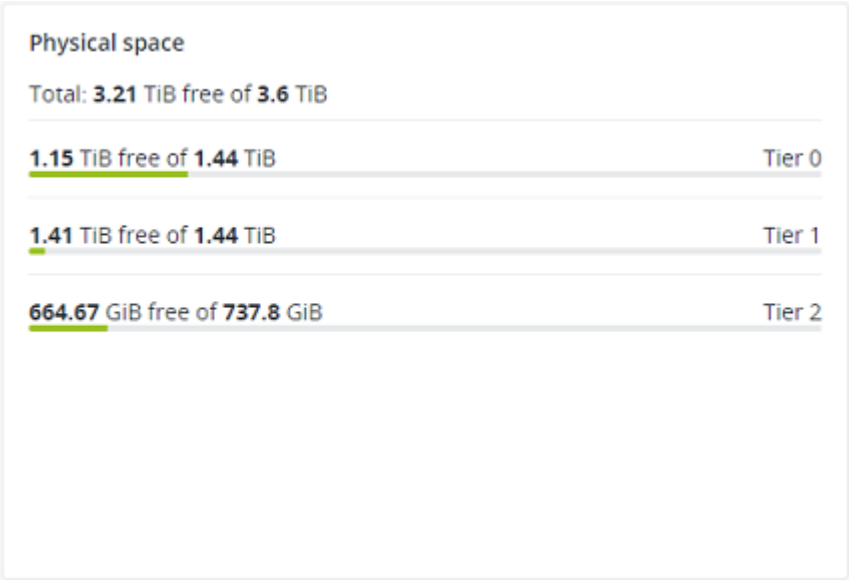
void

Количество фрагментов, которые были выделены, но еще ни разу не использовались. Такие фрагменты не содержат данных. Наличие в кластере некоторого числа пустых фрагментов — это нормальная ситуация.

8.5.10 Диаграмма «Физическое пространство»

Панель администратора

На диаграмме **Физическое пространство** отображается текущее использование физического пространства во всем кластере хранилища и на каждом уровне по отдельности. Используемое пространство включает в себя пространство, занятое всеми фрагментами данных и их репликами, а также пространство, занятое любыми другими данными.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster overview
```

Например, чтобы просмотреть использование физического пространства в кластере cluster1, взгляните на следующие строки в выводе команды:

```
+------------------+------------------------+
| Field            | Value                  |
+------------------+------------------------+
| ...              | ...                    |
| tiers            | - id: 0                |
|                  |   phys_space:          |
|                  |     free: 611533008896 |
|                  |     total: 675644723200|
|                  |     used: 64111714304  |
+------------------+------------------------+
```

Принцип расчета физического пространства

Общее физическое дисковое пространство представляет собой совокупность всего дискового пространства на всех дисках хранилища одного и того же уровня. Используемое физическое пространство – совокупность всех пользовательских данных на дисках хранилища того же уровня с учетом режима избыточности. Свободное дисковое пространство – это общее физическое пространство минус используемое физическое пространство.

Чтобы лучше понять, как вычисляется физическое дисковое пространство, рассмотрим следующий пример.

	Используется/всего (свободно), ГиБ		
	Уровень 0, кодирование 3+2 (67 % накладных расходов)	**Уровень 1, 2 реплики (100 % накладных расходов)**	**Уровень 2, без избыточности**
Сервер 1	334/1024 (690)	134/512 (378)	50/256 (206)
Сервер 2	334/1024 (690)	133/512 (379)	50/256 (206)
Сервер 3	334/1024 (690)	133/512 (379)	
Сервер 4	334/1024 (690)		
Сервер 5	334/1024 (690)		
Сводка в отчете	1670/5120 (3450)	400/1536 (1136)	100/512 (412)

Кластер содержит десять дисков с ролью хранилища: пять дисков по 1024 ГиБ назначены на уровень 0, три диска по 512 ГиБ – на уровень 1, два диска по 256 ГиБ – на уровень 2. Других данных (например, системных файлов) на дисках нет. На уровне 0 хранится 1000 ГиБ пользовательских данных в режиме кодирования 3+2. На уровне 1 хранится 200 ГиБ пользовательских данных в режиме 2 реплик. На уровне 2 хранится 100 ГБ пользовательских данных без избыточности.

Независимо от используемого режима избыточности, кластер пытается равномерно распределить фрагменты данных между дисками того же уровня.

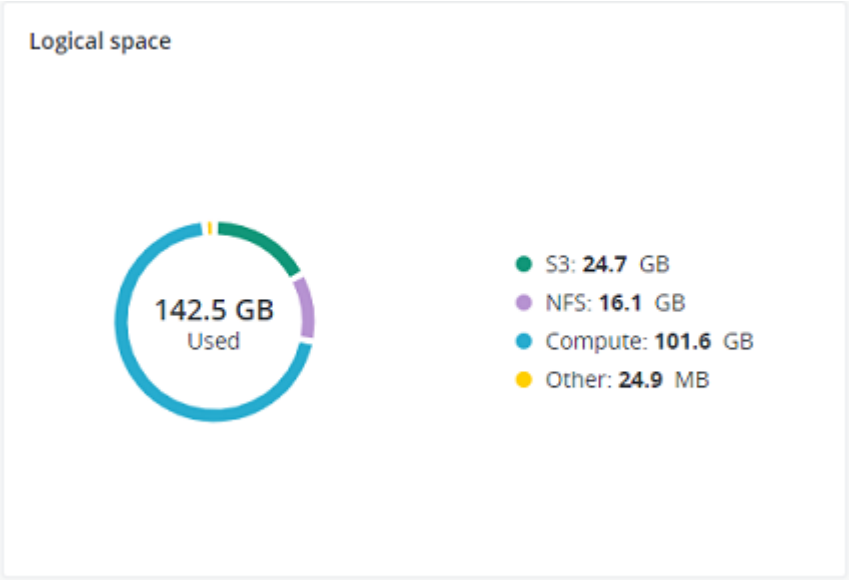
В данном примере отчет сообщает о физическом дисковом пространстве на каждом из уровней следующим образом.

- На уровне 0 общее дисковое пространство составляет 5120 ГиБ, используемое дисковое пространство – 1670 ГиБ, а свободное дисковое пространство – 3450 ГиБ.
- На уровне 1 общее дисковое пространство составляет 1536 ГиБ, используемое дисковое пространство – 400 ГиБ, а свободное дисковое пространство – 1136 ГиБ.
- На уровне 2 общее дисковое пространство составляет 512 ГиБ, используемое дисковое пространство – 100 ГиБ, а свободное дисковое пространство – 412 ГиБ.

8.5.11 Диаграмма «Логическое пространство»

Панель администратора

На диаграмме **Логическое пространство** представлено все пространство, выделенное различным сервисам для хранения пользовательских данных. К нему относится пространство, занятое исключительно пользовательскими данными. Реплики и метаданные кода избыточности (erasure coding) не учитываются.



Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster overview
```

Например, чтобы просмотреть использование логического пространства в кластере cluster1, взгляните на следующие строки в выводе команды:

```
+------------------+------------------------+
| Field            | Value                  |
+------------------+------------------------+
| ...              | ...                    |
| logic_space      | free: 1078130163512    |
|                  | total: 1099511627776   |
|                  | used: 21381464264      |
| ...              | ...                    |
| space_per_service | abgw: 0               |
|                  | compute: 20477967791   |
|                  | iscsi: 0               |
|                  | nfs: null              |
|                  | other: 903496473       |
|                  | s3: 0                  |
+------------------+------------------------+
```

Принцип расчета логического пространства

При мониторинге информации о дисковом пространстве в кластере помните, что логическое пространство – это количество свободного дискового пространства, которое может использоваться для хранения пользовательских данных в форме фрагментов данных и всех их реплик. Как только это пространство исчерпается, в кластер невозможно будет записывать данные.

Чтобы лучше понять, как рассчитывается логическое дисковое пространство, рассмотрим следующий пример.

- Кластер содержит три диска с ролью хранилища. На первом диске имеется 200 ГБ пространства, на втором – 500 ГБ, а на третьем – 1 ТБ.
- Если задан режим избыточности с тремя репликами, каждый фрагмент данных должен храниться в виде трех реплик на трех разных дисках с ролью хранилища.

В данном примере доступное логическое дисковое пространство будет равно 200 ГБ, то есть оно будет равно емкости наименьшего диска с ролью хранилища. Причина этого в том, что каждая реплика должна храниться на отдельном диске. Поэтому, как только пространство на наименьшем диске (то есть 200 ГБ) будет исчерпано, невозможно будет создать новые реплики фрагментов данных, если только не добавить новый диск с ролью хранилища или не изменить режим избыточности на две реплики.

В режиме избыточности с двумя репликами доступное логическое дисковое пространство составит 700 ГБ, так как два наименьших диска вместе могут содержать 700 ГБ данных.

Принцип расчета логического пространства iSCSI

Выделение пространства для хранилища блочных данных, которое используется LUN iSCSI и вычислительными томами, осуществляется с частичным соблюдением принципов экономного распределения. Несмотря на то что при создании тома блочного хранилища пространство не распределено, размер использованного пространства увеличивается в зависимости от потребностей и не может быть уменьшен. В этом случае логическое пространство занимают реальные данные. Размер используемого пространства не может превышать размер тома. После удаления данных неиспользуемое пространство не возвращается и помечается как используемое.

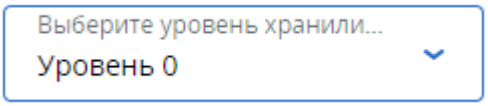
Чтобы лучше понять, как рассчитывается логическое дисковое пространство для вычислительных томов и iSCSI, рассмотрим следующий пример:

1. Пользователь создает LUN iSCSI размером 100 ТБ.
2. Пользователь подключает LUN к VMware в качестве хранилища данных.
3. Пользователь добавляет в хранилище данных данные/ВМ. Размер используемого логического пространства увеличивается до 100 ТБ.
4. Пользователь удаляет данные, освобождая место в хранилище. Однако пространство в хранилище блочных данных не освобождается, поэтому показатель использованного логического пространства по-прежнему составляет 100 ТБ.

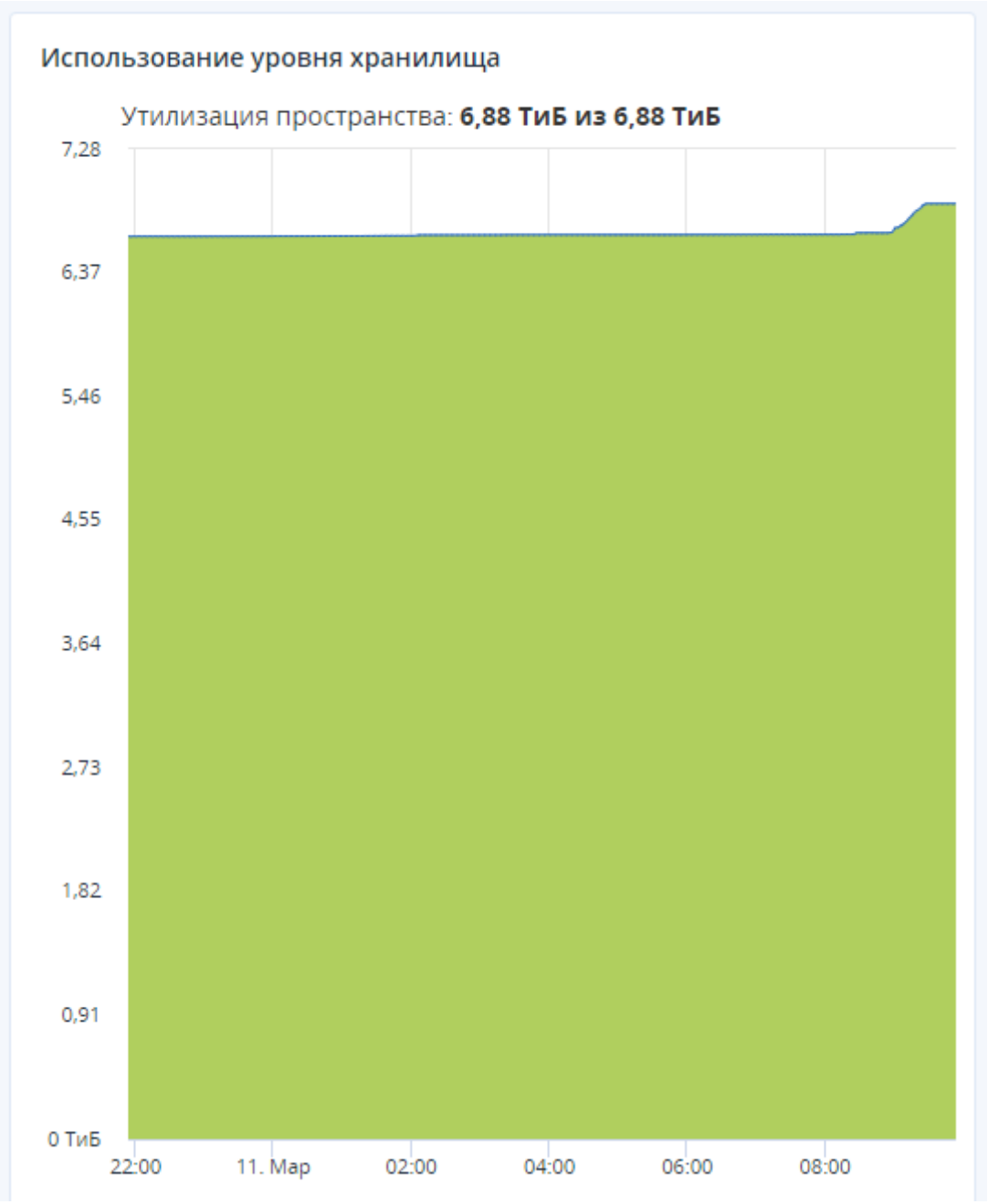
8.5.12 Мониторинг нагрузки на уровни хранилища

Просмотр сведений о нагрузке на уровни хранилища

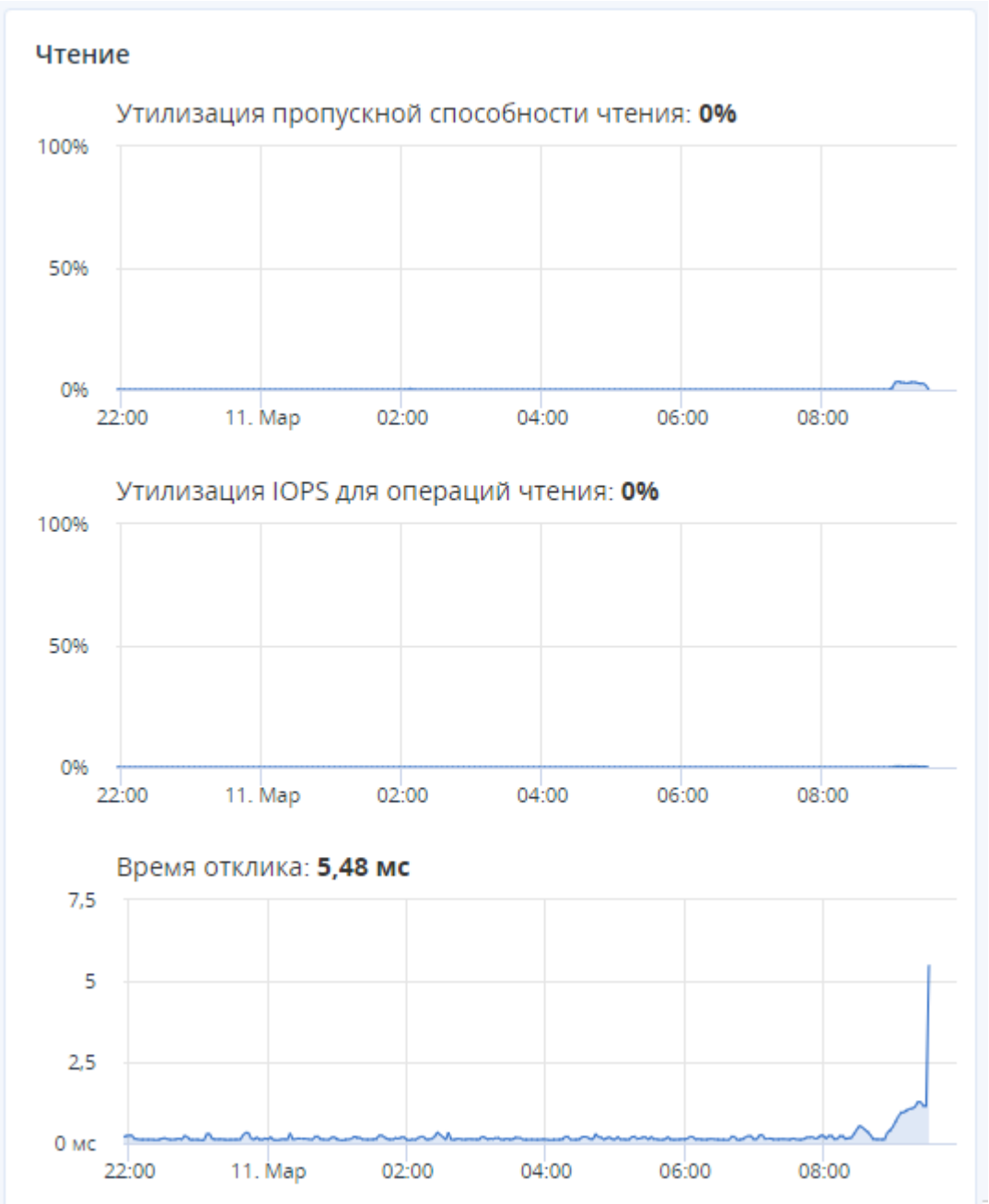
На экране **Сервисы хранилища** > **Обзор** откройте вкладку **Нагрузка на уровни хранилища** и выберите уровень.



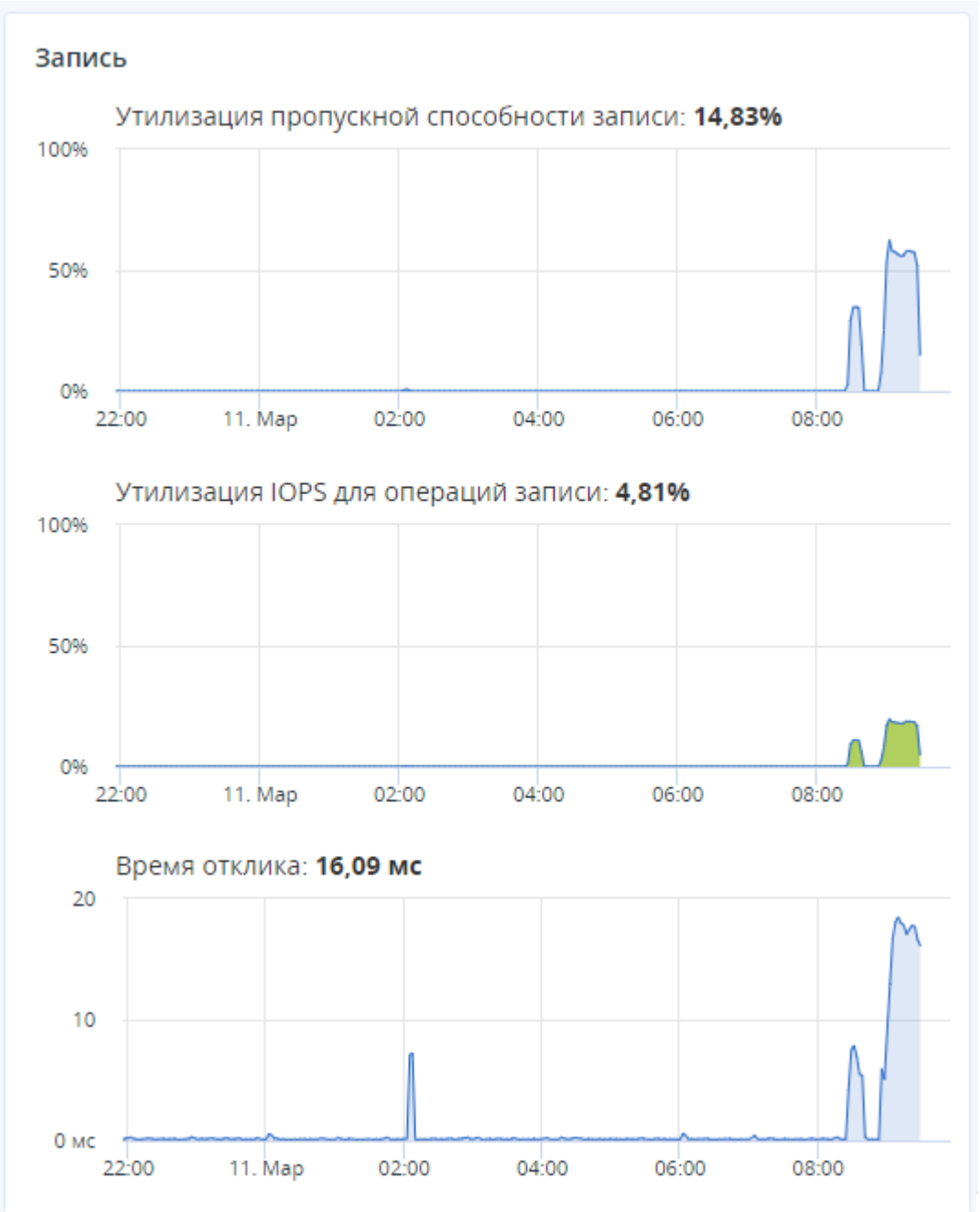
На графике в разделе **Использование уровня хранилища** представлена зависимость объема используемого дискового пространства от времени.



На графиках в разделе **Чтение** представлены зависимости от времени скорости чтения данных в процентах от ее максимального значения, скорости выполнения операций чтения в процентах от ее максимального значения, времени отклика при чтении данных.



На графиках в разделе **Запись** представлены зависимости от времени скорости записи данных в процентах от ее максимального значения, скорости выполнения операций записи в процентах от ее максимального значения, времени отклика при записи данных.



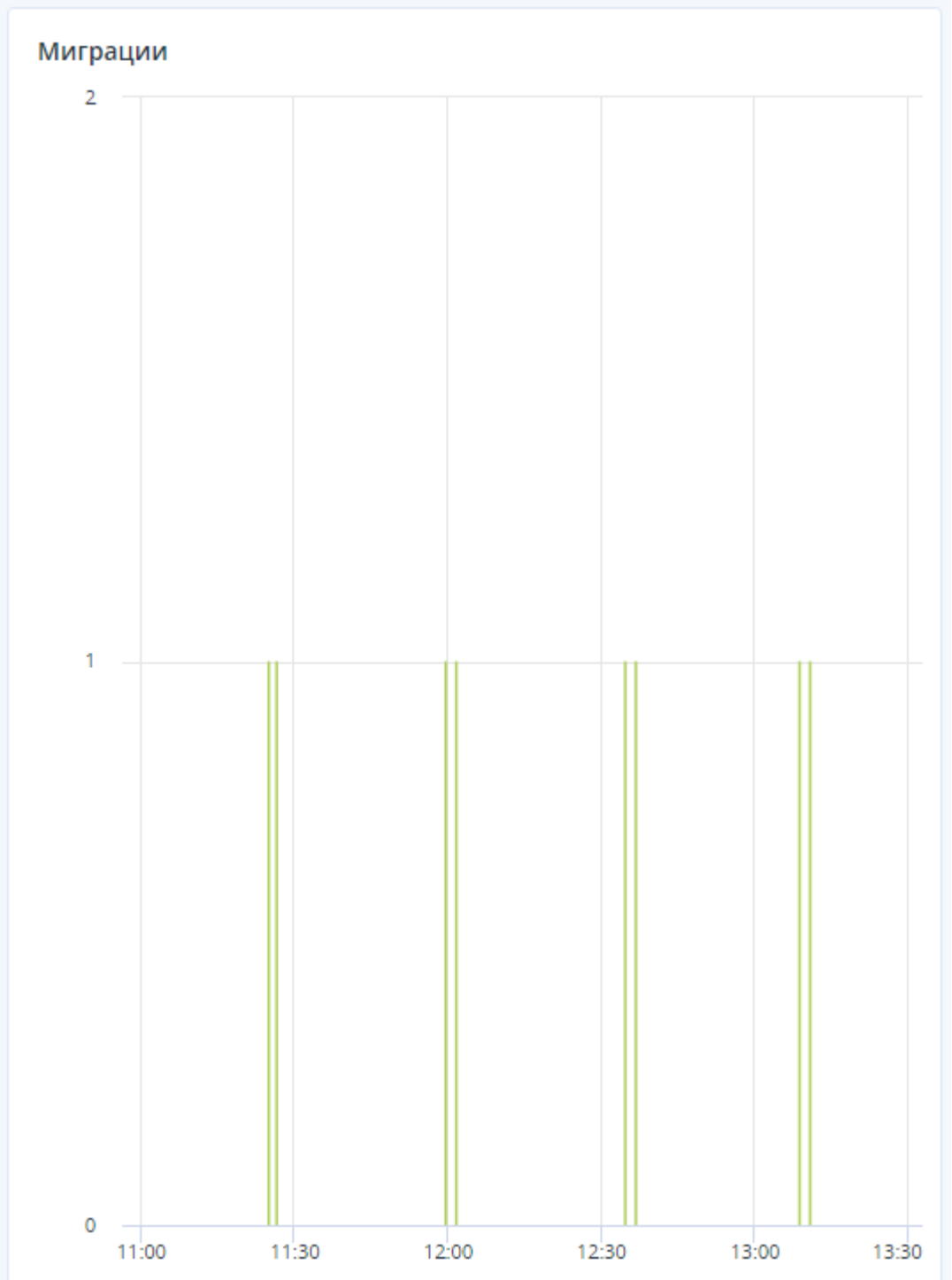
Примечание

После создания кластера хранилища балансировщику нагрузки необходимо до двух часов, чтобы собрать необходимую минимальную статистику для принятия решений и отображения ненулевых значений на странице мониторинга нагрузки на уровни.

В выключенном состоянии балансировщик нагрузки не выполняет ресурсоемкие измерения, а в качестве максимально достижимых значений скорости выполнения операций ввода-вывода и скорости передачи данных использует максимальные значения, измеренные под пользовательской нагрузкой.

Просмотр сведений о перемещениях томов

При включенной функции автоматической балансировки нагрузки на уровни хранилища осуществляются перемещения томов между уровнями. Сведения о перемещениях томов можно просмотреть на экране **Сервисы хранилища** > **Обзор** > **Миграции томов**. На графике в разделе **Миграции** представлена зависимость количества перемещений томов между уровнями от времени.



8.5.13 Мониторинг объектов кластера с помощью SNMP

Объекты кластера можно отслеживать с помощью протокола SNMP (Simple Network Management Protocol). Реализация соответствует тем же правилам структуры управляющей информации (SMI), что и данные в стандартном контексте SNMP: все объекты организуются в дерево; каждый идентификатор объекта (OID) представляет собой ряд целых чисел, соответствующих серверам дерева и разделяемых точками.

Общие сведения:

- OID корневого поддерева со всеми объектами, которые можно отслеживать, — 1.3.6.1.4.1.8072.161.1.
- Для мониторинга объектов необходим базовый файл с информацией VSTORAGE-MIB.txt. Этот файл можно загрузить по адресу https://<admin_panel_IP>:8888/api/v2/snmp/mibs/?x-session-id=0.

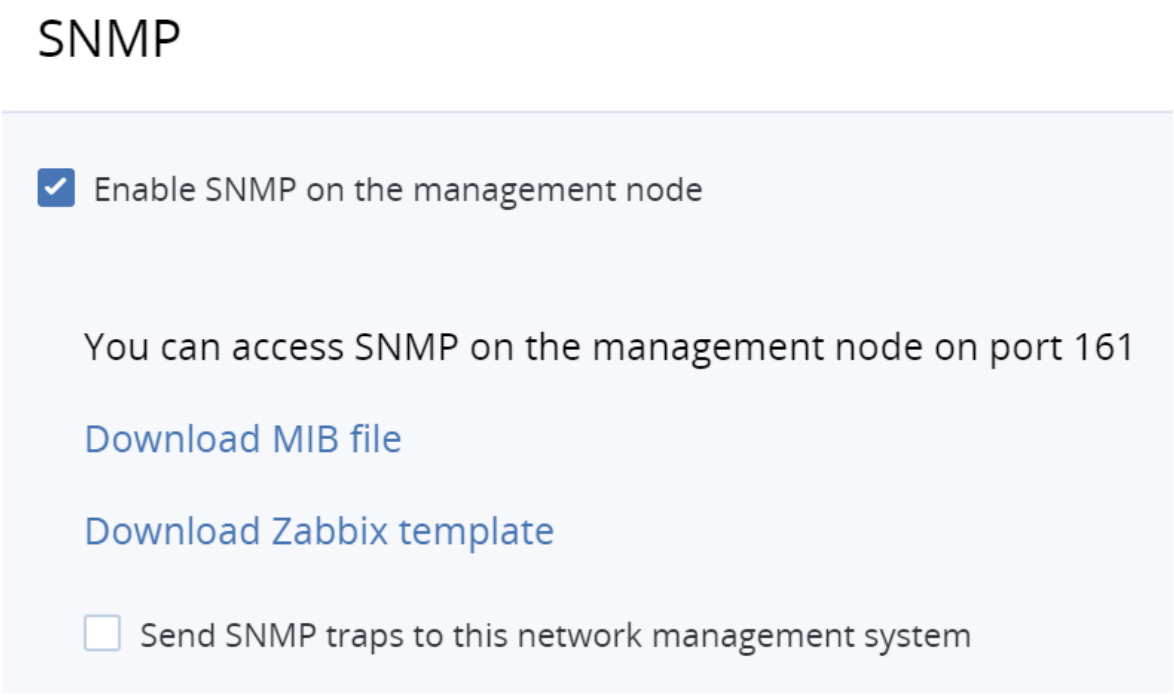
Обзор мониторинга SNMP

1. Включите доступ по SNMP.
2. Обеспечьте доступ к информационным объектам кластера с помощью инструментов SNMP (например, Net-SNMP или Zabbix).
3. Если необходимо использовать прослушку ловушек SNMP, настройте параметры и отправьте тестовую ловушку SNMP.

8.5.13.1 Включение доступа по SNMP

Чтобы включить доступ SNMP на сервере

1. Откройте порт UDP 161 на сервере управления следующим образом.
   a. На экране **Инфраструктура** > **Сети** нажмите **Изменить**.
   b. Добавьте тип трафика **SNMP** во внешнюю сеть, установив соответствующий флажок.
   c. Нажмите кнопку **Сохранить**, чтобы применить изменения.
2. Перейдите на вкладку **Настройки** > **Настройки системы** > **SNMP** и установите флажок **Включить SNMP на сервере управления**. Будет включена система управления сетью (SNMP-монитор), что обеспечит доступ к кластеру по протоколу SNMP.



3. Щелкните по предоставленной ссылке, чтобы загрузить MIB-файл и настроить его в SNMP-мониторе.
4. [Необязательно] Включите отправку ловушек SNMP в SNMP-монитор следующим образом.
   a. Установите флажок **Посылать ловушки SNMP этой системе управления сетью**.
   b. Укажите **IP-адрес**, **Порт** и **Сообщество** для системы управления сетью.
      По умолчанию демон snmptrapd использует порт 162. Сообщество по умолчанию – public.
   c. При необходимости нажмите **Послать тестовую ловушку**, чтобы проверить работу сервиса.
5. Нажмите кнопку **Сохранить**, чтобы применить изменения.

8.5.13.2 Доступ к информационным объектам кластера с помощью SNMP

К информационным объектам кластера можно обращаться с помощью любых инструментов SNMP, например бесплатного пакета Net-SNMP для Linux.

Предварительные требования

- Доступ по SNMP включен в соответствии с инструкциями в "Включение доступа по SNMP" на предыдущей странице.

Чтобы получить информацию о кластере хранилища на сервере управления

Поместите MIB-файл в каталог /usr/share/snmp/mibs и выполните команду snmpwalk, например:

```
# snmpwalk  -M /usr/share/snmp/mibs -m VSTORAGE-MIB -v 2c -c public localhost:161
VSTORAGE-MIB:cluster
```

Типичные выходные данные могут выглядеть следующим образом.

```
VSTORAGE-MIB::clusterName.0 = STRING: "cluster1"
VSTORAGE-MIB::healthStatus.0 = STRING: "healthy"
VSTORAGE-MIB::usedLogicalSpace.0 = Counter64: 173732322
VSTORAGE-MIB::totalLogicalSpace.0 = Counter64: 1337665179648
VSTORAGE-MIB::freeLogicalSpace.0 = Counter64: 1318963253248
VSTORAGE-MIB::licenseStatus.0 = STRING: "unknown"
VSTORAGE-MIB::licenseCapacity.0 = Counter64: 1099511627776
VSTORAGE-MIB::licenseExpirationStatus.0 = STRING: "None"
VSTORAGE-MIB::ioReadOpS.0 = Counter64: 0
VSTORAGE-MIB::ioWriteOpS.0 = Counter64: 0
VSTORAGE-MIB::ioReads.0 = Counter64: 0
VSTORAGE-MIB::ioWrites.0 = Counter64: 0
VSTORAGE-MIB::csActive.0 = Counter64: 11
VSTORAGE-MIB::csTotal.0 = Counter64: 11
VSTORAGE-MIB::mdsAvail.0 = Counter64: 4
VSTORAGE-MIB::mdsTotal.0 = Counter64: 4
<...>
```

8.5.13.3 Прослушивание ловушек SNMP

Предварительные требования

- Доступ по SNMP включен в соответствии с инструкциями в "Включение доступа по SNMP" на странице 739.

Чтобы начать прослушивание ловушек SNMP

1. Настройте демон snmptrapd, чтобы записывать ловушки SNMP в журнал, разрешать им запускать исполняемые действия и повторно отправлять данные в сеть. Для этого раскомментируйте следующую строку сообщества public в файле /etc/snmp/snmptrapd.conf:

   ```
   authCommunity log,execute,net public
   ```

2. Настройте брандмауэр так, чтобы разрешить входящий трафик на порте UDP 162.
3. Загрузите файл VSTORAGE-MIB.txt и поместите его в каталог /usr/share/snmp/mibs.
4. Запустите демон и укажите MIB-файл.

   ```
   # snmptrapd -M /usr/share/snmp/mibs -m VSTORAGE-MIB -n -f
   ```

   По умолчанию ловушки будут записываться в /var/log/messages. Можно перенаправить их в другой файл журнала с помощью параметра -Lf <path>, например:

   ```
   # snmptrapd -M /usr/share/snmp/mibs -m VSTORAGE-MIB -n -f -Lf /tmp/traps.log
   ```

5. Отправьте тестовую ловушку на вкладке **Настройки** > **Настройки системы** > **SNMP** на панели администрирования.
6. Просмотрите файл журнала.

```
# tail -f /tmp/traps.log
2019-10-14 12:51:50 node001.vstoragedomain [UDP: [10.94.80.22]:40029->\
[10.94.80.22]:162]:#012DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: \
(111150521) 12 days, 20:45:05.21#011SNMPv2-MIB::snmpTrapOID.0 = OID: \
NET-SNMP-MIB::netSnmp.161.3.100#011NET-SNMP-MIB::netSnmp.161.2.1 = STRING:
"TestTrap"\
#011NET-SNMP-MIB::netSnmp.161.2.2 = STRING: "It is the test trap from VStorage"\
#011NET-SNMP-MIB::netSnmp.161.2.3 = Counter64: 0
```

8.5.13.4 Мониторинг кластера с помощью Zabbix

Предварительные требования

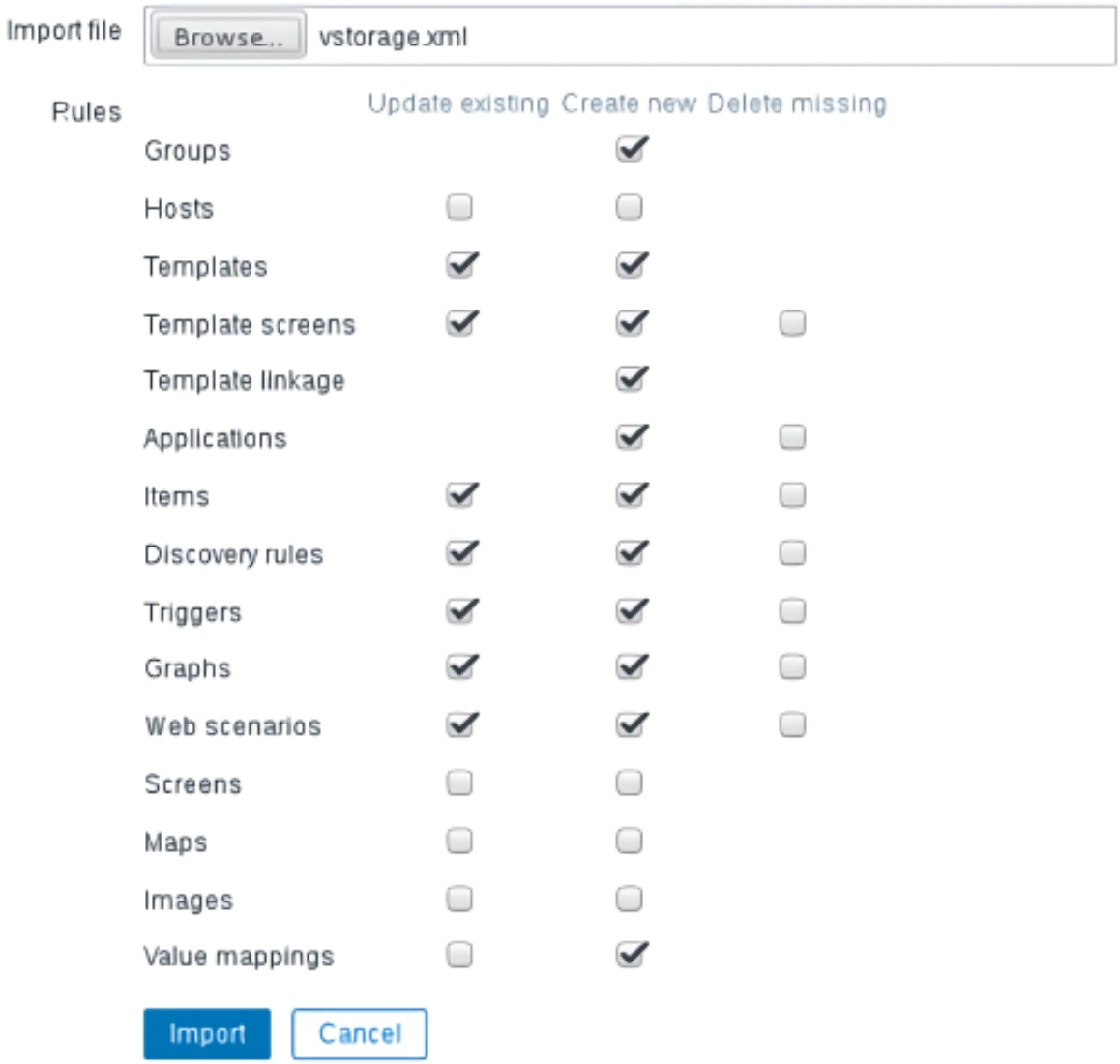
- Доступ по SNMP включен в соответствии с инструкциями в "Включение доступа по SNMP" на странице 739.

Чтобы настроить мониторинг кластера в Zabbix

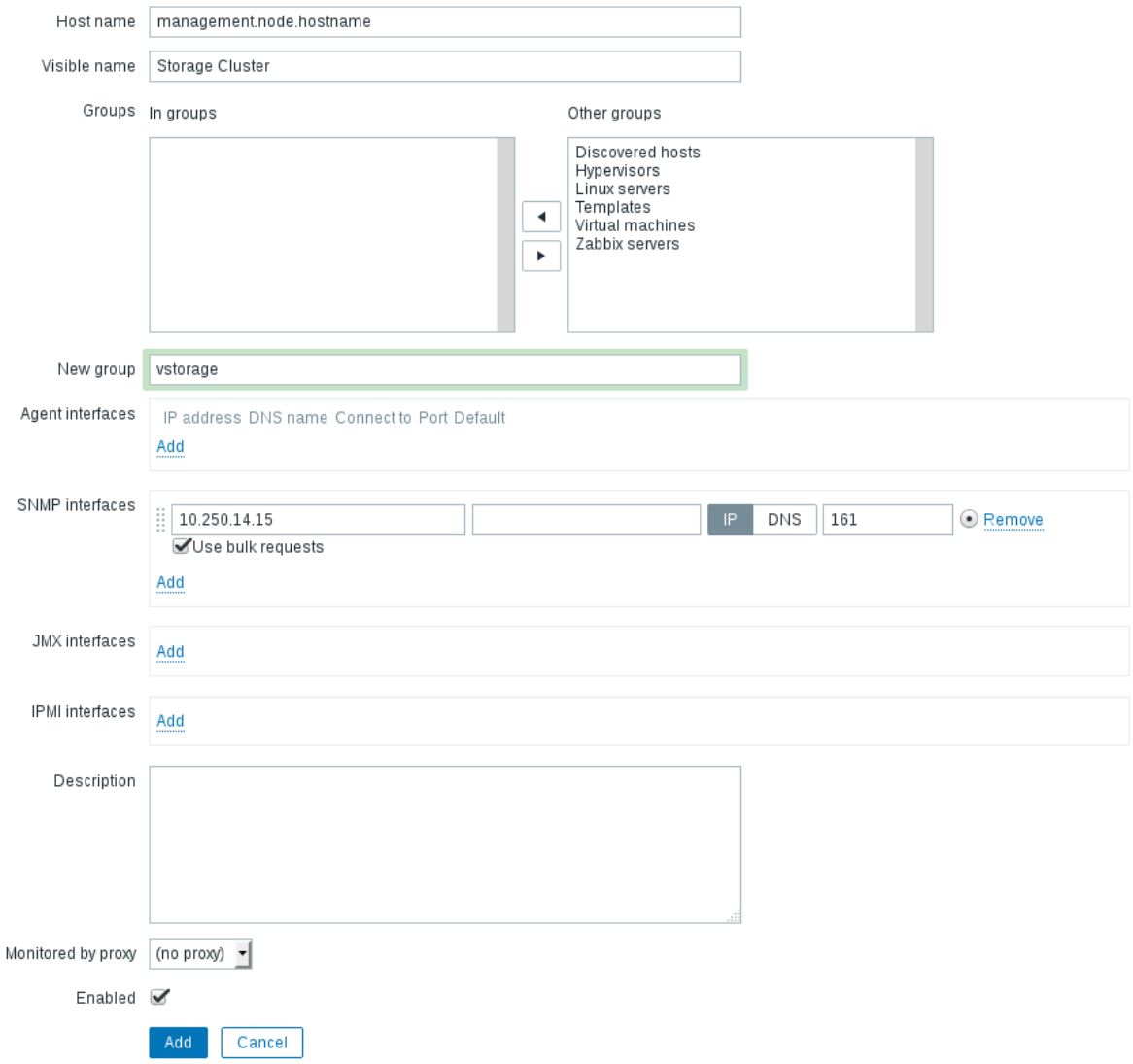
1. На вкладке **Настройки** > **Настройки системы** > **SNMP** щелкните по предоставленной ссылке, чтобы загрузить шаблон для Zabbix.

   Примечание
   Этот шаблон совместим с Zabbix 3.x.

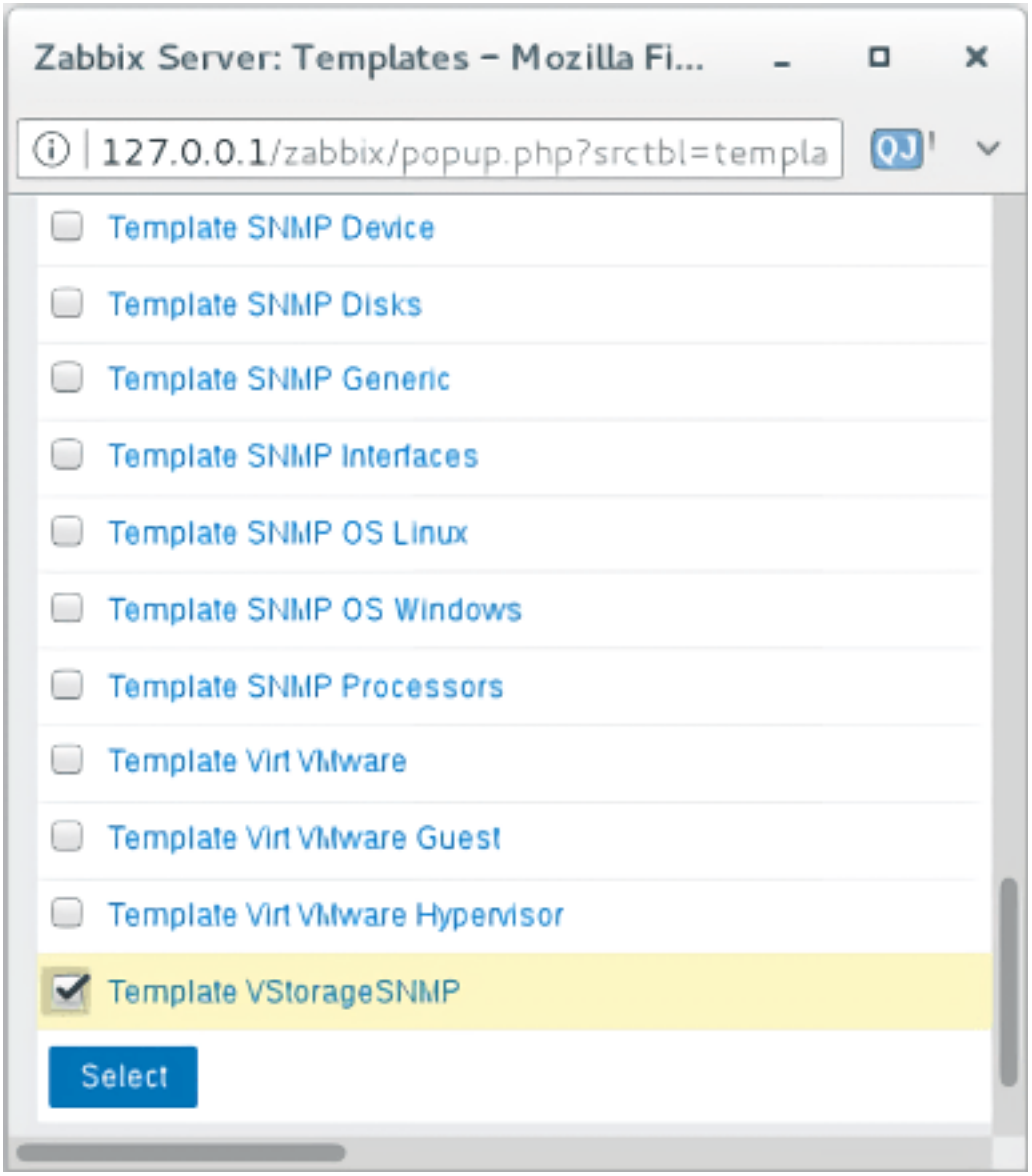
2. В Zabbix откройте **Configuration** (Конфигурация) > **Templates** (Шаблоны) > **Import** (Импорт) и нажмите **Browse** (Обзор).



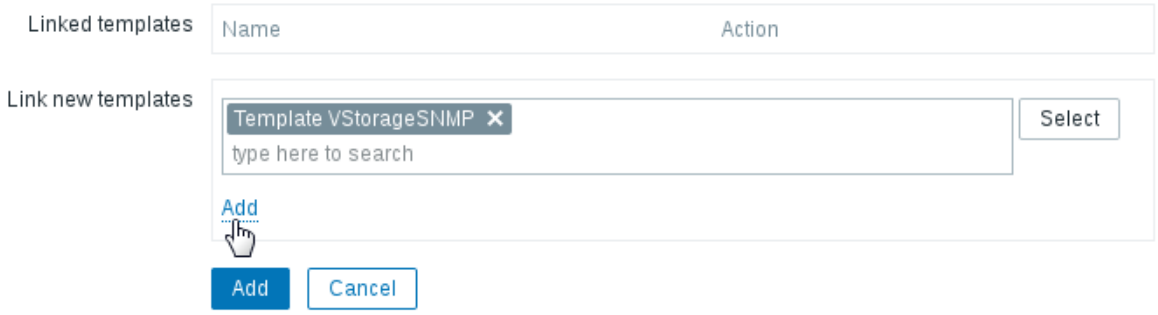
3. Перейдите к шаблону, выберите его и нажмите **Import** (Импорт).
4. Нажмите **Configuration (Конфигурация)** > **Hosts (Хосты)** > **Create host (Создать хост)**.



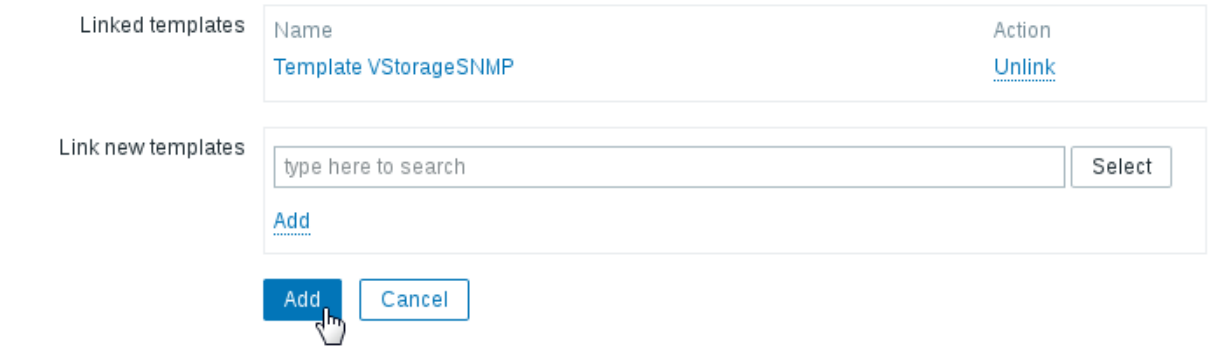
5. На вкладке **Host (Узел)** выполните следующие действия.
   a. Укажите **Host name (Имя узла)** сервера управления и его **Visible name (Видимое имя)** в Zabbix.
   b. Укажите **vstorage** в поле **New group (Новая группа)**.
   c. Удалите раздел **Agent Interfaces (Интерфейсы агентов)**.
   d. Добавьте раздел **SNMP interfaces (SNMP-интерфейсы)** и укажите IP-адрес сервера управления.
6. На вкладке **Templates (Шаблоны)** нажмите **Select (Выбрать)** рядом с полем **Link new templates (Ссылки на новые шаблоны)**.
7. В окне **Zabbix Server: Templates** (Сервер Zabbix: шаблоны) выберите шаблон **Template VStorageSNMP** и нажмите **Select** (Выбрать).



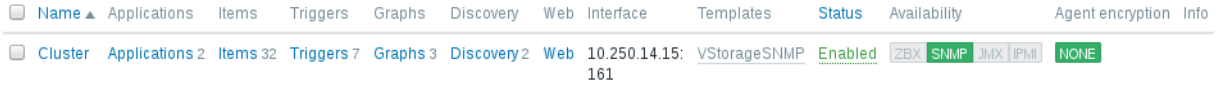
8. Вернувшись на вкладку **Templates (Шаблоны)**, щелкните по ссылке **Add (Добавить)** в разделе **Link new templates (Ссылки на новые шаблоны)**. Шаблон **VStorageSNMP** появится в группе **Linked templates (Связанные шаблоны)**.



9. После настройки хоста и добавления его шаблона нажмите кнопку **Add (Добавить)**.



Через несколько минут метка **SNMP** в столбце **Availability (Доступность)** на экране **Configuration (Конфигурация)** > **Hosts (Хосты)** станет зеленой.



Чтобы отслеживать состояние кластера с помощью Zabbix

Откройте экран **Monitoring** (Мониторинг) > **Latest data** (Последние данные), задайте для параметра фильтра **Host groups** (Группы хостов) значение **vstorage** и нажмите **Apply** (Применить).

Можно создать диаграммы производительности на вкладке **Configuration (Конфигурация)** > **Hosts (Хосты)** > **<cluster>** > **Graphs (Графики)** и рабочее место для них на вкладке **Monitoring (Мониторинг)** > **Screens (Экраны)**.

8.5.13.5 Объекты и ловушки кластера

Объекты, связанные с кластером

VSTORAGE-MIB:cluster

Общие сведения о кластере.

VSTORAGE-MIB:csStatTable

Таблица статистики сервера фрагментов данных.

VSTORAGE-MIB:mdsStatTable

Таблица статистики сервера метаданных.

VSTORAGE-MIB::clusterName

Наименование кластера.

VSTORAGE-MIB::healthStatus

Статус работоспособности кластера.

VSTORAGE-MIB::usedLogicalSpace

Пространство, занятое всеми фрагментами данных и их репликами, плюс пространство, занятое любыми другими данными, хранящимися на дисках серверов кластера.

VSTORAGE-MIB::totalLogicalSpace

Общее пространство на всех дисках серверов кластера.

VSTORAGE-MIB::freeLogicalSpace

Неиспользуемое пространство на всех дисках серверов кластера.

VSTORAGE-MIB::licenseStatus

Статус лицензии.

VSTORAGE-MIB::licenseCapacity

Максимально доступное дисковое пространство, определенное лицензией.

VSTORAGE-MIB::licenseExpirationStatus

Статус истечения срока действия лицензии.

VSTORAGE-MIB::ioReadOpS

Текущая скорость чтения в операциях в секунду.

VSTORAGE-MIB::ioWriteOpS

Текущая скорость записи в операциях в секунду.

VSTORAGE-MIB::ioReads

Текущая скорость чтения в байтах в секунду.

VSTORAGE-MIB::ioWrites

Текущая скорость записи в байтах в секунду.

VSTORAGE-MIB::csActive

Количество активных серверов фрагментов данных.

VSTORAGE-MIB::csTotal

Общее количество серверов фрагментов данных.

VSTORAGE-MIB::mdsAvail

Количество работающих серверов метаданных.

VSTORAGE-MIB::mdsTotal

Общее количество серверов метаданных.

VSTORAGE-MIB::s3OsAvail

Количество работающих серверов объектов S3.

VSTORAGE-MIB::s3OsTotal

Общее количество серверов объектов S3.

VSTORAGE-MIB::s3NsAvail

Количество работающих серверов имен S3.

VSTORAGE-MIB::s3NsTotal

Общее количество серверов имен S3.

VSTORAGE-MIB::s3GwAvail

Количество работающих шлюзов S3.

VSTORAGE-MIB::s3GwTotal

Общее количество шлюзов S3.

Объекты, связанные с CS

VSTORAGE-MIB::csId

Идентификатор сервера фрагментов данных.

VSTORAGE-MIB::csStatus

Текущий статус сервера фрагментов данных.

VSTORAGE-MIB::csIoReadOpS

Текущая скорость чтения сервера фрагментов данных в операциях в секунду.

VSTORAGE-MIB::csIoWriteOpS

Текущая скорость записи сервера фрагментов данных в операциях в секунду.

VSTORAGE-MIB::csIoWait

Процент времени, потраченного на ожидание операций ввода-вывода. Включает в себя время, потраченное на ожидание синхронизации.

VSTORAGE-MIB::csIoReadS

Текущая скорость чтения сервера фрагментов данных в байтах в секунду.

VSTORAGE-MIB::csIoWriteS

Текущая скорость записи сервера фрагментов данных в байтах в секунду.

Объекты, связанные с MDS

VSTORAGE-MIB::mdsId

Идентификатор сервера метаданных.

VSTORAGE-MIB::mdsStatus

Текущий статус сервера метаданных.

VSTORAGE-MIB::mdsMemUsage

Объем памяти, используемый сервером метаданных.

VSTORAGE-MIB::mdsCpuUsage

Процент мощности ЦП, используемый сервером метаданных.

VSTORAGE-MIB::mdsUpTime

Время с момента запуска сервера метаданных.

Ловушки SNMP, срабатывающие по указанным оповещениям

license expired

Закончился срок действия лицензии.

license_isnot_loaded

Лицензия не загружена.

too few free space

В кластере заканчивается логическое пространство.

too_few_free_phys_space

В кластере заканчивается физическое пространство.

offline node

Один из серверов кластера не в сети.

too few nodes

Осталось слишком мало серверов кластера.

too few mdses

Осталось слишком мало MDS.

too_much_mdses

Больше одного MDS на сервере.

too few cses

Осталось слишком мало CS.

failed mds

Сбой сервиса MDS.

failed cs

Сбой сервиса CS.

cses_on_single_tier_have_different_journalling_settings

Неверные настройки журналирования CS.

cses_on_single_tier_have_different_encryption_settings

Неверные настройки шифрования CS.

smart_failed

Диск не прошел проверку S.M.A.R.T.

disk_failed

Сбой диска.

too_few_root_space

Закончилось место на корневом разделе сервера.

too_few_space_on_metadata_disk

Закончилось место на диске MDS.

low_level_network_settings

На сетевом интерфейсе отсутствуют важные функции.

half_duplex

Сетевой интерфейс находится не в полнодуплексном режиме.

low_speed

Скорость сетевого интерфейса ниже 1 Гбит/с.

undefined_speed

Скорость сетевого интерфейса не определена.

network link

Сетевой интерфейс настроен неправильно.

abgw_cert_expired

Срок действия сертификата Backup Gateway истек или скоро истекает.

iscsi_redundancy_disk

Область отказа, установленная для iSCSI LUN, не обеспечивает его высокой доступности.

s3_redundancy_disk

Область отказа, установленная для кластера S3, не обеспечивает его высокой доступности.

software_updates

Доступны обновления для сервера.

no_internet_connection

На сервере отсутствует подключение к Интернету.

disk_write_cache_enabled

Кэширование записи на диск включено.

disk_write_cache_status_unknown

Статус кэширования записи на диск неизвестен.

compute_unavailable

Сбой вычислительного кластера.

oom_happened

Сработал механизм OOM Killer.

kernel_not_current

Устаревшее ядро на сервере.

no_ha

Не настроена высокая доступность для панели администрирования.

time_not_synced

Не синхронизировано время на сервере.

iscsi_upgrade_failed

Сбой крупного обновления iSCSI.

backend_backup_is_too_old

Последнее резервное копирование узла управления завершилось ошибкой, резервная его копия не существует или устарела.

spla_push_stats_failed

Не удается передать статистику использования пространства.

spla_license_load_failed

Не удается применить лицензию SPLA.

spla_get_space_usage_failed

Не удается получить статистику использования пространства.

other

Другие оповещения.

8.6 Удаленный мониторинг кластера

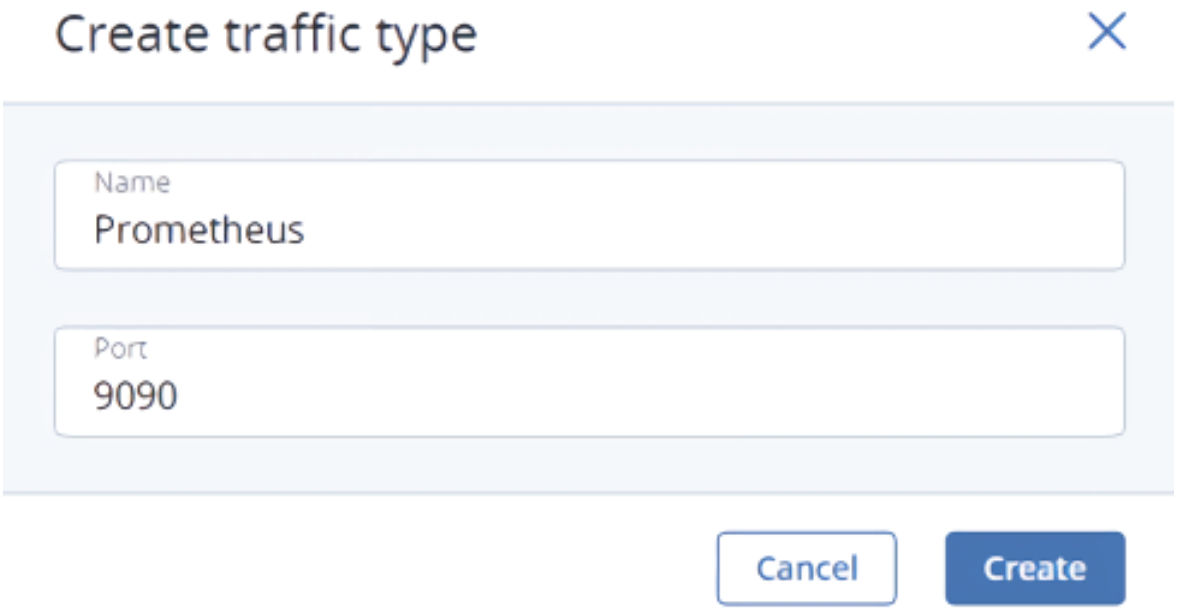
Отслеживать состояние кластера хранилища дистанционно можно с помощью встроенных инструментов мониторинга Prometheus и Alertmanager. Встроенный сервер Prometheus сохраняет данные в течение 7 дней. Если вам нужно сохранять значения показателей за более долгий период, используйте внешний сервер Prometheus. Alertmanager обрабатывает оповещения, генерируемые сервером Prometheus на основе правил оповещений. Можно также настроить Alertmanager для отправки оповещений во внешние системы, такие как PagerDuty.

8.6.1 Использование встроенного Prometheus для мониторинга

Чтобы использовать встроенный Prometheus, нужно открыть порт TCP для API-интерфейса Prometheus, чтобы тот стал доступен извне. Если у вас есть внешняя учетная запись Grafana и вы хотите использовать ее для мониторинга Кибер Инфраструктура, можно добавить в нее встроенный Prometheus в качестве источника данных. Используя добавленный источник данных Prometheus, можно импортировать панели мониторинга Grafana по умолчанию из Кибер Инфраструктура или создать новые панели.

Чтобы открыть порт для API-интерфейса Prometheus

1. На экране **Инфраструктура** > **Сети** нажмите **Изменить**, а затем **Создать тип трафика**.
2. В окне **Создать тип трафика** укажите пользовательское имя в поле **Имя** и **9090** в поле **Порт**. Затем нажмите кнопку **Создать**.



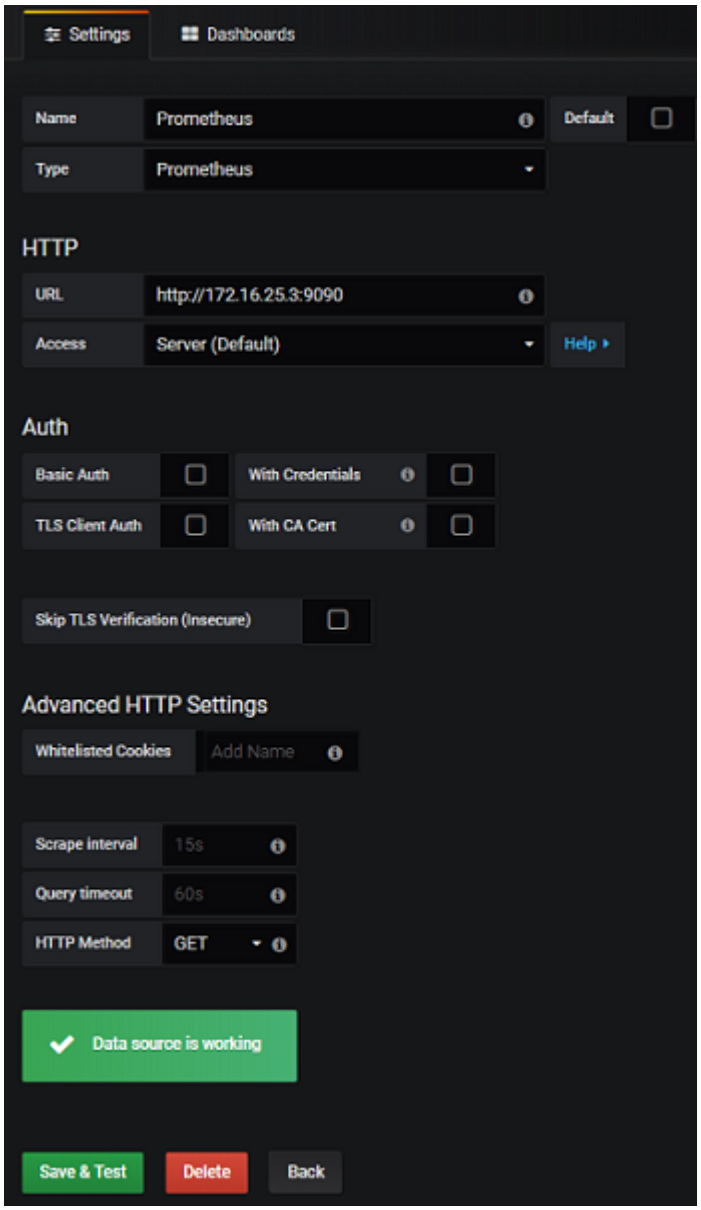
3. Нажмите **Назначить сетям** рядом с разделом **Пользовательские типы трафика**, затем добавьте созданный тип трафика во внешнюю сеть, установив соответствующий флажок.
4. Нажмите кнопку **Сохранить**, чтобы применить изменения.

Теперь доступ к пользовательскому веб-интерфейсу Prometheus можно получить по адресу http://<admin_panel_IP_address>:9090. Для получения дополнительных сведений об использовании Prometheus см. документацию по этому продукту.

Чтобы добавить Prometheus в качестве источника данных в Grafana

1. Выполните вход в пользовательский интерфейс Grafana.
2. Щелкните по значку шестерни в меню слева и выберите **Data Sources** (Источники данных).
3. На вкладке **Data Sources (Источники данных)** нажмите **Add data source (Добавить источник данных)**.
4. На экране **Data Sources / New (Источники данных / Создать)** укажите следующие параметры.
   a. Введите пользовательское имя источника данных в поле **Name (Имя)**.
   b. Задайте для параметра **Type (Тип)** значение **Prometheus**.
   c. Введите **http://<admin_panel_IP_address>:9090** в поле **URL**.
5. Нажмите **Save & Test (Сохранить и проверить)**.

Если указанные параметры правильны, появится сообщение Data source is working (Источник данных работает).

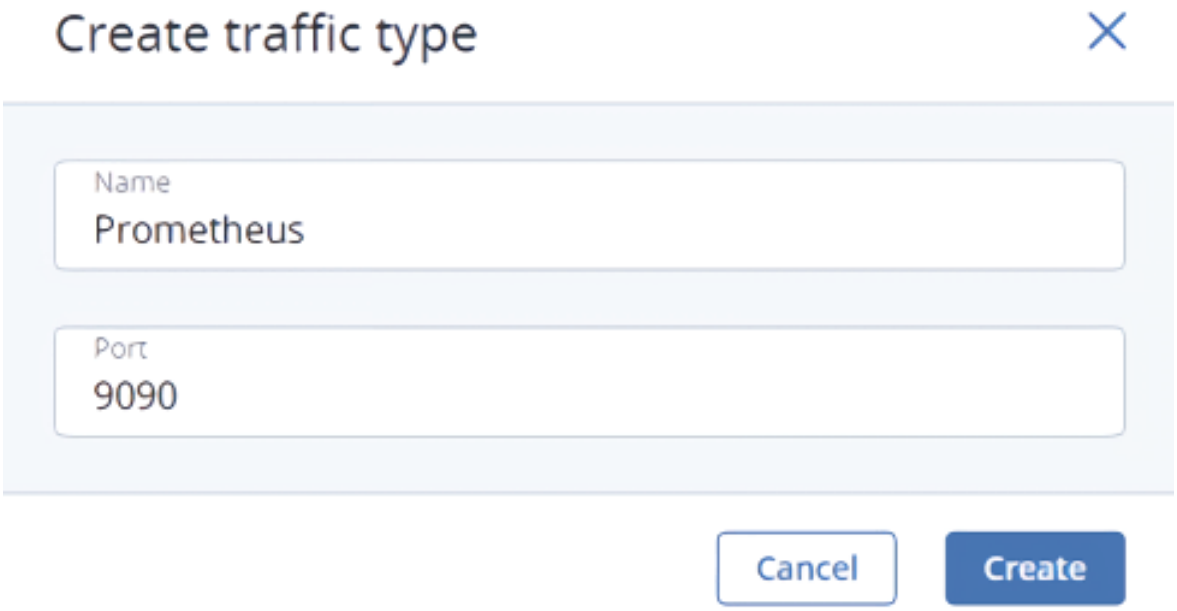


8.6.2 Использование внешнего Prometheus для мониторинга

Можно использовать федерацию Prometheus, чтобы собирать метрики со встроенного сервера Prometheus и сохранять их на внешнем сервере. Чтобы настроить федерацию, установите внешний сервер Prometheus, как описано в официальной документации, затем подключите его к своему кластеру через открытый порт API-интерфейса Prometheus.

Чтобы открыть порт для API-интерфейса Prometheus

1. На экране **Инфраструктура** > **Сети** нажмите **Изменить**, а затем **Создать тип трафика**.
2. В окне **Создать тип трафика** укажите пользовательское имя в поле **Имя** и **9090** в поле **Порт**. Затем нажмите кнопку **Создать**.



3. Нажмите **Назначить сетям** рядом с разделом **Пользовательские типы трафика**, затем добавьте созданный тип трафика во внешнюю сеть, установив соответствующий флажок.
4. Нажмите кнопку **Сохранить**, чтобы применить изменения.

Теперь можно подключиться к встроенному серверу Prometheus по адресу http://<admin_panel_IP_address>:9090.

Чтобы подключить ваш кластер к внешнему серверу Prometheus

На внешнем сервере Prometheus создайте файл конфигурации федерации. Например, он может быть следующим:

```
scrape_configs:
 - job_name: 'federate'
   scrape_interval: 15s

   honor_labels: true
   metrics_path: '/federate'

   params:
    'match[]':
     - '{job="ostor"}'
     - '{__name__=~"job:.*"}'

   static_configs:
    - targets:
     - '<admin_panel_IP_address>:9090'
```

где:

- metrics_path – это конечная точка сервера-источника Prometheus, с которого необходимо собирать метрики; /federate – это конечная точка по умолчанию для получения текущих значений выбранного временного ряда;
- honor_labels – это параметр выборки, который разрешает (false) или запрещает (true) перезапись любых меток, к которым предоставляет доступ сервер-источник Prometheus;
- match[] определяет временной ряд, из которого следует проводить выборку. Необходимо указать как минимум один параметр URL match[] и селектор моментального вектора, такой как up или {job="ostor"} для каждого из аргументов match[].

  В приведенном примере внешний сервер Prometheus будет собирать все ряды с меткой job="ostor" или именем метрики, которое начинается с job:.
- targets указывает на сервер-источник Prometheus.

8.6.3 Настройка политики хранения для метрик Prometheus

Сервис Prometheus, который используется для мониторинга кластера, работает и хранит данные на сервере управления. По умолчанию метрики Prometheus хранятся в течение семи дней. Этого срока хранения может быть недостаточно для поиска и устранения неисправностей. Срок можно увеличить в файле конфигурации Prometheus.

Однако при длительном сроке хранения может закончиться свободное пространство на корневом разделе, где хранятся данные. Во избежание этого можно указать максимальный размер для метрик Prometheus. Сначала будут удаляться самые старые данные.

Чтобы увеличить срок хранения

1. На сервере управления откройте для редактирования файл /etc/sysconfig/prometheus, задайте нужный срок хранения для параметра STORAGE_RETENTION и сохраните изменения, например:

   ```
   STORAGE_RETENTION="--storage.tsdb.retention.time=30d"
   ```

2. Перезапустите службу Prometheus:

   ```
   systemctl restart prometheus.service
   ```

Если для кластера хранилища включена высокая доступность, повторите эти шаги на двух других серверах управления.

Чтобы изменить политику хранения по времени на политику хранения по размеру

1. На сервере управления откройте для редактирования файл /etc/sysconfig/prometheus, измените флаг для параметра STORAGE_RETENTION и сохраните изменения, например:

   ```
   STORAGE_RETENTION="--storage.tsdb.retention.size=10GB"
   ```

2. Перезапустите службу Prometheus:

   ```
   systemctl restart prometheus.service
   ```

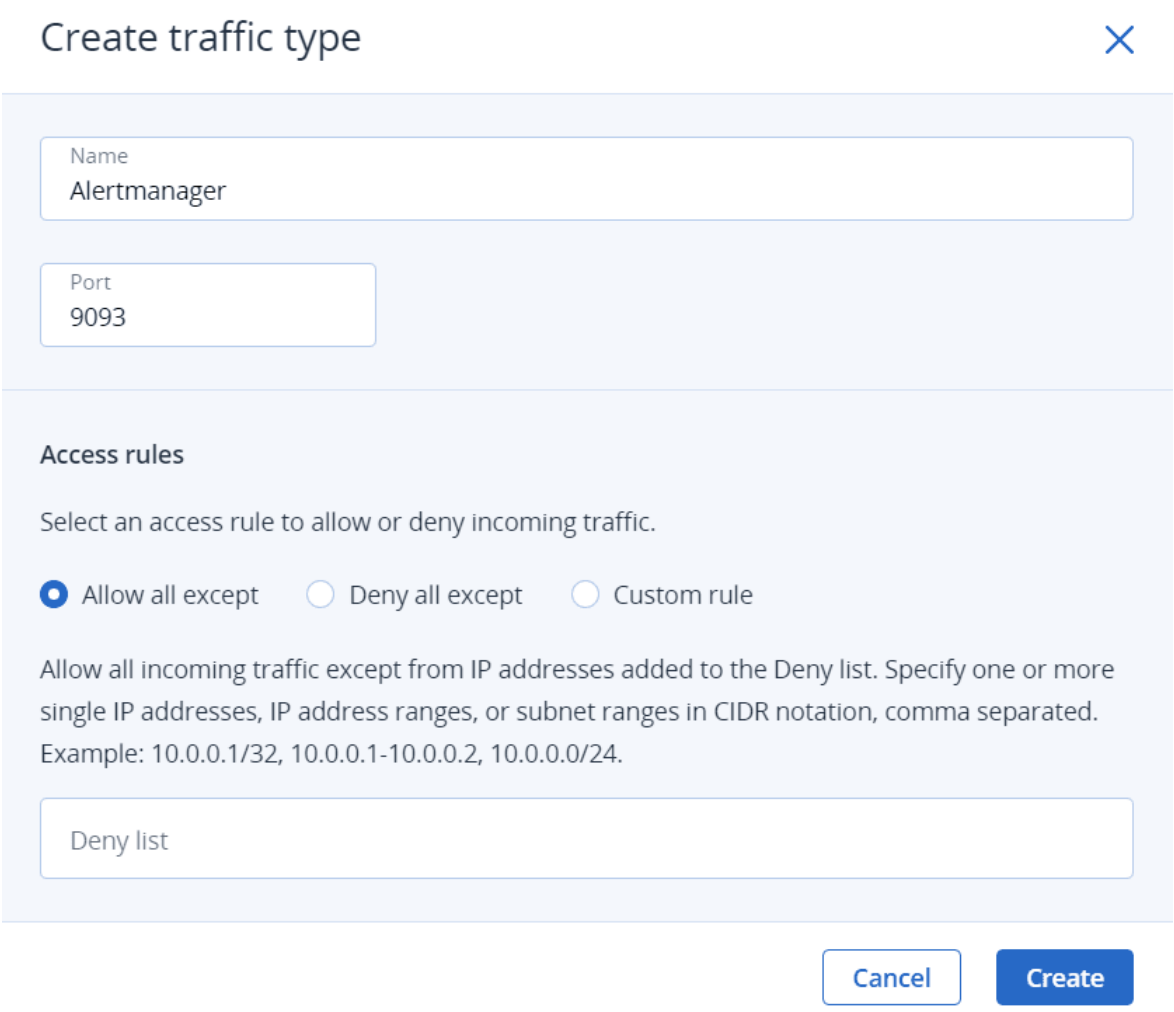
Если для кластера хранилища включена высокая доступность, повторите эти шаги на двух других серверах управления.

8.6.4 Использование Alertmanager для оповещений

Чтобы настроить встроенный Alertmanager для отправки оповещений, необходимо открыть TCP-порт для доступа к API-интерфейсу Alertmanager снаружи.

Чтобы открыть TCP-порт для доступа к API-интерфейсу Alertmanager

1. На экране **Инфраструктура** > **Сети** нажмите **Изменить**, а затем **Создать тип трафика**.
2. В окне **Создать тип трафика** укажите пользовательское имя в поле **Имя** и **9093** в поле **Порт**. Затем нажмите кнопку **Создать**.



3. Нажмите **Назначить сетям** рядом с разделом **Пользовательские типы трафика**, затем добавьте созданный тип трафика во внешнюю сеть, установив соответствующий флажок.
4. Нажмите кнопку **Сохранить**, чтобы применить изменения.

Теперь можно подключаться к API-интерфейсу Alertmanager по адресу http://<admin_panel_IP_address>:9093. Для получения подробной информации о настройке Alertmanager см. официальную документацию.

8.6.5 Метрики Prometheus

Кибер Инфраструктура использует в Prometheus три типа метрик:

- Метрики счетчиков (обычно с суффиксом _total) кумулятивны, и их значение растет со временем.
- Измерительные метрики отображают колеблющиеся значения.
- Метрики гистограмм кумулятивны и сохраняют измерения в различных корзинах в зависимости от измеряемого значения:
  - Метрики с суффиксом _bucket (корзина) показывают текущее значение для корзины.
  - Метрики с суффиксом _sum (сумма) показывают общую сумму всех значений для корзин.
  - Метрики с суффиксом _count (число) показывают количество сохраненных измерений на корзину.

8.6.5.1 Метрики основного хранилища

Метрики, используемые для мониторинга основного хранилища, настраиваются в правилах записи Prometheus, и их можно найти в следующих файлах на каждом из узлов в кластере:

- /var/lib/prometheus/rules/mdsd.rules
- /var/lib/prometheus/rules/csd.rules
- /var/lib/prometheus/rules/fused.rules
- /var/lib/prometheus/rules/rjournal.rules

Метрики, используемые для создания оповещений по основному хранилищу, добавляются в правила оповещений в файле /var/lib/prometheus/alerts/pcs.rules. Эти метрики описаны в следующей таблице.

Метрика	Описание
fused_stuck_reqs_30s	Количество запросов ввода-вывода, зависших на узле в течение более чем 30 секунд
fused_stuck_reqs_10s	Количество запросов ввода-вывода, зависших на узле в течение более чем 10 секунд
fused_maps_failed	Количество завершившихся сбоем запросов сопоставления на узле
fused_map_failures_total	Общее количество завершившихся сбоем запросов сопоставления на узле

Метрика	Описание
fused_unaligned_writes:rate5m	Количество невыровненных запросов записи в секунду за 5 минут
fused_writes:rate5m	Количество запросов записи в секунду за 5 минут
fused_unaligned_reads:rate5m	Количество невыровненных запросов чтения в секунду за 5 минут
fused_reads:rate5m	Количество запросов чтения в секунду за 5 минут
mdsd_cluster_replication_stuck_chunks	Количество фрагментов, блокирующих репликацию
mdsd_cluster_replication_touts_total	Общее количество фрагментов, замедляющих репликацию
job:mdsd_fs_chunk_maps:sum	Количество фрагментов в кластере хранилища
job:mdsd_fs_files:sum	Количество файлов в кластере хранилища
master:mdsd_cs_status	Статус сервиса фрагментов данных
mdsd_cluster_free_space_bytes	Объем свободного физического пространства в кластере хранилища
mdsd_cluster_space_bytes	Общий объем физического пространства в кластере хранилища
mdsd_is_master	Узел, на котором выполняется главный сервис метаданных
mdsd_master_uptime	Время непрерывной работы главного сервиса метаданных
instance_le:rjournal_commit_duration_seconds_bucket:rate5m	Текущая задержка фиксации для определенного сервиса метаданных в течение 5 минут, для каждой из корзин
instance_csid:csd_journal_usage_ratio:rate5m	Процент свободного пространства для журнала сервиса фрагментов за 5 минут
process_cpu_seconds_total	Суммарная длительность времени, в течение которого процесс использовал ЦП
process_swap_bytes	Объем пространства подкачки, используемого процессом

8.6.5.2 Метрики хранилища объектов

Метрики, используемые для мониторинга хранилища объектов, настраиваются в правилах записи Prometheus, и их можно найти в следующих файлах на каждом из узлов в кластере:

- /var/lib/prometheus/rules/s3.rules
- /var/lib/prometheus/rules/ostor.rules

Метрики, используемые для создания оповещений по хранилищу объектов, добавляются в правила оповещений в файле /var/lib/prometheus/alerts/s3.rules. Эти метрики описаны в следующей таблице:

Метрика	Описание
instance_vol_svc:ostor_s3gw_req:rate5m	Количество всех запросов за секунду для определенного сервиса шлюза S3 в течение 5 минут
instance_vol_svc:ostor_s3gw_req_cancelled:rate5m	Количество отмененных запросов за секунду для определенного сервиса шлюза S3 в течение 5 минут
instance_vol_svc:ostor_req_server_err:rate5m	Количество запросов, завершившихся сбоем с ошибкой сервера (код состояния 5XX) за секунду для определенного сервиса шлюза S3 в течение 5 минут
instance_vol_svc:ostor_s3gw_get_req_latency_ms_bucket:rate5m	Текущая задержка запросов GET для определенного шлюза S3 в течение 5 минут, для каждой из корзин
instance_vol_svc:ostor_commit_latency_us_bucket:rate5m	Текущая задержка фиксации в сервисе хранилища объектов в течение 5 минут, для каждой из корзин
instance_vol_svc_req:ostor_os_req_latency_ms_bucket:rate5m	Текущая задержка запросов для определенного сервиса OS в течение 5 минут, для каждой из корзин
instance_vol_svc_req:ostor_ns_req_latency_ms_bucket:rate5m	Текущая задержка запросов для определенного сервиса NS в течение 5 минут, для каждой из корзин
pcs_process_inactive_seconds_total	Суммарная длительность времени, в течение которого процесс был неактивен
process_cpu_seconds_total	Суммарная длительность времени, в течение которого процесс использовал ЦП
ostor_svc_start_failed_count_total	Общее количество неудавшихся попыток запустить сервис
ostor_svc_registry_cfg_failed_total	Общее количество неудавшихся попыток подключиться к сервису конфигурации

Метрики использования хранилища объектов корзинами и пользователями

Метрики использования хранилища объектов корзинами и пользователями выключены по умолчанию. Чтобы включить сбор этой статистики, выполните следующую команду на любом узле кластера S3:

```
# ostor-ctl set-vol -V 0100000000000002 --enable-stat
```

Следующие метрики появятся в Prometheus:

- account_control_buckets_size: Размер корзины в байтах
- account_control_user_size: Общий размер всех корзин пользователя в байтах

8.6.5.3 Метрики хранилища резервных копий

Метрики, используемые для мониторинга хранилища резервных копий, настраиваются в правилах записи Prometheus и находятся в файле /var/lib/prometheus/rules/abgw.rules на каждом узле кластера. Самые важные из этих метрик описаны в таблице ниже.

Метрика	Описание
Счетчики объектов FES	
abgw_ accounts	Количество учетных записей, с которыми хранилище резервных копий работает в настоящее время (то есть количество учетных записей с открытыми архивами резервных копий)
abgw_files	Количество архивов резервных копий, открытых в настоящее время. Архивы резервных копий открываются для чтения и записи только во время операции резервного копирования. Другие операции, такие как восстановление, просмотр и проверка, открывают архивы резервных копий только для чтения.
abgw_conns [proto]	Количество текущих соединений между хранилищем резервных копий и клиентами. Значение представляет собой набор счетчиков. Доступны подробные сведения о протоколе хранилища резервных копий (V1/V2).
Счетчики подключений	
abgw_conns_ total	Общее количество соединений между хранилищем резервных копий и клиентами с момента запуска сервиса
abgw_client_ conns_cur [name]	Количество клиентов, подключенных в настоящее время, с разделением по типам
abgw_client_ conns_total [name]	Общее количество клиентов с момента запуска сервиса с разделением по типам
Ошибки и сроки действия сертификатов	
abgw_verify_ certs_errors_ total[err]	Общее количество ошибок проверки сертификатов с момента запуска сервиса с разделением по типу ошибки
abgw_next_ certificate_ expiration [path]	Дата истечения срока действия сертификатов хранилища резервных копий
abgw_cert_	Количество неудачных попыток обновить список отзыва сертификатов. Этот список

Метрика	Описание
update_fail_total	требуется для правильного применения новой квоты в Кибер Бэкап Облачный, когда отзывается текущий сертификат клиента и запрашивается новый.
abgw_crl_download_fail_total	Количество неудачных попыток загрузить список отзыва сертификатов. Этот список требуется для правильного применения новой квоты в Кибер Бэкап Облачный, когда отзывается текущий сертификат клиента и запрашивается новый.
Гистограммы и счетчики запросов для протокола хранилища резервных копий V1	
abgw_read_reqs_total	Количество запросов на чтение с момента запуска сервиса
abgw_write_reqs_total	Количество запросов на запись с момента запуска сервиса
abgw_req_errs_total[req][err]	Набор ошибок запросов, с разделением по типу запроса и коду ошибки
abgw_req_latency_ms[req]	Гистограмма с задержкой запросов
Гистограммы и счетчики запросов для протокола хранилища резервных копий V2	
abgw_v2_ireq_errs_total[req][err]	Количество запросов на чтение с момента запуска сервиса
abgw_v2_ireq_latency_ms[req][lat]	Количество запросов на запись с момента запуска сервиса
abgw_v2_ereq_errs_total[req][err]	Набор ошибок запросов, с разделением по типу запроса и коду ошибки
abgw_v2_ereq_latency_ms[req][err]	Гистограмма с задержкой запросов
Счетчики байтов	
abgw_read_bytes_total[proxied]	Количество байтов, прочитанных с диска с момента запуска сервиса. Параметр proxied показывает данные, прочитанные через обратный прокси.
abgw_write_bytes_total	Количество байтов, записанных на диск с момента запуска сервиса. Параметр proxied показывает данные, записанные через обратный прокси.

Метрика	Описание
[proxied]	
abgw_write_rollback_bytes_total	Размер данных, перезаписанных хранилищем резервных копий по запросу клиента, когда хранилищу не удалось подтвердить клиенту, что данные уже записаны. Эта метрика используется только для протокола хранилища резервных копий V1 и старых клиентов резервного копирования.
Метрики операций с файлами и операций ввода-вывода	
abgw_file_lookup_errs_total[err]	Количество неудачных попыток открыть файлы или найти уже открытые файлы с разделением по коду ошибки
abgw_fop_latency_ms_bucket[fop][proxied][err]	Гистограмма с суммой задержки файловых операций с разделением по типу операции (чтение, запись, синхронизация, статистика), по использованию прокси, по номеру ошибки, а также другие файловые операции
abgw_iop_latency_ms_bucket[iop][proxied][err]	Гистограмма с задержкой операций ввода-вывода с разделением по типу операции, по использованию прокси и по номеру ошибки
abgw_io_limiting_failures_total[type]	Количество неудачных запросов ввода-вывода к хранилищу резервных копий с момента запуска сервиса вследствие низкой производительности базового хранилища
abgw_iop_wd_timeouts[iop]	Количество файловых операций, занимающих больше двух минут, с разделением по типу операции
Метрики миграции	
abgw_account_pull_errs_total[err]	Количество неудачных попыток целевого хранилища резервных копий получить список учетных записей из исходного хранилища перед началом миграции
abgw_nr_files_to_pull	Количество файлов для переноса из исходного хранилища резервных копий в целевое (включает все файлы, миграция которых не завершена)
abgw_pull_backlog_bytes	Количество байтов в исходном хранилище резервных копий, которые еще не перенесены в целевое хранилище
abgw_pull_progress_bytes_total	Количество байтов в целевом хранилище резервных копий, которые уже перенесены из исходного хранилища с момента запуска сервиса
abgw_file_	Количество неудачных попыток открыть файлы для миграции в исходном хранилище

Метрика	Описание
migration_ source_ open_errs_ total[err]	резервных копий с момента запуска сервиса
abgw_file_ migration_ source_read_ errs_total[err]	Количество неудачных попыток прочитать файлы для миграции в исходном хранилище резервных копий с момента запуска сервиса
Метрики хранилища объектов и георепликации	
abgw_push_ backlog_ bytes[ostor, replica]	Количество байтов для записи в целевое хранилище объектов или в подчиненный кластер в случае георепликации
abgw_push_ progress_ bytes_total [ostor, replica]	Количество байтов, записанных в целевое хранилище объектов или в подчиненный кластер в случае георепликации. Эта метрика помогает оценить скорость репликации или копирования данных.
abgw_push_ replica_errs_ total[err]	Количество неудачных попыток записать файлы в целевое хранилище объектов или в подчиненный кластер в случае георепликации с момента запуска сервиса с разделением по типу ошибки
abgw_ replica_ integrity_ checks_fail_ total	Количество поврежденных реплик в подчиненном кластере с момента запуска сервиса
abgw_file_ replica_auto_ errs_total[err]	Количество ошибок георепликации для новых файлов (созданных после настройки георепликации) с момента запуска сервиса с разделением по типу ошибки
abgw_file_ replica_ open_errs_ total[err]	Количество неудачных попыток главного кластера открыть файлы для записи в подчиненном кластере с момента запуска сервиса с разделением по коду ошибки
Метрики целевого хранилища объектов	
abgw_ostor_ used_space_ bytes	Размер пространства, занимаемого всеми архивами резервных копий, включая данные и неиспользуемое пространство, в целевом хранилище объектов
abgw_nr_	Количество файлов, которые хранилищу резервных копий не удалось открыть из-за

Метрика	Описание
ostor_ sequence_ mismatch_ total	несовпадения версий в целевом хранилище объектов
abgw_ostor_ garbage_ bytes	Размер неиспользуемого пространства внутри всех архивов резервных копий, которое еще не было физически очищено в целевом хранилище объектов
Результаты проверки архивов контейнера	
abgw_ containers_ validate_ segments_ fail_total	Количество архивов с ошибкой проверки (сегментов) в NFS и целевом хранилище объектов
abgw_ containers_ validate_ trees_fail_ total	Количество архивов с ошибкой проверки (деревьев) в NFS и целевом хранилище объектов
Другие метрики	
abgw_ append_ throttle_ delay_ms_ total	Общая сумма задержек, внедренных с момента запуска сервиса. Эта метрика помогает понять, включено ли регулирование для хранилища резервных копий.
abgw_iop_ ebusy	Количество ошибок ввода-вывода для операций открытия файлов с момента запуска сервиса

Метрики гистограммы с суффиксом _bucket имеют соответствующие метрики, заканчивающиеся на _sum и _counter, например:

- abgw_iop_latency_ms_bucket показывает текущее измерение для задержки операций ввода-вывода по отдельным корзинам
- abgw_iop_latency_ms_count показывает общую сумму всех измерений для задержки операций ввода-вывода по отдельным корзинам
- abgw_iop_latency_ms_sum показывает количество сохраненных измерений для задержки операций ввода-вывода по отдельным корзинам

8.6.5.4 Метрики обновления кластера

Метрики, используемые для создания оповещений об обновлениях ПО кластера, добавляются в правила оповещений в файле /var/lib/prometheus/alerts/backend.rules. Эти метрики описаны

в следующей таблице:

Метрика	Описание
softwareupdates_cluster_info	Статус обновлений ПО кластера
softwareupdates_cluster_ available	Наличие обновлений ПО кластера
softwareupdates_node_uptodate	Показывает, установлена ли самая последняя версия ПО на узле кластера
softwareupdates_node_available	Наличие обновлений ПО узла кластера
softwareupdates_node_info	Статус обновлений ПО узла кластера

8.7 Мониторинг хранилища резервных копий

После создания хранилища резервных копий его состояние можно отслеживать в окне **Сервисы хранилища** > **Резервное копирование** > **Сводка**. На диаграммах отображается следующая информация:

- **Серверы**. Диаграмма показывает количество и доступность серверов в кластере хранилища резервных копий.
- **Производительность**. Диаграмма показывает активность чтения и записи для сервисов хранилища резервных копий по времени.
- **Георепликация**. Диаграмма показывает скорость и остаток георепликации, то есть объем данных, которые еще не реплицированы. Если остаток не снижается со временем, это означает, что данные не удается реплицировать достаточно быстро. Причиной может быть недостаточная скорость передачи данных по сети, и может потребоваться проверить или обновить сетевое оборудование.
- **Задержка присоединения**. Диаграмма показывает время, потраченное на обработку запросов от агентов резервного копирования к хранилищу.
- **Регулировка присоединения**. Если диаграмма не пуста, значит, в базовом хранилище не хватает свободного пространства и хранилище резервных копий ограничивает пользовательские запросы для замедления потока данных.

  Два порога, мягкий и жесткий, устанавливаются для занятого пространства хранилища в процентах. При достижении мягкого порога хранилище резервных копий начинает ограничивать операции записи. Интенсивность ограничения зависит от использованного пространства и повышается до достижения жесткого порога. Когда занятое пространство достигает жесткого порога, ограничение начинает работать с максимальной интенсивностью. Значения порогов зависят от места назначения резервных копий и количества серверов в кластере хранилища.

Место назначения резервных копий	Количество серверов резервного копирования	Мягкий порог	Жесткий порог
Локальный кластер	1	93 %	95 %
	2+	90 %	92 %
NFS	1	93 %	95 %
Публичное облако	1	88 %	90 %
	2+	85 %	87 %

- **Объектное хранилище**. Диаграмма показывает скорость и остаток хранилища объектов, то есть объем данных, которые еще не загружены в публичное облако. Если остаток не снижается со временем, это означает, что данные не удается передать достаточно быстро. Причиной может быть недостаточная скорость передачи данных по сети, и может потребоваться проверить или обновить сетевое оборудование.

Также можно отслеживать состояние серверов хранилища резервных копий. Для этого перейдите в раздел **Сервисы хранилища** > **Резервное копирование** > **Серверы** и щелкните по нужному серверу. На вкладке **Сводка** на правой панели отображается статистика производительности.

- **ЦП/ОЗУ**: загрузка ЦП в процентах по времени и использование ОЗУ в ГиБ по времени
- **Частота успешных/неудачных запросов**: количество успешных и неудачных запросов на присоединение в секунду
- **Частота выходных/входных запросов**: количество запросов на чтение и запись в секунду
- **Пропускная способность**: объем данных, считываемых или записываемых в хранилище резервных копий в секунду
- **Задержка запросов**: время, потраченное на обработку запросов

8.7.1 Расширенный мониторинг Backup Gateway с помощью Grafana

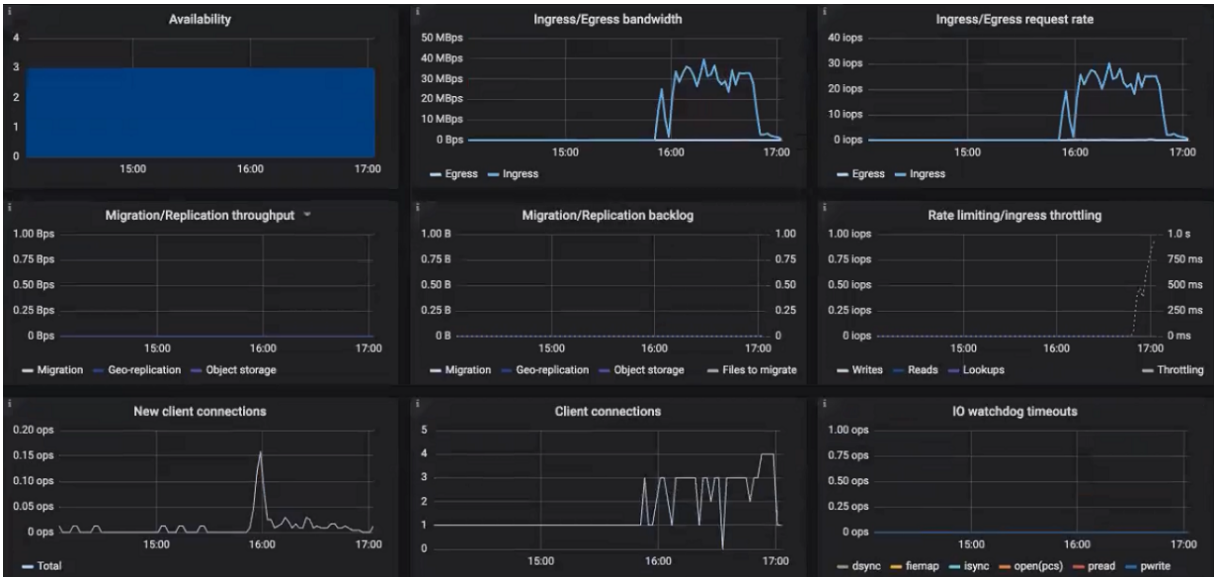
Для расширенного мониторинга кластера Backup Gateway перейдите на экран **Мониторинг** > **Обзор** и нажмите **Панель Grafana**. Откроется отдельная вкладка браузера с предварительно настроенными панелями Grafana, две из которых посвящены Cyber Backup Gateway. Чтобы просмотреть подробное описание каждой из диаграмм, щелкните по значку **i** в ее левом углу.

На панели **Cyber Backup Gateway** необходимо обратить внимание на следующие диаграммы:

- **Доступность**. Любой период времени, в течение которого шлюзы не были доступны, будет выделен красным. В этом случае необходимо просмотреть журналы на узлах с отказавшим сервисом и сообщить о проблеме. Чтобы просмотреть журнал Backup Gateway, воспользуйтесь следующей командой:

```
# zstdcat /var/log/vstorage/abgw.log.zst
```

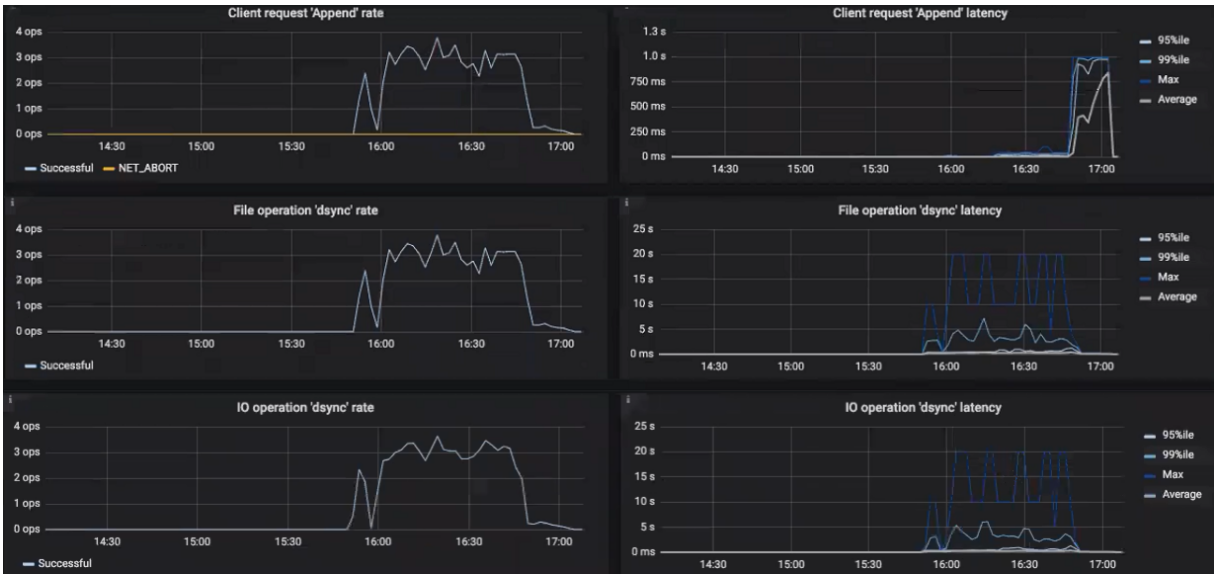
- **Пропускная способность миграции/репликации**. Диаграмма миграции должна отображаться во время миграции или в случае, если кластер служит главным в конфигурации георепликации. Диаграмма репликации должна зеркально отражать диаграмму входной пропускной способности.
- **Остаток миграции/репликации**. Диаграмма миграции со временем должна уменьшаться. Диаграмма репликации должна показывать значение около нуля, высокие значения указывают на проблемы с сетью.
- **Ограничение скорости или входное регулирование**. Если диаграмма не пуста, это означает, что в базовом хранилище не хватает свободного пространства и Backup Gateway ограничивает частоту пользовательских запросов для замедления потока данных. Добавьте дополнительное дисковое пространство в кластер, чтобы разрешить эту проблему. Дополнительные сведения см. в статье Добавление регулирования для установок ABGW с хранилищем в публичном облаке.
- **Новые клиентские подключения**. Высокая доля неудачных подключений из-за проблем верификации SSL-сертификатов означает, что клиенты передали недействительную цепочку сертификатов.
- **Превышения времени ожидания сторожа ввода-вывода**. Если диаграмма не пуста, это значит, что базовое хранилище испытывает неполадки и не может обеспечивать требуемую производительность.



Чтобы просмотреть диаграммы для определенного клиентского запроса, файла и операции ввода-вывода, выберите их из раскрывающихся меню выше. Высокая доля сбойных запросов или операций и высокие значения задержки в этих диаграммах указывают, что на Backup Gateway происходят проблемы, о которых необходимо сообщить. Например, можно проверить диаграммы для запроса «Присоединить».

- Диаграмма **Скорость присоединения** отображает поток данных резервных копий от агентов резервного копирования к хранилищу в операциях в секунду (одна операция равна одному большому блоку данных резервной копии; блоки могут быть разного размера).

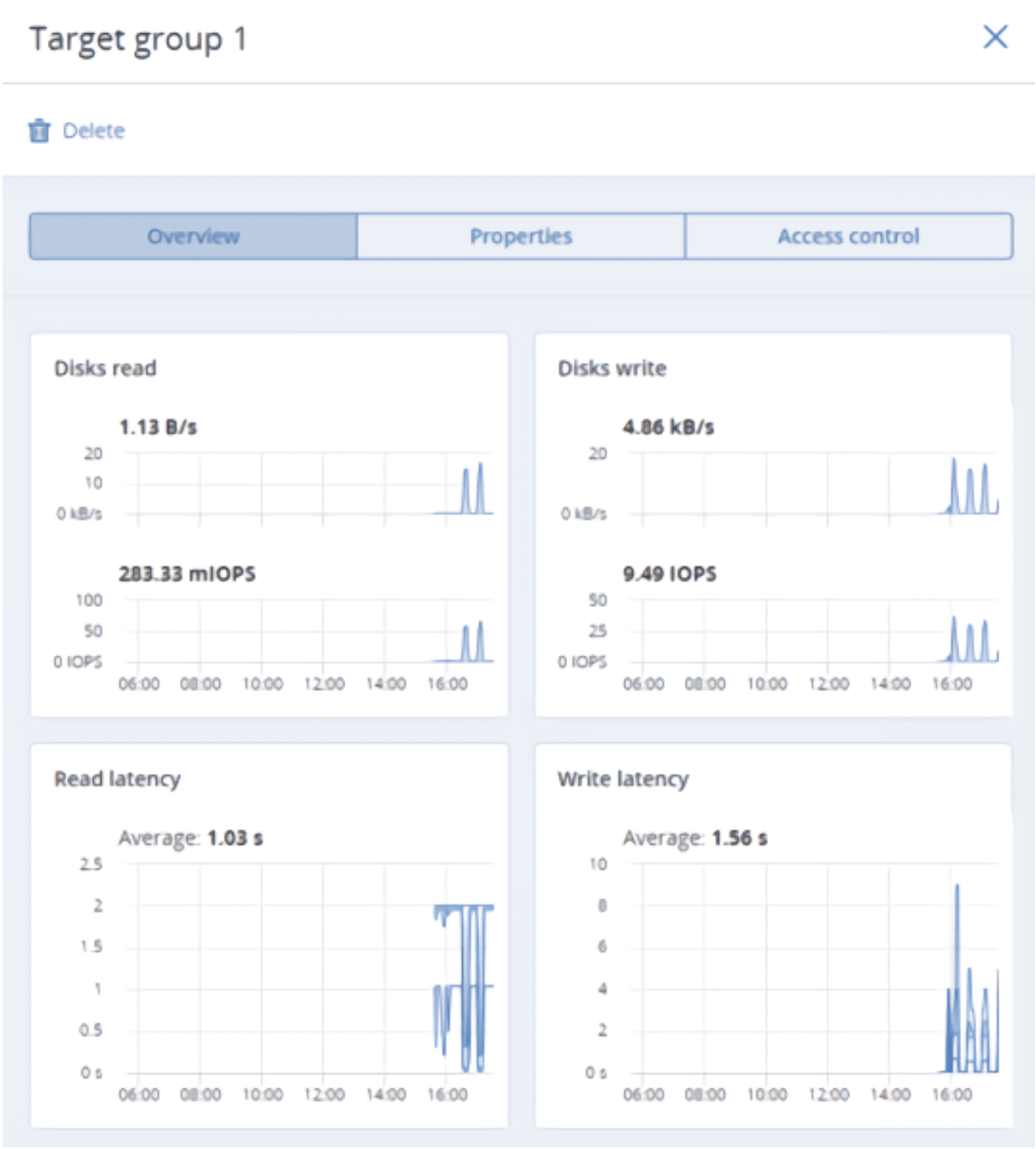
- Диаграмма **Задержка присоединения** показывает время, потраченное на обработку запросов, и должна в среднем показывать несколько десятков миллисекунд с пиковыми значениями ниже одной секунды.



Панель **Сведения об Cyber Backup Gateway** предназначена для низкоуровневого устранения неполадок службой поддержки. Для мониторинга отдельного узла, клиентского запроса, файла и операции ввода-вывода выберите их в раскрывающихся меню выше. На панели можно убедиться, что диаграмма **Неактивность цикла событий** пуста. Если это не так, то Backup Gateway на этом узле испытывает неполадки и о проблеме необходимо сообщить.

8.8 Мониторинг блочного хранилища

После создания группы целевых устройств ее состояние можно отслеживать на вкладке **Сводка**. Диаграммы показывают активность ввода-вывода чтения и записи, а также задержку по всем LUN, присоединенным к группе.

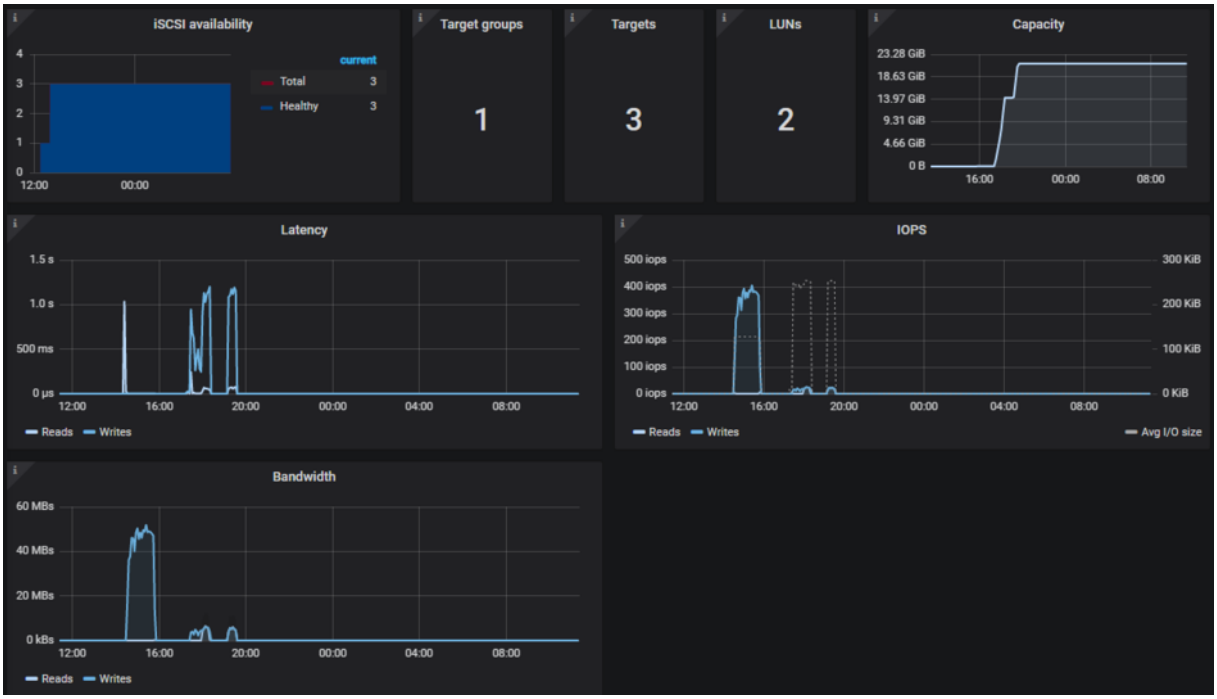


8.8.1 Расширенный мониторинг iSCSI с помощью Grafana

Для расширенного мониторинга групп целевых устройств перейдите на экран **Мониторинг** > **Обзор** и нажмите **Панель Grafana**. Откроется отдельная вкладка браузера с предварительно настроенными панелями Grafana, две из которых посвящены сервису iSCSI. Чтобы просмотреть подробное описание каждой из диаграмм, щелкните по значку **i** в ее левом верхнем углу.

На панели мониторинга **Обзор iSCSI** обратите внимание на следующие диаграммы:

- **Доступность iSCSI**. Диаграмма показывает доступность целевых устройств. Период времени, в течение которого они не были доступны, будет выделен красным. В таком случае проверьте журнал /var/log/vstorage/iscsi/vstorage-target-monitor.log на узлах с отказавшим сервисом и сообщите о проблеме.
- **Задержка**. Диаграмма показывает время, затраченное на операции ввода-вывода чтения и записи по всем устройствам iSCSI LUN. В среднем должно отображаться несколько десятков миллисекунд с пиковыми значениями ниже 1 секунды.



Панель мониторинга **Сведения iSCSI** предназначена для поиска и устранения неисправностей сотрудниками технической поддержки. Для мониторинга определенной группы целевых устройств, отдельного целевого устройства, сеанса или LUN выберите их в раскрывающемся списке выше.

8.9 Мониторинг хранилища объектов

Работу кластера S3 и его компонентов можно отслеживать на экране **Сервисы хранилища** > **S3** > **Сводка** с помощью следующих диаграмм:

- **Доступность** сервисов NS, OS и GW. Если сервис S3 GW имеет статус «ошибка», то, скорее всего, узел, на котором он размещен, не работает. Это некритично для кластера S3, поскольку высокая доступность сервиса S3 основана на записях DNS. Если записи DNS правильно настроены, сервис S3 остается полностью доступен через клиенты S3. С другой стороны, сбой сервиса OS или NS является критичным, поскольку в этом случае весь кластер S3 не сможет правильно работать. Если вы видите, что некоторые из сервисов NS или OS недоступны, но при этом все серверы кластера исправны и сеть с типом трафика **OSTOR внутр.** работает нормально, обратитесь в техническую поддержку. Также можно попытаться выяснить причины сбоя через панели мониторинга Grafana.
- **Частота операций**. Диаграмма показывает общую загрузку кластера запросами пользователей S3, включая все типы операций.
- **Частота сбоев запросов**. Запросы формируются пользователями или их приложениями. Некоторые запросы невозможно обработать. Например, они могут запрашивать несуществующие объекты, иметь неправильные права доступа или использовать неподдерживаемые функции (см. раздел "Поддерживаемые функции Amazon S3" на странице 395). Поэтому нормально, если ошибки составляют небольшую часть общего объема операций. Но это также может указывать на неправильную работу приложения S3, которое используется для доступа. Кроме того, если кластер S3 открыт для публичного доступа, его могут сканировать роботы поисковых систем. В этом случае резкие скачки количества ошибок будут отражать их проблемы с несоответствием прав доступа. Однако это не является критической проблемой для кластера.
- **Пропускная способность**. Диаграмма показывает общую загрузку кластера запросами пользователей S3.
- **Задержка PUT** и **Задержка GET**. Эти значения измеряются с момента получения последнего байта пользовательского запроса до момента отправки первого байта ответа.

8.9.1 Расширенный мониторинг кластера S3 с помощью Grafana

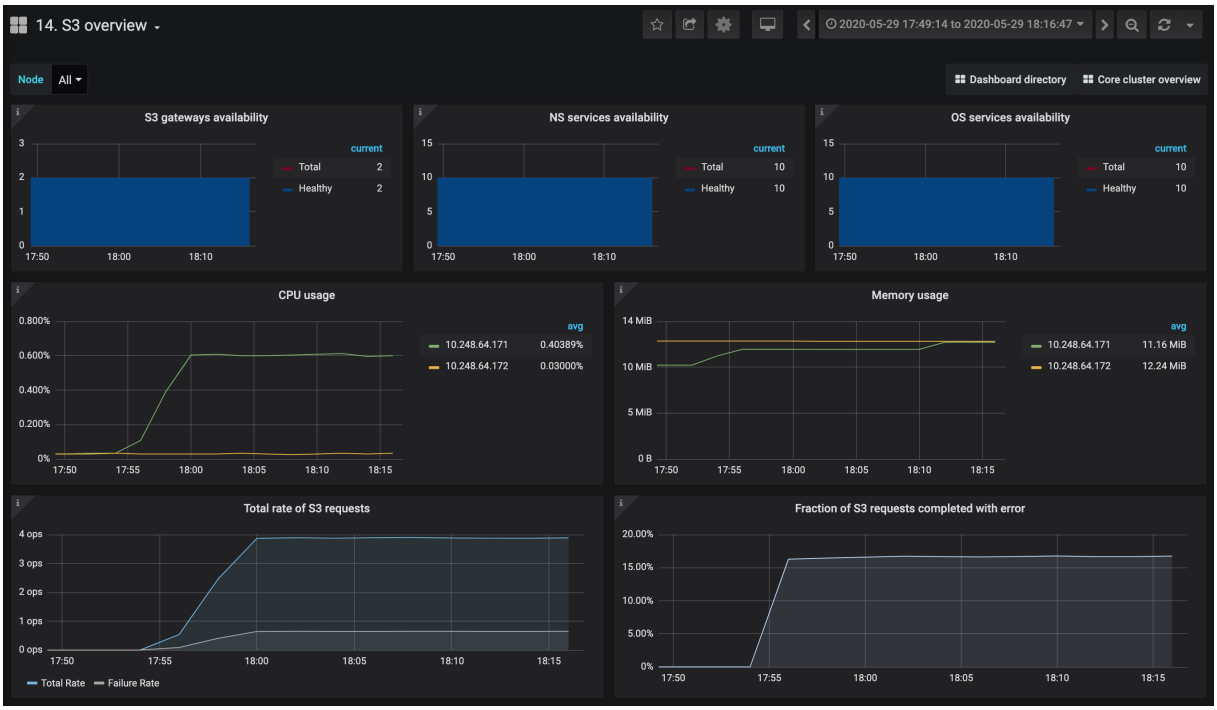
Для расширенного мониторинга кластера S3 перейдите на страницу **Сервисы хранилища** > **S3** > **Сводка** и нажмите **Панель Grafana**. Откроется отдельная вкладка браузера с предварительно настроенными панелями Grafana. Чтобы просмотреть подробное описание каждой диаграммы, щелкните по значку **i** в ее левом углу.

Для детального мониторинга сервисов OS и NS используйте панели **Обзор объектного хранилища**, **Сведения о сервисе OS (object server)** и **Сведения о сервисе NS (name server)**. Отфильтруйте данные по серверам и томам, чтобы выявить аномальное использование сервиса. Обратите внимание на диаграмму **Задержки заданий**: она показывает долю времени,

потраченного на ожидание ЦП, доступной памяти (отъема), переноса памяти из файла подкачки и завершения операций ввода-вывода.

Панель мониторинга **Обзор S3** показывает главным образом информацию о сервисе S3 GW. Здесь можно отслеживать работу объектного хранилища и интерфейса S3 с помощью следующих диаграмм:

- **Доступность шлюзов S3**, **Доступность сервисов NS** и **Доступность сервисов OS**. Диаграммы показывают информацию о соответствующих сервисах S3. Период времени, в течение которого они не были доступны, выделен красным.
- **Задержка GET** и **Задержка PUT**. Диаграмма показывает среднюю задержку и 95-й, 99-й и максимальный перцентиль задержки запросов S3 GET и PUT. Это значение измеряется с момента получения последнего байта запроса до момента отправки первого байта ответа.
- **Пропускная способность**. Диаграмма показывает общий объем операций чтения или записи, проходящих через все шлюзы S3, в секунду.
- **Частота операций**. Диаграмма показывает общее количество операций S3 GET, PUT, LIST и DELETE в секунду по всем шлюзам S3.



Панель мониторинга **Обзор георепликации S3** предназначена для отслеживания репликации данных по нескольким географически распределенным ЦОД.

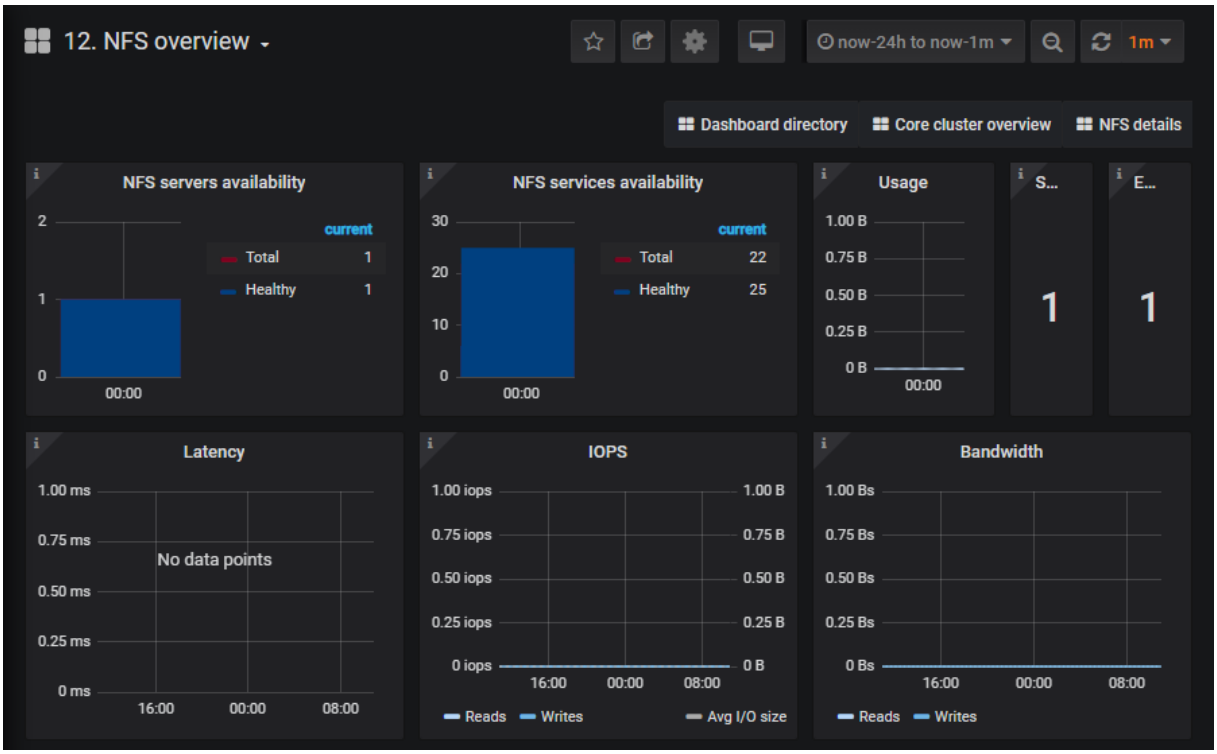
- Здесь самыми важными диаграммами являются **Остаток репликации** и **Глубина очереди репликации**. Если значения постоянно растут, то эффективность репликации падает. Это значит, что кластер получает больше данных, чем отправляет.
- **Частота ошибок локального S3** и **Частота ошибок удаленного S3** помогают обнаружить проблемы подключения. Небольшое количество ошибок возможно, если кластеры реплицируются через Интернет с нестабильной задержкой.

8.10 Мониторинг файлового хранилища

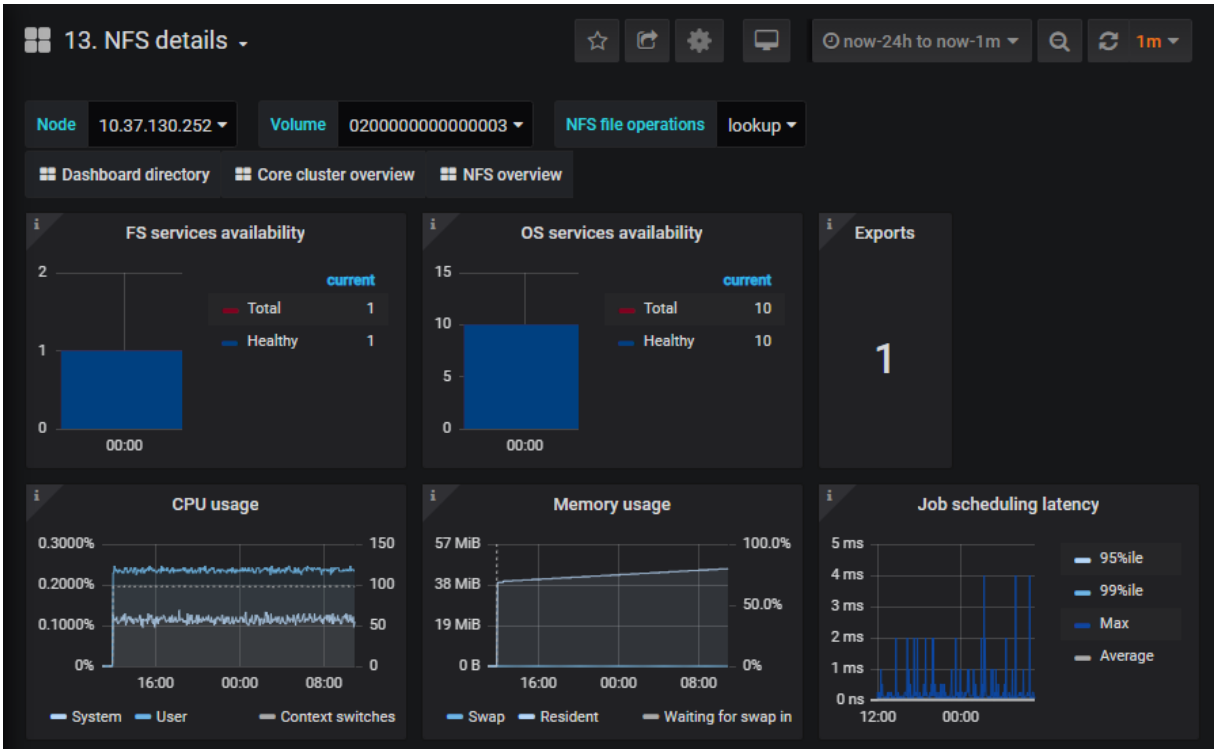
Для расширенного мониторинга узлов, сервисов и томов NFS перейдите на экран **Мониторинг** > **Обзор** и нажмите **Панель Grafana**. Откроется отдельная вкладка браузера с предварительно настроенными панелями Grafana, три из которых посвящены сервису NFS. Чтобы просмотреть подробное описание каждой из диаграмм, щелкните по значку **i** в ее левом верхнем углу.

На панели мониторинга **Обзор NFS** обратите внимание на следующие диаграммы:

- **Доступность серверов NFS**. Диаграмма показывает доступность хостов NFS. Период времени, в течение которого они не были доступны, будет выделен красным. В этом случае проверьте журналы /var/log/ganesha/ganesha.log и /var/log/ostor/ostorfs.log на этих узлах и сообщите о проблеме.
- **Доступность сервисов NFS**. Диаграмма показывает доступность сервисов файловой и операционной систем, которые использует NFS. Период времени, в течение которого они не были доступны, будет выделен красным. В этом случае проверьте журналы /var/log/ostor/FS-* и /var/log/ostor/OS-* на соответствующих узлах и сообщите о проблеме.
- **Задержка**. Диаграмма показывает среднюю задержку операций чтения и записи по всем томам NFS.
- **IOPS**. Диаграмма показывает общее количество операций чтения и записи, а также среднее число операций ввода-вывода в секунду по всем томам NFS.
- **Пропускная способность**. Диаграмма показывает общий объем считываемых или записываемых данных в секунду по всем томам NFS.



Панель мониторинга **Сведения о NFS** предназначена для мониторинга отдельных узлов, томов и файловых операций NFS.



Панель мониторинга **Сведения о ФС объектного хранилища** предназначена для мониторинга данных по определенным файловым сервисам.

8.11 Мониторинг вычислительного кластера

После создания вычислительного кластера можно отслеживать его состояние и статистику. Также можно отслеживать состояние отдельных вычислительных узлов, виртуальных машин и балансировщиков нагрузки.

Чтобы отобразить статус вычислительного кластера

Щелкните по имени кластера в нижней части левого меню. Статус может иметь следующие значения:

Исправен

Все компоненты и узлы вычислительного кластера работают нормально.

Настраивается

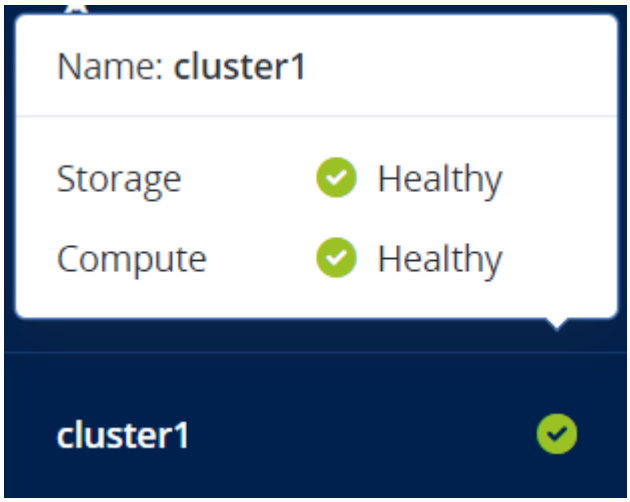
Конфигурация вычислительного кластера (модель ЦП по умолчанию для виртуальных машин или количество вычислительных узлов) изменяется.

Предупреждения

Вычислительный кластер работает нормально, но обнаружены некоторые неполадки.

Критические

В вычислительном кластере возникла критическая проблема, и он неработоспособен.



Чтобы отобразить статистику вычислительного кластера

Панель администратора

Перейдите на экран **Вычисления** > **Обзор**. На диаграммах отображаются сведения об использовании ЦП, ОЗУ и хранилища, количество виртуальных машин, сгруппированных по статусу и потреблению ресурсов, а также оповещения, связанные с вычислениями.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute stat
```

Например:

```
# vinfra service compute stat
+----------+-----------------------------------------------+
| Field    | Value                                         |
+----------+-----------------------------------------------+
| compute  | block_capacity: 74088185856                   |
|          | block_usage: 143654912                        |
|          | cpu_allocation_ratio: 8                       |
|          | cpu_usage: 0.16                               |
|          | ram_allocation_ratio: 1.0                     |
|          | vcpus: 2                                      |
|          | vcpus_free: 38                                |
|          | vm_mem_capacity: 42177212416                  |
|          | vm_mem_free: 37882245120                      |
|          | vm_mem_reserved: 4294967296                   |
|          | vm_mem_usage: 2773532672                      |
| datetime | 2021-11-08T15:29:23.388823                    |
| fenced   | physical_cpu_cores: 0                         |
|          | physical_cpu_usage: 0                         |
|          | physical_mem_total: 0                         |
|          | reserved_memory: 0                            |
|          | vcpus: 0                                      |
|          | vm_mem_capacity: 0                            |
| physical | block_capacity: 675644723200                  |
|          | block_free: 611533008896                      |
|          | cpu_cores: 12                                 |
|          | cpu_usage: 8.56                               |
|          | mem_total: 75331043328                        |
|          | vcpus_total: 96                               |
| reserved | cpus: 7                                       |
|          | memory: 33153830912                           |
|          | vcpus: 56                                     |
| servers  | count: 2                                      |
|          | error: 0                                      |
|          | in_progress: 0                                |
|          | running: 2                                    |
|          | stopped: 0                                    |
|          | top:                                          |
|          |   disk:                                       |
|          |   - id: d634179b-0730-4154-bc96-6fa4eb0cee78 |
|          |     name: vm-qcow                             |
|          |     size: 139460608                           |
|          |   - id: 192a2590-06d4-4c63-a84c-36c9de4e3c97 |
|          |     name: vm-iso                              |
|          |     size: 4194304                             |
|          |   memory:                                     |
|          |   - id: 192a2590-06d4-4c63-a84c-36c9de4e3c97 |
|          |     name: vm-iso                              |
```

```
|        |   size: 2244247552                    |
|        | - id: d634179b-0730-4154-bc96-6fa4eb0cee78 |
|        |   name: vm-qcow                       |
|        |   size: 529285120                     |
|        | vcpus:                                |
|        | - count: 0.01                         |
|        |   id: d634179b-0730-4154-bc96-6fa4eb0cee78 |
|        |   name: vm-qcow                       |
|        | - count: 0.01                         |
|        |   id: 192a2590-06d4-4c63-a84c-36c9de4e3c97 |
|        |   name: vm-iso                        |
+----------+-----------------------------------------+
```

8.11.1 Диаграмма «Выделено вЦП»

На этой диаграмме показано резервирование виртуальных ЦП в вычислительном кластере. Резервирование виртуальных ЦП представляет гарантированное количество ЦП, выделяемых сервису или виртуальной машине. Доступна следующая статистика:

Всего

Общее количество виртуальных ЦП в вычислительном кластере. Это произведение числа физических ЦП на всех вычислительных узлах и коэффициента перераспределения.

Система

Количество виртуальных ЦП, зарезервированных под систему и сервисы хранилища на всех узлах в вычислительном кластере. Подробнее о резервировании ЦП для различных сервисов см. в разделе "Требования к серверу" на странице 46.

ВМ

Количество виртуальных ЦП, выделенных для всех виртуальных машин в вычислительном кластере.

Свободно

Количество свободных виртуальных ЦП на всех узлах в вычислительном кластере.

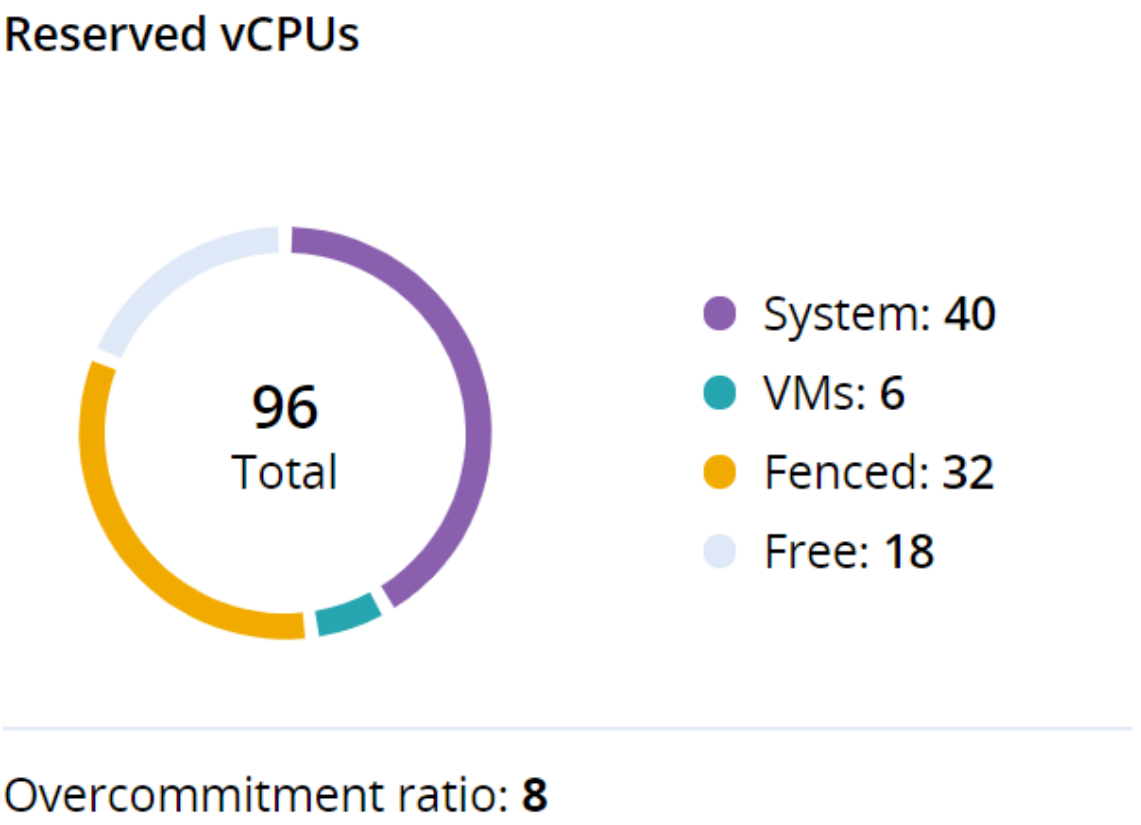
Огражден

Количество виртуальных ЦП на всех огражденных узлах в вычислительном кластере.

Коэффициент перераспределения

Соотношение количества виртуальных ЦП к физическим.

Этот параметр задается в файле /etc/kolla/nova-compute/nova.conf. Его можно изменить с помощью команды vinfra service compute set --nova-compute-cpu-allocation-ratio <value> (см. раздел "Изменение параметров в файлах конфигурации OpenStack" на странице 429).



Подобная диаграмма доступна для каждого отдельного узла в вычислительном кластере.

8.11.2 Диаграмма «Выделено ОЗУ»

На этой диаграмме показано резервирование ОЗУ в вычислительном кластере. Резервирование ОЗУ представляет гарантированный объем памяти, выделяемый службе или виртуальной машине. Доступна следующая статистика:

Всего

Общий объем ОЗУ на всех узлах в вычислительном кластере. Это произведение общего объема физического ОЗУ на всех вычислительных узлах и коэффициента перераспределения.

Система

Объем ОЗУ, зарезервированный под систему и службы хранилища на всех узлах в вычислительном кластере. Подробнее о резервировании ОЗУ для различных служб см. в разделе "Требования к серверу" на странице 46.

Система hugepages

Объем ОЗУ, зарезервированный под DPDK на всех узлах в вычислительном кластере. Эта память используется для обеспечения работы DPDK и не выделяется виртуальным машинам.

ВМ

Объем ОЗУ, выделенный на всех узлах в вычислительном кластере для виртуальных машин, которые используют стандартные страницы памяти.

ВМ с hugepages

Объем ОЗУ, выделенный на всех узлах в вычислительном кластере для виртуальных машин, которые используют большие страницы памяти. Страницы такого типа используются виртуальными машинами, подключенными к быстрой сети DPDK.

Свободно

Объем ОЗУ, доступный на всех узлах в вычислительном кластере для выделения виртуальным машинам, использующим стандартные страницы памяти.

Свободно hugepages

Объем ОЗУ, доступный на всех узлах в вычислительном кластере для выделения виртуальным машинам, использующим большие страницы памяти. Страницы такого типа используются виртуальными машинами, подключенными к быстрой сети DPDK.

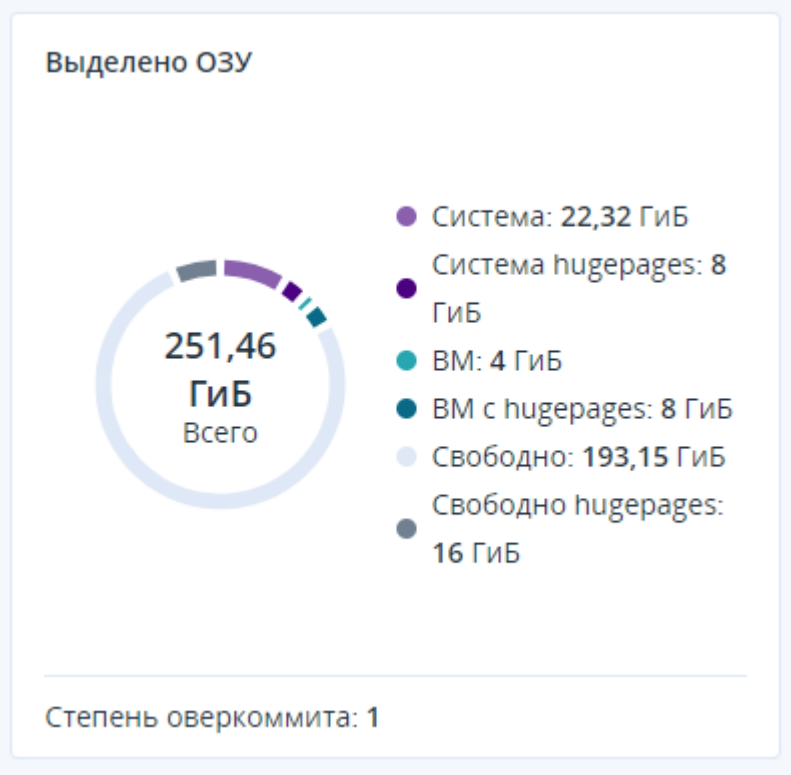
Огражден

Объем ОЗУ на всех огражденных узлах в вычислительном кластере.

Коэффициент перераспределения

Соотношение максимального объема резервируемого ОЗУ к объему физического ОЗУ.

Этот параметр задается в файле /etc/kolla/nova-compute/nova.conf. Его можно изменить с помощью команды vinfra service compute set --nova-compute-ram-allocation-ratio <value> (см. раздел "Настройка памяти для виртуальных машин" на странице 432).



Подобная диаграмма доступна для каждого отдельного узла в вычислительном кластере.

Просмотр подробных сведений о резервировании ОЗУ

- Для вывода сведений о резервировании ОЗУ для всех узлов кластера используйте следующую команду:

  ```
  vinfra node ram-reservation list [--long]
  ```

  --long

  Включение доступа и перечисления для всех полей объектов.

  Например, чтобы вывести список всех узлов кластера со сведениями о резервировании ОЗУ для них, выполните:

  ```
  # vinfra node ram-reservation list -c host -c reservations -c total
  +---------------+-----------------------------------------------------------+--------+
  | host          | reservations                                              | total  |
  +---------------+-----------------------------------------------------------+--------+
  | node001.<...> | - reserved_ram_mb: 3750                                   | 17978  |
  |               |   service_name: file_cache                                |        |
  |               |   slice_name: ''                                          |        |
  |               | - reserved_ram_mb: 1024                                   |        |
  |               |   service_name: fuse                                      |        |
  |               |   slice_name: system.slice                                |        |
  |               | - reserved_ram_mb: 1024                                   |        |
  |               |   service_name: management                                |        |
  |               |   slice_name: system.slice                                |        |
  |               | - reserved_ram_mb: 512                                    |        |
  |               |   service_name: user                                      |        |
  |               |   slice_name: user.slice                                  |        |
  |               | - reserved_ram_mb: 7700                                   |        |
  |               |   service_name: compute                                   |        |
  |               |   slice_name: vstorage.slice/vstorage-compute.slice       |        |
  |               | - reserved_ram_mb: 2048                                   |        |
  |               |   service_name: cses                                      |        |
  |               |   slice_name: vstorage.slice/vstorage-services.slice      |        |
  |               | - reserved_ram_mb: 256                                    |        |
  |               |   service_name: mdses                                     |        |
  |               |   slice_name: vstorage.slice/vstorage-services.slice      |        |
  |               | - reserved_ram_mb: 128                                    |        |
  |               |   service_name: agent                                     |        |
  |               |   slice_name: vstorage.slice/vstorage-ui.slice            |        |
  |               | - reserved_ram_mb: 1536                                   |        |
  |               |   service_name: management                                |        |
  |               |   slice_name: vstorage.slice/vstorage-ui.slice            |        |
  | <...>         |                                                           |        |
  +---------------+-----------------------------------------------------------+--------+
  ```

- Для вывода сведений о резервировании ОЗУ для одного узла кластера используйте следующую команду:

```
vinfra node ram-reservation show <node>
```

<node>

Идентификатор сервера или имя хоста.

Например, чтобы вывести подробные сведения о резервировании ОЗУ для сервера с идентификатором ed39298c-dc1f-f057-0b78-bcf4281eda73, выполните:

```
# vinfra node ram-reservation show ed39298c-dc1f-f057-0b78-bcf4281eda73
+--------------+-----------------------------------------------------+
| Field        | Value                                               |
+--------------+-----------------------------------------------------+
| host         | node001.vstoragedomain                              |
| id           | ed39298c-dc1f-f057-0b78-bcf4281eda73                |
| reservations | - reserved_ram_mb: 3749                             |
|              |   service_name: file_cache                          |
|              |   slice_name: ''                                    |
|              | - reserved_ram_mb: 1024                             |
|              |   service_name: fuse                                |
|              |   slice_name: system.slice                          |
|              | - reserved_ram_mb: 1024                             |
|              |   service_name: management                          |
|              |   slice_name: system.slice                          |
|              | - reserved_ram_mb: 512                              |
|              |   service_name: user                                |
|              |   slice_name: user.slice                            |
|              | - reserved_ram_mb: 7700                             |
|              |   service_name: compute                             |
|              |   slice_name: vstorage.slice/vstorage-compute.slice |
|              | - reserved_ram_mb: 2048                             |
|              |   service_name: cses                                |
|              |   slice_name: vstorage.slice/vstorage-services.slice |
|              | - reserved_ram_mb: 256                              |
|              |   service_name: mdses                               |
|              |   slice_name: vstorage.slice/vstorage-services.slice |
|              | - reserved_ram_mb: 128                              |
|              |   service_name: agent                               |
|              |   slice_name: vstorage.slice/vstorage-ui.slice      |
|              | - reserved_ram_mb: 1536                             |
|              |   service_name: management                          |
|              |   slice_name: vstorage.slice/vstorage-ui.slice      |
| total        | 17977                                               |
+--------------+-----------------------------------------------------+
```

- Для вывода общих сведений о резервировании ОЗУ в кластере используйте следующую команду:

```
vinfra node ram-reservation total
```

Например:

```
# vinfra node ram-reservation total
+--------------+-----------------------------------------------------+
| Field        | Value                                               |
+--------------+-----------------------------------------------------+
| reservations | - reserved_ram_mb: 11868                            |
|              |   service_name: file_cache                          |
|              |   slice_name: ''                                    |
|              | - reserved_ram_mb: 4096                             |
|              |   service_name: fuse                                |
|              |   slice_name: system.slice                          |
|              | - reserved_ram_mb: 1024                             |
|              |   service_name: management                          |
|              |   slice_name: system.slice                          |
|              | - reserved_ram_mb: 2048                             |
|              |   service_name: user                                |
|              |   slice_name: user.slice                            |
|              | - reserved_ram_mb: 9760                             |
|              |   service_name: compute                             |
|              |   slice_name: vstorage.slice/vstorage-compute.slice |
|              | - reserved_ram_mb: 7168                             |
|              |   service_name: cses                                |
|              |   slice_name: vstorage.slice/vstorage-services.slice |
|              | - reserved_ram_mb: 1024                             |
|              |   service_name: mdses                               |
|              |   slice_name: vstorage.slice/vstorage-services.slice |
|              | - reserved_ram_mb: 512                              |
|              |   service_name: agent                               |
|              |   slice_name: vstorage.slice/vstorage-ui.slice      |
|              | - reserved_ram_mb: 1536                             |
|              |   service_name: management                          |
|              |   slice_name: vstorage.slice/vstorage-ui.slice      |
| total        | 39036                                               |
+--------------+-----------------------------------------------------+
```

8.11.3 Диаграмма «Выделено хранилища»

На этой диаграмме отображается использование пространства хранилища вычислительным кластером. Доступна следующая статистика:

Всего

Общий размер томов, выделенных в вычислительном кластере.

Используется

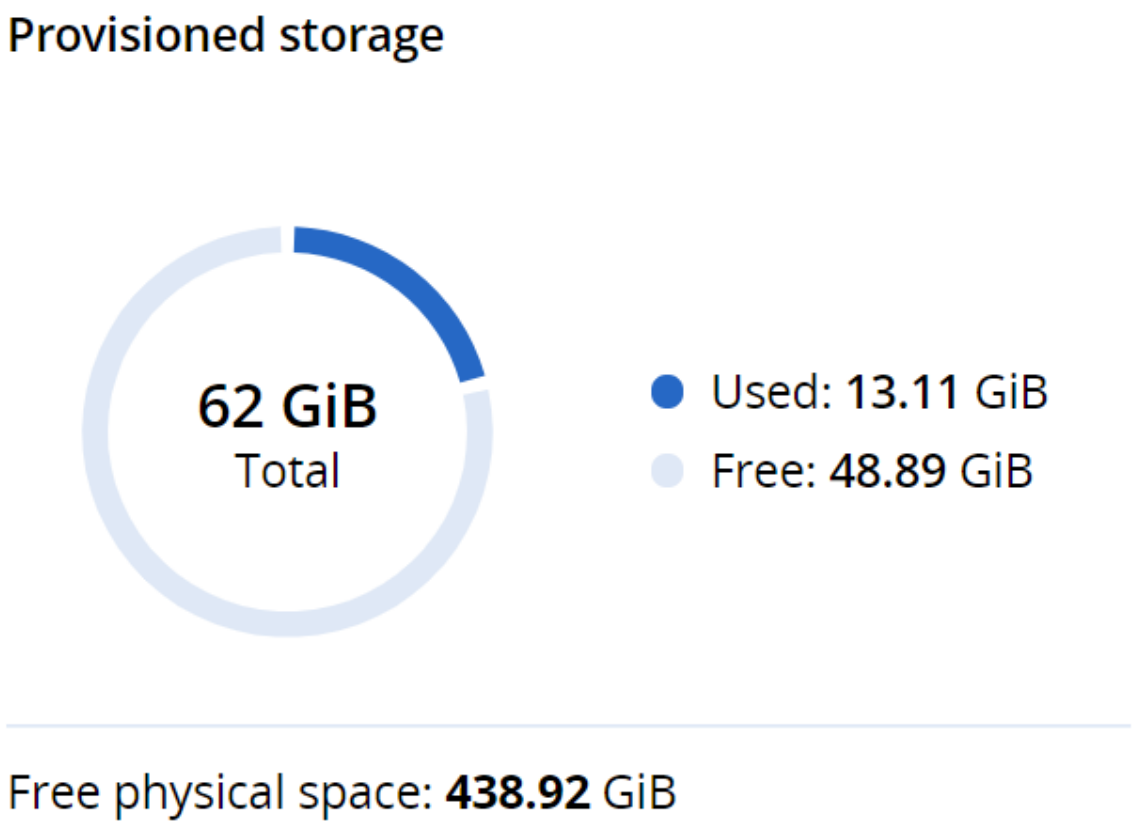
Объем пространства хранилища, фактически занятый данными во всех томах, выделенных в вычислительном кластере.

Свободно

Объем неиспользуемого пространства во всех томах, выделенных в вычислительном кластере.

Свободное физическое пространство

Объем физического пространства, доступного в кластере хранилища.



8.11.4 Диаграмма «Статус ВМ»

На диаграмме **Статус ВМ** отображается общее количество виртуальных машин в вычислительном кластере с группированием их по статусу, который может быть следующим:

Работает

Количество виртуальных машин, которые запущены и работают.

Выполняется

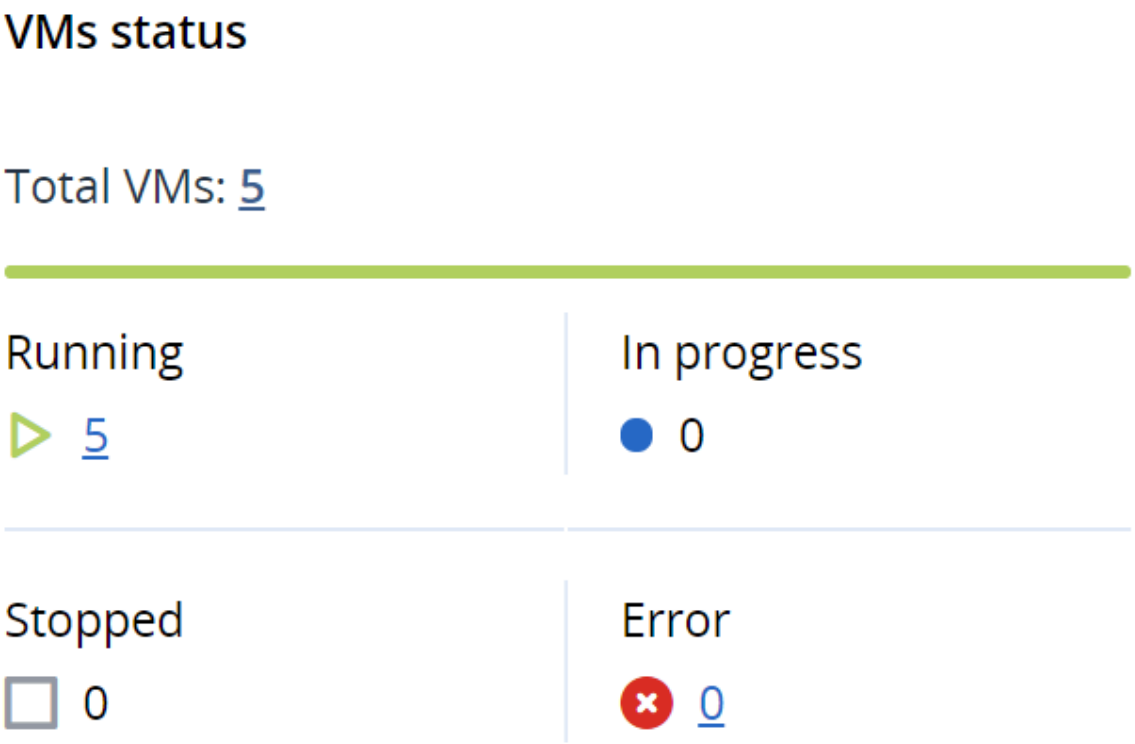
Количество виртуальных машин, которые находятся в переходном состоянии: построение, перезапуск, миграция и т. п.

Остановлена

Количество виртуальных машин, которые приостановлены или выключены.

Ошибка

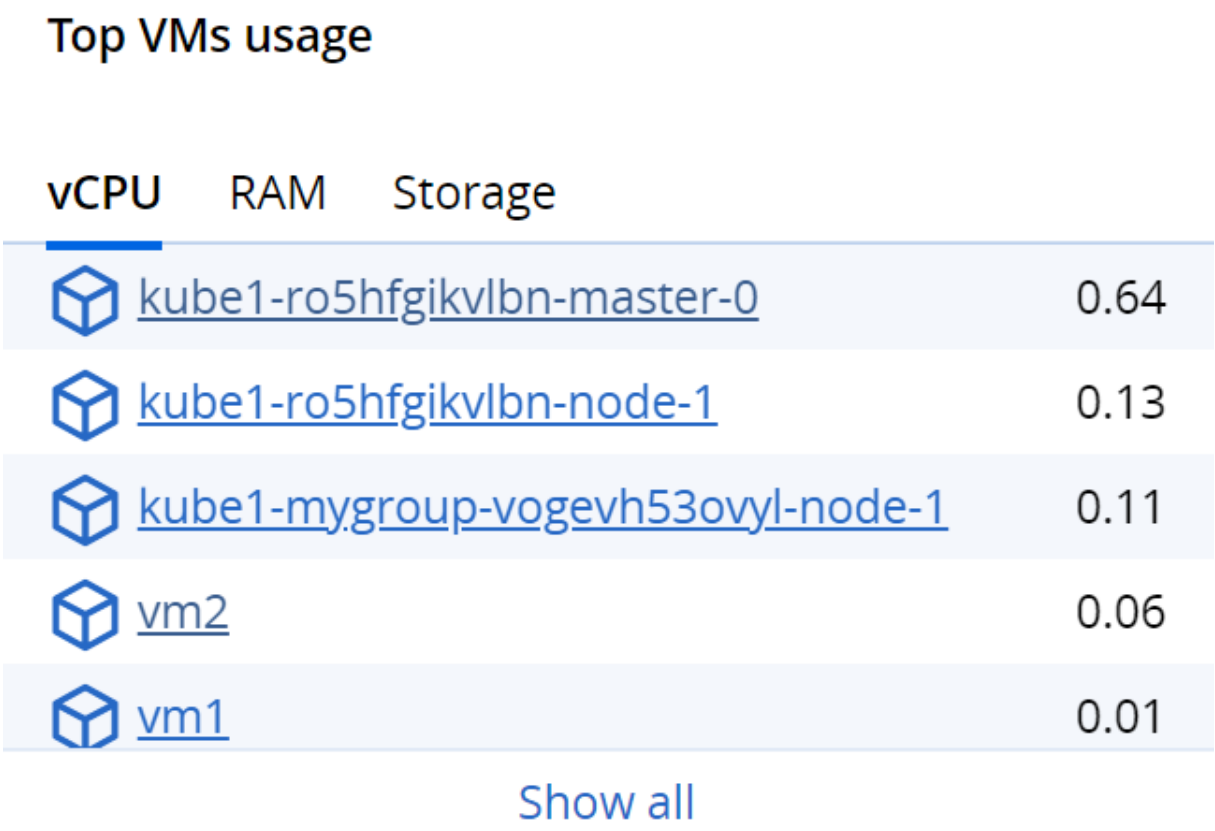
Количество виртуальных машин, в которых произошел сбой. Состояние таких ВМ можно сбросить до последнего стабильного состояния.



Чтобы просмотреть полный список виртуальных машин, отфильтрованный по выбранному статусу, щелкните по числу рядом со значком статуса.

8.11.5 Диаграмма «Список ВМ с наибольшим потреблением ресурсов»

На диаграмме **Список ВМ с наибольшим потреблением ресурсов** перечислены виртуальные машины с наибольшим потреблением ресурсов, отсортированные по параметрам **ЦП**, **ОЗУ** или **Хранилище** в порядке убывания. Для переключения между списками щелкните по нужному ресурсу.



Чтобы просмотреть полный список виртуальных машин в вычислительном кластере, нажмите кнопку **Показать все**.

8.11.6 Диаграмма «Оповещения»

На диаграмме **Оповещения** перечислены все оповещения, связанные с вычислительным кластером, отсортированные по уровню серьезности. Имеются следующие типы оповещений:

Критические

В вычислительном кластере обнаружена критическая проблема. Например, один или несколько его компонентов были недоступны в течение более чем 10 секунд или для какого-либо ресурса превышен программный лимит.

Предупреждения

Вычислительный кластер испытывает проблемы, которые могут повлиять на его производительность. Например, один или несколько его компонентов работают медленно или какой-либо ресурс приближается к программному лимиту.

Другие

В вычислительном кластере возникла какая-то другая неполадка. Например, срок действия его лицензии скоро истечет или уже истек.

Чтобы просмотреть полный список оповещений, связанных с вычислениями, нажмите кнопку **Показать все**.

8.11.7 Мониторинг вычислительных узлов

Статус вычислительных узлов можно отслеживать на экране **Вычисления** > **Серверы**. Узлы в вычислительном кластере могут иметь один из следующих статусов:

Исправен

Узел работает нормально.

Настраивается

Производится изменение конфигурации узла (модели ЦП по умолчанию для виртуальных машин или вычислительной роли).

Огражден

Узел стал снова доступен после отказа, но теперь он огражден, и размещение новых ВМ на нем не планируется.

Критические

На узле возникла критическая проблема, и он не функционирует.

Чтобы просмотреть подробные данные о вычислительном узле

Панель администратора

На экране **Вычисления** > **Серверы** щелкните по вычислительному узлу. Можно просматривать следующую информацию о вычислительном узле:

- Резервирования виртуальных ЦП и ОЗУ:
  - зарезервированные для системы и служб хранилища;
  - выделенные виртуальным машинам, расположенным на узле;
  - свободные виртуальные ЦП и ОЗУ, остающиеся на узле.

  Количество виртуальных ЦП – это произведение числа физических ЦП на узле и коэффициента перераспределения. Объем ОЗУ – это произведение объема физического ОЗУ на узле и коэффициента перераспределения. Чтобы узнать больше о резервированиях физических ЦП и ОЗУ для системы и служб хранилища, см. раздел "Требования к серверу" на странице 46.
- Объем ОЗУ, зарезервированный под DPDK. Эта память используется для обеспечения работы DPDK и не выделяется виртуальным машинам.
- Объем ОЗУ, доступный для размещения стандартных страниц памяти.
- Объем ОЗУ, доступный для размещения больших страниц памяти (страницы такого типа используются виртуальными машинами, подключенными к быстрой сети DPDK).
- Размещенные виртуальные машины и потребление ими ресурсов.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute node show <node>
```

<node>

Идентификатор или имя хоста узла

Например, чтобы просмотреть подробные сведения о вычислительном узле node001, выполните:

```
# vinfra service compute node show node001
+---------------+-----------------------------------------+
| Field         | Value                                   |
+---------------+-----------------------------------------+
| host          | node001.vstoragedomain                  |
| host_ip       | 10.37.130.101                           |
| hypervisor    | id: 86f1ca2c-71c7-47a0-9c7f-bb9dd705e67e |
|               | state: up                               |
|               | status: enabled                         |
|               | vms: 0                                  |
| id            | 7ffa9540-5a20-41d1-b203-e3f349d62565    |
| orig_hostname | node001                                 |
| placements    | []                                      |
| roles         | - controller                            |
|               | - compute                               |
| services      | - name: cinder-scheduler                |
|               |   state: healthy                        |
|               | - name: cinder-volume                   |
|               |   state: healthy                        |
|               | - name: neutron-dhcp-agent              |
|               |   state: healthy                        |
|               | - name: neutron-l3-agent                |
|               |   state: healthy                        |
|               | - name: neutron-metadata-agent          |
|               |   state: healthy                        |
|               | - name: neutron-openvswitch-agent       |
|               |   state: healthy                        |
|               | - name: nova-compute                    |
|               |   state: healthy                        |
|               | - name: nova-conductor                  |
|               |   state: healthy                        |
|               | - name: nova-scheduler                  |
|               |   state: healthy                        |
| state         | healthy                                 |
+---------------+-----------------------------------------+
```

8.11.8 Мониторинг виртуальных машин

Для мониторинга виртуальной машины

Панель администратора

Выберите виртуальную машину и откройте вкладку **Мониторинг**. Для виртуальных машин доступны следующие диаграммы мониторинга производительности:

ЦП/ОЗУ

Использование ЦП и ОЗУ виртуальной машиной.

Сеть

Входящий и исходящий сетевой трафик.

Чтение/запись в хранилище

Объем данных, считанных и записанных виртуальной машиной.

Задержка чтения/записи

Задержка чтения и записи. Наведя указатель мыши на ту или иную точку диаграммы, можно также просмотреть среднюю и максимальную задержку на соответствующий момент, а также 95-й и 99-й процентили.

Примечание

Средние значения рассчитываются каждые пять минут.

Интервал времени для диаграмм по умолчанию составляет двенадцать часов. Чтобы рассмотреть определенный интервал времени в большем масштабе, выделите его мышью; чтобы восстановить прежний масштаб, дважды щелкните по любой диаграмме.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute server stat <server>
```

<server>

Идентификатор или имя виртуальной машины

Например, чтобы просмотреть статистические показатели виртуальной машины myvm, выполните:

```
# vinfra service compute server stat myvm
+----------+----------------------------------+
| Field    | Value                            |
+----------+----------------------------------+
| datetime | 2019-05-29T11:39:46.429000+00:00 |
| metrics  | block_capacity: 1073741824       |
|          | block_usage: 268435456           |
|          | cpu_usage: 1                     |
|          | mem_usage: 149876736             |
+----------+----------------------------------+
```

8.11.9 Мониторинг балансировщиков нагрузки

Для мониторинга балансировщика нагрузки

Панель администратора

На вкладке **Вычисления** > **Сеть** > **Балансировщики нагрузки** выберите нужный балансировщик нагрузки и откройте вкладку **Обзор**. На ней доступны следующие диаграммы:

Состояние участников

Общее количество участников в пулах балансировки, сгруппированных по статусу «Исправен», «Неисправен», «Ошибка» и «Отключен».

Сеть

Входящий и исходящий сетевой трафик.

Активные подключения

Количество активных подключений.

Ошибочные запросы

Количество ошибочных запросов.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra service compute load-balancer stats <load-balancer>
```

<load-balancer>

Идентификатор или имя балансировщика нагрузки

Например, чтобы отобразить статистику для балансировщика нагрузки mylbaas, выполните:

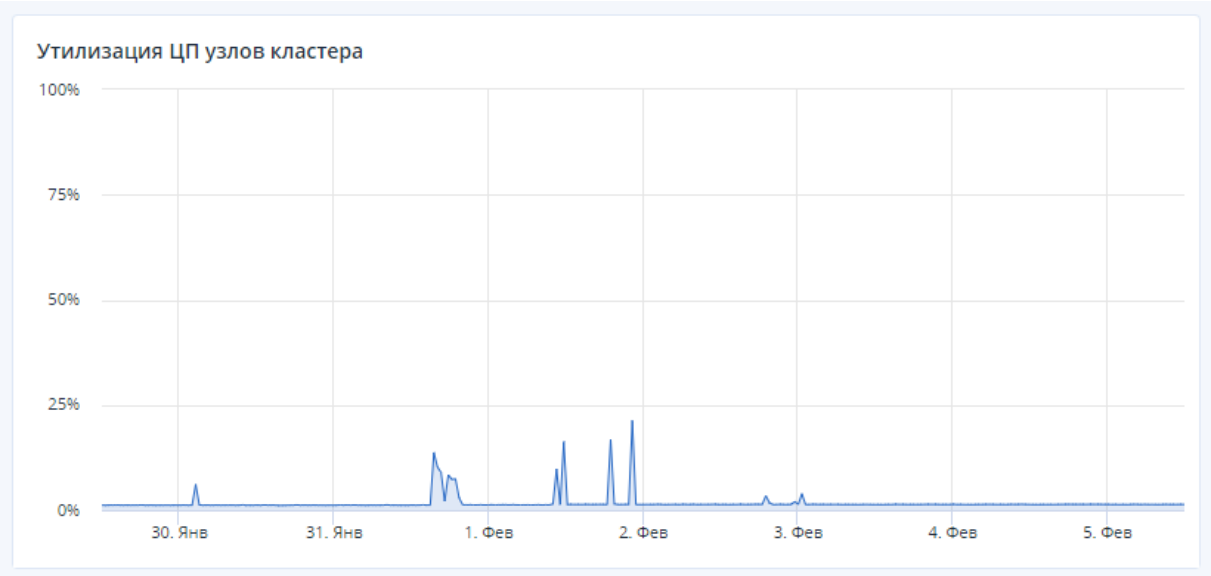
```
# vinfra service compute load-balancer stats mylbaas
+-------+-----------------------------------------------------+
| Field | Value                                               |
+-------+-----------------------------------------------------+
| stats | active_connections: 0                               |
|       | bytes_in: 0                                         |
|       | bytes_out: 0                                        |
|       | listeners: null                                     |
|       | loadbalancer_id: 17cfa86f-c374-4ca3-8cd6-f638a5234fe7 |
|       | request_errors: 0                                   |
|       | total_connections: 0                                |
+-------+-----------------------------------------------------+
```

8.11.10 Мониторинг нагрузки на вычислительные серверы

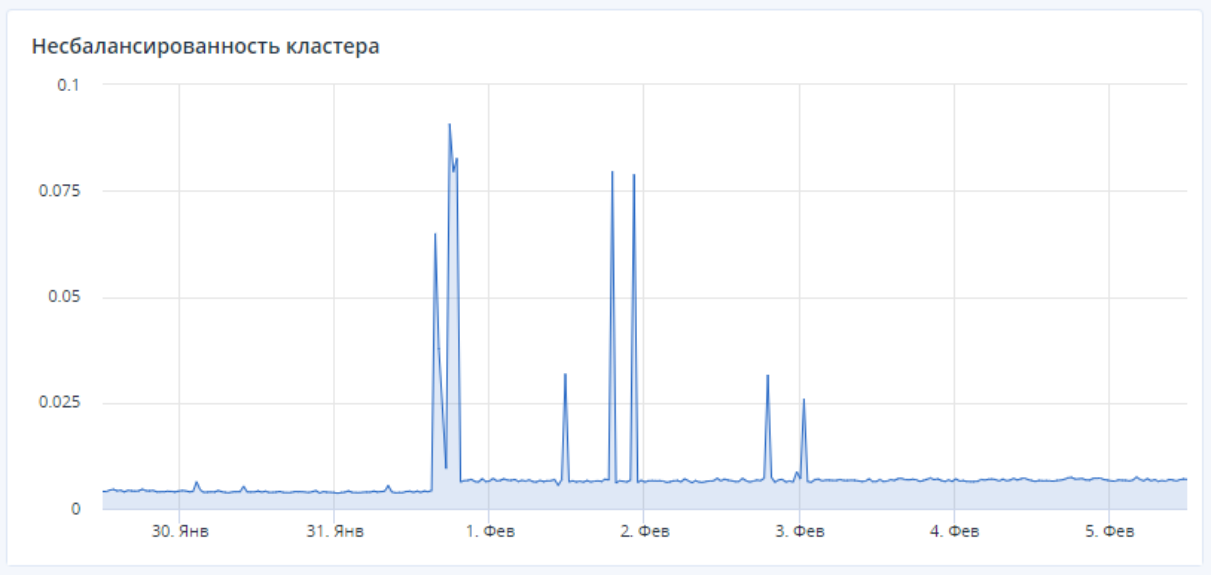
Просмотр сведений о нагрузке на вычислительные серверы

Перейдите на экран **Вычисления** > **DRS**.

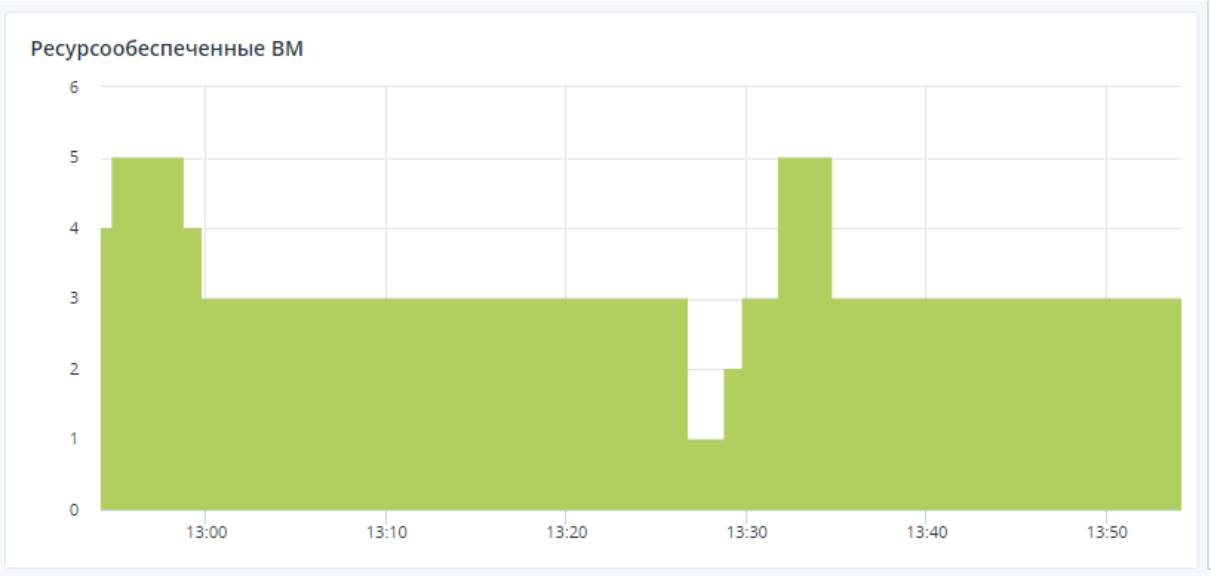
На графике **Утилизация ЦП узлов кластера** отображена зависимость использования ЦП вычислительного кластера от времени.



На графике **Несбалансированность кластера** отображена зависимость показателя несбалансированности нагрузки на серверы вычислительного кластера от времени.



На графике **Ресурсообеспеченные ВМ** отображена зависимость количества ресурсообеспеченных ВМ от времени. ВМ считается ресурсообеспеченной, если она получает у сервера от 80 % до 100 % требуемого ей процессорного времени.



Просмотр сведений о перемещениях ВМ

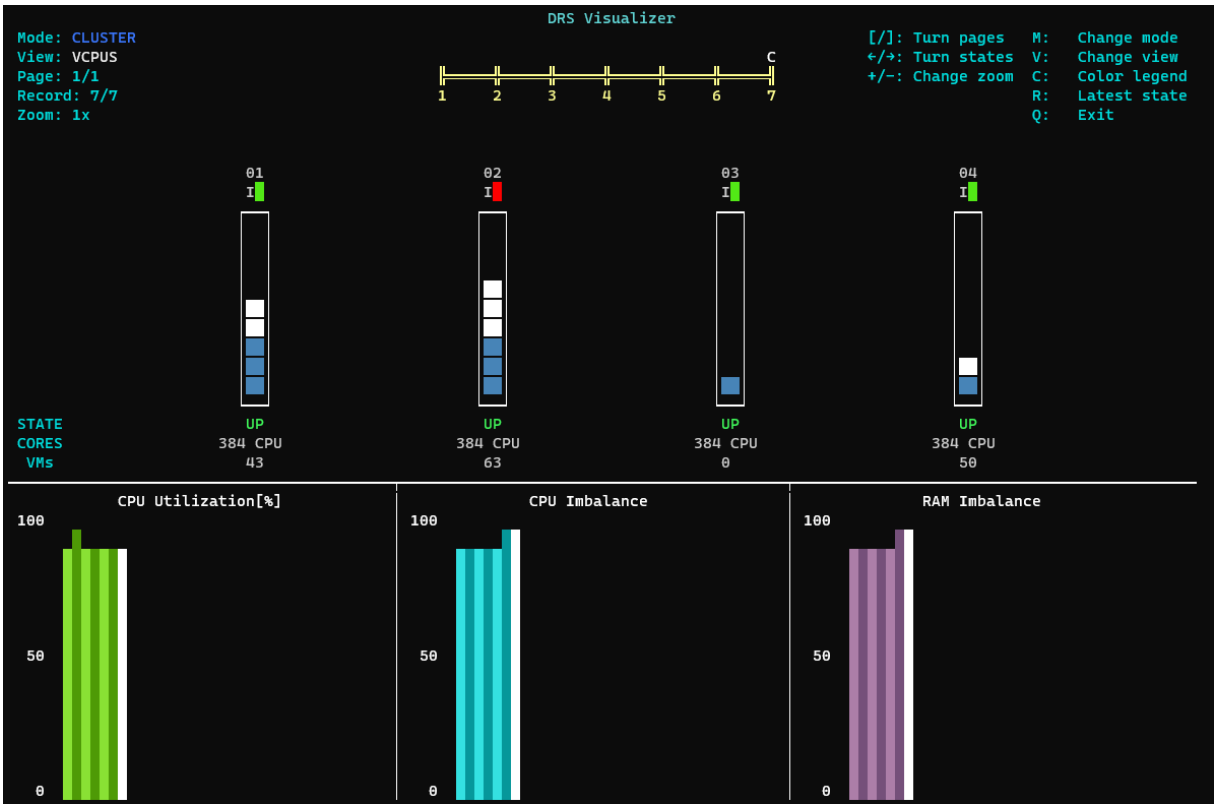
При включенной функции автоматической балансировки нагрузки на вычислительные серверы осуществляются перемещения ВМ между серверами. Сведения о перемещениях ВМ можно просмотреть на экране **Вычисления** > **DRS** на графике **Миграции**, где отображена зависимость количества перемещений ВМ от времени.

8.11.10.1 Использование программы DRS Visualizer

DRS Visualizer – это программа для представления в графическом виде сведений о нагрузке на вычислительный кластер и работе механизма автоматической балансировки нагрузки. С ее помощью можно отслеживать нагрузку на кластер и его серверы, степень несбалансированности распределения нагрузки, а также перемещения виртуальных машин, осуществляемые при балансировке. Кроме того, можно моделировать работу механизма автоматической балансировки нагрузки и оценивать полученные результаты.

При расчетах программа учитывает коэффициенты перераспределения виртуальных ЦП и ОЗУ. Ресурсы, выделенные службам хранилища и вычислений, исключаются из расчетов.

DRS Visualizer можно запустить на сервере управления. После запуска программа сохраняет сведения о состоянии кластера с заданной периодичностью и отображает сведения о состоянии, выбранном в данный момент.



Параметры программы и ее запуск

```
hci-tuning visual [--drs] [--update-timeout=<timeout>] [--autozoom]
```

--update-timeout=<timeout> или -t=<timeout>

Период сохранения и отображения состояний кластера в секундах (значение по умолчанию — 5 секунд).

--drs или -d

Запуск программы в режиме моделирования работы автоматической балансировки нагрузки. По умолчанию программа запускается в режиме мониторинга нагрузки и перемещений ВМ.

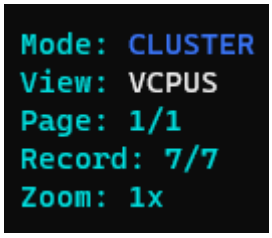
--autozoom или -z

Включить автоматическое масштабирование графиков и диаграмм.

Интерфейс программы

Интерфейс программы состоит из следующих областей:

- Параметры работы программы.

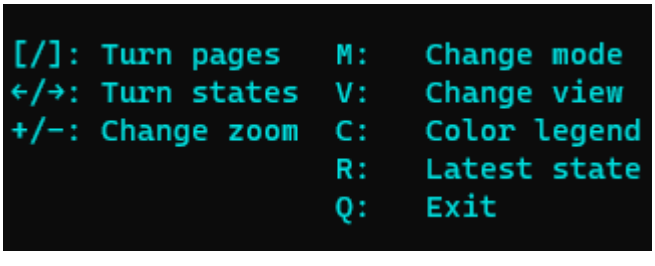


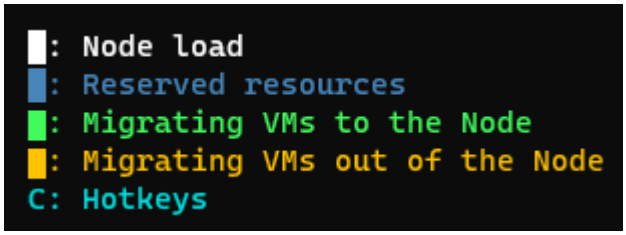
- **Mode**. Режим работы программы.
  - **CLUSTER**. Отслеживание нагрузки на кластер и его серверы, степени несбалансированности распределения нагрузки по серверам, перемещений виртуальных машин.
  - **CLUSTER (DRS)**. Моделирование работы механизма автоматической балансировки нагрузки и оценка полученных результатов.
- **View**. Режим расчета и отображения величины нагрузки на вычислительные серверы.
  - **VCPUS**. Величина нагрузки на сервер рассчитывается и отображается исходя из количества виртуальных ЦП сервера и количества виртуальных ЦП, выделенного виртуальным машинам на этом сервере.
  - **VCPUS USAGE**. Величина нагрузки на сервер рассчитывается и отображается исходя из количества виртуальных ЦП сервера и количества виртуальных ЦП, используемого виртуальными машинами на этом сервере.
  - **RAM**. Величина нагрузки на сервер рассчитывается и отображается исходя из объема ОЗУ сервера и объема ОЗУ, выделенного виртуальным машинам на этом сервере.
  - **RAM USAGE**. Величина нагрузки на сервер рассчитывается и отображается исходя из объема ОЗУ сервера и объема ОЗУ, используемого виртуальными машинами на этом сервере.
- **Page**. Номер текущей страницы с серверами и общее количество страниц.
- **Record**. Номер текущего состояния кластера и общее количество состояний.
- **Zoom**. Коэффициент увеличения графиков и диаграмм.

- Временная шкала.

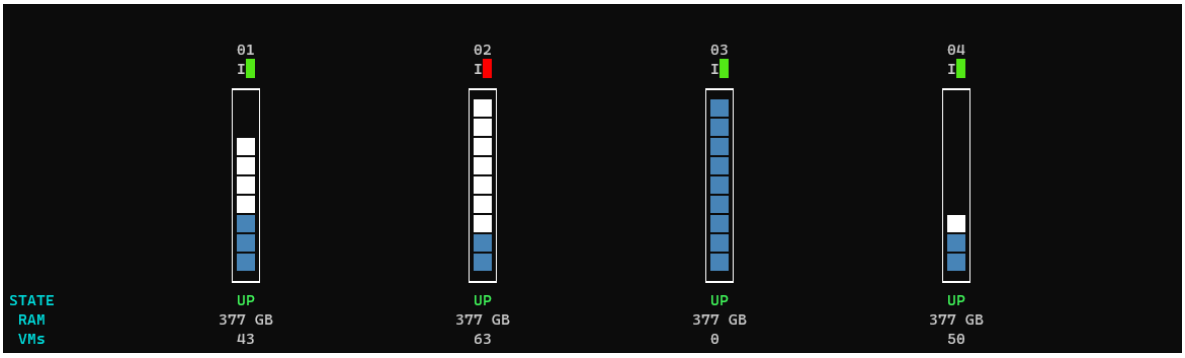
Все сохраненные состояния кластера пронумерованы и расположены в хронологическом порядке. Символом **C** отмечено текущее состояние, сведения о котором отображаются в областях ниже.

- Справочная информация.



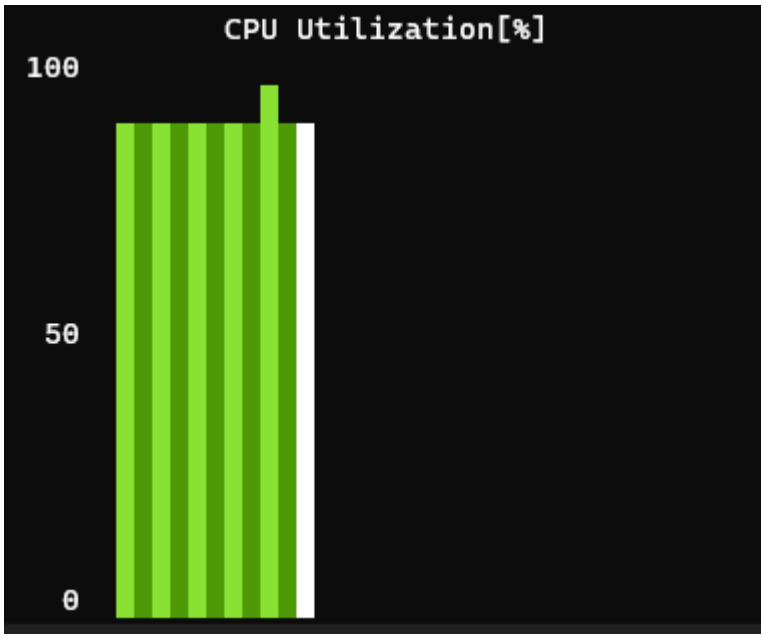


- Нагрузка на серверы, перемещения виртуальных машин.

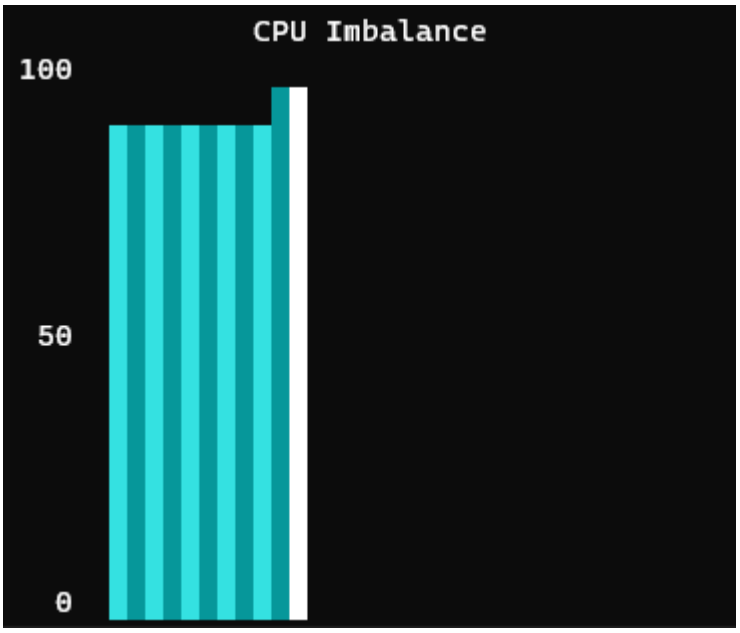


  Для каждого сервера отображается следующее:
  - Цветовой индикатор несбалансированности нагрузки на сервер, отражающий степень отклонения нагрузки на сервер от средней нагрузки в кластере. Зеленый цвет () индикатора означает минимальную степень отклонения, красный () – максимальную. Промежуточные цвета соответствуют промежуточным градациям степени отклонения.
  - Объем ресурса, потребляемый виртуальными машинами. Представлен в виде белых квадратов ().
  - Объем ресурса, зарезервированный для служб хранилища и вычислений. Представлен в виде синих квадратов ().
  - Виртуальные машины, перемещаемые с сервера при балансировке нагрузки. Обозначены квадратами желтого цвета ().
  - Виртуальные машины, перемещаемые на сервер при балансировке нагрузки. Обозначены квадратами зеленого цвета ().
  - Состояние сервера (включен или выключен).
  - Общий объем ресурса.
  - Количество виртуальных машин на сервере.

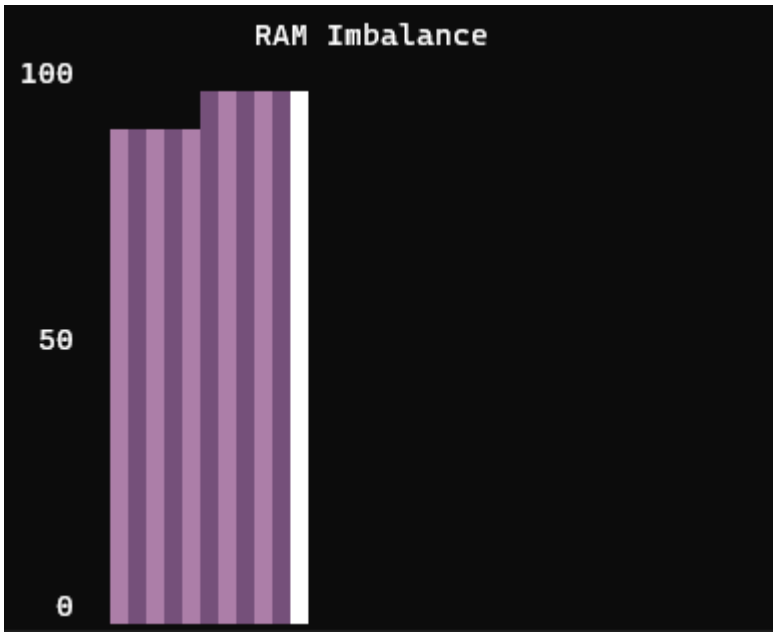
  Вид ресурса зависит от выбранного режима расчета и отображения.
- Потребление ресурсов ЦП в кластере.



- Показатель несбалансированности распределения нагрузки, основанный на общем количестве виртуальных ЦП в кластере и количестве виртуальных ЦП, используемом виртуальными машинами.



- Показатель несбалансированности распределения нагрузки, основанный на общем объеме ОЗУ в кластере и объеме ОЗУ, используемом виртуальными машинами.



Управление

- **[** и **]** – переход со страницы на страницу;
- ← и → – перемещение между состояниями кластера;
- **+** и **-** – изменение масштаба графиков и диаграмм;
- **D** – установка начального состояния кластера для моделирования работы автоматической балансировки нагрузки;
- **M** – переключение режима работы программы;
- **V** – переключение режима отображения;
- **C** – вывод цветовой схемы или списка горячих клавиш;
- **R** – переключение на последнее состояние кластера;
- **Q** – выход.

Мониторинг нагрузки и перемещений ВМ

Запустите программу, использовав следующую команду:

```
hci-tuning visual
```

Моделирование работы автоматической балансировки нагрузки

1. Запустите программу, использовав следующую команду:

   ```
   hci-tuning visual --drs
   ```

2. Выберите состояние кластера, которое будет использовано как начальное для расчета

последующих состояний, и нажмите **D**.

Последующие состояния будут рассчитаны на основе указанного начального состояния и текущих настроек автоматической балансировки нагрузки (см. раздел "Управление автоматической балансировкой нагрузки на вычислительные серверы" на странице 664).

9 Обслуживание

Плановое обслуживание кластера подразумевает установку обновлений, замену отказавших дисков, резервное копирование и восстановление базы данных управления. Также оно включает постепенное освобождение серверов из кластера хранилища данных без потери данных и их удаление из инфраструктуры. Для обслуживания сервер необходимо перевести в специальный режим. При замене серверов кластера может требоваться изменить конфигурацию высокой доступности или даже удалить и воссоздать ее. Кроме того, важно изучить рекомендуемый способ постепенного отключения всех серверов и перезапуска кластера.

9.1 Установка обновлений

Кибер Инфраструктура поддерживает последовательное обновление без перерывов в работе. Серверы обновляются по очереди без ущерба для доступности данных. Во время обновления сервер, который необходимо перезагрузить, может перейти в режим обслуживания. В этом случае рабочие нагрузки и виртуальные машины, размещенные на этом сервере, переносятся на другие серверы. После обновления сервер возобновляет работу, а перенесенные рабочие нагрузки и ВМ перемещаются обратно на этот сервер.

Примечание
Обычно для установки обновлений требуется доступ к Интернету. Для установки обновлений в среде без доступа к Интернету (в закрытом контуре) вы можете использовать локальное зеркало репозитория пакетов продукта. Подробную информацию см. в статье базы знаний Настройка локального зеркала репозитория Кибер Инфраструктуры.

Можно обновить различные компоненты кластера все вместе или по отдельности. В любом случае компоненты обновляются в следующем порядке.

1. Сначала обновляются серверы кластера.
2. Серверы управления обновляются, только когда обновлены все серверы кластера. Главный сервер управления обновляется в последнюю очередь.
3. Панель управления (администрирования и самообслуживания) и API вычислений обновляются на серверах управления, только когда обновлены все серверы кластера и серверы управления. При обновлении этого компонента не требуется перезагрузка серверов управления.

Ограничения

- Серверы необходимо обновлять только через панель администрирования или с помощью инструмента vinfra (см. раздел "Установка обновлений" выше. Не используйте yum update.
- Неназначенные серверы можно обновлять.
- Обновления применяются к одному серверу за раз.
- Серверы управления можно обновить только все вместе и только после обновления всех серверов кластера.

- Панель управления и API вычислений можно обновить только после обновления всех серверов управления и серверов кластера.
- При развертывании с одним узлом узел не входит в обслуживание во время обновления.
- Динамическая миграция не поддерживается для виртуальных машин с присоединенными виртуальными графическими процессорами или PCI-устройствами.

Предварительные требования

- Создан кластер хранилища данных, как показано в разделе "Развертывание кластера хранилища данных" на странице 141.
- Любые сторонние репозитории отключены.
- Кластер работоспособен, и каждый узел инфраструктуры подключен к сети.
- DNS кластера настроен, как описано в разделе "Добавление внешних DNS-серверов" на странице 139, и указывает на таблицу DNS для разрешения имен внешних хостов.

Для обновления компонентов кластера

Панель администратора

1. Откройте экран **Настройки** > **Обновления**. Дата последней проверки отображается в правом верхнем углу. Щелкните по круговой стрелке, чтобы проверить наличие обновлений. Если для компонента кластера есть обновления, его статус обновлений меняется на **Доступно**. Если сервер необходимо будет перезагрузить, то рядом с доступной версией будет добавлено **Требуется перезагрузка**.
2. Нажмите **Загрузить** в правом верхнем углу, чтобы получить обновления. Дождитесь загрузки обновлений и изменения статуса обновления на **Готово к установке**.
3. [Необязательно] Нажмите **Заметки о выпуске**, чтобы прочитать сведения о выпуске.
4. Выберите компоненты, которые следует обновить.
   - Для обновления серверов кластера выберите нужные серверы кластера.
   - Для обновления серверов управления выберите все серверы управления и те серверы кластера, которые требуют обновления.
   - Для обновления панели управления и API вычислений выберите этот компонент и все серверы управления, если они требуют обновления.
5. Нажмите **Обновить**, чтобы продолжить.
6. Если вы выбрали серверы, требующие перезагрузки, выполните следующие действия.
   a. Решите, будут ли эти серверы переходить в режим обслуживания. Выберите **Режим обслуживания**, если вы хотите перевести эти серверы в режим обслуживания.
   b. Если вы выбрали серверы с вычислительным сервисом, выберите способ миграции виртуальных машин, работающих на этих серверах.
      - С параметром **Игнорировать ВМ, которые нельзя перенести динамически** виртуальные машины с сервера, переходящего в режим обслуживания, будут динамически перенесены на другие вычислительные серверы. ВМ, которые нельзя перенести динамически, будут пропущены. Это применимо к виртуальным машинам с

присоединенными виртуальными графическими процессорами или PCI-устройствами, а также в случае недостаточных ресурсов виртуальных ЦП и ОЗУ на других вычислительных серверах. Пропущенные ВМ продолжат работать до перезагрузки или выключения сервера. В этом случае они будут остановлены, что приведет к перерыву в работе. Они будут запущены автоматически после возобновления работы сервера.

- С параметром **Игнорировать ВМ, которые нельзя или не удалось перенести динамически** виртуальные машины с сервера, переходящего в режим обслуживания, будут динамически перенесены на другие вычислительные серверы. ВМ, которые нельзя перенести динамически, будут пропущены. Это применимо к виртуальным машинам с присоединенными виртуальными графическими процессорами или PCI-устройствами, а также в случае недостаточных ресурсов виртуальных ЦП и ОЗУ на других вычислительных серверах. ВМ, которые были пропущены или которые не удалось перенести динамически, продолжат работать до перезагрузки или выключения сервера. В этом случае они будут остановлены, что приведет к перерыву в работе. Они будут запущены автоматически после возобновления работы сервера.
- С параметром **Перенести все ВМ динамически** все виртуальные машины с сервера, переходящего в режим обслуживания, будут динамически перенесены на другие вычислительные серверы.

c. [Необязательно] Выберите **Прервать обновление, если сервер не может войти в режим обслуживания**, чтобы остановить обновление в случае сбоя при входе в режим обслуживания.

7. Проверьте выбранные компоненты и нажмите **Установить**.

Во время установки обновлений можно приостановить или отменить процесс. После завершения обновления статусы компонентов изменятся на **Обновлено**.

При сбое обновления нажмите **Сведения**, чтобы просмотреть сведения о проблеме и выбрать дальнейшие действия. Можно отменить обновление, устранить проблемы и повторить попытку обновления без прерывания работы. Либо можно принудительно выполнить обновление без перевода серверов в режим обслуживания. Серверы будут перезагружены, что может привести к перерыву в работе размещенных на них рабочих процессов.

Интерфейс командной строки

Используйте следующие команды:

1. Проверьте наличие обновлений:

```
# vinfra software-updates check-for-updates
```

2. Просмотрите результаты проверки:

```
# vinfra software-updates status
+-------------------------+-----------------------------------------+
| Field                   | Value                                   |
+-------------------------+-----------------------------------------+
```

```
| available_storage_release | release: '234'                        |
|                           | version: 4.7.0                        |
| control_plane             | available_storage_release:            |
|                           |   release: '234'                      |
|                           |   version: 4.7.0                      |
|                           | installed_storage_release:            |
|                           |   release: '217'                      |
|                           |   version: 4.7.0                      |
|                           | status: available                     |
| last_check_datetime       | 2021-11-01T12:22:10.630818            |
| nodes                     | - available_storage_release:          |
|                           |    release: '234'                     |
|                           |    version: 4.7.0                     |
|                           |   current_storage_release:            |
|                           |    release: '217'                     |
|                           |    version: 4.7.0                     |
|                           |   downloaded_storage_release: null    |
|                           |   host: node001.vstoragedomain        |
|                           |   id: 0175ce44-c86d-7818-3259-3182f5fd83f6 |
|                           |   is_in_ha: false                     |
|                           |   is_primary: true                    |
|                           |   orig_hostname: node001              |
|                           |   reboot_required: false              |
|                           |   status: available                   |
|                           | - available_storage_release:          |
|                           |    release: '234'                     |
|                           |    version: 4.7.0                     |
|                           |   current_storage_release:            |
|                           |    release: '217'                     |
|                           |    version: 4.7.0                     |
|                           |   downloaded_storage_release: null    |
|                           |   host: node002.vstoragedomain        |
|                           |   id: 923926da-a879-5f56-1b24-1462917ed335 |
|                           |   is_in_ha: false                     |
|                           |   is_primary: false                   |
|                           |   orig_hostname: node002              |
|                           |   reboot_required: false              |
|                           |   status: available                   |
|                           | - available_storage_release:          |
|                           |    release: '234'                     |
|                           |    version: 4.7.0                     |
|                           |   current_storage_release:            |
|                           |    release: '217'                     |
|                           |    version: 4.7.0                     |
|                           |   downloaded_storage_release: null    |
|                           |   host: node003.vstoragedomain        |
|                           |   id: ef24c47c-620d-8726-2677-ed94d853de2e |
|                           |   is_in_ha: false                     |
|                           |   is_primary: false                   |
|                           |   orig_hostname: node003              |
|                           |   reboot_required: false              |
```

```
|                    |  status: available                  |
| status             | available                           |
+--------------------------+-----------------------------------------------+
```

В выводе команды выше показано, что доступно обновление.

3. Загрузите обновление:

```
# vinfra software-updates download
```

4. Проверьте пригодность серверов для установки обновления:

```
# vinfra software-updates eligibility-check
+---------+--------------------------------------+
| Field   | Value                                |
+---------+--------------------------------------+
| task_id | 88e51115-8f0e-4c6f-b33b-949728d1fb99 |
+---------+--------------------------------------+
# vinfra task show 88e51115-8f0e-4c6f-b33b-949728d1fb99
+---------+-------------------------------------------------------------------------+
| Field   | Value                                                                   |
+---------+-------------------------------------------------------------------------+
| details |                                                                         |
| name    | backend.presentation.software_updates.tasks.EligibilityCheckTask |
| result  | chunks_rebalancing_rate:                                                |
|         |   details: null                                                       |
|         |   exception: null                                                       |
|         |   message: null                                                         |
|         |   passed: true                                                          |
|         |   severity: info                                                        |
|         | cluster_has_releasing_nodes:                                            |
|         |   details: null                                                       |
|         |   exception: null                                                       |
|         |   message: null                                                         |
|         |   passed: true                                                          |
|         |   severity: critical                                                    |
|         | cluster_unhealthy:                                                        |
|         |   details: null                                                       |
|         |   exception: null                                                       |
|         |   message: null                                                         |
|         |   passed: true                                                          |
|         |   severity: critical                                                    |
|         | not_enough_space_on_agents:                                               |
|         |   details: null                                                       |
|         |   exception: null                                                       |
|         |   message: null                                                         |
|         |   passed: true                                                          |
|         |   severity: critical                                                    |
|         | not_enough_space_on_mn:                                                 |
|         |   details: null                                                       |
|         |   exception: null                                                       |
|         |   message: null                                                         |
```

```
|       |  passed: true                                  |
|       |  severity: critical                            |
|       | postgres_not_running:                                  |
|       |  details: null                                 |
|       |  exception: null                                 |
|       |  message: null                                  |
|       |  passed: true                                  |
|       |  severity: critical                            |
|       | request_accept_eula:                                   |
|       |  details: null                                 |
|       |  exception: null                                 |
|       |  message: null                                  |
|       |  passed: true                                  |
|       |  severity: critical                            |
|       | server_with_pci_devices:                               |
|       |  details: null                                 |
|       |  exception: null                                 |
|       |  message: null                                  |
|       |  passed: true                                  |
|       |  severity: info                                |
|       | shaman:                                        |
|       |  details: null                                 |
|       |  exception: null                                 |
|       |  message: null                                  |
|       |  passed: true                                  |
|       |  severity: critical                            |
|       | tgtd:                                          |
|       |  details: null                                 |
|       |  exception: null                                 |
|       |  message: null                                  |
|       |  passed: true                                  |
|       |  severity: critical                            |
|       | too_many_pending_chunks:                               |
|       |  details: null                                 |
|       |  exception: null                                 |
|       |  message: null                                  |
|       |  passed: true                                  |
|       |  severity: info                                |
| state   | success                                        |
| task_id | 88e51115-8f0e-4c6f-b33b-949728d1fb99                   |
+---------+----------------------------------------------------------------+
```

5. Запустите процесс установки обновления:

```
vinfra software-updates start [--maintenance enabled={yes,no}[,key=value,...]]
                              [--nodes <nodes>] [--skip-control-plane]
                              [--accept-eula]
```

--maintenance enabled={yes,no}[,key=value,...]>

Укажите параметры обслуживания.

- enabled: войти в режим обслуживания во время обновления (yes или no).
- разделенные запятыми пары key=value с ключами (необязательно):
  - on-fail: как следует поступить с обновлением при сбое обслуживания.
    - stop (по умолчанию): остановить обновление, если сервер не может перейти в режим обслуживания. Уже обновленные серверы останутся обновленными.
    - skip: пропустить и не обновлять серверы, которые не могут перейти в режим обслуживания.
    - force: принудительно обновить и перезагрузить (при необходимости) все серверы, даже если они не могут перейти в режим обслуживания. Использование этого параметра может привести к простоям.
  - compute-mode: как поступить с обновлением, если нельзя перенести работающую ВМ.
    - strict: остановить обновление, если нельзя перенести работающую ВМ.
    - ignore: игнорировать ВМ, которую нельзя перенести в работающем состоянии.
    - ignore_ext: игнорировать ВМ, которую нельзя или не удалось перенести в работающем состоянии.

--nodes <nodes>

Разделенный запятыми список идентификаторов или имен серверов.

--skip-control-plane

Обновить кластер без обновления панели управления.

--accept-eula

Принять лицензионное соглашение.

Например, чтобы начать обновление серверов node001, node002, node003 и перевести их в режим обслуживания, выполните:

```
# vinfra software-updates start --nodes node001,node002,node003 \
--maintenance enabled=yes,on-fail=skip,compute-mode=ignore
```

Серверы, которые нельзя перевести в режим обслуживания, будут пропущены. Виртуальные машины, которые нельзя динамически перенести на время обслуживания серверов, будут пропущены.

Для приостановки процесса установки обновлений используйте команду vinfra software-updates pause. Чтобы возобновить процесс, выполните команду vinfra software-updates resume.

Можно отменить установку обновлений и вывести серверы из режима обслуживания, использовав команду ниже.

```
vinfra software-updates cancel [--maintenance-mode {exit,exit-keep-resources,hold}]
```

--maintenance-mode {exit,exit-keep-resources,hold}

Режим обслуживания:

- exit: вывести сервер из режима обслуживания и вернуть на него эвакуированные ресурсы.
- exit-keep-resources (по умолчанию): вывести сервер из режима обслуживания, но оставить эвакуированные ресурсы на другом сервере.
- hold: не выходить из режима обслуживания.

Например, чтобы отменить установку обновлений и вывести серверы из режима обслуживания, выполните:

```
# vinfra software-updates cancel --maintenance-mode exit
```

Ресурсы, перенесенные на другие серверы на время обслуживания, будут перенесены обратно.

9.2 Выполнение обслуживания сервера

Каждый раз, когда необходимо выполнить сервисные операции на сервере кластера, переводите его в режим обслуживания. В этом случае сервер перестает распределять новые фрагменты данных хранилища, но продолжает обрабатывать операции ввода-вывода для основных сервисов хранилища, таких как MDS, CS и кэширование. Однако они не будут использоваться для распределения новых данных, поэтому помещение сервера в режим обслуживания может сократить объем свободного пространства в кластере хранилища. Все CS на сервере продолжат передавать данные даже в режиме обслуживания, если сервер не отключится. Другие сервисы (вычислительный, Backup Gateway, iSCSI, S3 и NFS) могут либо переноситься, либо оставаться как есть на время обслуживания.

Если по какой-то причине сервис нельзя эвакуировать с сервера, вход в режим обслуживания будет отложен. Вам нужно будет выбрать дальнейшие действия: выйти или принудительно включить режим обслуживания.

После перевода сервера в режим обслуживания отключите его и выполните необходимые сервисные операции. Завершив работы, включите сервер на панели администрирования и верните его в эксплуатацию.

Ограничения

- Приостановленные ВМ не могут быть перенесены с сервера и будут пропущены.
- Серверы на обслуживании можно вернуть в работу или освободить.

Предварительные требования

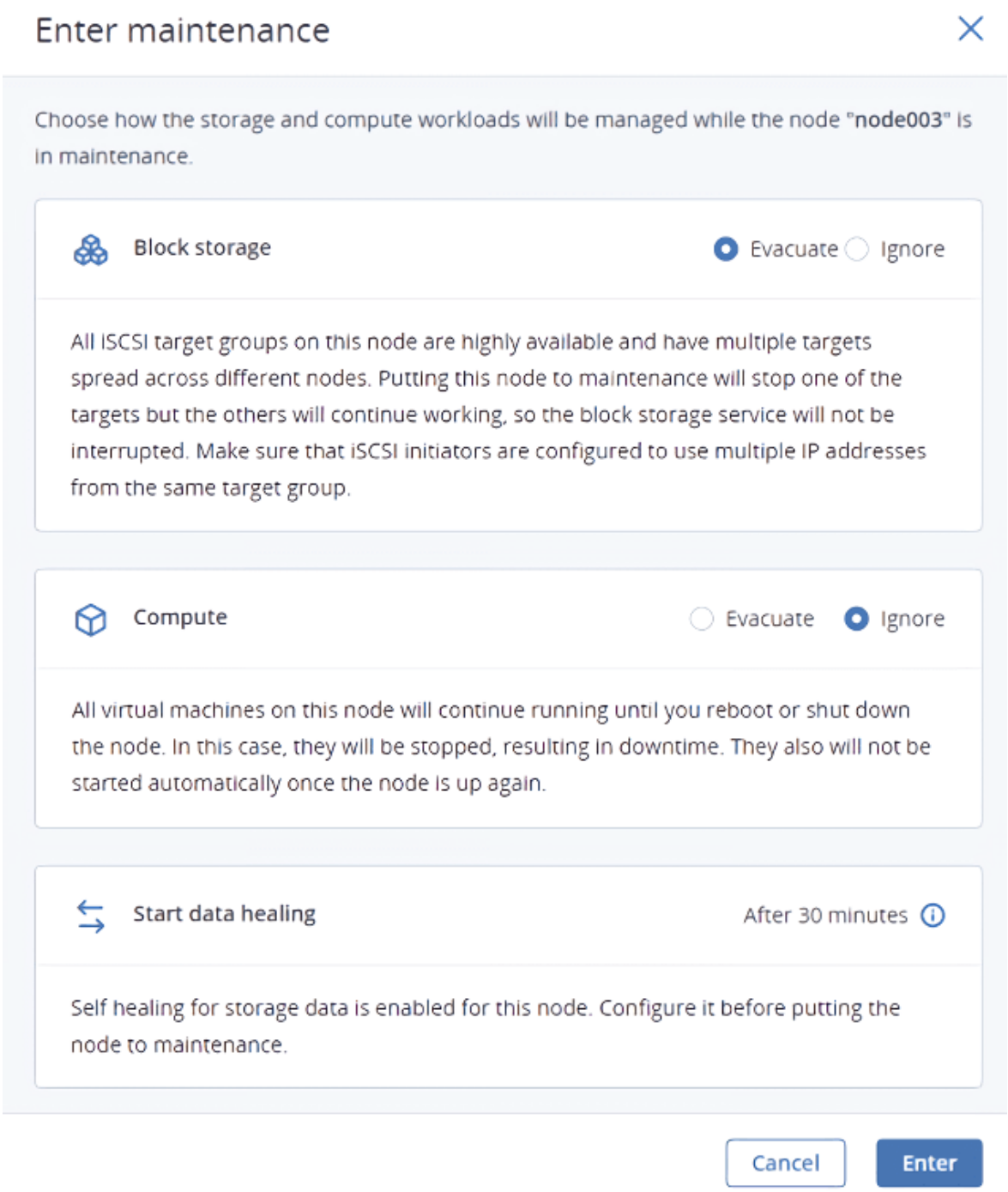
- Четкое понимание механизма самовосстановления кластера (см. раздел "Перестроение кластера" на странице 38).
- Наличие пяти сервисов MDS в кластере хранилища. В этом случае при отключении сервера, где работает сервис MDS, на время обслуживания кластер может выдержать отказ еще одного сервера.
- Если на сервере размещены виртуальные машины, на других вычислительных серверах должно быть достаточно ресурсов для размещения этих ВМ.

- Если на сервере размещены целевые устройства iSCSI, инициаторы iSCSI должны быть настроены на использование нескольких IP-адресов из одной группы целевых устройств.
- Если на сервере работает шлюз S3, его IP-адреса должны быть удалены из записей DNS точек доступа S3. Иначе у некоторых клиентов S3 могут возникнуть перебои в подключении.

Чтобы перевести сервер в режим обслуживания

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по строке с нужным сервером.
2. На правой панели сервера щелкните **Вход в режим обслуживания**.
3. В окне **Вход в режим обслуживания** выберите вариант **Эвакуировать** или **Игнорировать** следующие рабочие нагрузки на время обслуживания:
   - **Блочное хранилище**. Группы целевых устройств iSCSI высокодоступны с несколькими целевыми устройствами, работающими на разных серверах. Когда сервер входит в режим обслуживания, размещенное на нем целевое устройство останавливается, а предпочтительный путь переносится на другой сервер в группе целевых устройств в течение 60 секунд. Таким образом, работа сервиса не прерывается на время обслуживания.
   - **Вычисления**. Эвакуация виртуальных машин с сервера обозначает их поочередный перенос на другие вычислительные серверы без остановки работы. Если вы выберете игнорировать их, то они продолжат работу до перезагрузки или выключения сервера. В этом случае они будут остановлены, что приведет к простою. Они также не будут запущены автоматически, когда сервер возобновит работу.
   - **S3**. Можно эвакуировать сервисы S3 с этого сервера на другие серверы в кластере S3 либо игнорировать их. В последнем случае они продолжат работу до перезагрузки или выключения сервера, что приведет к простою. Они будут запущены автоматически, когда сервер возобновит работу.
   - **NFS**. Можно эвакуировать сервисы NFS с этого сервера на другие серверы в кластере NFS либо игнорировать их. В последнем случае они продолжат работу до перезагрузки или выключения сервера, что приведет к простою. Они будут запущены автоматически, когда сервер возобновит работу.
   - **ABGW**. Это сервис высокой доступности с несколькими экземплярами, распределенными по разным серверам. Перевод этого сервера в режим обслуживания приведет к остановке одного экземпляра, а остальные продолжат работать. Таким образом, перерывов в работе сервиса не будет.



4. **Запуск восстановления данных**. Самовосстановление кластера – это автоматическое восстановление данных кластера хранилища, которые становятся недоступны, когда отключается один из серверов (или дисков) хранилища. Если это происходит во время обслуживания, самовосстановление откладывается (по умолчанию на 30 минут) для экономии ресурсов кластера. Если сервер возобновляет работу до окончания этого интервала, то в самовосстановлении нет необходимости.

Время ожидания репликации можно настроить вручную, задав значение параметра mds.wd.offline_tout_mnt в миллисекундах с помощью команды vstorage -c <cluster_name> set-config.

5. Если на сервере есть неизбыточные фрагменты данных, отобразится параметр **Переносить неизбыточные данные**. Установите для него флажок, чтобы перенести неизбыточные данные на другие серверы хранения. В противном случае после отключения сервера они станут недоступны. Данные также можно временно переместить на другой уровень, если текущий заполнен.
6. Нажмите **Ввод**.

Интерфейс командной строки

Используйте следующие команды:

1. Запустите проверку возможности перевода сервера в режим обслуживания. Например:

```
# vinfra node maintenance precheck node001
```

2. Просмотрите сведения об обслуживании сервера. Например:

```
# vinfra node maintenance status node001
+-----------+------------------------------------------+
| Field     | Value                                    |
+-----------+------------------------------------------+
| node_id   | c3b2321a-7c12-8456-42ce-8005ff937e12     |
| params    |                                          |
| precheck  | flow: completed                          |
|           | id: c15bf919-9a81-45b1-8fef-5f626e68f957 |
|           | result:                                  |
|           | - has_resources: true                    |
|           |   relocation_is_possible: true           |
|           |   resources: null                        |
|           |   service: node                          |
|           |   service_is_available: true             |
|           | - has_resources: false                   |
|           |   relocation_is_possible: true           |
|           |   resources: null                        |
|           |   service: iscsi                         |
|           |   service_is_available: true             |
|           | - has_resources: false                   |
|           |   relocation_is_possible: true           |
|           |   resources:                             |
|           |     failed: []                           |
|           |   service: alua                          |
|           |   service_is_available: false            |
|           | - has_resources: true                    |
|           |   relocation_is_possible: false          |
|           |   resources: null                        |
|           |   service: compute                       |
|           |   service_is_available: true             |
```

```
|         | - has_resources: false               |
|         |   relocation_is_possible: null       |
|         |   resources: null                    |
|         |   service: nfs                       |
|         |   service_is_available: false        |
|         | - has_resources: true                |
|         |   relocation_is_possible: false      |
|         |   resources: null                    |
|         |   service: s3                        |
|         |   service_is_available: true         |
|         | state: success                       |
|         | updated_at: '2021-11-01T11:09:41.331926' |
| resources |                                    |
| state     | idle                             |
| task      |                                  |
+-----------+------------------------------------------+
```

В выводе выше показано, что на сервере есть сервис вычислений и сервис S3, которые не могут быть эвакуированы.

3. Запустите перевод сервера в режим обслуживания, выполнив следующую команду:

```
vinfra node maintenance start [--iscsi-mode <mode>] [--compute-mode <mode>]
                              [--s3-mode <mode>] [--storage-mode <mode>]
                              [--alua-mode <mode>] [--nfs-mode <mode>] <node>
```

--iscsi-mode <mode>

Игнорировать эвакуацию iSCSI во время обслуживания (ignore).

--compute-mode <mode>

Игнорировать эвакуацию вычислительных серверов во время обслуживания (ignore).

--s3-mode <mode>

Игнорировать эвакуацию S3 во время обслуживания (ignore).

--storage-mode <mode>

Игнорировать эвакуацию серверов хранения во время обслуживания (ignore).

--alua-mode <mode>

Игнорировать группы целевых устройств блочного хранения данных во время обслуживания (ignore).

--nfs-mode <mode>

Игнорировать эвакуацию серверов NFS во время обслуживания (ignore).

<node>

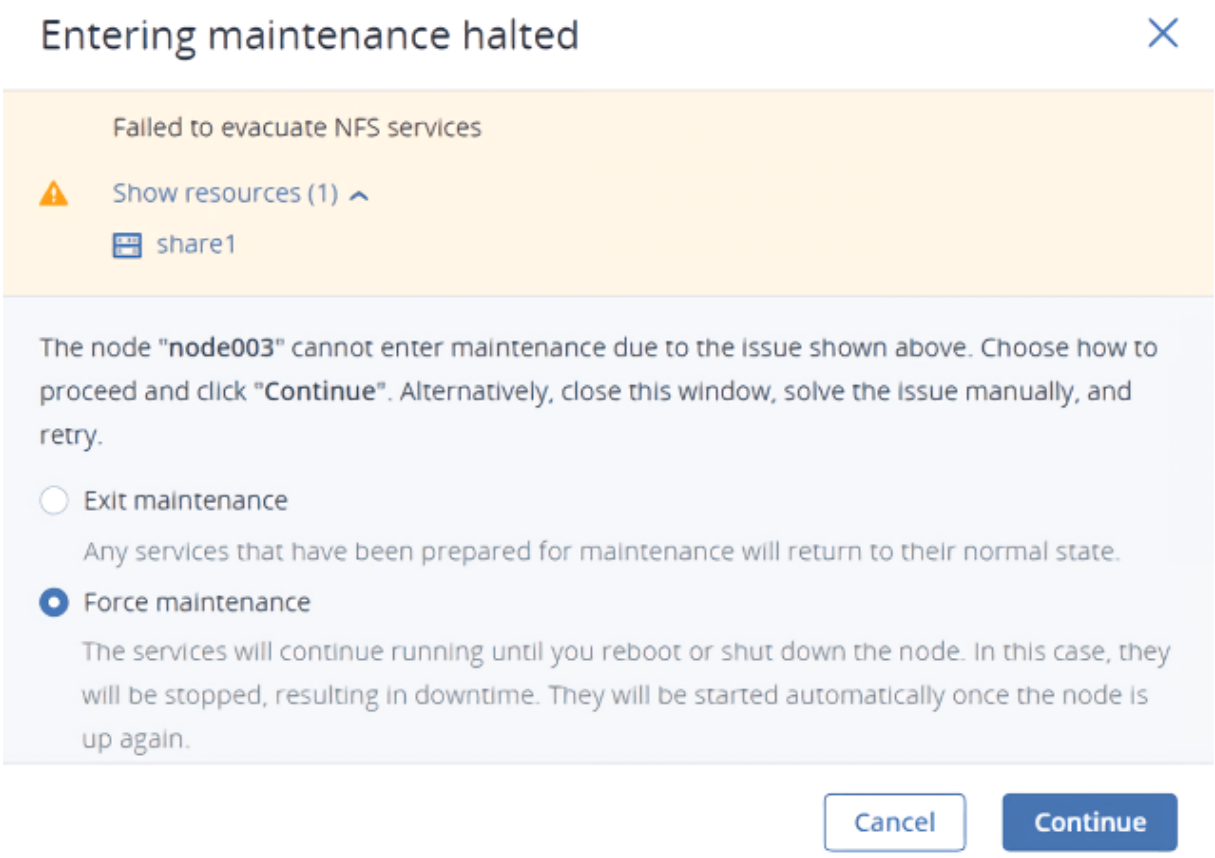
Идентификатор сервера или имя хоста

Например, чтобы запустить перевод сервера в режим обслуживания без эвакуации сервисов S3 и вычислений, выполните:

```
# vinfra node maintenance start node001 --s3-mode ignore --compute-mode ignore
```

Чтобы возобновить отложенный переход в режим обслуживания

1. На экране **Инфраструктура** > **Серверы** щелкните по строке с нужным сервером.
2. На правой панели сервера щелкните **Вход в режим обслуживания**.
3. Выберите нужное действие.
   - Выберите **Выход из режима обслуживания**, чтобы вернуть все службы на сервере в нормальное состояние.
   - Выберите **Принудительный вход в режим обслуживания**, чтобы остановить работу сервисов, которые нельзя эвакуировать во время перезагрузки или остановки сервера.
4. Нажмите кнопку **Продолжить**.



Чтобы вернуть сервер к работе

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по строке с нужным сервером.
2. На правой панели сервера щелкните **Выход из режима обслуживания**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node maintenance stop <node> [--ignore-compute]
```

<node>

Идентификатор сервера или имя хоста

--ignore-compute

Игнорировать вычислительные ресурсы при возврате сервера в работу

Например, чтобы вернуть сервер node001 в рабочий режим, выполните:

```
# vinfra node maintenance stop node001
```

9.3 Резервное копирование и восстановление базы данных управления

База данных продукта хранится на сервере управления (сервер, на котором размещена панель администрирования), и ее резервные копии создаются автоматически. Она также реплицируется на серверы, входящие в конфигурацию высокой доступности, если высокая доступность включена для сервера управления.

База данных управления содержит конфигурацию кластера, параметры мониторинга и управления сервисами и метаданные вычислительных объектов, таких как проекты, домены, пользователи, виртуальные машины, образы, типы ВМ, тома, сети и т. п. База данных не включает пользовательские данные, расположенные на дисках хранилища (например, тома, моментальные снимки томов и вычислительные образы), а также данные, хранящиеся на локальных корневых дисках (например, журналы, данные метрик и внутренние данные сервисов).

Резервные копии базы данных управления создаются автоматически путем запуска задания cron ежедневно в 3:00. Если для сервера управления не включена высокая доступность, то в случае отказа или повреждения базы данных сервер восстанавливается из такой резервной копии. Файлы резервных копий хранятся в каталоге /mnt/vstorage/webcp/backup/. Для резервных копий сервера управления применяется следующая политика хранения.

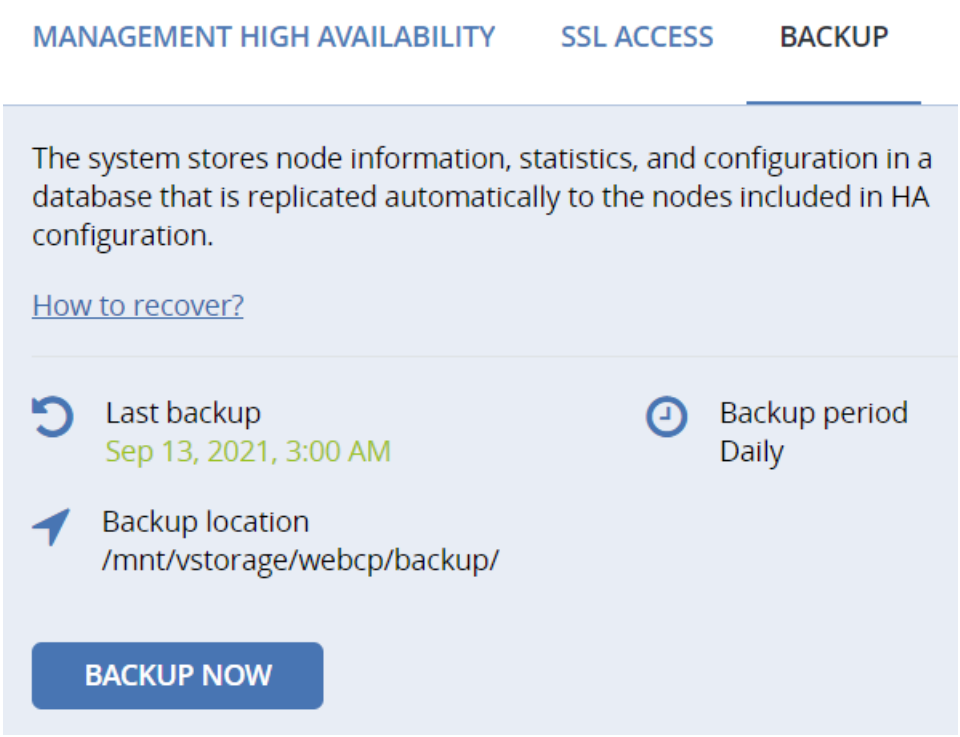
- Сохраняются все резервные копии, созданные за последний день.
- Из резервных копий, созданных за последние 7 дней, сохраняется самая новая копия каждого дня.
- Из резервных копий, созданных за последние 7–14 дней, сохраняется самая старая копия.
- Из резервных копий, созданных за последние 14–45 дней, сохраняется самая старая копия каждой недели.
- Резервные копии старше 45 дней удаляются.

9.3.1 Резервное копирование базы данных управления

Чтобы создать резервную копию базы данных вручную

Панель администратора

Откройте экран **Настройки** > **Сервер управления** > **Резервная копия** и нажмите **Создать резервную копию**.



После того как резервное копирование будет завершено, дата **Последняя копия** будет обновлена.

Предупреждение
Не переименовывайте файл резервной копии! В противном случае вы не сможете восстановить из него базу данных управления.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster backup create
```

Получить подробные данные о последней резервной копии кластера, а также идентификатор выполняемой в настоящее время задачи резервного копирования (если она имеется), можно в выводе команды vinfra cluster backup show:

```
# vinfra cluster backup show
+---------------------+---------------------------+
| Field               | Value                     |
+---------------------+---------------------------+
| last_backup_date    | 2019-08-21T15:41:24+00:00 |
| last_backup_location | /mnt/vstorage/webcp/backup/ |
| ready               | True                      |
| tasks               | []                        |
+---------------------+---------------------------+
```

9.3.2 Восстановление базы данных управления из резервной копии

Базу данных сервера управления можно восстановить из резервной копии на том же сервере управления или любом сервере в кластере хранилища.

Ограничения

- Если включена высокая доступность сервера управления, вы не сможете восстанавливать резервные копии базы данных с помощью этого сценария. В этом случае обратитесь в службу технической поддержки.
- Сервис vstorage-ui-backend должен работать только на одном сервере в кластере хранилища. Если база данных сервера управления восстанавливается на другом сервере, предыдущий сервер управления нужно развернуть повторно.

Предварительные требования

- Выполнено резервное копирование базы данных управления (вручную или автоматически) в соответствии с инструкциями "Резервное копирование базы данных управления" на предыдущей странице.

Чтобы восстановить базы данных сервера управления из резервной копии

Выполните следующий скрипт на сервере, где будет восстановлена база данных сервера управления:

```
/usr/libexec/vstorage-ui-backend/bin/restore-management-node.sh -x <public_net_iface> -i
<private_net_iface> \
-f /mnt/vstorage/webcp/backup/<backup_file>
```

где:

- <public_net_iface> и <private_net_iface> – интерфейсы, назначенные публичной и частной сети. При необходимости можно указать в обоих параметрах один и тот же сетевой интерфейс.
- -f – путь к файлу резервной копии. Если этот параметр не указать, база данных сервера управления будет восстановлена из последней резервной копии.

Например, если сетевой интерфейс **eth0** подключен к сети **Public**, интерфейс **eth1** подключен к сети **Private** и вы хотите восстановить базу данных сервера управления из резервной копии backup-20211026000001.tar, выполните:

```
# /usr/libexec/vstorage-ui-backend/bin/restore-management-node.sh -x eth0 -i eth1 \
-f /mnt/vstorage/webcp/backup/backup-20211026000001.tar
```

Для доступа к панели администрирования используйте общедоступный IP-адрес сервера с восстановленной базой данных сервера управления.

9.3.3 Восстановление базы данных управления в вычислительном кластере

Если у вас уже развернут вычислительный кластер, базу данных сервера управления следует восстанавливать только на одном из вычислительных серверов. После восстановления виртуальными машинами, которые находились на отказавшем сервере управления, нельзя будет управлять из панели администрирования и их можно будет только удалить. Однако их можно эвакуировать с помощью инструмента vinfra.

Ограничения

- Если включена высокая доступность сервера управления, вы не сможете восстанавливать резервные копии базы данных с помощью этого сценария. В этом случае обратитесь в службу технической поддержки.
- Если создать вычислительные объекты после резервного копирования, они будут потеряны.
- Если изменить или удалить вычислительные объекты после резервного копирования, они будут восстановлены следующим образом.
  - Вычислительные объекты, используемые как конфигурации (типы ВМ, политики хранения, виртуальные сети, SSH-ключи), будут восстановлены полностью.
  - Все остальные вычислительные объекты (виртуальные машины, тома, образы и т. д.) будут восстановлены частично. Они будут отображаться на панели администрирования, но их нельзя будет использовать. Вы сможете только удалить их из панели администрирования.

Предварительные требования

- Выполнено резервное копирование базы данных управления (вручную или автоматически) в соответствии с инструкциями раздела "Резервное копирование базы данных управления" на странице 812.

Чтобы восстановить базу данных управления на вычислительном сервере

Запустите скрипт восстановления, использовав параметр -n:

```
/usr/libexec/vstorage-ui-backend/bin/restore-management-node.sh -x <public_net_iface> -i
<private_net_iface> \
-f /mnt/vstorage/webcp/backup/<backup_file> -n
```

где:

- <public_net_iface> и <private_net_iface> — интерфейсы, назначенные публичной и частной сети.
- -f — путь к файлу резервной копии. Если этот параметр не указать, база данных сервера управления будет восстановлена из последней резервной копии.
- Параметр -n указывает, что вычислительный кластер будет перенастроен на использование другого сервера управления. Если вы восстанавливаете базу данных сервера управления на тот же сервер, опустите параметр -n.

Например, если сетевой интерфейс **eth0** подключен к сети **Public**, интерфейс **eth1** подключен к сети **Private** и вы хотите восстановить базу данных сервера управления с вычислительными объектами из последней резервной копии, выполните:

```
# /usr/libexec/vstorage-ui-backend/bin/restore-management-node.sh -x eth0 -i eth1 -n
```

Чтобы эвакуировать виртуальные машины с отказавшего сервера управления

1. Проверьте состояние ВМ: ВМ с включенной высокой доступностью появятся в состоянии пересоздания, а ВМ с отключенной высокой доступностью — в активном состоянии.
2. Если ВМ находится в состоянии пересоздания, выполните сброс состояния с помощью команды vinfra service compute server reset-state.
3. Чтобы эвакуировать все ВМ, используйте команду vinfra service compute server evacuate.

9.4 Управление конфигурацией высокой доступности

Поскольку конфигурация высокой доступности сервера управления должна в каждый момент содержать ровно три сервера, удаление сервера из такой конфигурации невозможно без одновременного добавления другого сервера. Например, чтобы удалить из конфигурации высокой доступности вышедший из строя сервер, можно заменить его исправным.

При миграции сети требуется удалить конфигурацию высокой доступности, чтобы заменить конфигурацию сети.

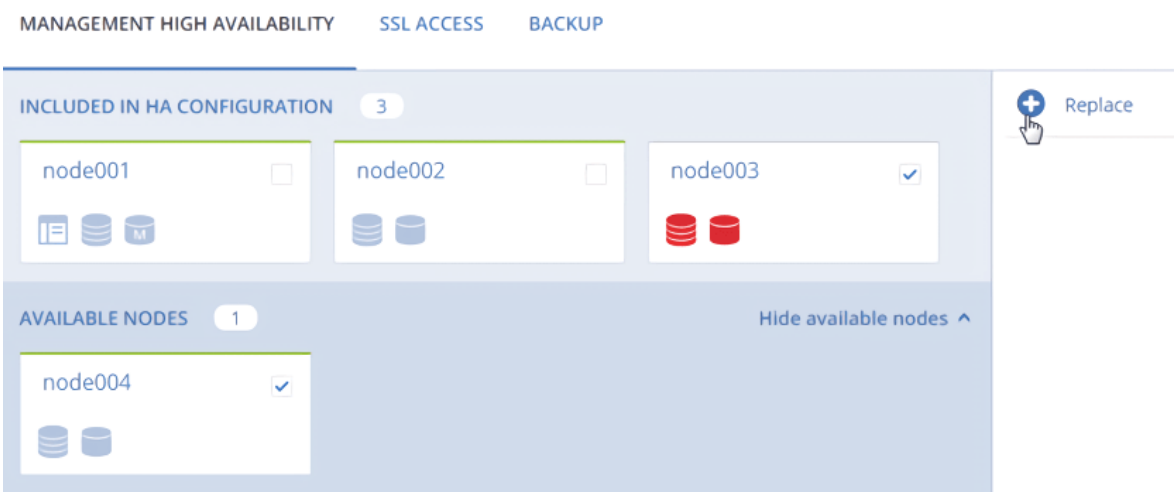
Предварительные требования

- Четкое понимание ограничений, перечисленных в разделе "Высокая доступность и вычислительный кластер" на странице 29.
- Конфигурация высокой доступности создана в соответствии с инструкциями раздела "Включение высокой доступности сервера управления" на странице 146.

Чтобы заменить конфигурацию высокой доступности

Панель администратора

1. На вкладке **Настройки** > **Сервер управления** > **Высокая доступность** выберите один или два сервера, которые следует удалить из конфигурации высокой доступности, а также один или два доступных сервера, которые будут добавлены в конфигурацию вместо них, и нажмите кнопку **Заменить**.



2. На шаге **Настройте сеть** убедитесь, что на каждом добавляемом сервере выбраны правильные сетевые интерфейсы. Если это не так, щелкните по значку шестерни для сервера и назначьте его сетевым интерфейсам сети с типами трафика **Управление системными сервисами** и **Панель администрирования**. Нажмите **Продолжить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster ha update [--virtual-ip <network:ip>] [--nodes <nodes>] [--force]
```

--virtual-ip <network:ip>

Сопоставление конфигурации высокой доступности в формате:

- network: сеть, включаемая в конфигурацию высокой доступности (должна включать по меньшей мере один из следующих типов трафика: Управление системными сервисами, Панель администрирования, Панель самообслуживания или API вычислений).
- ip: виртуальный IP-адрес, который будет использоваться в конфигурации высокой доступности.

Укажите этот параметр несколько раз, чтобы создать конфигурацию высокой доступности сразу для нескольких сетей.

--nodes <nodes>

Разделенный запятыми список идентификаторов или имен серверов

--force

Пропустить проверки на соответствие минимальным аппаратным требованиям

Например, чтобы обновить конфигурацию высокой доступности сервера управления, то есть включить в нее серверы node001, node002 и node005, выполните:

```
# vinfra cluster ha update --nodes node001,node002,node005
```

Чтобы удалить конфигурацию высокой доступности

Панель администратора

Перейдите на вкладку **Настройки** > **Сервер управления** > **Высокая доступность** и щелкните **Удалить конфигурацию высокой доступности**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster ha delete
```

9.5 Замена дисков серверов

Чтобы установить новый диск, нужно сначала освободить старый. Если на новом диске есть данные, помещенные без помощи Кибер Инфраструктура, диск будет считаться непригодным для использования в кластере хранилища.

После замены нужно назначить роль освобожденного диска новому.

- Роль **хранилища** назначается автоматически, если автоматическая настройка новых дисков была включена до отказа диска.
- Все остальные роли необходимо назначать вручную.

9.5.1 Автоматическая настройка новых дисков хранилища

Ограничения

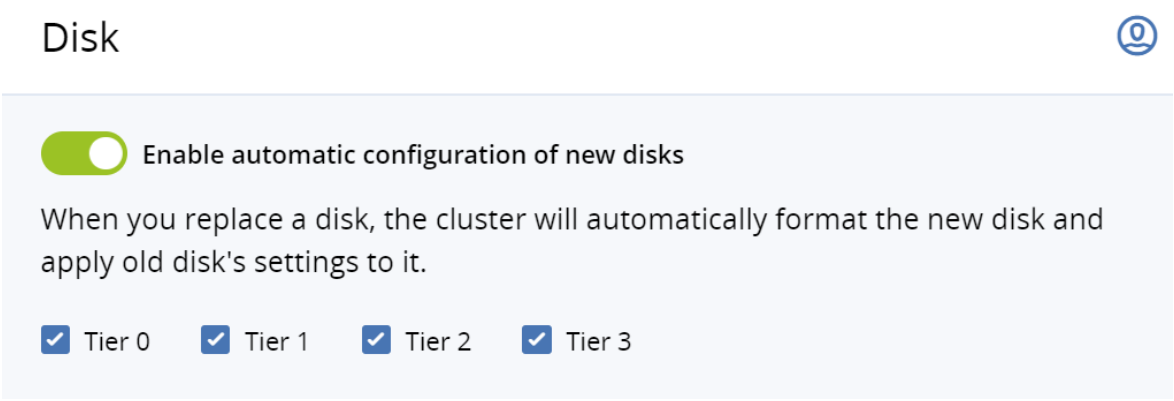
- Если новый диск меньше старого, ему не будет назначена роль **Хранилище**. Вместо этого вы получите уведомление о разнице в размерах и должны будете назначить роль вручную (либо заменить диск на больший по размеру).
- Если новый диск имеет другой тип (например, при замене твердотельного накопителя на жесткий диск или наоборот), ему не будет назначена роль **Хранилище**. Вместо этого вы получите уведомление о разных типах и должны будете назначить роль вручную (либо заменить диск на нужный тип).
- Если включить эту функцию после отказа диска, то новому диску не будет назначена роль **Хранилище**.
- Если вы случайно удалите и снова присоедините исправный диск с ролью **Хранилище**, его данные будут использоваться снова.
- Если добавить диск, который не заменяет никакой отказавший диск, ему не будет назначена роль **Хранилище**.
- Если при добавлении диска один из CS-сервисов неактивен или отключен, диску будет назначена роль **Хранилище** и будет создан новый CS.

- Если одновременно присоединить несколько новых дисков на замену, роль **Хранилище** будет назначена им в произвольном порядке, если их размер и тип соответствуют требованиям. Они также будут назначены на нужные уровни (если применимо).

Чтобы роль «Хранилище» назначалась новым дискам автоматически

Панель администратора

1. Перейдите в раздел **Настройки** > **Системные настройки** > **Диск**.
2. Установите переключатель **Включить автоматическую настройку новых дисков**.
3. При необходимости выберите уровни, которые следует сканировать на наличие дисков со сбоем. Если выйдет из строя диск на невыбранном уровне, то новому диску нужно будет назначить роли вручную.



4. Нажмите **Сохранить**.

С этого момента при замене отказавшего диска с ролью **Хранилище** новый диск будет автоматически обнаружен, отформатирован, получит ту же роль и будет помещен на тот же уровень (если применимо). Результаты отобразятся на экране **Диски** сервера.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster settings automatic-disk-replacement set [--tier0 {on,off}] [--tier1 {on,off}]
                                                       [--tier2 {on,off}] [--tier3 {on,off}]
```

--tier0 {on,off}

Включение (on) или выключение (off) автоматической конфигурации дисков хранилища для уровня 0

--tier1 {on,off}

Включение (on) или выключение (off) автоматической конфигурации дисков хранилища для уровня 1

--tier2 {on,off}

Включение (on) или выключение (off) автоматической конфигурации дисков хранилища для уровня 2

--tier3 {on,off}

Включение (on) или выключение (off) автоматической конфигурации дисков хранилища для уровня 3

Например, чтобы включить автоматическую конфигурацию дисков хранилища для всех уровней, выполните:

```
# vinfra cluster settings automatic-disk-replacement set --tier0 on --tier1 on --tier2 on --tier3 on
```

Параметры автоматической конфигурации дисков можно просмотреть в выводе команды vinfra cluster settings automatic-disk-replacement show:

```
# vinfra cluster settings automatic-disk-replacement show
+-------+-------+
| Field | Value |
+-------+-------+
| tier0 | True  |
| tier1 | False |
| tier2 | True  |
| tier3 | False |
+-------+-------+
```

9.5.2 Освобождение дисков сервера

В процессе освобождения диска его данные безопасным образом переносятся на другие диски, что требует некоторого времени. Во избежание потери данных дождитесь окончания миграции.

Ограничения

- Штатное освобождение диска хранилища возможно, только если остальные диски в кластере хранилища могут обеспечить настроенную схему избыточности. Тем не менее можно освободить диск принудительно без миграции данных, но это приведет к деградации кластера и запустит процесс самовосстановления.

Предварительные требования

- Перед заменой диска, которому назначена роль **Метаданные**, **Кэш** или **Метаданные+Кэш**, сначала назначьте эту роль новому диску, а затем освободите старый.
- Чтобы автоматически назначать диски с ролью **Хранилище** после замены, включите автоматическую настройку новых дисков (см. раздел "Автоматическая настройка новых дисков хранилища" на странице 817).

Чтобы освободить диск из кластера хранилища

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по имени сервера.
2. На вкладке **Диски** щелкните по диску, который требуется заменить.
3. На правой панели диска нажмите **Освободить**.
4. (Необязательно, настоятельно не рекомендуется) Если вы не хотите ждать окончания переноса данных, выберите **Освободить без миграции данных**.

   Предупреждение
   При этом есть риск потери данных. Этот способ следует использовать только для избыточных данных.

5. Нажмите кнопку **Освободить**.

Когда перенос данных с диска завершится, для диска перестанет отображаться роль на панели **Диски** и его можно будет заменить новым.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node disk release [--force] [--node <node>] <disk>
```

--force
: Освобождение без миграции данных

--node <node>
: Идентификатор или имя хоста сервера (по умолчанию node001.vstoragedomain)

<disk>
: Идентификатор или имя устройства диска

Например, чтобы освободить от роли cs диск sdc на сервере node003, выполните:

```
# vinfra node disk release sdc --node node003
```

9.5.3 Настройка новых дисков вручную

Ограничения

- Диску можно назначить роль, только если его размер превышает 1 ГиБ.
- Системному диску можно назначить дополнительную роль, только если его размер не меньше 100 ГиБ.
- Жесткие диски с черепичной магнитной записью (SMR) можно использовать только с ролью **Хранилище** и только в случае, если на сервере есть твердотельный диск с ролью **Кэш**.
- Нельзя использовать на одном уровне хранилища стандартные и SMR-диски.
- Нельзя одновременно назначить роли системным и несистемным дискам.

Предварительные требования

- Четкое понимание архитектуры кластера хранения данных и ролей дисков, которые разъясняются в разделе "О кластере хранилища данных" на странице 12.
- Отказавший диск освобожден (см. раздел "Освобождение дисков сервера" на странице 819), новый диск для замены подключен к серверу.

Чтобы вручную назначить роли новому диску

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по имени сервера.
2. На вкладке **Диски** щелкните по новому диску, которому не присвоена роль.
3. На правой панели диска нажмите **Назначить роль**.
4. В окне **Назначить роль** выберите роль, то есть способ использования диска.
   - [Только для твердотельных накопителей] Как хранить кэш записи
     a. Выберите роль **Кэш**.
     b. Выберите уровень хранилища, который следует кэшировать.

     Примечание
     Для того чтобы диски использовали кэш, роль **Кэш** необходимо назначить до назначения роли **Хранилище**.

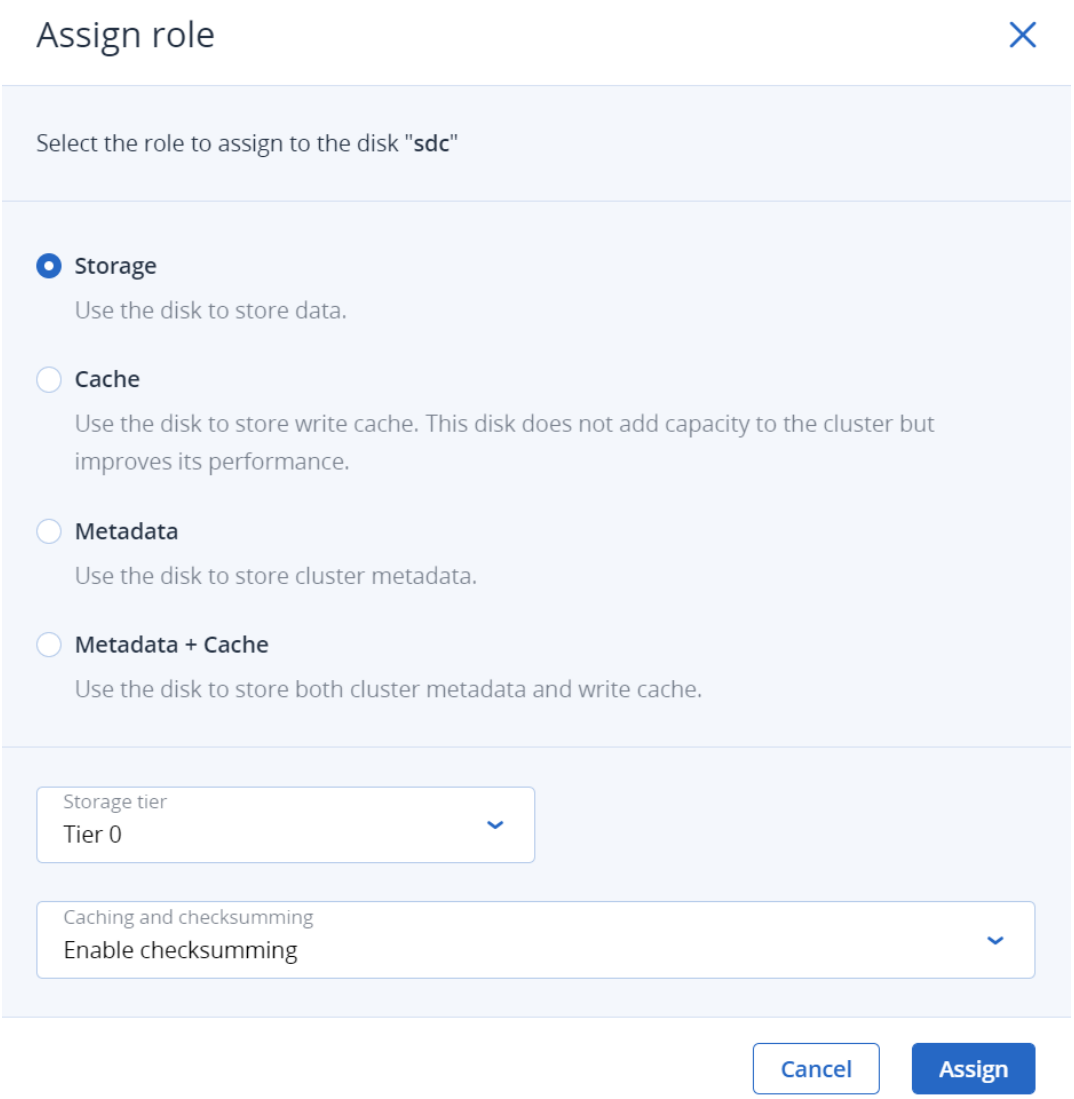
   - Как организовать хранение данных
     a. Выберите роль **Хранилище**.
     b. Выберите уровень хранилища для размещения данных. Чтобы повысить эффективность избыточности данных, не назначайте все диски сервера на один и тот же уровень. Вместо этого убедитесь, что каждый из уровней равномерно распределен по кластеру и на каждом сервере ему назначено по одному диску.
     c. Включите кэширование данных и проверку контрольных сумм:
        - **Использовать диск SSD для кэширования и проверки контрольных сумм**. Доступно и рекомендуется только для серверов с твердотельными накопителями.
        - **Включить проверку контрольных сумм** (по умолчанию). Рекомендуется для серверов с жесткими дисками, так как обеспечивает повышенную надежность.
        - **Отключить проверку контрольных сумм**. Не рекомендуется для производственной среды. В среде оценки или тестирования можно отключить проверку контрольных сумм для серверов с жесткими дисками для повышения производительности.
   - Как хранить метаданные кластера
     Выберите роль **Метаданные**.

     Примечание
     Рекомендуется не больше одного сервиса метаданных на сервер и не больше пяти сервисов метаданных для кластера.

   - [Только для твердотельных накопителей] Как хранить метаданные и кэш записи

a. Выберите роль **Метаданные+Кэш**.

b. Выберите уровень хранилища, который следует кэшировать.



5. Нажмите **Назначить**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node disk assign --disk <disk>:<role>[:<key=value,...>]
                        [--node <node>]
```

--disk <disk>:<role>[:<key=value,...>]

Конфигурация диска в формате:

- <disk>: идентификатор или имя дискового устройства
- <role>: роль диска (cs, mds, journal, mds-journal, mds-system, cs-system, system)

- разделенные запятыми пары key=value с ключами (необязательно):
  - tier: уровень диска (0, 1, 2 или 3)
  - journal-tier: уровень диска журнала (кэша) (0, 1, 2 или 3)
  - journal-type: тип диска журнала (кэша) (no_cache – без кэша, inner_cache – внутренний кэш или external_cache – внешний кэш)
  - journal-disk: идентификатор или имя устройства диска журнала (кэша)
  - bind-address: IP-адрес привязки для сервиса метаданных

  Например: sda:cs:tier=0,journal-type=inner_cache.
  Этот параметр можно указывать несколько раз.

--node <node>

Идентификатор или имя хоста сервера (по умолчанию node001.vstoragedomain)

Например, чтобы назначить роль cs диску sdc на сервере node003, выполните:

```
# vinfra node disk assign --disk sdc:cs --node node003
```

Просмотреть сведения о конфигурации дисков сервера можно в выводе команды vinfra node disk list:

```
# vinfra node disk list --node node003
+--------------------------------------+--------+------+------------+-------------+---------+----------+---------------+-----
-------+---------------+
| id                                   | device | type | role       | disk_status | used    | size     | physical_size | service_id |
service_status |
+--------------------------------------+--------+------+------------+-------------+---------+----------+---------------+-----
-------+---------------+
| 2A006CA5-732F-4E17-8FB0-B82CE0F28DB2 | sdc    | hdd  | cs         | ok          | 11.2GiB | 125.8GiB |
128.0GiB     | 1026       | active        |
| 642A7162-B66C-4550-9FB2-F06866FB7EA1 | sdb    | hdd  | cs         | ok          | 8.7GiB  | 125.8GiB |
128.0GiB     | 1025       | active        |
| 45D38CD2-3B94-4F0F-8864-9D51F716D3B1 | sda    | hdd  | mds-system | ok          | 21.0GiB |
125.9GiB | 128.0GiB     | 1          | avail         |
+--------------------------------------+--------+------+------------+-------------+---------+----------+---------------+-----
-------+---------------+
```

9.6 Выключение и запуск кластера

Предварительные требования

- Если развернут вычислительный кластер, остановите все запущенные виртуальные машины и убедитесь, что ВМ не находятся в переходном состоянии.
- Если развернут кластер блочного хранилища или NFS, перед остановкой сервисов отключите iSCSI LUN и экспорты NFS на стороне клиента. В противном случае при остановке кластера данные могут быть утеряны.

Чтобы выключить весь кластер

1. Выключите серверы кластера, на которых не работают сервисы метаданных. Чтобы определить такие серверы, перейдите на экран **Инфраструктура** > **Серверы** и найдите серверы без сервиса **Метаданные**. На каждом из этих серверов выполните следующие действия.
   - Если у вас есть удаленный доступ к серверу, выполните следующую команду:

     ```
     # shutdown -h now
     ```

   - Если у вас есть физический доступ к серверу, один раз кратковременно нажмите кнопку питания.
2. Выключите серверы кластера с сервисами метаданных с помощью команды из предыдущего шага.

Чтобы запустить кластер

1. Загрузите серверы, на которых размещены сервисы **Метаданные** и (или) **Панель администрирования**.
2. Включите остальные узлы кластера.
3. Проверьте статусы кластера хранилища и вычислительного кластера, прежде чем приступить к работе с Кибер Инфраструктура.

9.7 Освобождение серверов из кластера хранилища

Освобождение сервера означает его удаление из кластера. После инициирования освобождения кластер хранилища начнет реплицировать фрагменты данных, которые хранились на освобождаемом сервере, а затем распределять их между другими серверами хранилища в кластере. В зависимости от объема реплицируемых данных этот процесс может занять до нескольких часов. При необходимости можно также освободить сервер принудительно, то есть без репликации.

Предупреждение
Принудительное освобождение серверов может привести к потере данных.

Предварительные требования

- Если на этом сервере работает один из трех необходимых сервисов метаданных, добавьте роль метаданных другому серверу. Нужно гарантировать работу в любой момент времени как минимум трех сервисов метаданных.
- Если сервер содержит точки доступа, такие же точки доступа настроены и на других серверах кластера.
- Если сервер входит в группу целевых устройств iSCSI, удалите его сначала из группы целевых устройств.
- Если на сервере есть шлюз S3 или Backup Gateway, удалите IP-адреса из записей DNS для точек доступа S3 и Backup Gateway. Затем освободите сервер из кластеров S3 и Backup Gateway.

- Если сервер входит в вычислительный кластер, удалите его из вычислительного кластера.
- В кластере достаточно пространства для размещения данных с освобождаемого сервера.

Чтобы освободить сервер из кластера хранилища

Панель администратора

1. На экране **Инфраструктура** > **Серверы** щелкните по строке с сервером, который следует освободить.
2. На правой панели нажмите **Освободить сервер**.
3. (Необязательно, настоятельно не рекомендуется) Для освобождения сервера без переноса данных выберите **Освободить без миграции данных**.
4. Нажмите кнопку **Освободить**.

Освобожденный сервер будет отображаться со статусом **Не назначен** на экране **Инфраструктура** > **Серверы**.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node release [--force] <node>
```

--force
: Освобождение сервера без миграции данных

<node>
: Идентификатор сервера или имя хоста

Например, чтобы освободить сервер node005 из кластера хранилища с миграцией данных для обеспечения соответствия заданному уровню избыточности, выполните:

```
# vinfra node release node005
```

9.8 Удаление неназначенных серверов

Чтобы полностью удалить сервер из инфраструктуры, требуется удалить его из кластера хранилища.

Предварительные требования

- Сервер полностью удален из кластера хранилища в соответствии с инструкциями в разделе "Освобождение серверов из кластера хранилища" на предыдущей странице.

Чтобы удалить сервер из инфраструктуры

Панель администратора

1. Выберите неназначенный сервер на экране **Инфраструктура** > **Серверы** и нажмите **Удалить**.
2. В целях безопасности очистите сертификаты и удостоверения серверов путем удаления следующих элементов из сервера:

```
# rm -rf /usr/libexec/vstorage-ui-backend/ca
# rm -rf /etc/nginx/ssl
# rm -f /etc/vstorage/host_id
# rm -f /etc/vstorage/vstorage-ui-agent.conf
```

Примечание
После такой очистки единственным способом добавить сервер обратно в кластер будет повторная установка на него программы Кибер Инфраструктура с нуля.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra node forget <node>
```

<node>

Идентификатор сервера или имя хоста

Например, чтобы удалить сервер node005 из продукта Кибер Инфраструктура, выполните:

```
# vinfra node forget node005
```

9.9 Повторное добавление неназначенных серверов

Серверы, удаленные из инфраструктуры, можно повторно добавить как неназначенные. Если инфраструктура не содержит узлов, сначала добавьте сервер управления, а затем подчиненные серверы.

Ограничения

- Если перед освобождением сервер был очищен, повторно установите на него Кибер Инфраструктура.

Предварительные требования

- Сервер полностью удален из инфраструктуры в соответствии с инструкциями в разделе "Удаление неназначенных серверов" на предыдущей странице.

Чтобы повторно добавить сервер управления в инфраструктуру

Выполните вход на сервер с помощью SSH и запустите следующий скрипт:

```
# /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <MN_IP_address> -x <public_
iface>
```

где:

- <MN_IP_address> – это IP-адрес сервера управления во внутренней сети управления;
- <public_iface> – имя интерфейса общедоступной сети, подключенного к сети панели администрирования.

Чтобы получить значения обоих параметров, используйте команду ip a.

Чтобы повторно добавить сервер в инфраструктуру

Выполните вход на сервер с помощью SSH и запустите следующий скрипт:

```
# /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <MN_IP_address> -t <token>
```

где:

- <MN_IP_address> – IP-адрес частного сетевого интерфейса на сервере с панелью администрирования;
- <token> – токен, полученный на панели администрирования.

9.10 Возможные ошибки при входе в систему

В данном разделе описаны возможные ошибки при входе в продукт Кибер Инфраструктура и методы их устранения.

1. **Системный администратор не может войти в панель администратора или интерфейс командной строки vinfra. Пользовательский интерфейс показывает ошибку "Служба недоступна".**

   Возможные причины:

   - Неправильный URL-адрес для входа в систему.

     В обычной конфигурации используйте IP-адрес узла с установленным сервисом "Панель администратора".

     В конфигурации высокой доступности используйте виртуальный IP-адрес, указанный при создании конфигурации. В случае если при использовании виртуального IP-адреса ошибка сохраняется, попробуйте использовать IP-адрес каждого узла, который входит в конфигурацию высокой доступности (возможно, на каком-то узле работает служба vstorage-ui-backend).
   - Служба vstorage-ui-backend на узле выключена или находится в состоянии сбоя.

     Проверьте статус службы с помощью команды:

     ```
     systemctl status vstorage-ui-backend
     ```

     Перезапустите службу, если она выключена или находится в состоянии сбоя. В конфигурации высокой доступности служба vstorage-ui-backend запускается только на главном узле.
2. **Пользовательский интерфейс показывает ошибку "Неверный логин или пароль".**

Возможные причины:

- Неправильный пароль.

  Восстановите пароль с помощью следующих команд:

  ```
  su - vstoradmin
  source /opt/rh/rh-python36/enable
  UI_BACKEND_CONFIG=~/etc/backend.cfg python manage.py admin -p <new-password>
  ```

- Не работает служба идентификации.

  Проверьте логи в файле var/log/storage-ui-backend/messages.log.

- Пользователь заблокирован за несколько (по умолчанию – 10) попыток входа в систему с неверным паролем.

  Чтобы найти IP-адрес заблокированной учетной записи, найдите в файле /var/log/messages запись вида "Вход с 10.250.9.9 заблокирован" или используйте журнал аудита. Открыть журнал можно с помощью команды:

  ```
  vinfra cluster auditlog show <audit-log-id>
  ```

  Узнать ID журнала аудита можно с помощью команды:

  ```
  vinfra cluster auditlog list
  ```

  Разблокируйте учетную запись пользователя с помощью команд:

  ```
  su - vstoradmin
  source /opt/rh/rh-python36/enable
  UI_BACKEND_CONFIG=~/etc/backend.cfg python manage.py login-unlock --user <user-
  name> --
  ip-address <blocked-ip>
  ```

  где:

  - <user-name> – имя заблокированной учетной записи;
  - <blocked-ip> – IP-адрес заблокированной учетной записи.

3. **Программа командной строки vinfra выдает ошибку "Incorrect password or username (UNAUTHORIZED)".**

   Возможные причины:

   - Пользователь может быть заблокирован после нескольких попыток ввода неправильного пароля (см. выше).
   - Указана недопустимая переменная окружения VINFRA_PASSWORD.

     Сбросьте значение переменной с помощью команд:

     ```
     env | grep VINFRA_PASSWORD
     unset VINFRA_PASSWORD
     ```

   - Указана недопустимая переменная окружения VINFRA_PORTAL.

     Сбросьте значение переменной с помощью команды:

```
env | grep VINFRA_PORTAL
unset VINFRA_PORTAL
```

- Доменное имя сервера управления (по умолчанию backend-api.svc.vstoragedomain) не ссылается на IP-адрес узла с установленным сервисом "Панель администратора" (IP-адрес из сети с эксклюзивным типом трафика "Internal management").

  Проверьте IP-адреса, на которые ссылается доменное имя сервера управления, с помощью команды:

  ```
  getent hosts backend-api.svc.vstoragedomain
  ```

10 Получение технической поддержки

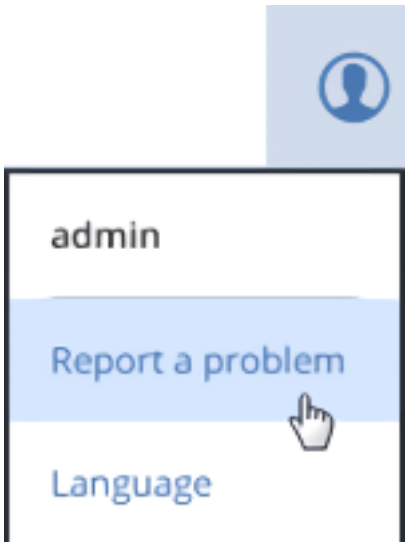
Если вам понадобится техническая поддержка, можно отправить отчет о неполадке в службу технической поддержки и связаться с ней. При создании отчета о неполадке ему присваивается идентификатор. Обязательно укажите этот идентификатор в запросе в службу поддержки.

В случае проблем с подключением к серверу отчетов или в случае, если отчет слишком большой для отправки по электронной почте, этот отчет можно найти в каталоге /var/cache/problem-reports/ на сервере управления.

Создание и отправка отчета о неполадке

Панель администратора

1. На любом экране щелкните по значку пользователя в правом верхнем углу и выберите **Сообщить о проблеме**.



2. Введите свой контактный адрес электронной почты, опишите проблему в сообщении и нажмите **Сформировать и отправить**. Статус отчета будет отображаться в правом нижнем углу.

Всплывающее окно можно скрыть, не прерывая создания отчета. Идентификатор отчета будет доступен в центре уведомлений.

Интерфейс командной строки

Используйте следующую команду:

```
vinfra cluster problem-report [--email <email>] [--description <description>] [--send]
```

--email <email>

Контактный адрес электронной почты

--description <description>

Описание неполадки

--send

Создать архив с отчетом о неполадке и отправить его в службу технической поддержки

Например, чтобы отправить отчет о неполадке с описанием “Test report” в службу технической поддержки, использовав адрес test@example.com в качестве обратного адреса электронной почты, выполните:

```
# vinfra cluster problem-report --email test@example.com --description "Test report" --send
+---------+--------------------------------------+
| Field   | Value                                |
+---------+--------------------------------------+
| task_id | 8bcfb92f-f02b-4de8-8e44-3426047630e3 |
+---------+--------------------------------------+
# vinfra task show 8bcfb92f-f02b-4de8-8e44-3426047630e3
+---------+------------------------------------------------------------+
| Field   | Value                                                      |
+---------+------------------------------------------------------------+
| details |                                                            |
| name    | backend.presentation.reports.tasks.ReportProblemTask       |
| result  | id: '1001923113'                                           |
|         | path: /var/cache/problem-reports/report-<...>.391329.tar.gz |
| state   | success                                                    |
| task_id | 8bcfb92f-f02b-4de8-8e44-3426047630e3                       |
+---------+------------------------------------------------------------+
```

Обратите внимание на идентификатор отчета о неполадке в сведениях о задаче. Его нужно будет ввести в запросе в службу поддержки.

Обращение в службу технической поддержки

Зайдите на страницу поддержки по адресу https://cyberprotect.ru/support.

Указатель

С

Сетевые карты для DPDK 46

А

Аварийное восстановление виртуальных машин 520

Автоматическая балансировка данных 40

Автоматическая настройка новых дисков хранилища 817

Авторизация пользователей томов NFS с помощью LDAP 421

Анализаторы состояния диска 697

Архитектура вычислительного кластера 23

Архитектура вычислительных сетей 23

Архитектура хранилища объектов 20

Аутентификация пользователей томов NFS с помощью Kerberos 418

Б

Без избыточности 31

В

Включение RDMA 136

Включение ведения журнала для виртуальных машин 446

Включение высокой доступности сервера управления 146

Включение георепликации 356

Включение георепликации S3 409

Включение горячей замены ЦП и ОЗУ для каждого домена 305

Включение доступа по SNMP 739

Включение и выключение балансировщиков нагрузки 584

Включение и отключение перераспределения ОЗУ 434

Включение межрегиональной репликации S3 411

Включение поддержки сквозной передачи и виртуализации графических карт в

вычислительном кластере 501

Включение шифрования данных 320

Возвращение огражденных узлов к работе 654

Возможные ошибки при входе в систему 827

Восстановление базы данных управления в вычислительном кластере 814

Восстановление базы данных управления из резервной копии 813

Восстановление стандартных правил брандмауэра для исходящих подключений 267

Вход через поставщиков удостоверений 301

Выключение и запуск кластера 823

Выполнение команд в виртуальных машинах без сетевого подключения 511

Выполнение обслуживания сервера 805

Выполнение переключения при сбое 360

Выполнение переключения при сбое балансировщика нагрузки 585

Высвобождение серверов из хранилища резервных копий 370

Высокая доступность 27

Высокая доступность для служб 27

Высокая доступность и вычислительный кластер 29

Д

Диаграмма «Выделено в ЦП» 777

Диаграмма «Выделено ОЗУ» 778

Диаграмма «Выделено хранилища» 782

Диаграмма «Логическое пространство» 732

Диаграмма «Оповещения» 785

Диаграмма «Сервисы» 726

Диаграмма «Список ВМ с наибольшим потреблением ресурсов» 784

Диаграмма «Статус ВМ» 783

Диаграмма «Физическое пространство» 730

Диаграмма «Фрагменты данных» 727

Диаграммы активности ввода-вывода 725

Добавление внешних DNS-серверов 139

Добавление ключей SSH для виртуальных машин 457

Добавление пользователей S3 214

Добавление поставщиков удостоверений 297

Добавление пространства подкачки 433

Добавление серверов в кластер NFS 417

Добавление серверов в кластер S3 400

Добавление узлов в вычислительный кластер 641

Добавление узлов в хранилище резервных копий 350

Добавление хранилищ резервных копий в Кибер Бэкап и Кибер Бэкап облачный 167

Добро пожаловать в Кибер Инфраструктура! 11

Доступ к информационным объектам кластера с помощью SNMP 740

Доступ к панели администрирования через SSL 316

З

Загрузка образов виртуальных машин 437

Замена дисков серверов 817

Защита данных во время отключений электроэнергии 71

Защита трафика API OpenStack с помощью SSL 181

Заявление об авторских правах 2

И

Избыточность данных 29

Избыточность посредством избыточного кодирования 31

Избыточность посредством репликации 30

Изменение IP-адреса панели самообслуживания 314

Изменение и удаление вычислительных сетей 548

Изменение и удаление поставщиков удостоверений 302

Изменение и удаление размещений 652

Изменение конфигурации виртуальных машин 478

Изменение конфигурации сети 268

Изменение назначения групп безопасности 557

Изменение параметров в файлах конфигурации OpenStack 429

Изменение параметров вычислительного кластера 427

Изменение параметров кластеров Kubernetes 633

Изменение параметров сервиса Kubernetes 640

Изменение параметров сетевого интерфейса 230

Изменение политики хранилища тома 608

Изменение правил политики качества обслуживания 600

Изменение размера томов 607

Изменение ресурсов виртуальных машин 478

Изменение сетевых интерфейсов 117

Изменение срока хранения метрик 660

Изменение схемы избыточности для хранилища резервных копий 354

Изменение типа виртуальной графической карты для физических графических карт 505

Изменение типа ВМ по умолчанию для балансировщика нагрузки 593

Использование Alertmanager для оповещений 756

Использование SSD-накопителей 65

Использование внешнего Prometheus для мониторинга 753

Использование встроенного Prometheus для мониторинга 751

Использование интерфейса командной строки 108

Использование политик качества обслуживания для томов 625

Использование программы DRS Visualizer 791

Использование сетевых политик качества обслуживания 596

Использование учета для вычислительных ресурсов 656

К

Клонирование томов 610

Количество дисков на сервер 60

Количество серверов 49

Конфигурация кэша 67

Конфигурация с жесткими дисками и твердотельными накопителями 61

М

Масштабирование кластера хранилища 240

Масштабирование файлового хранилища 223

Масштабирование хранилища объектов 215

Метрики Prometheus 757

Метрики дисков в Prometheus 699

Метрики обновления кластера 764

Метрики основного хранилища 757

Метрики хранилища объектов 758

Метрики хранилища резервных копий 760

Миграция виртуальных машин 491

Миграция виртуальных машин в Кибер Инфраструктуру 513

Миграция виртуальных машин в Кибер Инфраструктуру в автономном режиме 515

Миграция виртуальных машин в Кибер Инфраструктуру онлайн 518

Мониторинг 667

Мониторинг балансировщиков нагрузки 788

Мониторинг блочного хранилища 768

Мониторинг виртуальных машин 787

Мониторинг вычислительного кластера 775

Мониторинг вычислительных узлов 786

Мониторинг дисков сервера 688

Мониторинг журналов событий 720

Мониторинг кластера с помощью Zabbix 742

Мониторинг кластера хранилища данных 706

Мониторинг клиентов 716

Мониторинг нагрузки на вычислительные серверы 789

Мониторинг нагрузки на уровни хранилища 734

Мониторинг объектов кластера с помощью SNMP 739

Мониторинг параметров репликации 724

Мониторинг производительности сервера 688

Мониторинг серверов инфраструктуры 686

Мониторинг серверов метаданных 710

Мониторинг серверов фрагментов данных 711

Мониторинг сетевых интерфейсов сервера 704

Мониторинг файлового хранилища 773

Мониторинг физических дисков 718

Мониторинг хранилища объектов 771

Мониторинг хранилища резервных копий 765

Мультитенантность 40

Н

Назначение и отмена назначения расположений 649

Назначение политик качества обслуживания 599

Назначение пользователей нескольким доменам 309

Назначение стандартной политики качества обслуживания 599

Настройка PXE-сервера 87

Настройка RDMA 139

Настройка аутентификации и авторизации пользователей 418

Настройка аутентификации на виртуальной машине устройства 514

Настройка быстрой сети DPDK для виртуальных машин 194

Настройка высокой доступности виртуальных машин 487

Настройка загрузочных томов Windows 442

Настройка инструмента командной строки для управления блочным хранилищем 199

Настройка модели ЦП виртуальных машин 178

Настройка мультитенантности 182

Настройка новых дисков вручную 820

Настройка памяти для виртуальных машин 432

Настройка панели самообслуживания 314

Настройка параметров TLS для хранилища объектов 415

Настройка параметров TLS для хранилища резервных копий 365

Настройка параметров памяти для кластера 332

Настройка параметров памяти для сервера 334

Настройка параметров памяти для сервисов хранилища 331

Настройка политики хранения для метрик Prometheus 755

Настройка пользовательских режимов избыточности данных 224

Настройка правил брандмауэра для входящих подключений 258

Настройка правил брандмауэра для исходящих подключений 263

Настройка производительности дисков NVMe 339

Настройка прокси для хранилища резервных копий 363

Настройка сетевых интерфейсов виртуальных машин 481

Настройка сетевых интерфейсов серверов 117

Настройка сетей 110

Настройка сетей в вычислительном кластере 113

Настройка сетей для блочного хранилища 111

Настройка сетей для файлового хранилища 113

Настройка сетей для хранилища объектов 112

Настройка сетей для хранилища резервных копий 110

Настройка томов виртуальных машин 485

Настройка устройств InfiniBand 134

Настройка устройств RoCE 136

Настройка фирменной символики для панели самообслуживания 315

О

О вычислительном кластере 22

О кластере хранилища данных 12

О файловом хранилище 21

О хранилище блочных данных 17

О хранилище объектов 19

О хранилище резервных копий 16

Об архитектуре кэша хранилища 15

Об инфраструктуре 12

Обеспечение административного доступа к серверам кластера через SSH 318

Обеспечение доступа к панели самообслуживания 190

Области отказа 35

Обновление кластеров Kubernetes 639

Обновление конфигурации георепликации 361

Обновление сертификата для хранилища резервных копий 351

Обновление сертификатов кластеров Kubernetes 639

Обслуживание 798

Общие сведения о распределяемом дисковом пространстве 714

Общие сведения об использовании дискового пространства 713

Общие требования 46

Объекты и ловушки кластера 746

Ограничение доступа к группам целевых устройств 383

Оповещения инфраструктуры 669

Оповещения основного хранилища 675

Оповещения хранилища объектов 678

Определение классов хранения объектов 407

Освобождение дисков сервера 819

Освобождение ресурсов виртуальных машин 493

Освобождение серверов из кластера хранилища 824

Освобождение серверов из кластеров S3 416

Освобождение узлов из вычислительного кластера 655

Отключение георепликации 362

Отправка уведомлений по электронной почте 329

П

Параметры kickstart 91

Переключение между режимом сквозной передачи и виртуализацией графических карт 503

Перестроение кластера 38

Повторная регистрация хранилища резервных копий в новом экземпляре Кибер Бэкап 352

Повторное добавление неназначенных серверов 826

Подготовка вычислительных ресурсов к работе 168

Подготовка загрузочного носителя 81

Подготовка загрузочного носителя для виртуальных машин 437

Подготовка загрузочных томов 449

Подготовка к работе балансировщиков нагрузки 191

Подготовка к работе кластеров Kubernetes 192

Подготовка к работе учета и биллинга 193

Подготовка пространства для блочного хранилища к работе 197

Подготовка пространства для файлового хранилища 217

Подготовка пространства для хранилища объектов 207

Подготовка пространства для хранилища резервных копий к работе 150

Подготовка серверов для использования SR-IOV 499

Подготовка серверов для виртуализации графических карт 497

Подготовка серверов для сквозной передачи GPU 495

Подготовка шаблонов 440

Поддерживаемые гостевые операционные системы 435

Поддерживаемые заголовки запросов Amazon 398

Поддерживаемые заголовки ответов Amazon 399

Поддерживаемые заголовки ответов об ошибках Amazon 399

Поддерживаемые операции и методы REST Amazon S3 396

Поддерживаемые схемы проверки подлинности 400

Поддерживаемые функции Amazon S3 395

Подключение виртуальных коммутаторов к магистральным интерфейсам 530

Подключение к виртуальным машинам 469

Подключение к интерфейсу командной строки OpenStack 427

Подключение к серверу с помощью консоли VNC 89

Подключение удаленных устройств iSCSI к серверам кластера 235

Поиск и устранение неисправностей виртуальных машин 527

Поиск и устранение неисправностей установки 106

Политики хранения 37

Получение технической поддержки 830

Получение файла kubeconfig 632

Получение шаблонов Linux 440

Понятия и функции 27

Правила политики качества обслуживания 596

Предоставление учетных данных для vinfra 109

Пример файла kickstart 94

Пример хранилища объектов 21

Присоединение ISO-образов к виртуальным машинам 476

Присоединение виртуального диска IPMI 84

Присоединение и отсоединение томов 605

Присоединение томов к группам целевых устройств 205

Присоединение физических устройств PCI к виртуальным машинам 494

Проверка сетевой инфраструктуры RDMA 137

Проверка функций сброса данных на диски 71

Прослушивание ловушек SNMP 741

Просмотр журнала аудита 681

Просмотр журналов кластера 683

Просмотр и изменение параметров хранилища резервных копий 367

Просмотр использования исходящего трафика 661

Просмотр использования ресурсов на уровне проекта 662

Просмотр оповещений 667

Просмотр пространства, занятого фрагментами данных 716

Просмотр ресурсов, метрик и измерений 658

Просмотр сведений о балансировщиках нагрузки 583

Просмотр сведений о виртуальных маршрутизаторах 565

Просмотр сведений о вычислительных сетях 547

Просмотр сведений о группах безопасности 558

Просмотр сведений о кластерах Kubernetes 632

Просмотр сведений о томах 612

Р

Развертывание виртуальной машины устройства 514

Развертывание и настройка 108

Развертывание кластера хранилища данных 141

Разрешение администраторам домена управлять проектами 307

Расчет размера журнала записи 66

Расчет состояния диска 696

Редактирование и удаление доменных групп 295

Режимы избыточности 32

Режимы размещения 643

Резервное копирование базы данных управления 812

Резервное копирование и восстановление базы данных управления 811

Рекомендации для конфигурации серверов с несколькими дисками 64

Рекомендации по использованию S3 в продукте 404

Рекомендации по оборудованию 45

Рекомендации по сети 76

Рекомендуемое оборудование 45

Репликация данных S3 между центрами обработки данных 408

С

Серверы 46

Сетевые карты для RDMA 45

Сетевые порты 78

Снятие назначенных политик качества обслуживания 601

Создание виртуальных вычислительных сетей 540

Создание виртуальных маршрутизаторов 562

Создание виртуальных машин 460

Создание виртуальных машин с виртуальными графическими процессорами 506

Создание виртуальных машин с загрузкой UEFI 509

Создание виртуальных машин с сетевыми портами SR-IOV 507

Создание виртуальных машин с физическим графическим процессором 505

Создание вычислительного кластера 169

Создание групп целевых устройств 199

Создание дисков virtIO для виртуальных машин 510

Создание доменных групп 289

Создание загрузочного USB-накопителя 82

Создание и назначение роли менеджера квот 307

Создание и удаление балансировщиков нагрузки 580

Создание и удаление групп безопасности 550

Создание и удаление кластеров Kubernetes 628

Создание и удаление томов 602

Создание интерфейсов VLAN 131

Создание кластера NFS 217

Создание кластера S3 208

Создание объединений сетевых интерфейсов 127

Создание политик качества обслуживания 597

Создание пользовательских типов виртуальных машин 453

Создание правил брандмауэра для исходящих подключений 265

Создание размещений 647

Создание томов 204

Создание томов NFS 218

Создание файла kickstart 91

Создание физических вычислительных сетей 532

Создание хранилища резервных копий в локальном кластере 151

Создание хранилища резервных копий в публичном облаке 154

Создание хранилища резервных копий на внешнем томе NFS 163

Создание шаблонов 447

Создание экспортов NFS 220

Составление списка правил брандмауэра для исходящих подключений 267

Стандартные правила брандмауэра для исходящих подключений 264

Сценарии kickstart 92

Т

Типы трафика 42

Требования для вычислительного кластера 54

Требования для панели администрирования 80

Требования для хранилища объектов 56

Требования к дискам 58

Требования к серверу 46

Требования к сети 73

Требования к сети для вычислительного кластера 74

Требования к сети для компонента «Kubernetes как услуга» 75

Требования к сети для хранилища резервных копий 73

Требования к сети и рекомендации 73

Требования к системе 45

Требования к хранилищам в виртуальных машинах 54

Требования к хранилищам в локальных кластерах 51

Требования к хранилищам в публичных облаках 53

Требования к хранилищам в томах NFS 52

Требования к хранилищу резервных копий 50

У

Увеличение количества шлюзов S3 на серверах кластера S3 215

Удаление виртуальных маршрутизаторов 576

Удаление виртуальных машин 528

Удаление дополнений гостевой ОС 473

Удаление неназначенных серверов 825

Удаление правил брандмауэра для исходящих подключений 266

Удаление серверов из кластера NFS 426

Удаленный мониторинг кластера 751

Управление 225

Управление автоматической балансировкой нагрузки на вычислительные серверы 664

Управление автоматической балансировкой нагрузки на уровни хранилища 341

Управление балансировщиками нагрузки 580

Управление безопасностью 316

Управление блочным хранилищем 372

Управление виртуальными маршрутизаторами 561

Управление виртуальными машинами 435

Управление виртуальными машинами в размещениях 490

Управление вычислительной сетью 529

Управление вычислительным кластером 427

Управление вычислительным хранилищем 602

Управление вычислительными подсетями 546

Управление вычислительными серверами 641

Управление вычислительными сетями 529

Управление вычислительными томами 602

Управление георепликацией для хранилища резервных копий 356

Управление группами безопасности 550

Управление группами домена 289

Управление группами рабочих серверов 635

Управление группами целевых устройств 373

Управление доменами, пользователями и проектами 273

Управление дополнениями гостевой ОС 470

Управление заданиями vinfra 110

Управление интерфейсами маршрутизаторов 566

Управление инфраструктурой 225

Управление кластерами Kubernetes 628

Управление конфигурацией высокой доступности 815

Управление корзинами S3 403

Управление лицензиями 322

Управление моментальными снимками томов 615

Управление назначением пользователей в группы домена 292

Управление назначением проекта в группы домена 293

Управление образами 524

Управление обычными типами трафика 249

Управление паролем кластера хранилища 336

Управление плавающими IP-адресами 576

Управление политиками хранения 619

Управление пользовательскими типами трафика 250

Управление пользователями CHAP 386

Управление пользователями S3 401

Управление пользователями панели администратора 275

Управление пользователями самообслуживания 279

Управление поставщиками удостоверений 296

Управление правилами групп безопасности 553

Управление представлениями LUN 393

Управление проектами 283

Управление проектами в качестве администратора домена 308

Управление пулами балансировки 585

Управление размещениями для вычислительных узлов 643

Управление расположением серверов 225

Управление свойствами домена 311

Управление серверами в группах целевых устройств 389

Управление серверами инфраструктуры 225

Управление сетевыми интерфейсами 233

Управление сетями 254

Управление сетями инфраструктуры 245

Управление соединениями VPN 594

Управление состоянием активности виртуальных машин 474

Управление списками управления доступом 383

Управление статическими маршрутами 572

Управление технологией Fast Path 338

Управление типами трафика 245

Управление токенами 337

Управление томами 379

Управление томами NFS 422

Управление уведомлениями 326

Управление хранилищем объектов 395

Управление хранилищем резервных копий 350

Управление хранилищем файлов 417

Управление целевыми устройствами и их порталами 376

Управление эксклюзивными типами трафика 245

Управление экспортами NFS 424

Уровни хранения данных 36

Установка 81

Установка в автоматическом режиме 103

Установка в ручном режиме 96

Установка доменного имени для API вычислений 180

Установка дополнений гостевой ОС 471

Установка лицензий SPLA 325

Установка лицензионных ключей 323

Установка обновлений 798

Устранение неполадок дисков сервера 701