КИБЕРПРОТЕКТ

КИБЕР Инфраструктура

Версия 5.0.1

Руководство по знакомству с продуктом

Редакция: 13.03.2024

Заявление об авторских правах

Все права защищены.

Все остальные упоминаемые товарные знаки могут быть зарегистрированными товарными знаками соответствующих владельцев.

Распространение существенно измененных версий данного руководства запрещено без явного разрешения владельца авторских прав.

Распространение настоящих или переработанных материалов, входящих в данное руководство, в виде печатного издания (книги) запрещено без письменного разрешения их владельца.

ДОКУМЕНТАЦИЯ ПОСТАВЛЯЕТСЯ «КАК ЕСТЬ». НЕ СУЩЕСТВУЕТ НИКАКИХ ЯВНО ВЫРАЖЕННЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ОБЯЗАТЕЛЬСТВ, ПОДТВЕРЖДЕНИЙ ИЛИ ГАРАНТИЙ, В ТОМ ЧИСЛЕ И СВЯЗАННЫХ С ТОВАРНОСТЬЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИЛИ ПРИГОДНОСТЬЮ ЕГО ДЛЯ ИСПОЛЬЗОВАНИЯ В ОПРЕДЕЛЕННЫХ ЦЕЛЯХ, НАСКОЛЬКО ТАКАЯ ОГРАНИЧЕННОСТЬ ОТВЕТСТВЕННОСТИ ДОПУСКАЕТСЯ ЗАКОНОМ.

С ПО или Услугой может быть предоставлен исходный код сторонних производителей. Лицензии этих сторонних производителей подробно описаны в файле license.txt, находящемся в корневом каталоге установки.

© ООО Киберпротект, 2024

Содержание

1 Введение ... **5**

2 Планирование инфраструктуры ... **6**

2.1 Аппаратные требования ... 6

2.2 Общие сведения о политиках хранилища ... 7

3 Управление кластером хранилища данных ... **10**

3.1 Установка Кибер Инфраструктура ... 10

3.2 Настройка сетей ... 11

3.3 Создание кластера хранилища данных ... 12

4 Управление вычислительным кластером ... **15**

4.1 Создание вычислительного кластера ... 15

4.2 Выделение ресурсов ... 17

4.2.1 Создание доменов, проектов и пользователей ... 17

4.2.2 Создание политик хранилища ... 18

4.2.3 Создание вычислительных сетей ... 19

4.3 Создание виртуальных машин ... 19

5 Экспорт дискового пространства ... **21**

5.1 Экспорт дискового пространства через iSCSI ... 21

5.1.1 Создание групп целевых устройств ... 21

5.1.2 Создание томов ... 22

5.1.3 Присоединение томов к группам целевых устройств ... 22

5.1.4 Доступ к целевым устройствам iSCSI из VMware vSphere ... 22

5.2 Экспорт дискового пространства через S3 ... 23

5.2.1 Создание кластера S3 ... 24

5.2.2 Управление пользователями и корзинами S3 ... 25

5.3 Экспорт дискового пространства через NFS ... 26

5.3.1 Создание кластера NFS ... 26

5.3.2 Создание томов NFS ... 26

5.3.3 Создание и подключение экспортов NFS ... 27

6 Подключение ПО Кибер Бэкап Облачный к хранилищу резервных копий ... **28**

6.1 Создание хранилища резервных копий ... 28

6.2 Настройка Кибер Бэкап Облачный ... 29

7 Мониторинг кластера хранилища данных ... **31**

8 Включение высокой доступности ... **32**

8.1 Высокая доступность для узла управления ... 32

8.2 Высокая доступность для сервисов ... 32

© ООО Киберпротект, 2024

8.3 Проверка высокой доступности ……33

© ООО Киберпротект, 2024

1 Введение

Кибер Инфраструктура представляет собой новое поколение гиперконвергентных инфраструктур, предназначенных как для поставщиков услуг, так и для конечных пользователей. Это горизонтально масштабируемое, экономичное и многофункциональное решение, которое сочетает в себе универсальное хранилище данных с высокопроизводительной виртуализацией.

Кибер Инфраструктура работает как единое целое с Кибер Бэкап, набором продуктов Кибер Бэкап Облачный. Решение сводит к минимуму количество технологий, необходимых в центрах обработки данных, и обеспечивает дополнительные улучшения в плане производительности.

Это руководство помогает начать работу с продуктом Кибер Инфраструктура и описывает следующие шаги для тестирования основных функций.

1. Установка и настройка продукта Кибер Инфраструктура.
2. Создание кластера хранилища данных.
3. Создание вычислительного кластера и распределение его ресурсов.
4. Создание виртуальных машин.
5. Экспорт дискового пространства через iSCSI, S3, NFS, Backup Gateway.
6. Обзор встроенных средств мониторинга.
7. Включение и проверка высокой доступности.

Существует множество различных сценариев, но в этом руководстве мы подробно рассмотрим только самые распространенные. Описанные здесь процедуры являются типовыми и упрощенными в целях тестирования. Однако для продукта Кибер Инфраструктура доступна полная и подробная документация, к которой следует обратиться для дальнейших инструкций. Дополнительные сведения см. в руководстве по быстрому старту, руководстве по установке, руководстве администратора, руководстве по самообслуживанию и руководстве пользователя хранилища.

© ООО Киберпротект, 2024

2 Планирование инфраструктуры

2.1 Аппаратные требования

Продукт поддерживает множество конфигураций оборудования, которые описаны в разделе «Требования к системе» руководства администратора. Однако в целях тестирования рекомендуем развертывать три узла. Таким образом кластер гарантированно выдержит отказ одного узла без потери данных. В следующей таблице перечислены *минимальные* аппаратные требования для каждого из трех узлов. Для включения высокой доступности необходимы три узла, соответствующие требованиям к узлу управления с функциями хранения и вычислений.

Минимальные аппаратные требования к узлу

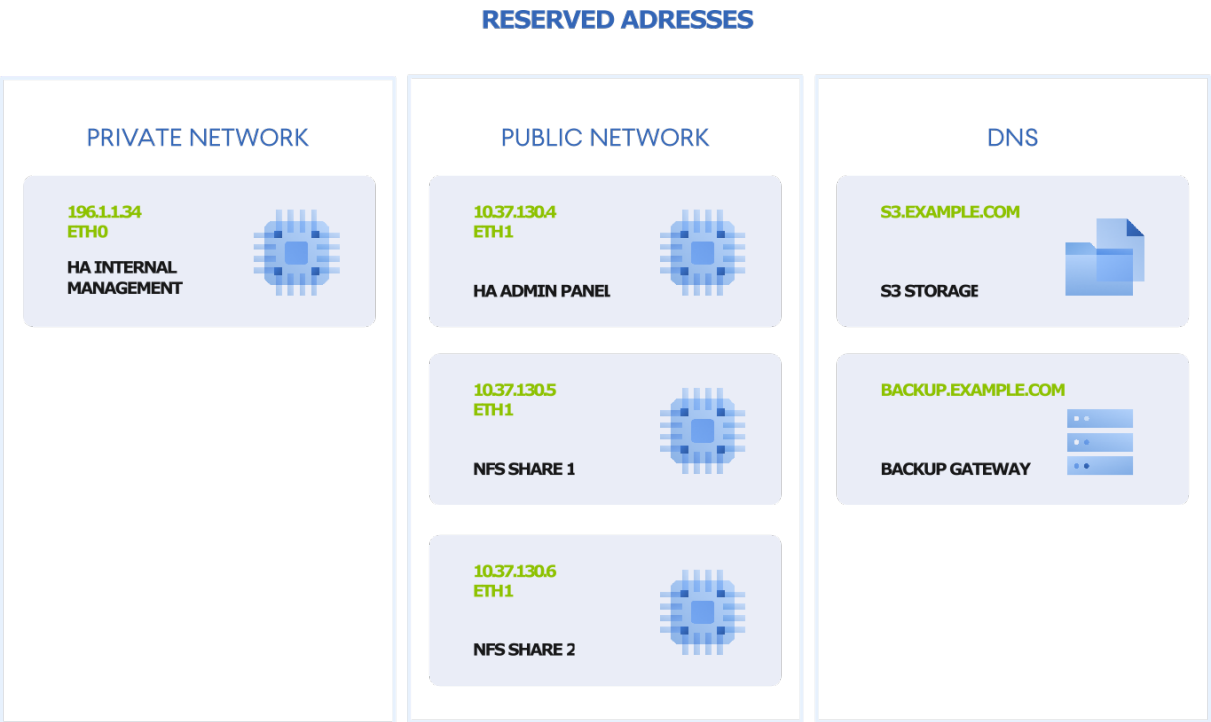
Тип	Узел управления с функциями хранения и вычислений	Подчиненный узел с функциями хранения и вычислений	Сервер управления с хранилищем и Backup Gateway
ЦП	64-разрядные процессоры x86 с включенными аппаратными расширениями виртуализации AMD-V или Intel VT		
	16 ядер*	8 ядер*	4 ядра*
ОЗУ	32 ГБ	16 ГБ	8 ГБ
Хранилище	1 диск: система + метаданные, жесткий диск SATA 100+ ГБ 1 диск: хранилище, жесткий диск SATA, размер по необходимости	1 диск: система, жесткий диск SATA 100 ГБ 1 диск: метаданные, жесткий диск SATA 100 ГБ (только на первых трех узлах в кластере) 1 диск: хранилище, жесткий диск SATA, размер по необходимости	1 диск: система + метаданные, жесткий диск SATA 120 ГБ 1 диск: хранилище, жесткий диск SATA, размер по необходимости
Сеть	10 GbE для частной сети 1 GbE для публичной сети		

*Ядро ЦП здесь означает физическое ядро в многоядерном процессоре (гиперпоточность не учитывается).

Вам также потребуются как минимум два IP-адреса во внешней сети (для высокодоступной панели администрирования и для каждого тома NFS), один IP-адрес в частной сети (для высокодоступного узла управления) и два доменных имени (для S3 и Backup Gateway).

Ниже приведен пример конфигурации сети для тестового сценария. Имена хостов и адреса могут отличаться в зависимости от ваших настроек.

© ООО Киберпротект, 2024



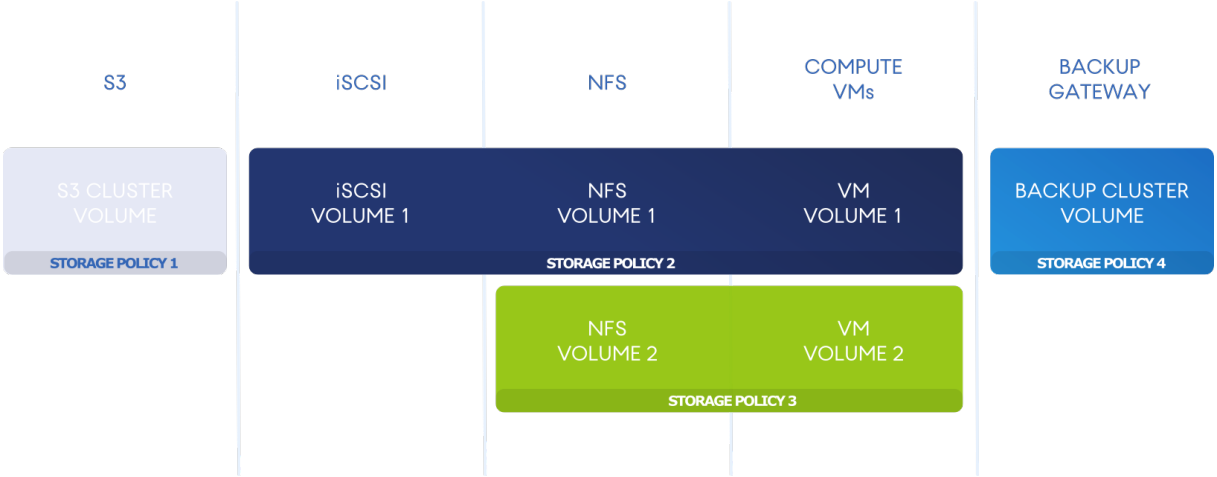
Доменные имена используются агентами резервного копирования для отправки резервных копий в облачное хранилище и извлечения из него. Если клиентские машины и узлы продукта Кибер Инфраструктура расположены в разных ЦОД, настоятельно рекомендуется настроить доменное имя. Если по какой-то причине это невозможно, необходимо вручную добавить доменное имя в файл /etc/hosts на каждом узле. Когда клиентские машины и узлы продукта Кибер Инфраструктура расположены в одном ЦОД, можно использовать локальный DNS-сервер вместо публичного, чтобы ускорить резервное копирование. Поскольку локальный DNS-сервер может работать только с локальным IP-адресом, в этом случае рекомендуется использовать NAT.

В этом тестовом сценарии рекомендуем использовать браузер Google Chrome для доступа к продукту Кибер Инфраструктура и хранилищу S3.

2.2 Общие сведения о политиках хранилища

Кибер Инфраструктура может использоваться для следующих сценариев: блочного хранилища iSCSI, файлового хранилища NFS, объектного хранилища S3, хранилища резервных копий (созданных в решениях Кибер Бэкап). Также можно использовать встроенный в продукт гипервизор для создания вычислительных виртуальных машин (ВМ). Во всех этих сценариях общей единицей организации данных является том. Для вычислительного сервиса том – это виртуальный диск, который можно подключить к ВМ. Для iSCSI, S3, Backup Gateway и NFS том – это единица данных, которая используется при экспорте дискового пространства. Во всех этих случаях при создании тома необходимо указать его *режим избыточности*, *уровень хранилища* и *область отказа*. Эти параметры составляют *политику хранилища*, которая определяет уровень избыточности тома и его расположение.

© ООО Киберпротект, 2024



Избыточность означает, что данные хранятся на разных узлах хранилища и остаются высокодоступными даже при отказе некоторых узлов. Если один из узлов хранилища недоступен, копии данных на нем заменяются новыми, которые распределяются между исправными узлами хранилища. Когда узел возобновляет работу, устаревшие данные на нем обновляются.

При использовании репликации Кибер Инфраструктура разбивает том на фрагменты фиксированного размера (фрагменты данных). Каждый фрагмент реплицируется столько раз, сколько указано в политике хранилища. Реплики хранятся на разных узлах хранилища, если областью отказа является хост, чтобы на каждом узле была только одна реплика определенного фрагмента.

При использовании помехоустойчивого кодирования (или просто кодирования) входящий поток данных разбивается на фрагменты определенного размера. Затем каждый фрагмент не копируется сам по себе, вместо этого группируется определенное количество (M) таких фрагментов и создается определенное количество (N) паритетных блоков для избыточности. Все блоки распределяются по M+N узлам хранилища (выбранным из доступных узлов). Кластер может выдержать отказ любых N узлов хранилища без потери данных. Значения M и N указаны в названиях режимов избыточности помехоустойчивого кодирования. Например, в режиме 5+2 входящие данные разбиваются на 5 фрагментов и добавляются еще 2 паритетных блока для избыточности. Подробные сведения об избыточности, дополнительной передаче данных, количестве узлов и требованиях к нераспределенному пространству см. в руководстве администратора.

Чтобы лучше понять политику хранилища, 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 хранилища для каждой рабочей нагрузки.

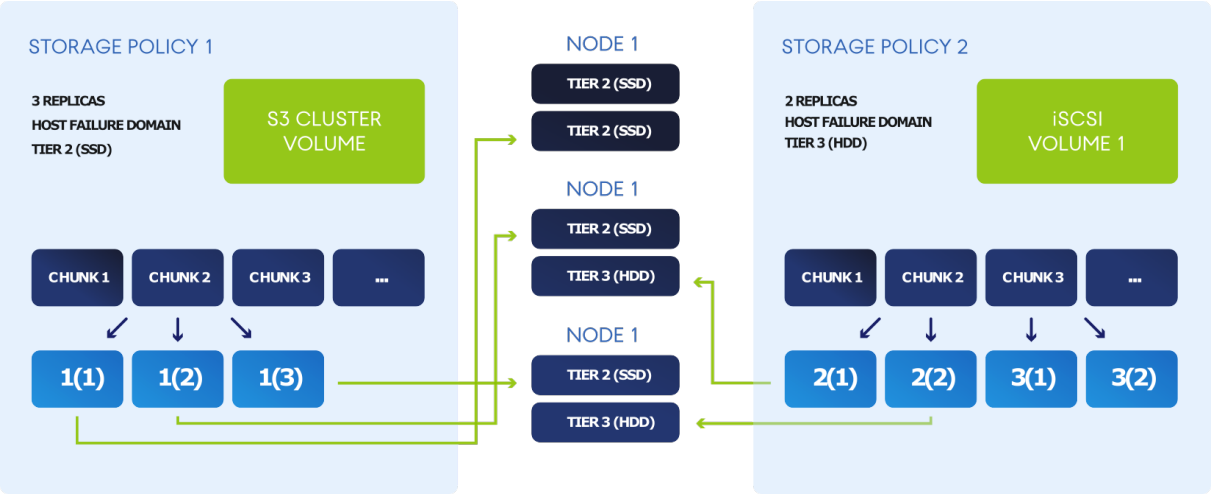
- Первый параметр, уровень, определяет группу дисков, объединенных по какому-либо критерию (как правило, это тип накопителя) в соответствии с определенной рабочей нагрузкой

© ООО Киберпротект, 2024

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 (см. раздел "Создание кластера хранилища данных" (стр. 12)). 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 хранилища, 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 хранилища, можно хранить только 1 или 2 реплики на двух узлах. В обоих случаях также можно применять кодирование, но для нашего тестирования ограничимся репликацией: 3 реплики для твердотельных накопителей и 2 реплики для жестких дисков.

В результате получатся следующие политики хранилища:



© ООО Киберпротект, 2024

3 Управление кластером хранилища данных

В этой главе описываются шаги по установке продукта Кибер Инфраструктура и настройке начальных параметров для дальнейшего развертывания. Сначала необходимо создать базовую инфраструктуру на узле управления, а затем добавить в нее подчиненные узлы аналогичным образом. В целях тестирования рекомендуем добавить два подчиненных узла. Затем следует настроить сети и создать на узлах кластер хранилища данных.

3.1 Установка Кибер Инфраструктура

Чтобы установить продукт Кибер Инфраструктура, выполните следующие действия.

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 (подключите его к виртуальному диску IPMI, создайте загрузочный USB-накопитель или настройте PXE-сервер).
3. Загрузите сервер с выбранного носителя.
4. На экране приветствия выберите **Установить Кибер Инфраструктура**.
5. На шаге 1 внимательно прочитайте лицензионное соглашение с конечным пользователем. Примите условия, установив флажок **Я принимаю лицензионное соглашение с конечным пользователем**, и нажмите кнопку **Далее**.
6. На шаге 2 настройте статический IP-адрес для сетевого интерфейса и укажите имя хоста: либо полное доменное имя (**<имя_хоста>.<имя_домена>**), либо краткое имя (**<имя_хоста>**). Не рекомендуется использовать динамический IP-адрес, поскольку это может вызвать проблемы с доступом к серверам. Проверьте правильность сетевых настроек.
7. На шаге 3 выберите часовой пояс. Дата и время будут заданы посредством NTP. Для выполнения синхронизации потребуется подключение к Интернету.
8. На шаге 4 укажите тип устанавливаемого сервера. Сначала разверните один первичный сервер. Затем разверните нужное количество вторичных серверов.
   - Если вы развертываете первичный сервер, выберите два сетевых интерфейса: один для настройки и управления системными сервисами и один для доступа к панели администрирования. Также создайте и подтвердите пароль для учетной записи суперадминистратора панели администрирования. Этот сервер будет сервером управления.
   - Если вы развертываете вторичный сервер, укажите IP-адрес сервера управления и токен. И то и другое можно получить из панели администрирования. Войдите на панель администрирования через порт 8888. IP-адрес панели отображается в консоли после развертывания первичного сервера. Введите имя пользователя по умолчанию **admin** и пароль учетной записи суперадминистратора. На панели администрирования откройте раздел **Инфраструктура** > **Серверы** и нажмите **Подключить сервер**, чтобы вызвать экран с

© ООО Киберпротект, 2024

адресом сервера управления и токеном.

Сервер может появиться на экране **Инфраструктура** > **Серверы** со статусом **Без назначения** сразу после проверки токена. Однако его можно будет присоединить к кластеру хранилища только после завершения установки.

9. На шаге 5 выберите диск для операционной системы. Диску будет назначена дополнительная роль **Система**, хотя вы все равно сможете настроить его для хранения данных на панели администрирования. Также можно создать программный массив RAID1 для системного диска, чтобы обеспечить его высокую производительность и доступность.
10. На шаге 6 введите и подтвердите пароль для учетной записи пользователя root и нажмите **Начать установку**.

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

Для получения подробной информации об узле выполните вход на панель управления на порту 8888, перейдите на экран **Инфраструктура** > **Узлы** и щелкните по имени узла. Перейдите на вкладку **Диски**, чтобы настроить или просмотреть диски узла, или на вкладку **Сеть**, чтобы настроить сетевые интерфейсы узла.

3.2 Настройка сетей

После установки продукта Кибер Инфраструктура на узел управления и два подчиненных узла необходимо настроить сети и интерфейсы. Используйте отдельные сети для внутреннего и внешнего трафика. Таким образом, публичный трафик не будет влиять на производительность ввода-вывода кластера, а также будут исключены возможные DoS-атаки из внешней сети.

1. Для настройки сетей перейдите на экран **Инфраструктура** > **Сети** на панели администрирования. Расширенная конфигурация рассматривается в руководстве администратора, но для нашего упрощенного развертывания достаточно настроить стандартные сети **Внешняя** и **Частная** следующим образом.

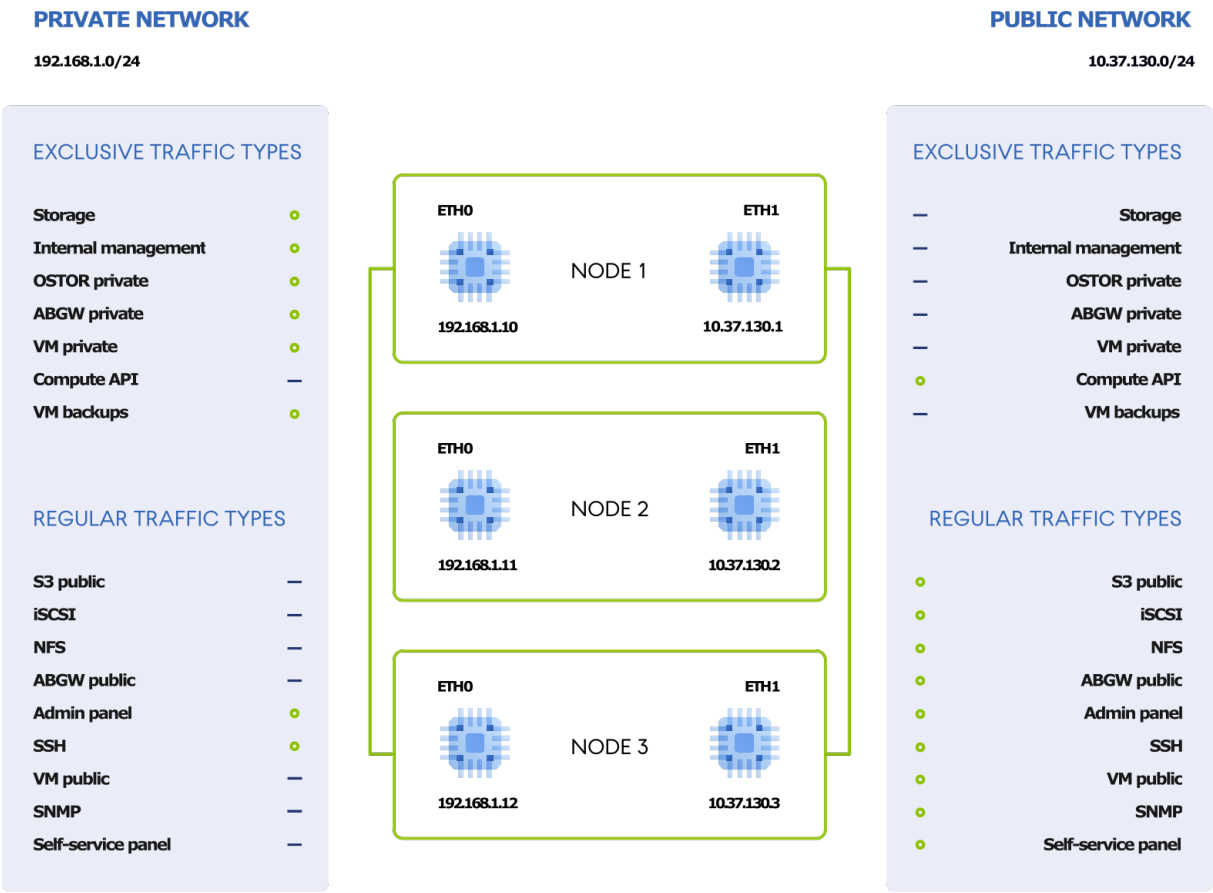
Сеть	Типы трафика
Внешняя	API вычислений, S3 внешн., iSCSI, NFS, Резервные копии (ABGW) внешн., Панель управления, SSH, ВМ внешн., SNMP, Панель самообслуживания
Частная	Хранилище, Управление, OSTOR внутр., Резервные копии (ABGW) внутр., ВМ внутр., Панель управления, SSH

2. Для настройки интерфейсов перейдите на экран **Инфраструктура** > **Узлы** и щелкните имя узла. Перейдите на вкладку **Сетевые интерфейсы**. Для узла управления оба интерфейса уже настроены, однако следует также настроить внешние сетевые интерфейсы для каждого подчиненного узла. Выберите интерфейс и нажмите **Изменить** в меню справа. В поле **Сеть** выберите **Внешняя**. Таким образом, один интерфейс должен быть подключен к частной сети, а другой назначен внешней сети. Повторите эти шаги для каждого подчиненного узла, чтобы подключить их к частной и внешней сети.

© ООО Киберпротект, 2024

3. Порты, которые будут открыты на узлах кластера, зависят от сервисов, которые будут работать на конкретном узле, и от связанных с ними типов трафика. Дополнительные сведения о портах и сервисах см. в разделе «Сетевые порты» руководства администратора.
4. Проверьте правильность настроек DNS. Для этого перейдите на экран **Настройки** > **Встроенный сервер DNS**. Убедитесь, что DNS-сервис кластера правильно настроен и указывает на сервер DNS, способный разрешать внешние имена хостов.

На рисунке ниже показан пример сетевой инфраструктуры, которую мы создадим для тестового сценария.



Примечание
Если у вас только одна сеть, не подключайте к ней один узел через два интерфейса. В этом случае следует работать с одним внешним интерфейсом узла.

3.3 Создание кластера хранилища данных

Создав узел управления и подчиненные узлы и настроив сети, можно приступать к созданию кластера хранилища.

1. Откройте экран **Инфраструктура** > **Серверы** и нажмите **Создать кластер хранилища**.
2. [Необязательно] Чтобы настроить роли дисков или расположение сервера, нажмите значок шестерни.

© ООО Киберпротект, 2024

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**.

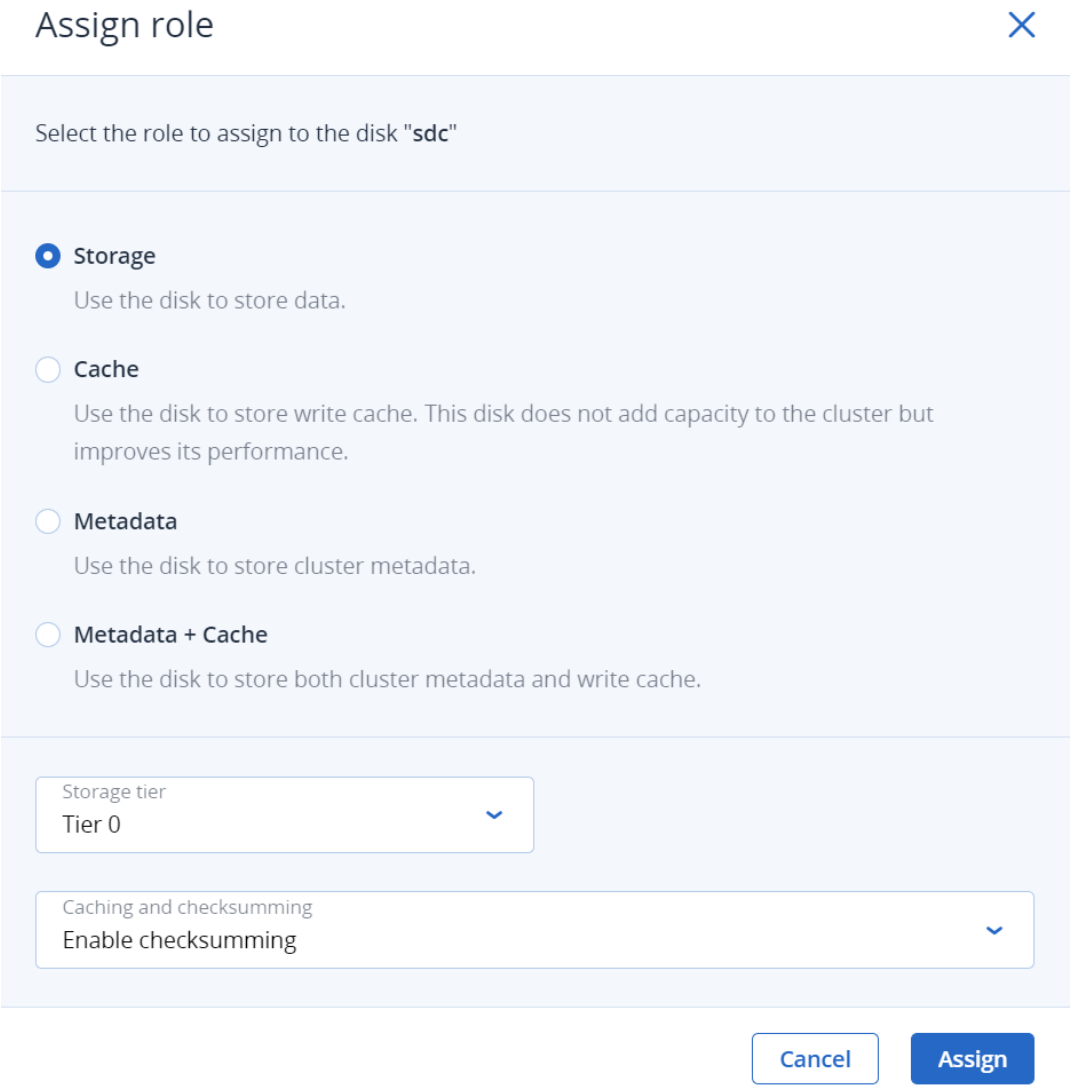
Отслеживать создание кластера можно на экране **Инфраструктура** > **Серверы**. Создание может занять некоторое время в зависимости от количества настраиваемых дисков. Кластер будет создан после завершения настройки.

Чтобы добавить подчиненный узел, выполните следующие действия.

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.

В тестовом сценарии нужно будет назначить диски хранилища узла различным уровням (см. раздел "Общие сведения о политиках хранилища" (стр. 7)). Для каждого из узлов назначьте твердотельные накопители уровню 2, а жесткие диски – уровню 3.

© ООО Киберпротект, 2024



© ООО Киберпротект, 2024

4 Управление вычислительным кластером

Кибер Инфраструктура предоставляет высокопроизводительную виртуализацию, базовым компонентом которой является вычислительный кластер. Администраторы продукта могут создавать множество тенантов, виртуальных машин и программно определяемых сетей, а также легко развертывать решения для оркестрации контейнеров, такие как Kubernetes.

В этом разделе мы рассмотрим два распространенных сценария для вычислительного кластера.

- Поставщик услуг предоставляет сервисы виртуализации конечным клиентам. В этом случае поставщик может пользоваться преимуществами панелей самообслуживания с возможностью поставки сервисов под собственным брендом, мультитенантной архитектурой и удобным управлением и выделением ресурсов.
- Предприятие планирует внедрить новое программное обеспечение по всей инфраструктуре. Можно развернуть виртуальные машины и установить на них ПО, чтобы все сотрудники могли с ним работать.

Хотя два этих сценария значительно различаются, процедура, выполняемая в продукте Кибер Инфраструктура, будет похожа.

1. Создание вычислительного кластера.
2. Выделение ресурсов для доменов, проектов (тенантов) и пользователей.
3. Создание виртуальных машин для конечных пользователей.

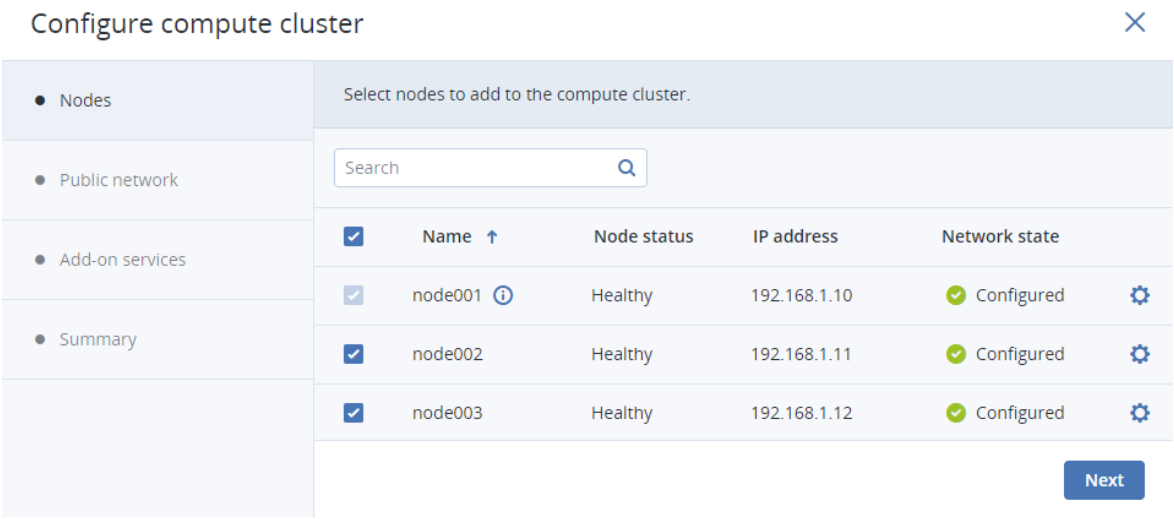
В этой главе мы рассмотрим каждый из этих шагов.

4.1 Создание вычислительного кластера

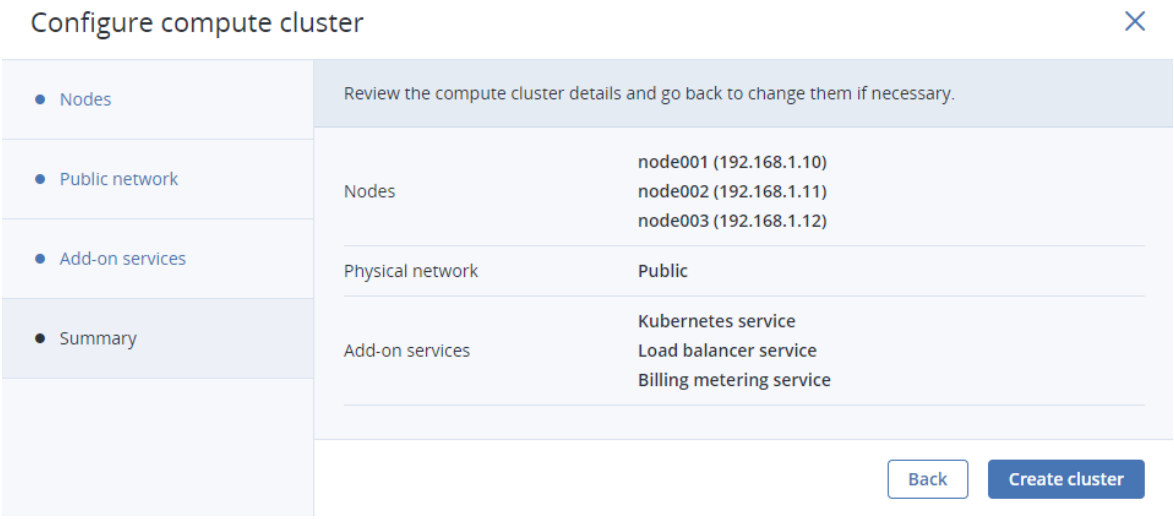
Чтобы создать вычислительный кластер, откройте экран **Вычисления**, нажмите **Создать вычислительный кластер** и выполните следующие действия в окне **Настроить вычислительный кластер**.

1. В разделе **Узлы** выберите узлы, которые следует добавить в вычислительный кластер. Состояние сети каждого выбранного узла должно быть **Настроено**, если вы выполнили инструкции в разделе "Настройка сетей" (стр. 11). Нажмите **Далее**.

© ООО Киберпротект, 2024



2. В разделе **Физическая сеть** можно включить управление IP-адресами, если в вашем распоряжении есть пул IP-адресов. Это также необходимо для виртуальных маршрутизаторов, плавающих общедоступных IP-адресов и сетевых балансировщиков нагрузки. Иначе можно оставить управление IP-адресами отключенным. Выберите сеть инфраструктуры, к которой будет подключена физическая сеть, а также ее тип: выберите **VLAN** и укажите идентификатор VLAN для создания сети на базе VLAN либо выберите **Untagged** (Без тега) для создания плоской физической сети.
3. В разделе **Дополнительные сервисы** можно установить дополнительные сервисы, если вы хотите также протестировать их. Либо можно сделать это позже, как описано в руководстве администратора.
4. На шаге **Сводка** просмотрите конфигурацию и нажмите **Создать кластер**.



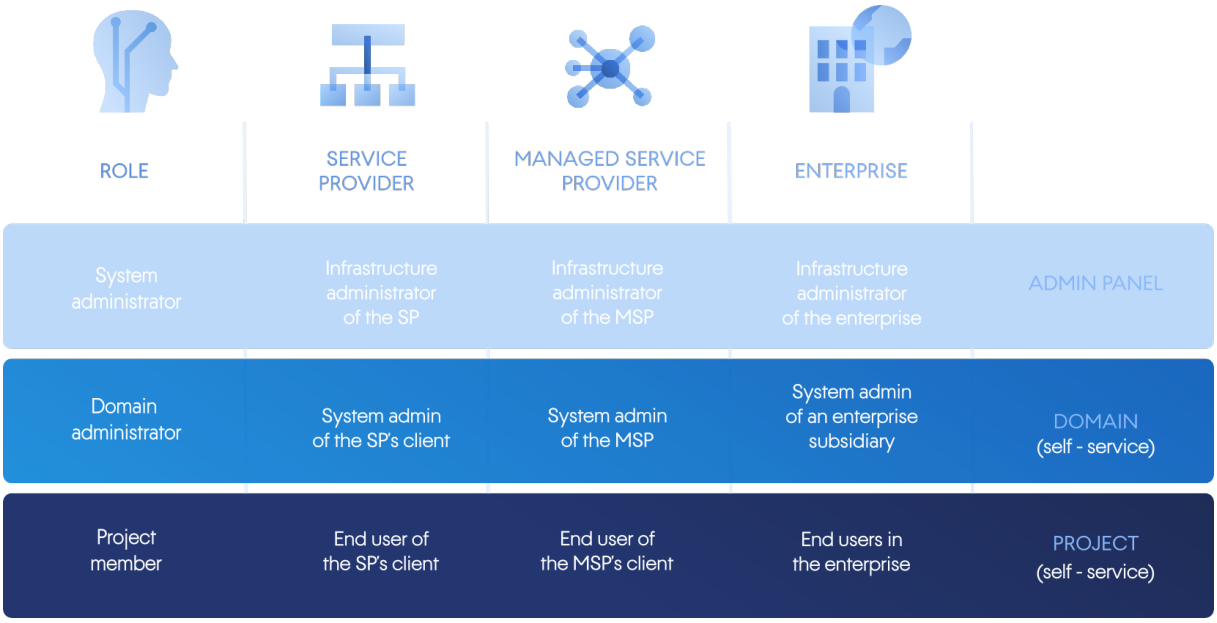
Отслеживать развертывание вычислительного кластера можно на экране **Вычисления**.

© ООО Киберпротект, 2024

4.2 Выделение ресурсов

4.2.1 Создание доменов, проектов и пользователей

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 имеют полный контроль над продуктом Кибер Инфраструктура и доступ к панели администрирования. Эту роль вы получаете по умолчанию при установке продукта Кибер Инфраструктура. Обычно это администраторы инфраструктуры поставщика управляемых услуг или главный ИТ-отдел предприятия в зависимости от вашей бизнес-модели.
- Администраторы доменов отвечают за свои домены. Домен представляет собой набор проектов виртуализации (тенантов) и пользователей (конечных клиентов). У администраторов доменов есть доступ к панели самообслуживания. Они могут создавать пользователей, а также использовать ресурсы проектов в рамках разрешенных квот: развертывать и контролировать виртуальные машины, образы, тома, сети, маршрутизаторы, плавающие IP-адреса и SSH-ключи.
- Участники проектов могут управлять ресурсами в рамках своих проектов: развертывать и контролировать виртуальные машины, образы, тома, сети, маршрутизаторы, плавающие IP-адреса и SSH-ключи. Проект представляет собой набор ресурсов хранилища и вычислительных ресурсов, ограниченный квотами и доступный назначенным пользователям.

Роли администратора домена и участника проекта имеют определенные ограничения. В частности, они не могут переносить виртуальные машины между узлами, поскольку узлы отсутствуют на этом уровне абстрагирования.

© ООО Киберпротект, 2024

В нашем тестовом сценарии вы являетесь системным администратором. После создания вычислительного кластера вам необходимо будет создать домен, проект и несколько конечных пользователей, которых следует назначить на проект. Затем создайте политику хранилища для томов ВМ и определите их параметры избыточности. Далее настройте виртуальные сети. После этого пользователи доменов получат доступ к своим доменам и проектам через панель самообслуживания. Там они смогут создавать собственные виртуальные машины, тома, сети и т. п.

Примечание
IP-адрес панели самообслуживания показан на экране **Настройки** > **Портал самообслуживания** на панели администрирования.

Действия, выполняемые на панели самообслуживания, описаны в руководстве по самообслуживанию. В целях тестирования мы ограничимся операциями с вычислительным кластером, выполняемыми из панели администрирования.

1. Создайте домен. Для этого выполните вход на панель администрирования и откройте экран **Настройки** > **Проекты и пользователи**. Нажмите **Создать домен** в правом верхнем углу. Укажите имя и описание для нового домена. Нажмите **Создать**.
2. Создайте учетную запись администратора для нового домена. Для этого выберите созданный домен и нажмите **Создать пользователя**. Укажите имя пользователя и пароль, а затем выберите роль **Администратор домена**. Установите флажок **Загрузка образа**, чтобы разрешить новому администратору загружать образы для развертывания виртуальных машин. Нажмите **Создать**.
3. Создайте проект. Для этого перейдите на вкладку **Проекты** домена и нажмите **Создать проект**. Задайте квоты и нажмите **Создать**. Убедитесь, что у вас достаточно ресурсов ЦП, ОЗУ, хранилища и сетевых ресурсов для развертывания виртуальных машин (и дополнительных сервисов, если вы выберете их включение).
4. Создайте участника проекта. Для этого откройте вкладку **Пользователи домена** и нажмите **Создать пользователя**. Укажите имя пользователя и пароль, а затем выберите роль **Участник проекта**. Выберите проект, на который следует назначить пользователя, и нажмите **Создать**.
5. По желанию измените внешний вид панели самообслуживания на экране **Настройки** > **Портал самообслуживания**, добавив логотипы и выбрав цветовую схему. Таким образом, например, поставщики управляемых услуг могут предоставлять конечным пользователям сервисы виртуализации под своим брендом.

4.2.2 Создание политик хранилища

Чтобы создать новую политику хранилища, перейдите на экран **Вычисления** > **Хранилище**, откройте вкладку **Политики хранилищ** и нажмите **Создать политику хранения**. Укажите имя, уровень, область отказа и схему избыточности. Для тестового сценария выберите режим **2 реплики** и **Хост** в качестве **области отказа**.

Создав политику хранилища, вы сможете выбирать ее для томов при создании виртуальных машин (см. раздел "Создание виртуальных машин" (стр. 19)). Ее также можно применять при создании томов непосредственно на вкладке **Тома**.

© ООО Киберпротект, 2024

Политики хранилища могут использоваться в квотах проектов. Политика, созданная перед созданием проекта, будет включена в его квотах. Политика, созданная после создания проекта, не будет включена для него автоматически. Необходимо будет изменить квоты этого проекта и выбрать политику вручную.

4.2.3 Создание вычислительных сетей

Перед развертыванием виртуальных машин необходимо настроить сети на экране **Вычисления** > **Сеть**. Виртуальная сеть позволяет подключенным к ней виртуальным машинам взаимодействовать друг с другом. Физическая сеть подключает ваши виртуальные машины к существующей сети инфраструктуры для доступа к Интернету, например.

Для создания новой сети нажмите **Создать сеть** и укажите ее тип. Введите имя для новой сети, CIDR подсети, например **192.168.0.1/24**, и шлюз. Нажмите **Далее**, чтобы продолжить. Если у вас есть пул IP-адресов для виртуальных машин, можно включить встроенный DHCP-сервер, чтобы эти IP-адреса автоматически назначались виртуальным машинам. Нажмите **Создать сеть**, чтобы завершить процесс.

Вместе с вычислительными сетями можно задать плавающие IP-адреса. Плавающий IP-адрес – это общедоступный IP-адрес, который можно вручную назначить частному IP-адресу виртуальной машины. Он позволит обращаться к виртуальной машине из внешней сети, хотя у нее есть только частный IP-адрес. Чтобы создать плавающий IP-адрес, сначала необходимо связать физическую и виртуальную сеть с помощью виртуального маршрутизатора. Дополнительные сведения см. в разделе «Управление плавающими IP-адресами» руководства администратора.

4.3 Создание виртуальных машин

Создав вычислительный кластер, домен, проект, политику хранилища и сети, можно приступать к созданию виртуальных машин.

В этом тестовом сценарии вы создадите виртуальную машину из образа. Можно отправить свой образ или использовать образ Cirros, поставляемый по умолчанию. Чтобы отправить образ, откройте вкладку **Вычисления** > **Виртуальные машины** > **Образы**. Можно использовать ISO-образы и шаблоны (готовые к использованию тома в формате облачных образов QCOW2 с установленной ОС и приложениями). Нажмите **Добавить образ** и выберите ISO-образ с локальной машины. Укажите имя для нового образа и выберите совместимую операционную систему из раскрывающегося списка. Установите флажок **Использовать во всех проектах**, ы хотите использовать этот образ в качестве шаблона для будущих развертываний ВМ. Нажмите **Добавить**.

© ООО Киберпротект, 2024

Примечание
Кибер Инфраструктура поддерживает широкий спектр гостевых операционных систем Windows и Linux, из которых можно развертывать виртуальные машины (см. раздел «Поддерживаемые гостевые операционные системы» в руководстве администратора). Кроме того, в продукте используются различные запатентованные инновации, которые оптимизируют производительность развернутых ВМ. Например, ВМ на базе Windows должны работать так, как будто они развернуты на Hyper-V.

1. На экране **Вычисления** > **Виртуальные машины** нажмите **Создать виртуальную машину** и укажите имя.
2. Чтобы создать ВМ из образа, выберите образ, загруженный ранее. В разделе **Тома** будет автоматически добавлен загрузочный том на основе данных образа. Можно изменить политику хранилища этого тома. Для этого нажмите значок карандаша в разделе **Тома**, нажмите значок с многоточием в окне **Тома**, выберите **Изменить**, а затем измените политику в окне **Изменить том**. Здесь также можно добавить в ВМ новые тома.
3. В разделе **Тип ВМ** выберите тип. Это готовая настройка, определяющая количество виртуальных ЦП и объем памяти виртуальной машины.
4. В разделе **Сети** добавьте интерфейсы в виртуальные сети, к которым должна быть подключена виртуальная машина.
5. Нажмите **Развернуть**, чтобы начать создание виртуальной машины. Следите за статусом новой виртуальной машины. Как только появится статус **Запущена**, ВМ готова к работе.

Для доступа к созданной виртуальной машине щелкните по ее имени, а затем нажмите **Консоль** на панели справа. На вкладке **Мониторинг** ВМ можно просмотреть количество потребляемых ресурсов.

Примечание
Также можно перенести виртуальные машины из VMware vCenter с помощью инструмента virt-v2v, как описано в разделе «Миграция виртуальных машин в Кибер Инфраструктуру» в руководстве администратора.

Когда виртуальная машина будет готова, с ней можно будет выполнять широкий спектр операций, таких как остановка и запуск, приостановка и возобновление, перезагрузка, миграция и т. д. Дополнительные сведения см. в разделе «Управление виртуальными машинами» руководства администратора.

© ООО Киберпротект, 2024

5 Экспорт дискового пространства

Кибер Инфраструктура позволяет экспортировать дисковое пространство.

- Как блочное хранилище через iSCSI для виртуализации, баз данных и других целей. Можно экспортировать дисковое пространство кластера на внешние физические и виртуальные хосты в форме блочных устройств LUN по протоколу iSCSI и подобно сети SAN.
- Как хранилище объектов для хранения неограниченного количества файлов посредством S3-совместимого протокола. В объектном хранилище типа S3 можно хранить такие данные, как медиафайлы, резервные копии и файлы Open-Xchange с доступом через приложения типа Dropbox. Конечные пользователи могут продолжать работать с приложениями для S3 после миграции данных из Amazon S3 в продукт Кибер Инфраструктура. Они также могут создать собственные сервисы хранилища объектов, совместимые с Amazon S3.
- Через NFS. Можно объединить узлы в кластер NFS высокой доступности, в котором можно создавать тома NFS. В каждом томе можно создать несколько экспортов NFS, представляющих собой фактические экспортированные каталоги для пользовательских данных. Каждый экспорт можно подключить с помощью стандартных команд. С технической стороны тома NFS основаны на хранилище объектов. Кластер NFS представляет собой идеальное «холодное» и «теплое» хранилище файлов, но не рекомендуется для «горячих» рабочих нагрузок с высокими требованиями к производительности. Для наилучшей интеграции с VMware vSphere рекомендуется использовать протокол iSCSI.

5.1 Экспорт дискового пространства через iSCSI

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.

5.1.1 Создание групп целевых устройств

Чтобы создать группу целевых устройств, откройте **Сервисы хранилища** > **Блочное хранилище** > **Группы целей** и нажмите **Создать группу целей**. Откроется мастер, в котором необходимо выполнить следующие действия.

© ООО Киберпротект, 2024

1. В разделе **Имя и тип** введите имя группы целевых устройств и выберите тип iSCSI. Далее выберите как минимум два узла, чтобы добавить их в группу целевых устройств для высокой доступности.
2. В разделе **Цели** выберите интерфейсы iSCSI для добавления в группу целевых устройств. В разделе **Тома** выберите тома для присоединения к LUN группы целевых устройств либо добавьте их позже. Для этого тестового сценария пропустите раздел настроек **Контроль доступа**.
3. В разделе **Сводка** проверьте сведения о группе целевых устройств. Нажмите **Создать**.

Созданная группа целевых устройств появится на вкладке **Группы целей**. Целевые устройства группы запустятся автоматически. Щелкните по имени группы, чтобы просмотреть подробные сведения. На вкладке **Цели** можно добавить узлы для новых целевых устройств. Также можно просматривать и добавлять устройства LUN на вкладке **LUN**.

5.1.2 Создание томов

1. Откройте **Сервисы хранилища** > **Блочное хранилище** > **Тома** и нажмите **Создать том**. Откроется мастер.
2. В разделе **Имя и размер** введите имя тома и укажите его размер. Учтите, что размер томов можно в дальнейшем увеличивать, но не уменьшать.
3. В разделе **Политика хранилища** выберите режим избыточности, уровень хранения данных и область отказа.
4. В разделе **Сводка** проверьте сведения о томе. Нажмите **Создать**.

5.1.3 Присоединение томов к группам целевых устройств

1. Откройте **Сервисы хранилища** > **Блочное хранилище** > **Группы целей**, щелкните по значку с многоточием возле нужной группы целевых устройств и нажмите **Добавить LUN**.
2. В открывшемся окне **Присоединить** выберите тома для присоединения к группе целевых устройств или создайте их. Нажмите **Применить**.
3. На вкладке **Группы целей** щелкните по имени нужной группы целевых устройств и перейдите на вкладку **LUN**. Здесь можно просмотреть все доступные устройства LUN.

5.1.4 Доступ к целевым устройствам iSCSI из VMware vSphere

К целевым устройствам iSCSI можно обращаться из Linux, Microsoft Hyper-V и VMware vSphere. Дополнительные сведения о доступе из Linux и Microsoft Hyper-V см. в разделе «Осуществление доступа к целевым устройствам iSCSI» руководства пользователя хранилища. В следующем разделе описывается тестовый сценарий для VMware vSphere.

Перед использованием томов Кибер Инфраструктура с VMware vSphere необходимо настроить продукт для надлежащей работы с активными или пассивными массивами хранения данных ALUA. Рекомендуется изменить политику пути по умолчанию на политику RR с помощью следующей команды:

© ООО Киберпротект, 2024

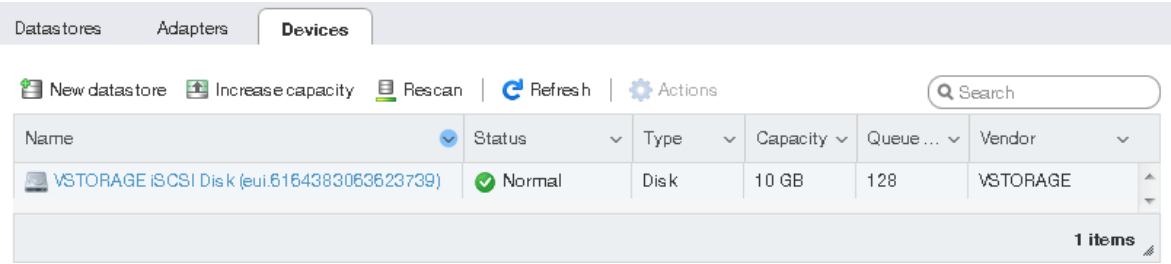
```
# esxcli storage nmp satp set -s VMW_SATP_ALUA -P VMW_PSP_RR
```

Теперь можно перезагрузить хост и создать хранилища данных из томов Кибер Инфраструктура, экспортированных через iSCSI. Выполните вход на веб-панель VMware ESXi и выполните следующие действия.

1. В Navigator перейдите на вкладку **Storage** (Хранилище) > **Adapters** (Адаптеры) и нажмите **Software iSCSI** (Программный iSCSI).
2. В окне **Configure iSCSI** (Настройка iSCSI) выберите **Enabled** (Включено). В разделе **Dynamic targets** (Динамические цели) нажмите **Add dynamic target** (Добавить динамическую цель) и введите IP-адреса ваших узлов.

   Примечание
   'IP-адреса отображаются на панели администрирования. На экране **Инфраструктура** > **Узлы** щелкните по имени нужного узла. Затем перейдите на вкладку **Сеть** и скопируйте его внешний IP-адрес.

3. Нажмите **Save configuration** (Сохранить конфигурацию).
4. Перейдите на вкладку **Устройства** и нажмите **Обновить**. В списке устройств появится только что добавленный диск.



5. Выберите диск и нажмите **New datastore** (Создать хранилище данных). В открывшемся мастере введите имя для хранилища данных и выберите параметры создания разделов. Нажмите **Finish** (Завершить), чтобы разбить диск на разделы.

   Предупреждение
   При разбивке диска на разделы все данные с него будут удалены.

6. В списке хранилищ данных появится готовый к использованию диск. Выберите его и нажмите **Database browser** (Обзор базы данных), чтобы просмотреть содержимое и загрузить файлы для проверки доступности.

5.2 Экспорт дискового пространства через S3

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

Объектное хранилище оптимизировано для хранения миллиардов объектов, в частности: данных приложений, размещения статического веб-контента, сервисов онлайн-хранилища, больших

© ООО Киберпротект, 2024

данных и резервных копий. Ключевое отличие, по сравнению с другими типами хранилищ, состоит в том, что части объекта нельзя изменить, поэтому при изменении объекта вместо этого формируется его новая версия. Такой подход устраняет проблему конфликтов.

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, как описано в разделе «Репликация данных S3 между центрами обработки данных» в руководстве администратора.

Перед созданием кластера S3 убедитесь, что у вас есть доменное имя для шлюза S3.

5.2.1 Создание кластера S3

Для создания кластера S3 выполните следующие действия.

1. В меню слева нажмите **Сервисы хранилища** > **S3**. Выберите три узла для тестового сценария и нажмите **Создать кластер S3** в меню справа.
2. Далее, выберите политику хранилища.
3. 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**.
4. Из раскрывающегося списка выберите протокол конечной точки S3: HTTP, HTTPS или оба. Для простого тестового сценария рекомендуем выбрать HTTPS и установить флажок **Сгенерировать самозаверяющий сертификат**. Нажмите **Готово**, чтобы создать кластер S3.

После того как будет создан кластер S3, откройте экран **Обзор S3**, чтобы просмотреть на нем состояние кластера, имя хоста, используемый объем дисков, количество пользователей, активность ввода-вывода и состояние сервисов S3.

Чтобы убедиться, что кластер S3 успешно развернут и у пользователей есть к нему доступ, откройте в браузере адрес https://<S3_DNS_name>. Должен отобразиться следующий ответ XML:

```
<Error>
<Code>AccessDenied</Code>
<Message/>
</Error>
```


© ООО Киберпротект, 2024

Чтобы начать пользоваться хранилищем S3, также потребуется создать как минимум одного пользователя S3.

5.2.2 Управление пользователями и корзинами S3

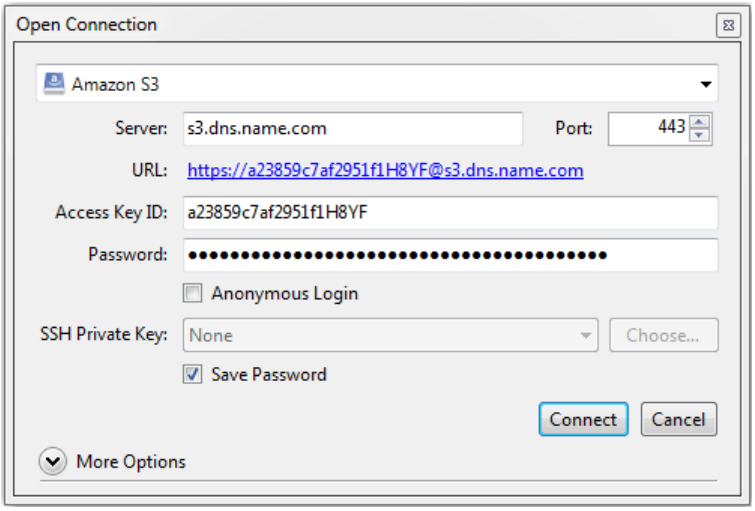
Чтобы добавить пользователя S3, выполните следующие действия.

1. На экране **Сервисы хранилища** > **S3** > **Пользователи** нажмите **Добавить пользователя**.
2. Укажите адрес электронной почты в качестве имени пользователя и нажмите **Добавить**.

Чтобы автоматически входить на портал S3 с учетными данными пользователя, используя созданные ключи, перейдите на панель администрирования, выберите пользователя и нажмите **Обзор**. В этой рабочей области можно создавать новые корзины и отслеживать состояние существующих.

Также можно выполнять вход в хранилище S3 с помощью сторонних приложений, таких как CyberDuck, MountainDuck или Backup Exec. Для этого тестового сценария подключитесь к хранилищу S3 через CyberDuck, выполнив следующие шаги.

1. В CyberDuck нажмите **Открыть подключение**.
2. Получите учетные данные из панели администрирования Кибер Инфраструктура.
   - Получите доменное имя оконечной точки S3 на вкладке **Сервисы хранилища** > **S3** > **Сводка**.
   - Получите **ID ключа доступа** и **Пароль** на вкладке **Сервисы хранилища** > **S3** > **Пользователи**. Выберите нужного пользователя и нажмите **Ключи** справа. Отобразятся идентификатор ключа доступа и ключ защищенного доступа.
3. Укажите свои учетные данные в CyberDuck.



4. После установки соединения можно просматривать существующие корзины и создавать новые. Нажмите **Файл** > **Новая папка**, чтобы создать корзину. Укажите имя для новой корзины и нажмите **Создать**. Используйте имена корзин, соответствующие соглашениям об именовании DNS.

© ООО Киберпротект, 2024

Для управления файлами в корзинах необходимо войти на портал S3 как пользователь. Дополнительные сведения см. в разделе «Доступ к корзинам S3» руководства пользователя хранилища.

5.3 Экспорт дискового пространства через NFS

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.

5.3.1 Создание кластера NFS

1. В меню слева нажмите **Сервисы хранилища** > **NFS**.
2. Выберите один или несколько узлов и нажмите **Создать кластер NFS** в меню справа. Для тестового сценария рекомендуем выбрать три узла.
3. Нажмите кнопку **Создать**.

После того как будет создан кластер NFS, можно перейти к созданию томов NFS.

5.3.2 Создание томов NFS

1. На экране **Сервисы хранилища** > **NFS** > **Тома** нажмите **Добавить том NFS**.
2. На панели **Добавить том NFS** укажите имя (например, **share1**) и уникальный разрешимый статический IP-адрес из внешней сети.
3. В поле **Размер тома** укажите размер. Для пользователей, обращающихся к экспортам, этим

© ООО Киберпротект, 2024

значением будет размер файловой системы.

4. Выберите нужный уровень, область отказа и тип избыточности данных. Нажмите **Готово**.

   После того как том будет создан, можно перейти к созданию экспортов NFS.

5.3.3 Создание и подключение экспортов NFS

1. На экране **Сервисы хранилища** > **NFS** > **Тома** щелкните по номеру в столбце **Экспорты** в строке нужного тома. Откроется экран тома.
2. На экране тома нажмите **Добавить экспорт**, укажите **root** в качестве имени экспорта и **/** в качестве пути и выберите режим доступа **Чтение и запись**. Будет создан каталог с путем по умолчанию, который указывает на расположение экспорта внутри тома и используется (наряду с IP-адресом папки) для подключения экспорта. Корневой экспорт будет отображаться в списке экспортов.
3. После создания корневого экспорта можно подключить его в Linux или macOS, как описано в руководстве пользователя хранилища. Для этого тестового сценария подключите экспорт в Linux с помощью следующих команд:

   ```
   # mkdir /mnt/nfs
   # mount -t nfs -o vers=4.0 <share_IP>:/<share_name>/ /mnt/nfs
   ```

   где:

   - -o vers=4.0 – версия NFS, которая будет использоваться.
   - <share_IP> – IP-адрес тома NFS. Также можно использовать имя хоста тома NFS.
   - /<share_name>/ – путь корневого экспорта, например share1.
   - /mnt/nfs – существующий локальный каталог, к которому будет подключен экспорт.

   Чтобы проверить подключенное хранилище, можно выполнить команду df -h.

© ООО Киберпротект, 2024

6 Подключение ПО Кибер Бэкап Облачный к хранилищу 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.

В этом разделе мы покажем, как развернуть хранилище резервных копий в продукте Кибер Инфраструктура, создать нового клиента в Кибер Бэкап Облачный, а затем настроить хранилище для резервных копий в Кибер Бэкап Облачный. Соответствующие шаги для Кибер Бэкап выполняются аналогично.

6.1 Создание хранилища резервных копий

Перед настройкой хранилища резервных копий убедитесь, что конфигурация DNS соответствует требованиям, указанным в разделе "Аппаратные требования" (стр. 6). Кроме того, порт 44445 должен быть открыт для входящих/исходящих подключений для сетевого интерфейса с ролью **Резервные копии (ABGW) внешн.** (это внешняя сеть в нашем тестовом сценарии).

1. Настройте новое хранилище для хранения резервных копий клиента и управления ими с помощью панели администрирования продукта Кибер Инфраструктура. Для этого выполните вход в Кибер Инфраструктура и перейдите в раздел **Сервисы хранилища**, затем выберите **Резервные копии**.
2. Щелкните **Создать хранилище резервных копий**.
3. На этапе **Место назначения резервной копии** выберите кластер **Кибер Инфраструктура**. В нашем тестовом сценарии данные клиента будут сохраняться и управляться на узлах кластера хранилища.
4. На шаге **Серверы** выберите серверы, которые нужно добавить в кластер хранилища резервных копий, и нажмите **Далее**.

© ООО Киберпротект, 2024

5. На этапе **Политика хранилища** выберите требуемые уровень, область отказа и режим избыточности данных, которые будут применяться к резервным копиям вашего клиента. Затем нажмите **Далее**.
6. На этапе **DNS** укажите доменное имя, которое будет привязано к выбранному кластеру и будет использоваться для регистрации этого кластера в Кибер Бэкап Облачный (например, **backup.example.com**). Новое доменное имя привязывается к IP-адресу каждого узла в выбранном кластере. Конкретный узел для операций резервного копирования выбирается агентом резервного копирования автоматически. Это зависит от различных факторов, таких как доступность и загрузка узлов. Нажмите **Далее**.
7. На этапе **Учетная запись Киберпротект** укажите URL-адрес вашего экземпляра Кибер Бэкап Облачный. Если вы используете Кибер Бэкап, на этом этапе следует использовать IP-адрес соответствующей машины для доступа к консоли управления резервным копированием. Для этого тестового сценария укажите имя пользователя и пароль учетной записи администратора Кибер Бэкап Облачный. Нажмите **Далее**.
8. [Необязательно] Проверьте настройку DNS локально перед выходом во внешнюю сеть. Для этого добавьте DNS-имя в файл /etc/hosts на машинах, которые будут использоваться для доступа к хранилищу резервных копий, например **192.168.1.10 backup.example.com**.
9. На шаге **Сводка** просмотрите конфигурацию и нажмите **Создать**.

Развертывание запустится сразу после этого. По завершении процесса отобразятся четыре вкладки: **Сводка**, **Узлы**, **Георепликация** и **Настройки**. На вкладке **Сводка**, например, можно просмотреть информацию о зарегистрированных шлюзах и их производительности.

Примечание
Если у текущего хранилища нет общедоступного IP-адреса и доменного имени, инструмент Web Restore для Кибер Бэкап Облачный не сможет правильно работать.

6.2 Настройка Кибер Бэкап Облачный

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.

© ООО Киберпротект, 2024

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. Для этого тестового сценария выберите рабочую станцию с операционной системой, которая используется в настоящий момент. 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.

Чтобы создать резервную копию с машины клиента, выполните следующие действия.

1. Щелкните устройство и выберите **Защитить** в меню справа.
2. Щелкните **Добавить план** и укажите подробные характеристики плана. Для этого тестового сценария включите только функцию **Резервное копирование**:
   a. В поле **Выбор данных** выберите **Файлы/папки**.
   b. В разделе **Элементы для резервного копирования** выберите требуемый файл или папку.
   c. В разделе **Место сохранения резервной копии** выберите целевое облачное хранилище.
   d. В разделе **Расписание** выберите **Нет**, выключив его.
3. Нажмите **Создать**, после чего план резервного копирования появится в списке слева.
4. Нажмите кнопку **Запустить сейчас**, чтобы начать процесс резервного копирования.

После завершения процесса можно просмотреть резервные копии файлов на экране **Хранилище резервных копий** > **Хранилища**. Щелкните по имени нужного клиента, чтобы просмотреть файлы, загруженные в хранилище ранее. Дважды щелкните по имени резервной копии, чтобы отобразить подробные сведения справа. Можно нажать **Восстановить файлы/папки**, чтобы перейти к отправленным файлам и загрузить их при необходимости.

© ООО Киберпротект, 2024

7 Мониторинг кластера хранилища данных

Кибер Инфраструктура предоставляет встроенные средства мониторинга, включая преинтегрированную систему Prometheus и настроенные панели мониторинга Grafana, которые показывают состояние сервисов, их доступность и производительность, а также пропускную способность сети, невыполненные задания по репликации, расход памяти и загрузку ЦП. Интеграция со сторонними системами возможна посредством полностью совместимых API-интерфейсов OpenStack. Вы можете гарантировать бесперебойную работу систем и устранять проблемы до того, как они повлияют на работу сторонних систем или конечных пользователей.

1. Для мониторинга кластера хранилища перейдите на экран **Мониторинг** > **Обзор**. Здесь можно просмотреть общую информацию о выбранном кластере хранилища за последние 30 минут, 1, 6 и 12 часов, а также за последние семь дней. Отображаемая информация включает операции чтения и записи, состояние сервисов фрагментов данных и расход физического и логического пространства. Дополнительные сведения см. в разделе «Мониторинг кластера хранилища данных» руководства администратора.
2. Для расширенного мониторинга перейдите на экран **Мониторинг** > **Обзор** и нажмите **Панель Grafana**. Откроется отдельная вкладка браузера с предварительно настроенными панелями мониторинга Grafana для кластера хранилища, аппаратных узлов, экспортов и т. д. Две панели посвящены хранилищу резервных копий. Подробное описание каждого графика см. в разделе «Мониторинг хранилища резервных копий» руководства администратора.
3. Также можно отслеживать состояние хранилища резервных копий на экране **Сервисы хранилища** > **Резервные копии**. Здесь отображается информация о развернутом кластере хранилища и его производительности. Кроме того, можно получить сведения о георепликации выбранных кластеров резервного копирования, а также данные об использовании пространства хранилища в публичных облачных сервисах, таких как Amazon S3, Microsoft Azure, Google Cloud или Alibaba Cloud.

© ООО Киберпротект, 2024

8 Включение высокой доступности

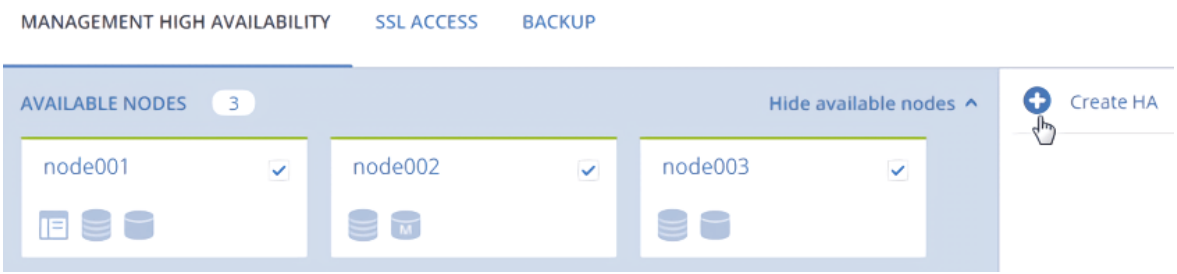
Высокая доступность поддерживает работу сервисов продукта Кибер Инфраструктура даже в случае отказа узла, на котором они расположены. В таких случаях сервисы с отказавшего узла перемещаются на исправные узлы.

Ранее вы создали кластер из трех узлов, который теперь можно сделать более устойчивым и избыточным. Для этого включите высокую доступность для узла управления, панели администрирования и сервисов.

8.1 Высокая доступность для узла управления

Чтобы включить высокую доступность для сервера управления и панели администрирования, выполните следующие действия.

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).

8.2 Высокая доступность для сервисов

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

© ООО Киберпротект, 2024

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.

8.3 Проверка высокой доступности

В этом разделе моделируется ситуация с отказом узла управления.

© ООО Киберпротект, 2024

1. Принудительно отключите питание узла управления Кибер Инфраструктура.

   Примечание
   Высокая доступность поддерживает сервисы в рабочем состоянии, если узел, на котором они расположены, откажет из-за сбоя ядра, отключения электричества или станет недоступен по сети. Корректное завершение работы не считается ситуацией отказа. Для проверки высокой доступности следует принудительно выключить узел или отсоединить от него сетевой кабель.

2. Откройте экран **Инфраструктура** > **Узлы**. Отказавший узел будет иметь статус **Неисправен** и выделен красным цветом.
3. Хотя один узел отказал и теперь недоступен, вы по-прежнему сможете обращаться к следующим сервисам:
   - Панель администрирования.
   - Виртуальные машины.
   - iSCSI: в VMware vSphere у вас сохранится доступ к томам, экспортированным через iSCSI.
   - S3: у вас сохранится доступ к корзинам через CyberDuck.
   - NFS: в подключенном корневом экспорте у вас сохранится доступ к загруженным вами данным.
   - Backup Gateway: в консоли управления резервным копированием вы по-прежнему сможете перейти к резервной копии, созданной ранее (она доступна при правильно настроенном доменном имени).

Вы успешно выполнили проверку с принудительным отключением узла, в результате чего сервисы и данные были эвакуированы на исправные узлы и оставались доступны без перебоев.

© ООО Киберпротект, 2024