Acronis

Acronis Инфраструктура 4.0

Installation Guide

5 ноября 2020 г.

Заявление об авторских правах

Оглавление

ГЛАВА 1

Общие сведения о развертывании

Для развертывания продукта Acronis Инфраструктура в тестовой или производственной среде необходимо сделать следующее.

1. Составить план инфраструктуры.
2. Установить и настроить продукт Acronis Инфраструктура на нужных серверах.
3. Создать кластер хранилища данных.
4. Создать вычислительный кластер и/или настроить сервисы экспорта данных.

ГЛАВА 2

Планирование инфраструктуры

Для планирования инфраструктуры необходимо определить аппаратную конфигурацию каждого сервера, составить план сетей, выбрать метод и режим избыточности и решить, как распределить данные по уровням хранилища.

Информация в этой главе поможет вам в выполнении всех этих задач.

2.1 Обзор архитектуры хранилища

Базовым компонентом продукта Acronis Инфраструктура является кластер хранилища — группа физических серверов, связанных посредством сети. Каждому серверу в кластере назначены одна или несколько ролей, и на нем обычно работают сервисы, соответствующие следующим ролям:

- Роль хранилища: сервис фрагментов данных (CS)
- Роль метаданных: сервис метаданных (MDS)
- Дополнительные роли:
    - Кэш на SSD
    - Система

Любому серверу в кластере можно назначить сочетание ролей хранилища, метаданных и вспомогательных ролей.

Для каждого кластера также требуется установка веб-панели администратора на один (и только один) из серверов. Эта панель позволяет администраторам управлять кластером.

2.1.1 Роль хранилища

На серверах хранения работают сервисы фрагментов данных. Эти серверы хранят данные в виде фрагментов фиксированного размера и предоставляют доступ к этим фрагментам. Все фрагменты данных реплицируются, и реплики располагаются на разных серверах хранения для обеспечения высокой доступности данных. При отказе одного из серверов хранения оставшиеся исправные серверы продолжат предоставлять доступ к фрагментам данных, которые хранились на отказавшем сервере.

Роль хранилища можно назначить только серверу с дисками определенной емкости.

2.1.2 Роль метаданных

На серверах метаданных работают сервисы метаданных. Эти серверы хранят метаданные кластера и контролируют разделение пользовательских файлов на фрагменты, а также расположение этих фрагментов. серверы метаданных также обеспечивают наличие достаточного количества реплик для фрагментов. И наконец, они записывают в журнал все важные события, происходящие в кластере.

Для обеспечения надежности системы Acronis Инфраструктура использует алгоритм консенсуса Паксос. Он гарантирует отказоустойчивость при исправности большинства серверов, на которых работают сервисы метаданных.

Чтобы обеспечить высокую доступность метаданных в производственной среде, сервисы метаданных должны работать как минимум на трех серверах кластера. В этом случае при сбое одного сервиса оставшиеся два продолжат контролировать кластер. Однако рекомендуется не менее пяти сервисов метаданных, чтобы кластер мог выдержать одновременный отказ двух серверов без потери данных.

2.1.3 Дополнительные роли

Кэш на SSD

Повышает производительность чтения/записи фрагментов данных путем создания кэша записи на выбранных твердотельных накопителях (SSD). Также рекомендуется использовать такие накопители для метаданных, дополнительные сведения см. в разделе *Роль метаданных*

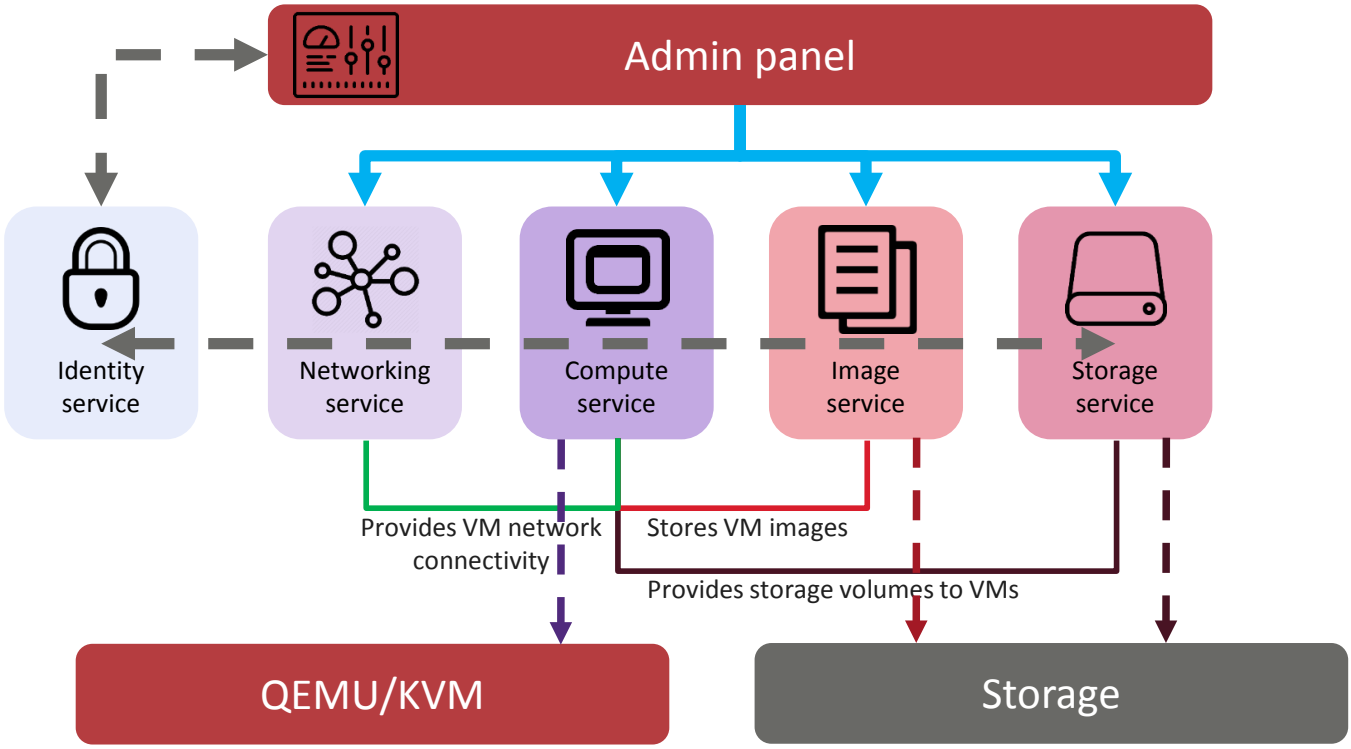
(страница 3). Использование журналов записи может более чем вдвое увеличить скорость записи в кластере.

Система

Один диск на сервер, зарезервированный для операционной системы и недоступный для хранения данных.

2.2 Обзор вычислительной архитектуры

На следующей схеме показаны основные вычислительные компоненты продукта Acronis Инфраструктура.



- Сервис хранилища предоставляет виртуальные диски виртуальным машинам. Этот сервис зависит от базового кластера хранилища в плане обеспечения избыточности данных.
- Сервис образов дает пользователям возможность загружать, хранить и использовать образы поддерживаемых гостевых операционных систем и виртуальных дисков. Этот сервис зависит от базового кластера хранилища в плане обеспечения избыточности данных.
- Сервис идентификации предоставляет функции проверки подлинности и авторизации для продукта Acronis Инфраструктура.

- Сервис вычислений дает пользователям возможность создавать, запускать и контролировать виртуальные машины. Этот сервис зависит от пользовательского гипервизора QEMU/KVM.
- Сетевой сервис обеспечивает функции физических и виртуальных сетей для виртуальных машин.

2.3 Планирование аппаратной конфигурации серверов

Acronis 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.

Примечание: Если вы не уверены, какое оборудование следует выбрать, обратитесь к торговому представителю. Также можно воспользоваться онлайн-калькулятором оборудования. Если вы хотите избежать хлопот с тестированием, установкой и настройкой аппаратного и/или программного обеспечения, стоит рассмотреть Acronis Appliance. Это готовое решение, представляющее собой отказоустойчивую инфраструктуру корпоративного класса из пяти серверов с высокопроизводительным хранилищем, которая работает в форм-факторе 3U.

2.3.1 Аппаратные ограничения

В следующей таблице приведены актуальные аппаратные ограничения для серверов продукта Acronis Инфраструктура.

Таблица 2.3.1.1: Аппаратные ограничения серверов

Оборудование	Теоретически	Сертификация
ОЗУ	64 ТБ	1 ТБ
ЦП	5120 логических ЦП	384 логических ЦП

Логический ЦП — это ядро (поток) в многоядерном (многопоточном) процессоре.

2.3.2 Аппаратные требования

В следующей таблице приведены минимальные и рекомендуемые требования к дискам в соответствии с ролями (см. *Обзор архитектуры хранилища* (страница 2)).

Таблица 2.3.2.1: Требования к дискам

Роль диска	**Количество**	**Минимум**	**Рекомендуется**
Система	Один диск на сервер	Жесткий диск SATA/SAS 100 ГБ	Твердотельный накопитель SATA/SAS 250 ГБ
Метаданные	Один диск на сервер Рекомендуется пять дисков на один кластер	Твердотельный накопитель корпоративного класса 100 ГБ с защитой от перебоев питания, стойкость минимум 1 DWPD	
Кэш	Дополнительно Один твердотельный накопитель на 4–12 жестких дисков	Твердотельный накопитель корпоративного класса 100+ ГБ с защитой от перебоев питания и скоростью последовательной записи 75 МБ/с на обслуживаемый жесткий диск; стойкость минимум 1 DWPD, рекомендуется 10 DWPD	
Хранилище	Дополнительно Как минимум один на кластер	Минимум 100 ГБ, рекомендуется 16 ТБ Жесткий диск SATA/SAS или твердотельный накопитель SATA/SAS/NVMe (корпоративного класса с защитой от перебоев питания, стойкость минимум 1 DWPD)	

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

Таблица 2.3.2.2: Требования к ОЗУ и ЦП

Сервис	**ОЗУ**	**Кол-во ядер ЦП***
Система	6 ГБ	2 ядра
Сервисы хранилища: каждый диск с ролью Storage или Cache (любого размера)**	1 ГБ	0,2 ядра
Вычислительный сервис***	8 ГБ	3 ядра
Сервис балансировщика нагрузки***	1 ГБ	1 ядро

Продолжается на следующей странице

Таблица 2.3.2.2 – продолжение с предыдущей страницы

Сервис		**ОЗУ**	**Кол-во ядер ЦП***
Сервис Kubernetes***		2 ГБ	2 ядра
S3		4,5 ГБ	3 ядра
Backup Gateway****		1 ГБ	2 ядра
NFS	Сервис	4 ГБ	2 ядра
	Каждая общая папка	0,5 ГБ	0,5 ядра
iSCSI	Сервис	1 ГБ	1 ядро
	Каждый том	0,1 ГБ	0,5 ядра

* 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. Рекомендуется использовать одинаковую модель ЦП на всех серверах во избежание проблем при динамической миграции ВМ. Ядро ЦП здесь означает физическое ядро в многоядерном процессоре (гиперпоточность не учитывается).

** Для кластеров с размером физического пространства более 1 ПБ добавьте еще 0,5 ГБ ОЗУ на каждый сервис метаданных.

*** Требования для вычислительного сервиса, балансировщика нагрузки и Kubernetes относятся только к серверу управления.

**** При работе с публичным облаком и NFS шлюз Backup Gateway потребляет столько же ОЗУ и ресурсов ЦП, сколько с локальным хранилищем.

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

Рассмотрим несколько примеров и рассчитаем требования для конкретных случаев.

- Если у вас 1 сервер (1 системный диск и 4 диска хранилища), который вы хотите использовать для Backup Gateway, см. расчеты в таблице ниже.

Таблица 2.3.2.3: Пример: 1 сервер для Backup Gateway

Сервис	**Каждый сервер**
Система	6 ГБ, 2 ядра
Сервисы хранения	4 диска хранилища с 1 ГБ ОЗУ и 0,2 ядра, т. е. всего 4 ГБ и 0,8 ядра
Backup Gateway	1 ГБ, 2 ядра
Итого	11 ГБ ОЗУ и 4,8 ядра

- Если у вас 3 сервера (1 системный диск и 4 диска хранилища), которые вы хотите использовать для вычислительного сервиса, см. расчеты в таблице ниже.

Таблица 2.3.2.4: Пример: 3 сервера для вычислительного сервиса

Сервис	**Сервер управления**	**Каждый подчиненный сервер**
Система	6 ГБ, 2 ядра	6 ГБ, 2 ядра
Сервисы хранения	4 диска хранилища с 1 ГБ ОЗУ и 0,2 ядра, т. е. всего 4 ГБ и 0,8 ядра	4 диска хранилища с 1 ГБ ОЗУ и 0,2 ядра, т. е. всего 4 ГБ и 0,8 ядра
Вычисления	8 ГБ, 3 ядра	
Балансировщик нагрузки	[redacted] ГБ, 1 ядро	
Kubernetes	2 ГБ, 2 ядра	
Итого	21 ГБ ОЗУ и 8,8 ядра	10 ГБ ОЗУ и 2,8 ядра

- Если у вас 5 серверов (1 диск «система+хранилище» и 10 дисков хранилища), которые вы хотите использовать для Backup Gateway, см. расчеты в таблице ниже. Обратите внимание, что, если не развернут вычислительный кластер, требования будут одинаковыми для сервера управления и подчиненных серверов.

Таблица 2.3.2.5: Пример: 5 серверов для Backup Gateway

Сервис	**Каждый сервер**
Система	6 ГБ, 2 ядра

Продолжается на следующей странице

Таблица 2.3.2.5 – продолжение с предыдущей страницы

Сервис	**Каждый сервер**
Сервисы хранения	11 дисков хранилища с 1 ГБ ОЗУ и 0,2 ядра, т. е. всего 11 ГБ и 2 ядра
Backup Gateway	1 ГБ, 2 ядра
Итого	18 ГБ ОЗУ и 6 ядер

- Если у вас 10 серверов (1 системный диск, 1 диск кэша, 3 диска хранилища), которые вы хотите использовать для вычислительного сервиса, см. расчеты в таблице ниже. Обратите внимание, что для высокой доступности сервера управления используются три сервера, каждый из которых соответствует требованиям для сервера управления.

Таблица 2.3.2.6: Пример: 10 серверов для вычислительного сервиса с высокой доступностью сервера управления

Сервис	**Каждый сервер управления**	**Каждый подчиненный сервер**
Система	6 ГБ, 2 ядра	6 ГБ, 2 ядра
Сервисы хранения	3 диска хранилища + 1 диск кэша с 1 ГБ ОЗУ и 0,2 ядра, т. е. всего 4 ГБ и 0,8 ядра	3 диска хранилища + 1 диск кэша с 1 ГБ ОЗУ и 0,2 ядра, т. е. всего 4 ГБ и 0,8 ядра
Вычисления	8 ГБ, 3 ядра	
Балансировщик нагрузки	ГБ, 1 ядро	
Kubernetes	2 ГБ, 2 ядра	
Итого	21 ГБ ОЗУ и 8,8 ядра	10 ГБ ОЗУ и 2,8 ядра

Чем больше ресурсов вы выделите для кластера, тем лучше он будет работать. Дополнительная оперативная память используется для кэширования операций чтения с диска. А дополнительные ядра ЦП повышают производительность и уменьшают задержку.

2.3.3 Рекомендации по оборудованию

В целом Acronis Инфраструктура работает на том же оборудовании, которое рекомендуется для Red Hat Enterprise Linux 7, включая процессоры AMD EPYC: серверы, компоненты.

В следующих рекомендациях подробнее описываются преимущества определенного оборудования, указанного в таблице аппаратных требований. Используйте их для оптимальной настройки кластера.

2.3.3.1 Рекомендации по составу кластера хранилища

Проектирование эффективного кластера хранилища данных предполагает нахождение компромисса между производительностью и стоимостью кластера, предназначенного для определенных целей. При планировании учитывайте, что 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.

Таблица 2.3.3.1.1: Рекомендации по составу кластера

Аспекты проектирования	**Минимум серверов (3), много дисков на сервер**	**Много серверов, мало дисков на сервер (флеш-конфигурация)**
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.

Продолжается на следующей странице

Таблица 2.3.3.1.1 – продолжение с предыдущей страницы

Аспекты проектирования	**Минимум серверов (3), много дисков на сервер**	**Много серверов, мало дисков на сервер (флеш-конфигурация)**
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, 24 твердотельных накопителя Samsung PM1643 1,9 ТБ).

Обратите внимание на следующие моменты.

1. Эти аспекты применимы, только если областью отказа является хост.
2. Скорость перестройки в режиме репликации не зависит от количества серверов в кластере.
3. Acronis 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.

2.3.3.2 Общие рекомендации по оборудованию

- Для производственной среды требуется не менее пяти серверов. Это необходимо для того, чтобы гарантировать отсутствие потери данных при отказе двух серверов.
- Одним из самых сильных качеств продукта Acronis Инфраструктура является масштабируемость. Чем больше кластер, тем лучше работает Acronis Инфраструктура. Рекомендуется создавать производственные кластеры с использованием не менее десяти серверов для повышения надежности, производительности и отказоустойчивости в производственных сценариях.
- Хотя кластер можно создать поверх различного оборудования, использование серверов со сходной аппаратной конфигурацией обеспечит лучшую производительность, мощность и балансировку кластера.
- 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.

- В производственной среде не рекомендуется использовать продукт Acronis Инфраструктура на оборудовании SAN/NAS с собственными механизмами обеспечения избыточности. Это может отрицательно сказаться на производительности и доступности данных.
- Для наилучшей производительности оставьте свободными не менее 20 процентов ресурсов кластера.
- Во время аварийного восстановления продукту Acronis Инфраструктура может потребоваться дополнительное дисковое пространство для репликации. Зарезервируйте пространство объемом не менее одного сервера хранения.
- Рекомендуется использовать одинаковую модель ЦП на всех серверах во избежание проблем при динамической миграции ВМ. Подробнее см. в руководстве администратора по командной строке.
- Если вы планируете использовать Backup Gateway для хранения резервных копий в облаке, убедитесь, что в локальном кластере хранилища достаточно логического пространства для промежуточного копирования (локального сохранения резервных копий перед отправкой в облако). Например, при ежедневном резервном копировании обеспечьте достаточно места для резервных копий как минимум за 1,5 дня. Дополнительные сведения см. в руководстве администратора.
- Рекомендуется использовать UEFI вместо BIOS, если позволяет оборудование. Особенно это рекомендуется при использовании дисков NVMe.

2.3.3.3 Рекомендации по оборудованию хранилища

- 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.
- Применение рекомендуемых моделей твердотельных накопителей поможет избежать потери данных. Не все накопители способны выдержать производственные нагрузки и могут отказать уже в первые месяцы эксплуатации, что приведет к резкому повышению совокупной стоимости владения.
    - Ячейки памяти твердотельного накопителя выдерживают ограниченное количество циклов перезаписи. Такой накопитель следует рассматривать как расходный материал, который потребуется заменить через некоторое время. Бюджетные накопители рассчитаны на очень

небольшое количество операций перезаписи (настолько малое, что эти цифры даже не указываются в технических характеристиках). 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.

- 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. по ссылке http://www.postgresql.org/docs/current/static/wal-reliability.html). 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).

- Настоятельно рекомендуется проверить функции сброса данных для всех ваших дисков, как описано в разделе *Проверка функций сброса данных на диски* (страница 23).

- 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.

- 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.

- 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.

- Настоятельно не рекомендуется использовать жесткие диски с черепичной магнитной записью (SMR), даже для целей резервного копирования. Такие диски имеют непредсказуемую задержку, которая может привести к неожиданным перебоям обслуживания и резкому снижению производительности.
- Работа сервисов метаданных на твердотельных накопителях повышает производительность кластера. Для снижения капитальных затрат можно использовать те же накопители для кэширования записи.
- 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.
- 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.
- Экономичнее использовать жесткие диски SATA с одним твердотельным накопителем для кэширования, чем только жесткие диски SAS без такого накопителя.
- 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 Acronis 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.
- Размер блока на диске (например, 512 байт или 4 КБ) не имеет значения и не влияет на производительность.

2.3.3.4 Рекомендации по сетевому оборудованию

- Используйте отдельные сети (и в идеале, хотя 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.
- 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.
- Во избежание вторжений Acronis Инфраструктура должна быть развернута в выделенной внутренней сети, недоступной извне.
- 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 ошибкам пользователя. Сетевые

адаптеры со скоростью 10+ Гбит/с, напротив, следует настроить на использование крупных кадров для достижения максимальной производительности.

- Адаптеры шины (HBA) Fibre Channel, поддерживаемые в настоящее время: QLogic QLE2562-CK и QLogic ISP2532.
- В качестве адаптеров InfiniBand рекомендуется использовать Mellanox ConnectX-4 и ConnectX-5. Карты Mellanox ConnectX-2 и ConnectX-3 не поддерживаются.
- Адаптеры, использующие драйвер BNX2X, такие как Broadcom Limited BCM57840 NetXtreme II 10/20-Gigabit Ethernet / HPE FlexFabric 10Gb 2-port 536FLB Adapter, не рекомендуются. Они ограничивают значение MTU до 3616, что влияет на производительность кластера.

2.3.4 Аппаратные и программные ограничения

Аппаратные ограничения

- 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 трех дисков (один для системы, один для метаданных, один для хранилища).
- Для тестирования всех функций продукта требуются три сервера.
- На системном диске должно быть не менее 100 ГБ пространства.
- Для правильного отображения панели администратора требуется монитор с разрешением Full HD.
- Максимальный поддерживаемый размер физического раздела — 254 ТиБ.

Программные ограничения

- сервер может входить только в один кластер.
- Поверх кластера хранилища можно создать только один кластер S3.
- В панели администратора доступны только стандартные режимы избыточности.
- Для всех данных всегда включено экономное распределение, которое нельзя настроить по-другому.

- Панель администратора протестирована в работе с разрешением 1280x720 и выше в следующих веб-браузерах: последняя версия Firefox, Chrome, Safari.

Сетевые ограничения см. в разделе *Сетевые ограничения* (страница 28).

2.3.5 Минимальная конфигурация хранилища

Минимальная конфигурация, приведенная в этой таблице, позволит протестировать функции кластера хранилища. Она не предназначена для производственной среды.

Таблица 2.3.5.1: Минимальная конфигурация кластера

№ сервера	1-я роль диска	2-я роль диска	3-я роль диска	Точки доступа
1	Система	Метаданные	Хранилище	iSCSI, S3 внутр., S3 внешн., NFS, Backup Gateway
2	Система	Метаданные	Хранилище	iSCSI, S3 внутр., S3 внешн., NFS, Backup Gateway
3	Система	Метаданные	Хранилище	iSCSI, S3 внутр., S3 внешн., NFS, Backup Gateway
Всего 3 серверa		Всего 3 MDS	Всего 3+ CS	Всего три сервера, на которых работают сервисы точек доступа.

Примечание: Твердотельным накопителям можно назначить роли **Система**, **Метаданные** и **Кэш** одновременно, чтобы освободить больше дисков для роли хранилища.

Хотя даже в минимальной конфигурации рекомендуется три сервера, можно начать тестировать продукт Acronis Инфраструктура всего с одним сервером и добавить остальные серверы позже. Как минимум в кластере хранилища должен работать один сервис метаданных и один сервис фрагментов данных. Установка на одном сервере позволит опробовать работу сервисов, таких как iSCSI, Backup Gateway и т. д. Однако такая конфигурация имеет два ключевых ограничения:

1. Один сервер MDS будет единой точкой отказа. Если он откажет, весь кластер перестанет работать.

2. Один сервер CS сможет хранить только одну реплику фрагмента данных. Если он откажет, данные будут потеряны.

Важно: Если Acronis Инфраструктура развертывается на одном сервере, необходимо позаботиться о том, чтобы ее хранилище было устойчивым и избыточным, во избежание потери данных. Если это физический сервер, на нем должно быть несколько дисков, чтобы можно было реплицировать данные между ними. Если это виртуальная машина, убедитесь, что высокая доступность ВМ обеспечивается решением, на базе которого она работает.

Примечание: Backup Gateway использует локальное хранилище объектов в режиме промежуточного копирования. Это означает, что данные, предназначенные для репликации, переноса или загрузки в публичное облако, сначала сохраняются локально и только после этого отправляются в место назначения. Крайне важно, чтобы локальное хранилище объектов было устойчивым и избыточным, во избежание потери данных. Существует несколько способов обеспечить устойчивость и избыточность локального хранилища. Можно развернуть Backup Gateway на нескольких серверах и выбрать нужный режим избыточности. Если Acronis Инфраструктура с шлюзом развернута на одном физическом сервере, ее локальное хранилище можно сделать избыточным путем его репликации по нескольким локальным дискам. Если Acronis Инфраструктура полностью установлена на одной виртуальной машине исключительно с целью создания шлюза, убедитесь, что высокая доступность ВМ обеспечивается решением, на базе которого она работает.

2.3.6 Рекомендуемая конфигурация хранилища

Рекомендуется как минимум пять сервисов метаданных, чтобы кластер мог выдержать одновременный отказ двух серверов без потери данных. Следующая конфигурация поможет создать кластеры для производственных сред.

Таблица 2.3.6.1: Рекомендуемая конфигурация кластера

№ сервера	1-я роль диска	2-я роль диска	3-я роль диска	Точки доступа
серверы 1–5	Система	SSD; метаданные, кэш	Хранилище	iSCSI, S3 внутр., S3 внешн., Backup Gateway
серверы 6+	Система	SSD; кэш	Хранилище	iSCSI, S3 внутр., Backup Gateway
Всего 5+ серверов		Всего 5 MDS	Всего 5+ CS	На всех серверах работают нужные точки доступа.

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.

Ниже приведены примеры конкретных конфигураций, которые можно использовать в производственной среде. Каждую конфигурацию можно расширить путем добавления чанк-серверов и серверов.

2.3.6.1 Только жесткие диски

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

Таблица 2.3.6.1.1: 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

2.3.6.2 Жесткие диски + системные твердотельные накопители (без кэширования)

Эта конфигурация подходит для кластеров, ориентированных на емкость.

Таблица 2.3.6.2.1: 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

2.3.6.3 HDD + SSD

Эта конфигурация подходит для кластеров, ориентированных на производительность.

Таблица 2.3.6.3.1: 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

2.3.6.4 Только твердотельные накопители

В этой конфигурации не требуются твердотельные накопители для кэширования.

При выборе оборудования для этой конфигурации учитывайте следующее.

- Каждый клиент продукта Acronis Инфраструктура сможет получить из кластера устойчивое значение до 40000 IOPS (чтение + запись).

- При использовании схемы избыточного кодирования каждый файл кодирования, например один жесткий диск ВМ, получит устойчивое значение до 2000 IOPS. То есть пользователь, работающий внутри ВМ, будет иметь в своем распоряжении до 2000 IOPS на виртуальный жесткий диск. Несколько ВМ на сервере могут использовать большее значение IOPS, до лимита клиента.
- 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.

Таблица 2.3.6.4.1: 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

2.3.6.5 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).

Таблица 2.3.6.5.1: 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

Таблица 2.3.6.5.2: 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

2.3.6.6 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.

Таблица 2.3.6.6.1: 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 У2	
3	HDD	CS	1
4	HDD	CS	2
5	SSD	CS	3
…	…	…	…
N	HDD/SSD	CS	1/2/3

Таблица 2.3.6.6.2: 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 У2	
3	HDD	CS	1
4	HDD	CS	2
5	SSD	CS	3
…	…	…	…
N	HDD/SSD	CS	1/2/3

2.3.7 Неформатированное дисковое пространство

При планировании инфраструктуры учитывайте следующее, во избежание путаницы.

- 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 Acronis Инфраструктура.
- 5 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.

2.3.8 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.

Acronis 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.

2.4 Планирование конфигураций виртуальных машин

Хотя Acronis Инфраструктура обеспечивает наилучшую производительность на «голом железе», она также может работать внутри виртуальных машин. Однако для виртуальных машин будут доступны только сервисы хранилища, и вы не сможете создать вычислительный кластер.

2.4.1 Работа на VMware vSphere

Для работы продукта Acronis Инфраструктура на VMware vSphere убедитесь в соблюдении следующих требований.

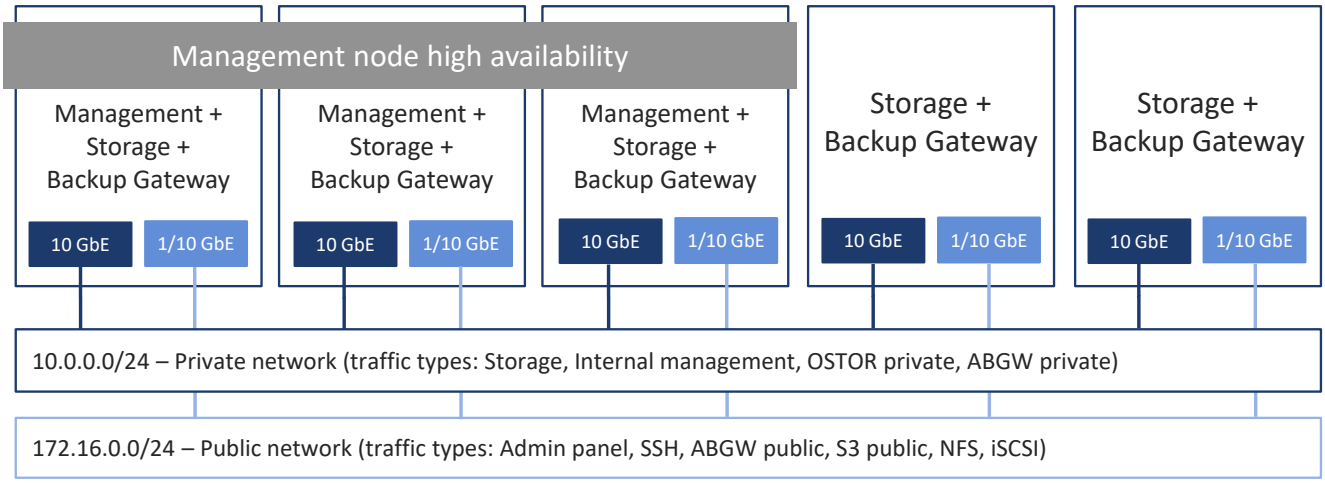
- Версия VMware vSphere: 6.7 и выше
- Версия ВМ: 14 и выше
- На хосте должно быть достаточно памяти. Для сервера с одним диском хранилища, на котором работает Backup Gateway, требуется как минимум 8 ГБ ОЗУ.
- В хранилище данных vSphere должно быть достаточно свободного пространства. Каждая виртуальная машина занимает как минимум 425 ГБ (два диска хранилища по 200 ГБ и системный диск на 25 ГБ). Шаблон продукта Acronis Инфраструктура также занимает около 35 ГБ. Максимальный рекомендуемый размер одного виртуального диска — 16 ТБ.

Важно: Планируйте размер виртуальных дисков заранее и резервируйте достаточно пространства для ожидаемого увеличения объема данных. Размер дисков нельзя изменить позже, но можно добавить новые диски.

2.5 Планирование сети

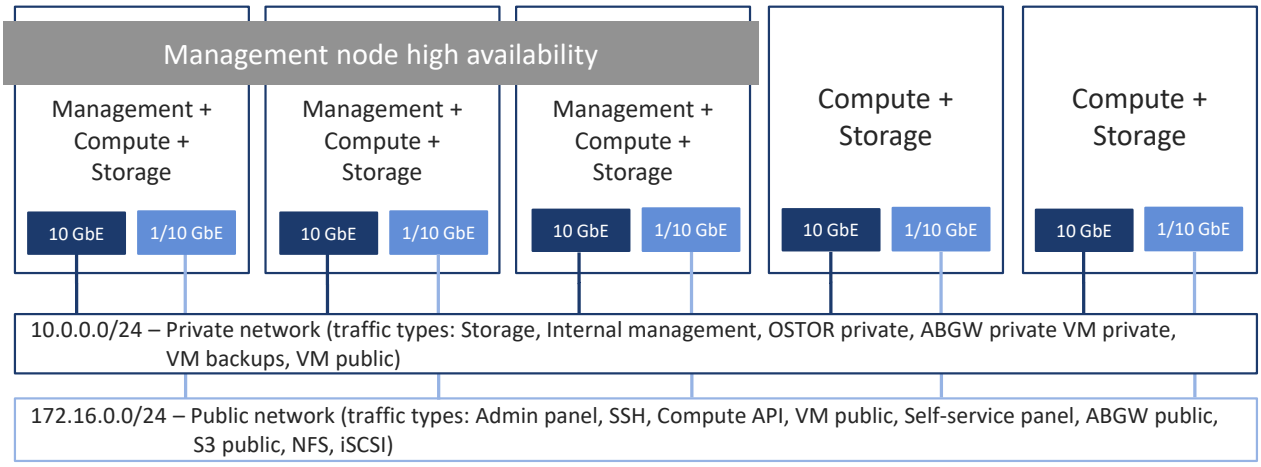
Сетевая конфигурация для продукта Acronis Инфраструктура зависит от сервисов, которые вы планируете развернуть.

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



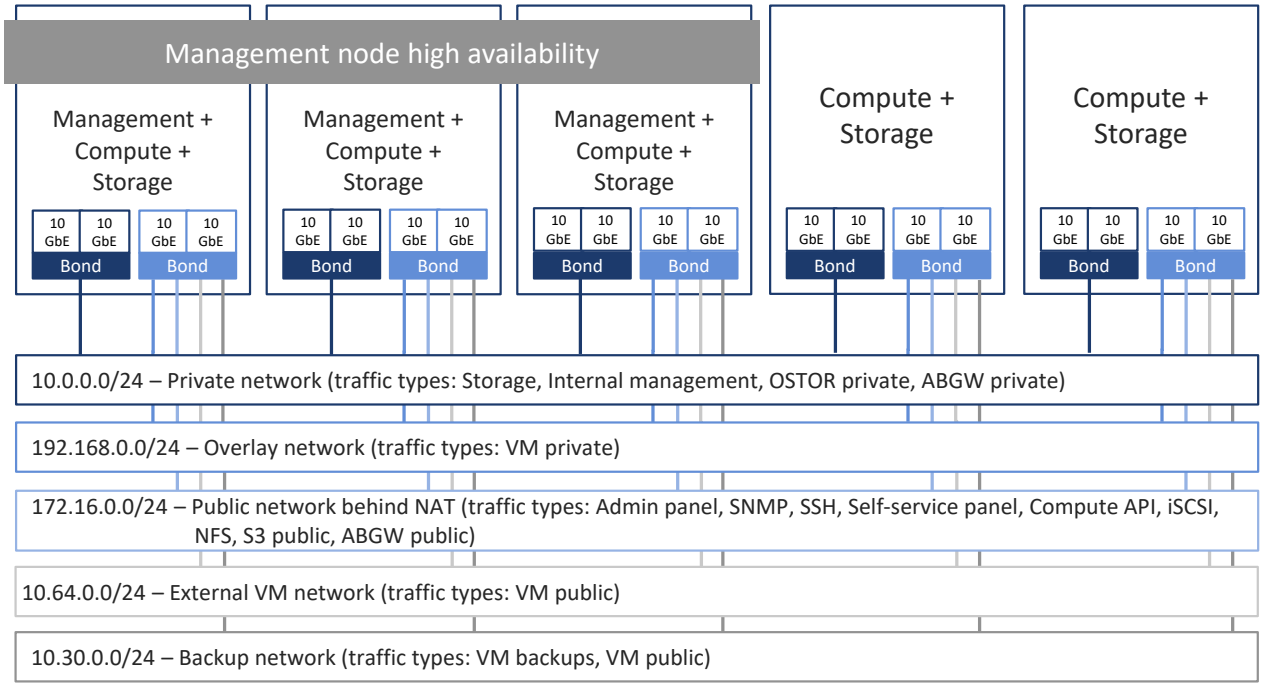
Если вы планируете развернуть вычислительный сервис поверх кластера хранилища, можно создать минимальную сетевую конфигурацию в целях тестирования либо расширить ее до более сложной конфигурации, рекомендуемой для производственной среды.

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



- Рекомендуемая конфигурация расширена до пяти сетей, подключенных к следующим логическим сетевым интерфейсам:
  - 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



2.5.1 Общие требования к сети

- Внутренний трафик хранилища должен быть отделен от других типов трафика.
- Сеть для внутреннего трафика может быть немаршрутизируемой, с минимальной пропускной способностью 10 Гбит/с.

2.5.2 Сетевые ограничения

- 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 MTU по умолчанию установлено значение 1500. Сведения об установке оптимального значения MTU см. в разделе *Шаг 2. Настройка сети* (страница 48).
- 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`.
- Тип трафика **Управление системными сервисами** назначается автоматически во время установки и не может быть изменен позже в панели администратора.
- Хотя сервер управления доступен из веб-браузера по имени хоста, при установке необходимо указать его IP-адрес, а не имя хоста.

2.5.3 Требования к сети и рекомендации для каждого сервера

- 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.
- Хотя на серверах кластера настроены необходимые правила `iptables`, рекомендуется использовать внешний брандмауэр для непроверенных публичных сетей, таких как Интернет.
- 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`.

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

Таблица 2.5.3.1: Открытые порты на серверах кластера

Сервис	Тип трафика	Порт	Описание
Веб-панель управления	Панель управления*	TCP 8888	Внешний доступ к панели администрирования.
	Панель самообслу-живания	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	ABGW внешн.	TCP 44445	Внешний обмен данными с агентами Acronis Backup и Acronis Cyber Backup Cloud.
	ABGW внутр.	Любой доступный порт	Управление системными сервисами и обмен данными между несколькими сервисами Backup Gateway.
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.

Продолжается на следующей странице

Таблица 2.5.3.1 – продолжение с предыдущей страницы

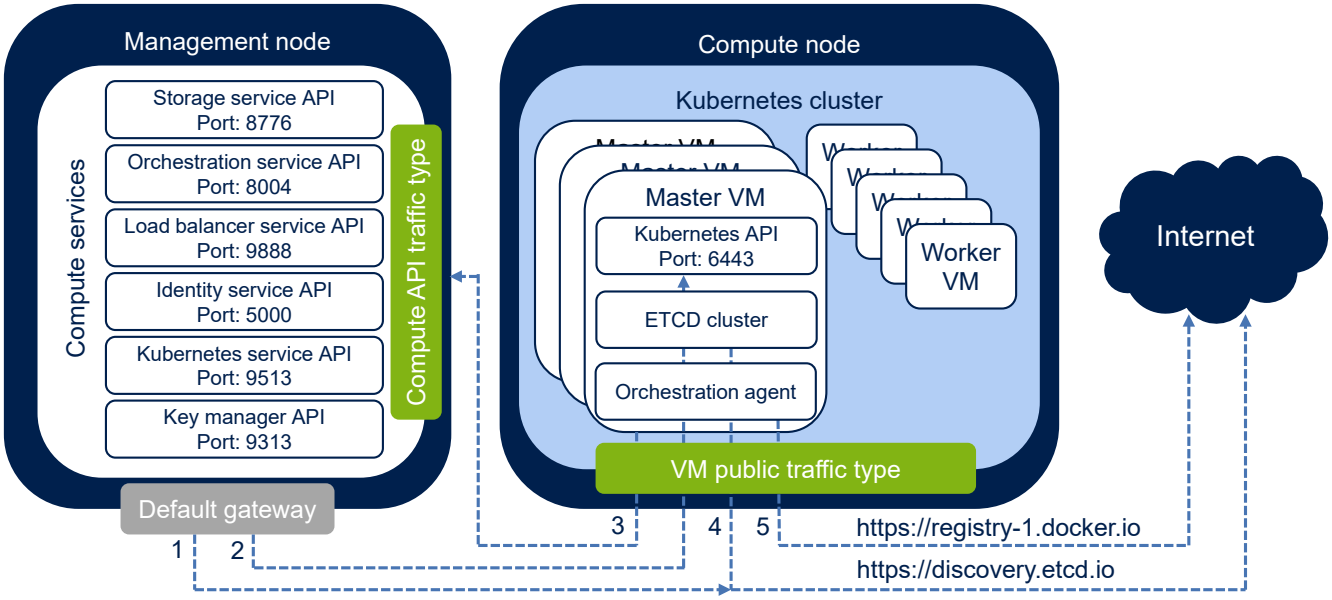
Сервис	Тип трафика	Порт	Описание
	OSTOR внутр.	Любой доступный порт	Внутренний обмен данными между несколькими сервисами NFS.
Вычисления	API вычисле-ний*		Внешний доступ к стандартным оконечным точкам OpenStack API:
		TCP 5000	API идентификации, версия 3
		TCP 6080	noVNC Websocket Proxy
		TCP 8004	API 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 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 5900–5999	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*	UDP 161	Внешний доступ к статистике мониторинга кластера хранилища по протоколу SNMP.

* Порты для этих типов трафика должны быть открыты только на серверах управления.

2.5.4 Требования к сети для Kubernetes

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 (см. раздел Setting a DNS name for the compute API).
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

2.5.5 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.

Таблица 2.5.5.1: 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 x 1 Гбит/с	~175 МБ/с	100 МБ/с	~130 МБ/с

Продолжается на следующей странице

Таблица 2.5.5.1 – продолжение с предыдущей страницы

Сетевой интерфейс хранилища	**Макс. скорость ввода-вывода сервера**	**Макс. скорость ввода-вывода ВМ (репликация)**	**Макс. скорость ввода-вывода ВМ (избыточное кодирование)**
3 x 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 x 10 Гбит/с	1,75 ГБ/с	1 ГБ/с	1,3 ГБ/с

2.6 Общие сведения об избыточности данных

Acronis Инфраструктура защищает каждый фрагмент данных путем обеспечения его избыточности. Это означает, что копии каждого фрагмента данных размещаются на разных серверах хранения, чтобы гарантировать доступность этих данных, даже если некоторые серверы будут недоступны.

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

Избыточность достигается одним из двух методов: репликацией или избыточным кодированием (подробнее описывается в следующем разделе). 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.

Acronis Инфраструктура поддерживает несколько режимов для каждого метода обеспечения избыточности. В следующей таблице показаны дополнительные затраты ресурсов для различных режимов избыточности. Первые три строки представляют репликацию, а остальные — избыточное кодирование.

Таблица 2.6.1: Сравнение режимов избыточности

Режим избыточности	**Мин. необходимое кол-во серверов**	**Сколько серверов могут отказать без потери данных**	**Доп. затраты ресурсов хранилища, %**	**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
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
Кодирование 5+2	7	2	40	140 ГБ
Кодирование 7+2	9	2	29	129 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 серверов 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 подходящие режимы избыточности.

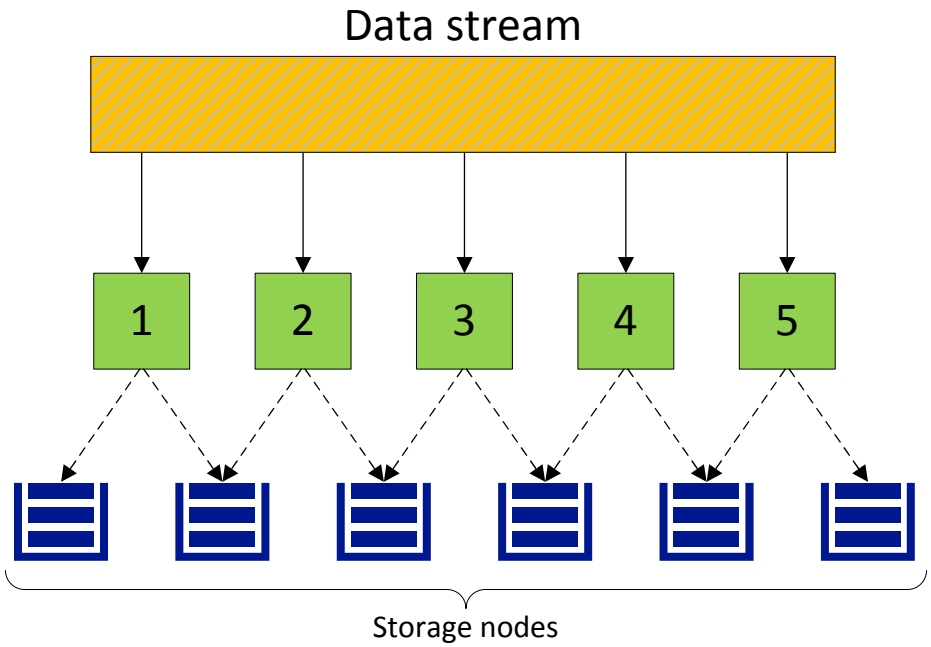
Режим избыточности данных можно выбрать при настройке сервисов хранилища и создании томов хранения данных для виртуальных машин. Независимо от того, какой режим вы выберете, настоятельно рекомендуется обеспечить защиту на случай одновременного отказа двух серверов, поскольку это часто происходит в реальных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

Все режимы избыточности разрешают операции записи, если недоступен один сервер хранения. Если недоступны два сервера хранения, операции записи могут быть заморожены до завершения самовосстановления кластера.

2.6.1 Избыточность посредством репликации

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

На следующей схеме показан режим избыточности с двумя репликами.



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

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

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

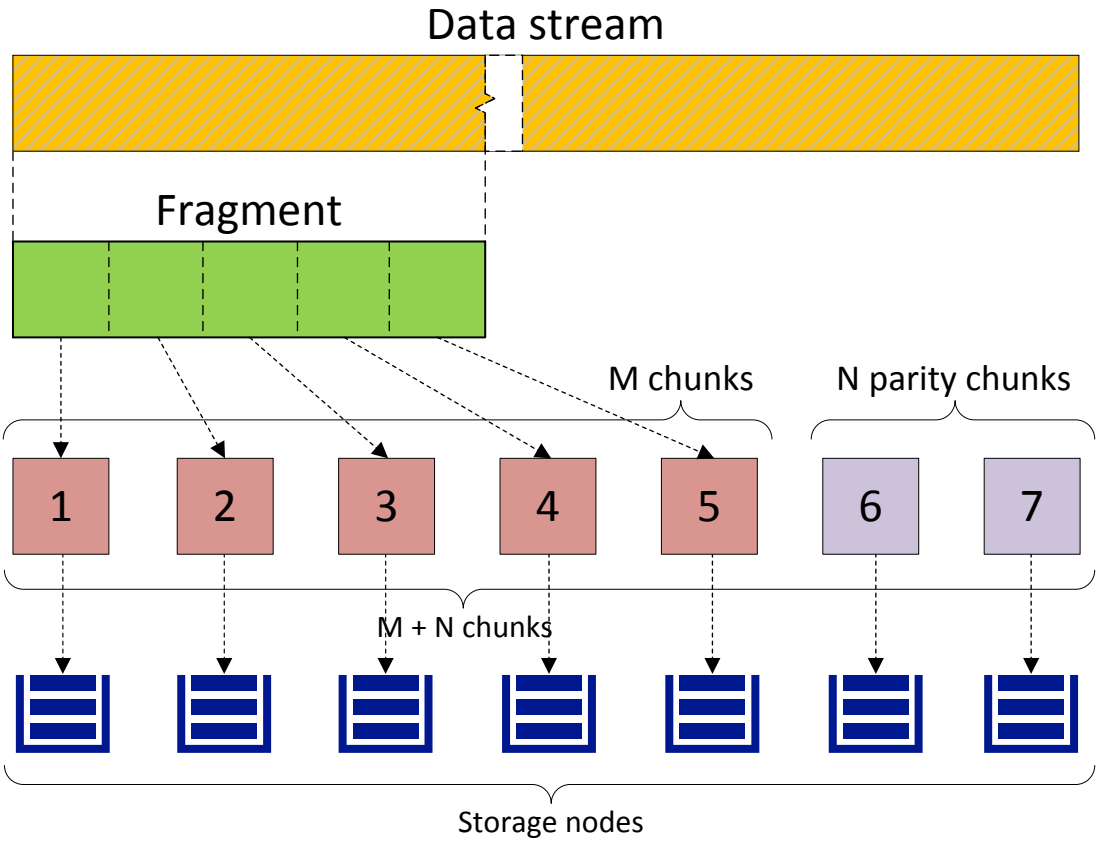
- Количество доступных серверов хранилища. Репликация выполняется параллельно, поэтому чем больше доступно источников и мест назначения репликации, тем больше ее скорость.
- Производительность дисков в серверах хранения.
- Производительность сети. Все реплики перемещаются между серверами хранилища по сети. Например, пропускная способность 1 Гбит/с может стать узким местом системы (см. раздел *Требования к сети и рекомендации для каждого сервера* (страница 29)).
- Распределение данных в кластере. На некоторых серверах 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.

2.6.2 Избыточность посредством избыточного кодирования

При использовании избыточного кодирования Acronis 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) паритетных блоков. Все блоки распределяются по серверам хранилища M+N, то есть один блок на сервер. На серверах хранилища блоки хранятся в обычных фрагментах по 256 МБ, но такие фрагменты не реплицируются, поскольку избыточность уже достигнута. Кластер может выдержать отказ любых N серверов хранилища без потери данных.

Значения M и N указаны в названиях режимов избыточного 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, данные кодируются с использованием схемы RAID6, а если N больше 2, применяются избыточные коды.

На схеме ниже показан режим 5+2.



2.6.3 Без избыточности

Предупреждение: Риск потери данных!

Без применения избыточности одиночные фрагменты данных размещаются на серверах хранения по одному фрагменту на сервер. При отказе сервера данные могут быть потеряны. Такой режим настоятельно не рекомендуется независимо от сценария использования, за исключением случаев, когда вы хотите опробовать продукт Acronis Инфраструктура на одном сервере.

2.7 Общие сведения об областях 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 кластера 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, Acronis 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 Acronis Инфраструктура никогда не размещает больше одной реплики данных на одном диске. Несмотря на защиту от отказов диска, 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 сервером.
- Хост как область отказа. При использовании этой политики Acronis Инфраструктура никогда не размещает больше одной реплики данных на одном хосте. Поэтому, если один из серверов хранилища откажет (сбой операционной системы) и все его диски станут недоступны, данные по-прежнему будут доступны с исправных серверов.
- Стойка как область отказа. При использовании этой политики Acronis Инфраструктура никогда не размещает больше одной реплики данных на одну стойку. Поэтому, если одна из стоек откажет (сбой стоечного коммутатора верхнего уровня) и все серверы в ней станут недоступны, данные по-прежнему будут доступны из других стоек.
- Ряд стоек как область отказа. При использовании этой политики Acronis Инфраструктура никогда не размещает больше одной реплики данных на один ряд. 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 Acronis 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 сервисы метаданных распределены по областям. Например, если вы выбрали комнату как область отказа и равномерно распределили данные по нескольким комнатам, необходимо также распределить сервисы метаданных. Если разместить все сервисы метаданных в одной 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 сервисы 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 серверами.
- Дисковое пространство должно быть равномерно распределено между областями отказа. Например, если выбрать стойку как область 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 фактор 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) останется свободное пространство, недоступное для распределения.

2.8 Общие сведения об уровнях хранения

В терминологии продукта Acronis Инфраструктура уровнями называются группы дисков, которые позволяют организовать рабочие нагрузки хранилища в соответствии с определенными критериями. Например, можно использовать уровни для разделения нагрузок, производимых разными клиентами. 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.

При назначении дисков на уровни (которое можно выполнить 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 SSD), уровень 1 — для виртуальных сред, то есть большого объема холодных данных, но с быстрыми операциями произвольной записи (CS с кэшем на SSD), уровень 2 — для горячих данных (CS на SSD), кэширования, конкретных дисков и т. п.

Эта рекомендация связана с тем, как Acronis Инфраструктура работает с пространством хранилища. Если на каком-либо уровне хранения заканчивается свободное место, Acronis Инфраструктура попытается временно использовать пространство более низких уровней вплоть до самого нижнего. Если самый нижний уровень также заполняется, Acronis Инфраструктура попытается задействовать более высокий уровень. Если вы позже добавите дополнительное пространство на исходный уровень, то данные, временно хранящиеся в другом месте, будут перемещены на свой исходный уровень. Например, если вы пытаетесь записать данные на уровень 2, который заполнен, Acronis Инфраструктура попытается записать эти данные на уровень 1, а затем на уровень 0. Если вы позже добавите дополнительное пространство на уровень 2, вышеупомянутые данные, теперь хранящиеся на уровне 1 или 0, будут перемещены обратно на уровень 2, где они должны были храниться изначально.

Распределение данных между уровнями, а также перемещение данных на исходный уровень выполняются в фоновом режиме. Можно отключить эту миграцию и сохранять строгое разделение уровней, как описано в руководстве администратора по командной строке.

Примечание: За исключением ситуаций с нехваткой места, автоматическая миграция данных между уровнями не поддерживается.

2.9 Общие сведения о перестройке кластера

кластер хранилища имеет функции самовосстановления. При отказе сервера или диска кластер автоматически попытается восстановить потерянные данные, т. е. перестроиться.

Процесс перестройки включает несколько этапов. Каждый CS-сервер отправляет heartbeat-сообщение на один из MDS-серверов каждые пять секунд. Если сообщение не отправлено, CS-сервер считается *неактивным* и MDS-сервер указывает всем компонентам кластера остановить операции с запросами к данным на этом CS-сервере. Если heartbeat-сообщения не поступают от CS-сервера 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 CS-серверы, 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 CS-сервер. 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 CS-сервер 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.

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

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

Для успешной перестройки кластер должен иметь как минимум:

1. столько исправных серверов, сколько требует режим избыточности;
2. достаточно свободного пространства для размещения данных любого сервера.

Первое условие можно проиллюстрировать следующим примером. В кластере, который работает в режиме избыточного кодирования 5+2 и состоит из семи серверов (то есть минимума), каждый фрагмент пользовательских данных распределен по 5+2 серверам для избыточности, то есть задействованы все серверы. При отказе одного или двух серверов данные не будут потеряны, но производительность кластера снизится, а перестройка будет невозможна, пока не будут исправны как минимум семь серверов (то есть пока вы не добавите отсутствующие серверы). Для сравнения: в кластере, который работает в режиме избыточного кодирования 5+2 и состоит из десяти серверов, каждый фрагмент пользовательских данных распределен по произвольным 5+2 серверам из десяти для равномерной нагрузки на CS-серверы. Даже если откажут сразу три сервера, в таком кластере останется достаточно серверов для перестройки.

Второе условие можно проиллюстрировать следующим примером. В кластере с десятью серверами по 10 ТБ следует оставить свободным как минимум 1 ТБ на каждом сервере, чтобы при отказе одного сервера 9 ТБ данных можно было восстановить на оставшихся девяти серверах. Однако, если в

кластере десять серверов по 10 ТБ и один сервер на 20 ТБ, то на каждом из меньших серверов должно быть свободно не менее 2 ТБ на случай сбоя большого сервера (при этом на большом сервере достаточно оставить свободным 1 ТБ).

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

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

ГЛАВА 3

Установка с помощью графического интерфейса

После планирования инфраструктуры следует установить продукт на каждый сервер, включенный в план.

Важно: Необходимо синхронизировать время посредством NTP на всех серверах одного кластера. Убедитесь, что все серверы имеют доступ к серверу NTP.

3.1 Получение образа дистрибутива

Чтобы получить ISO-образ дистрибутива, зайдите на страницу продукта и отправьте запрос на пробную версию.

3.2 Подготовка к установке

Продукт Acronis Инфраструктура можно установить из следующих источников:

- виртуальные диски IPMI,
- PXE-серверы (в этом случае синхронизация времени через NTP включена по умолчанию),
- USB-накопители.

3.2.1 Подготовка к установке с USB-накопителей

Чтобы установить продукт Acronis Инфраструктура с USB-накопителя, потребуется накопитель размером 4 ГБ или более и ISO-образ дистрибутива продукта Acronis Инфраструктура.

Создайте загрузочный USB-накопитель, скопировав на него образ дистрибутива:

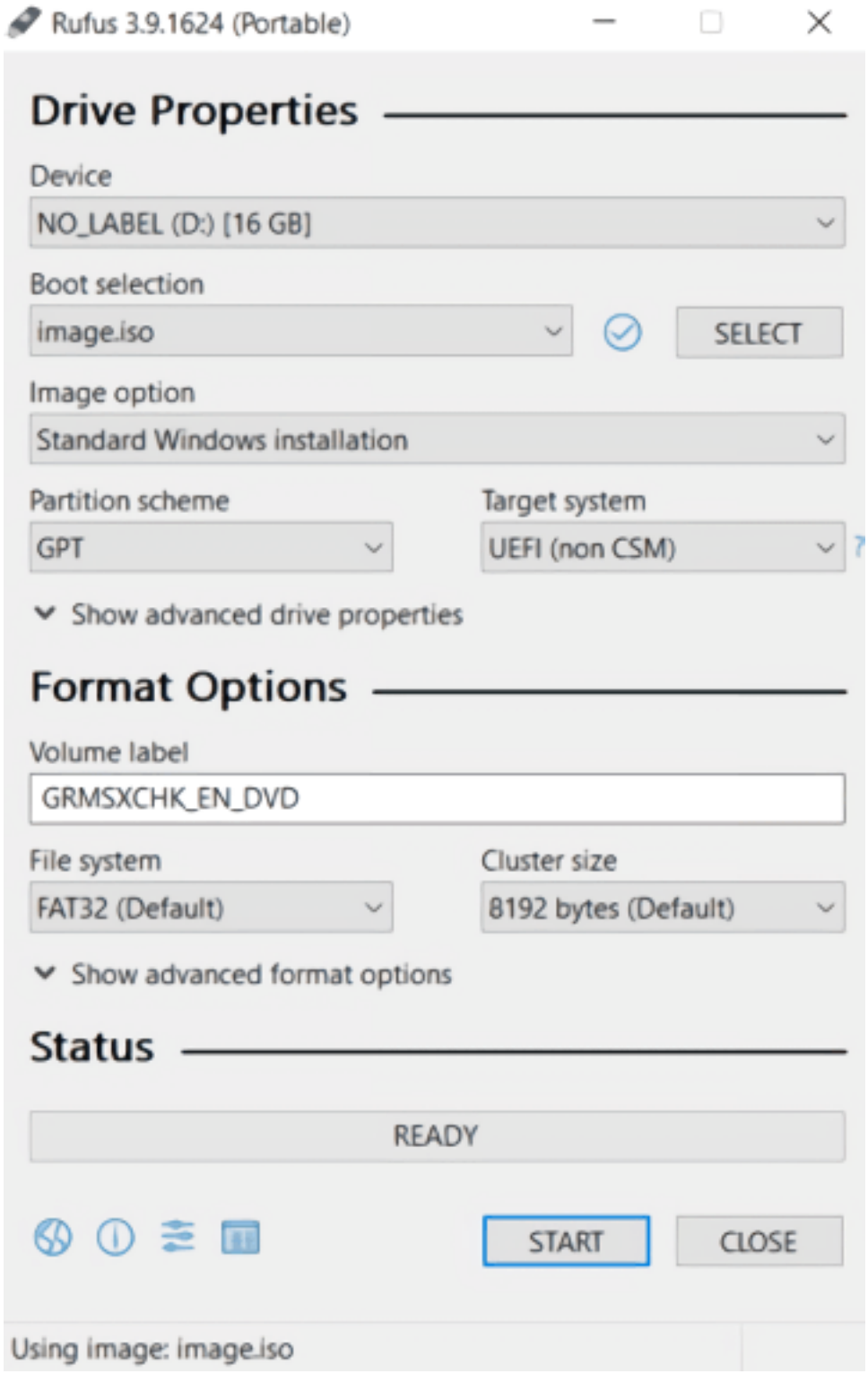
- в Linux с помощью команды dd:

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

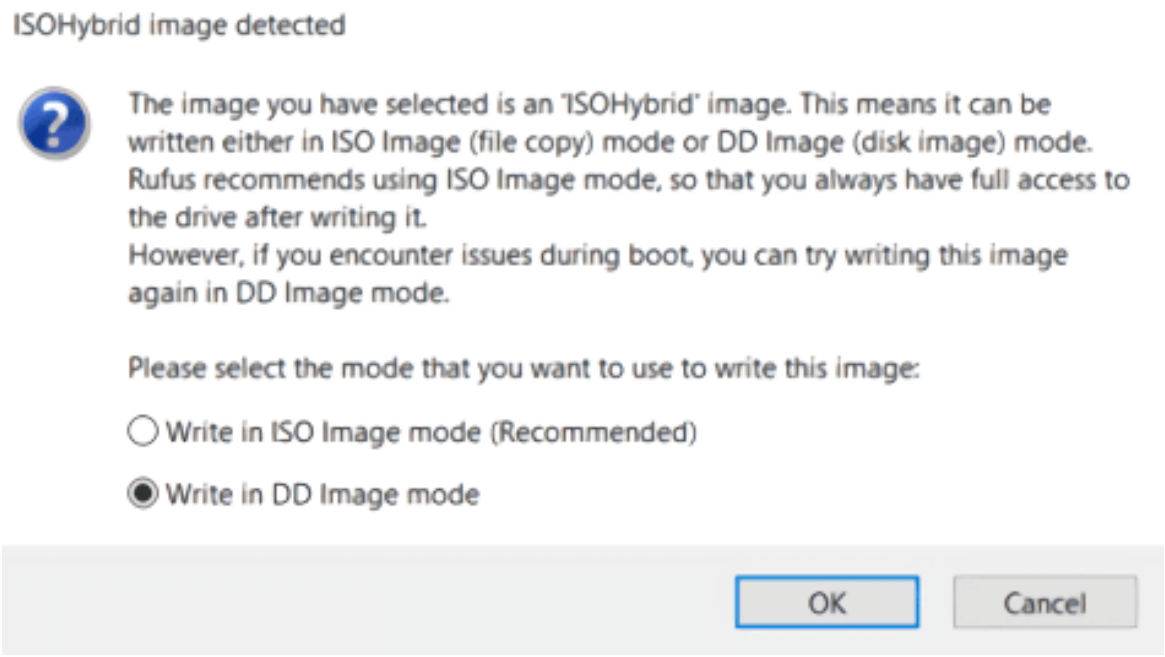
Важно: Убедитесь, что указан правильный диск для переноса образа.

- в Windows с помощью утилиты Rufus:

1. Зайдите на сайт https://rufus.ie/ и загрузите переносимую версию.
2. Запустите Rufus.
3. В разделе **Свойства диска** выберите флэш-накопитель в раскрывающемся списке **Устройство** и нажмите **Выбрать**. Затем выберите образ дистрибутива с локальной машины. При необходимости можно изменить другие параметры.
4. Нажмите **Старт**.



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



3.3 Начало установки

Для программы установки требуется разрешение экрана не менее 800x600. Однако, с этим разрешением могут возникнуть проблемы в пользовательском интерфейсе. Например, некоторые элементы могут быть недоступны. Рекомендуется разрешение не менее 1024x768.

Чтобы начать установку, сделайте следующее.

1. Настройте сервер на загрузку с выбранного носителя.
2. Загрузите сервер и дождитесь экрана приветствия.
3. На экране приветствия выполните одно из следующих действий.
   - Чтобы задать параметры установки вручную, выберите **Установить продукт Acronis Инфраструктура**.
   - Чтобы установить продукт Acronis Инфраструктура в автоматическом режиме, нажмите клавишу **E**, чтобы изменить пункт меню, добавьте расположение файла kickstart в строку `linux` и нажмите **Ctrl+X**. Например:

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

> Инструкции по созданию и использованию файла kickstart см. в разделах *Создание файла kickstart* (страница 63) и *Использование файла kickstart* (страница 69).

Если выбран вариант **Установить продукт Acronis Инфраструктура**, необходимо будет выполнить следующие шаги.

1. Прочитать и принять пользовательское соглашение.
2. Настроить сеть.
3. Выбрать часовой пояс. Дата и время будут настроены через NTP.
4. Выбрать, какой сервер кластера хранилища устанавливается: первый или второй/другой. Этот шаг можно пропустить, чтобы позже добавить сервер в кластер хранилища вручную.
5. Выбрать целевой диск для установки продукта Acronis Инфраструктура.
6. Создать пароль привилегированного пользователя и начать установку.

Эти шаги подробно описаны в следующих разделах.

3.4 Шаг 1. Принятие пользовательского соглашения

На этом шаге внимательно прочитайте лицензионное соглашение с конечным пользователем. Примите условия, установив флажок **Я принимаю лицензионное соглашение с конечным пользователем**, и нажмите кнопку **Далее**.

3.5 Шаг 2. Настройка сети

Acronis Инфраструктура требует наличия одного сетевого интерфейса на сервер для управления. Необходимо указать сетевой интерфейс, которому будет назначена сеть с типом трафика **Управление системными сервисами**. После установки этот тип трафика нельзя будет удалить из предварительно настроенной сети в панели администратора.

На странице **Network and hostname** (Сеть и имя хоста) должна быть настроена как минимум одна сетевая карта. Обычно сеть настраивается автоматически (через DHCP). Если требуется ручная настройка, выберите сетевую карту, нажмите **Configure...** (Настроить...) и укажите необходимые параметры.

В частности, можно откорректировать значение MTU. Как уже было сказано в разделе *Сетевые ограничения* (страница 28), по умолчанию для MTU установлено значение 1500, но рекомендуется 9000. Если вы интегрируете продукт Acronis Инфраструктура в существующую сеть, установите значение MTU, используемое в этой сети. Если вы развертываете продукт Acronis Инфраструктура с нуля вместе с новой сетью, установите рекомендуемое значение 9000.

Важно: Значение MTU должно быть одинаковым по всей сети.

Потребуется настроить одинаковое значение MTU для:

- каждого маршрутизатора и коммутатора в сети (сведения см. в руководствах по сетевому оборудованию);
- сетевой карты каждого сервера, а также каждого объединенного интерфейса или интерфейса VLAN.

Также рекомендуется создать два объединенных соединения, как описано в разделе *Планирование сети* (страница 26), и три интерфейса VLAN на одном из объединенных интерфейсов. Один из интерфейсов VLAN необходимо создать в программе установки и назначить сети панели администратора, чтобы обеспечить доступ к панели после установки. Остальные интерфейсы VLAN можно создать и назначить сетям более удобным способом на панели управления, как описано в руководстве администратора.

Дополнительно необходимо указать уникальное имя хоста: либо полное доменное имя (< >.< >), либо краткое имя (< >) в поле **Host name** (Имя хоста).

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

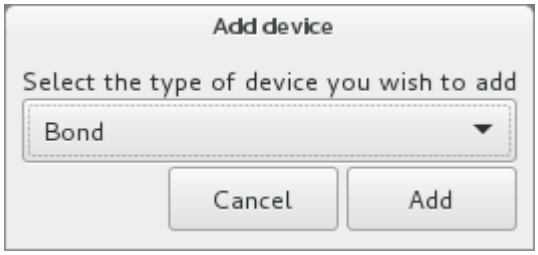
Завершив настройку сети, нажмите **Далее**.

3.5.1 Создание объединенных соединений

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

Объединенные сетевые интерфейсы можно создать на странице **Network and hostname** (Сеть и имя хоста), как описано ниже.

1. Чтобы добавить новое объединенное соединение, нажмите кнопку «плюс» внизу страницы, выберите **Bond** (Агрегация) из раскрывающегося списка и нажмите **Добавить**.

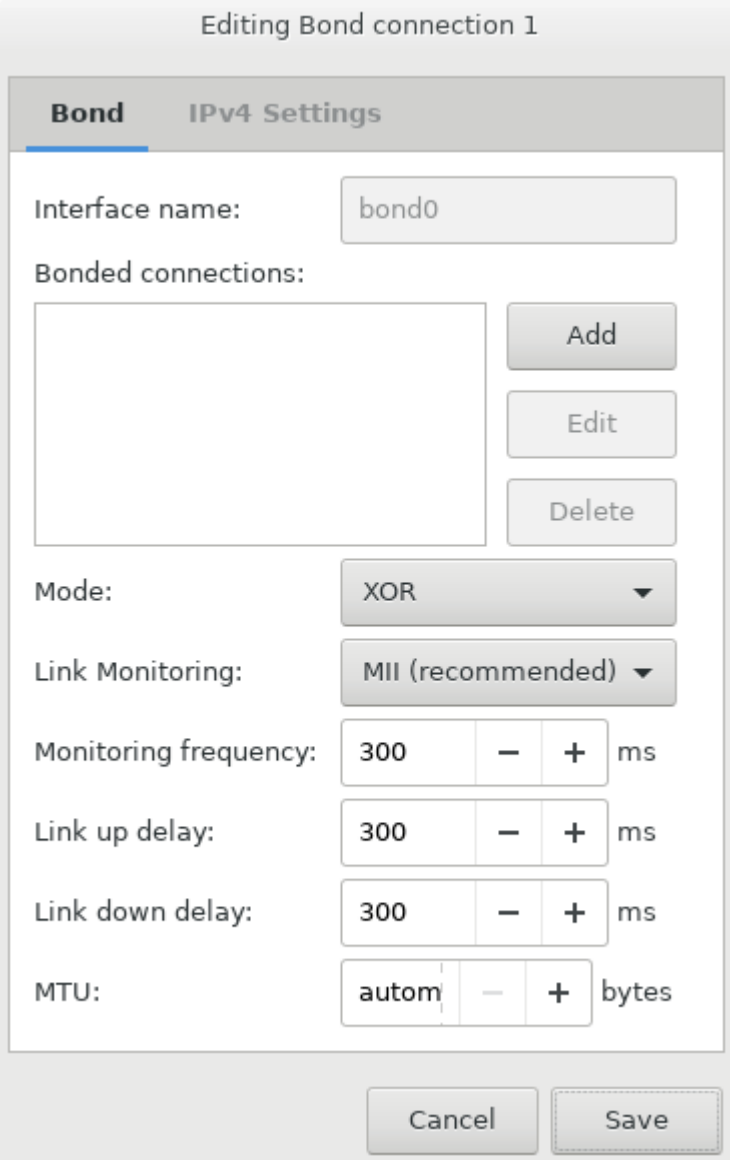


2. В окне **Editing Bond connection<N>** (Изменение объединенного соединения) установите следующие параметры для объединенного интерфейса Ethernet.

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

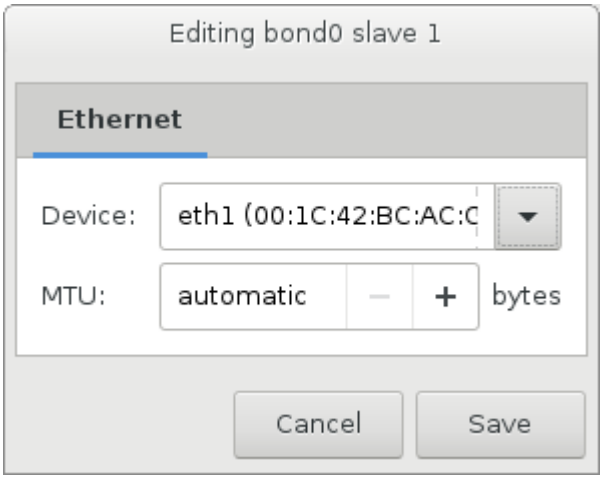
   2.2. **Link Monitoring** (Мониторинг каналов) — `MII (  )`

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



Примечание: Также рекомендуется вручную установить для `xmit_hash_policy` значение `layer3+4` после установки.

3. В разделе **Bonded connections** (Объединенные соединения) на вкладке **Bond** (Агрегация) нажмите **Добавить**.
4. В окне **Editing bond<N> slave<N>** (Изменение подчиненного интерфейса агрегации) выберите сетевой интерфейс для объединения в раскрывающемся списке **Device** (Устройство).



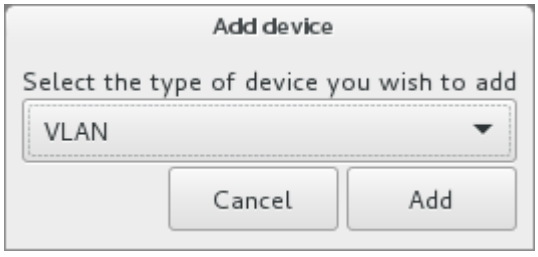
5. При необходимости настройте значение MTU и нажмите кнопку **Сохранить**.
6. Повторите шаги 3–5 для каждого сетевого интерфейса, который необходимо добавить в объединенное соединение.
7. При необходимости настройте параметры IPv4 и нажмите кнопку **Сохранить**.

Соединение появится в списке на странице **Network and hostname** (Сеть и имя хоста).

3.5.2 Создание адаптеров VLAN

При установке продукта Acronis Инфраструктура также можно создать адаптеры виртуальной локальной сети (VLAN) на базе физических адаптеров или объединенных соединений на странице **Network and hostname** (Сеть и имя хоста), как описано ниже.

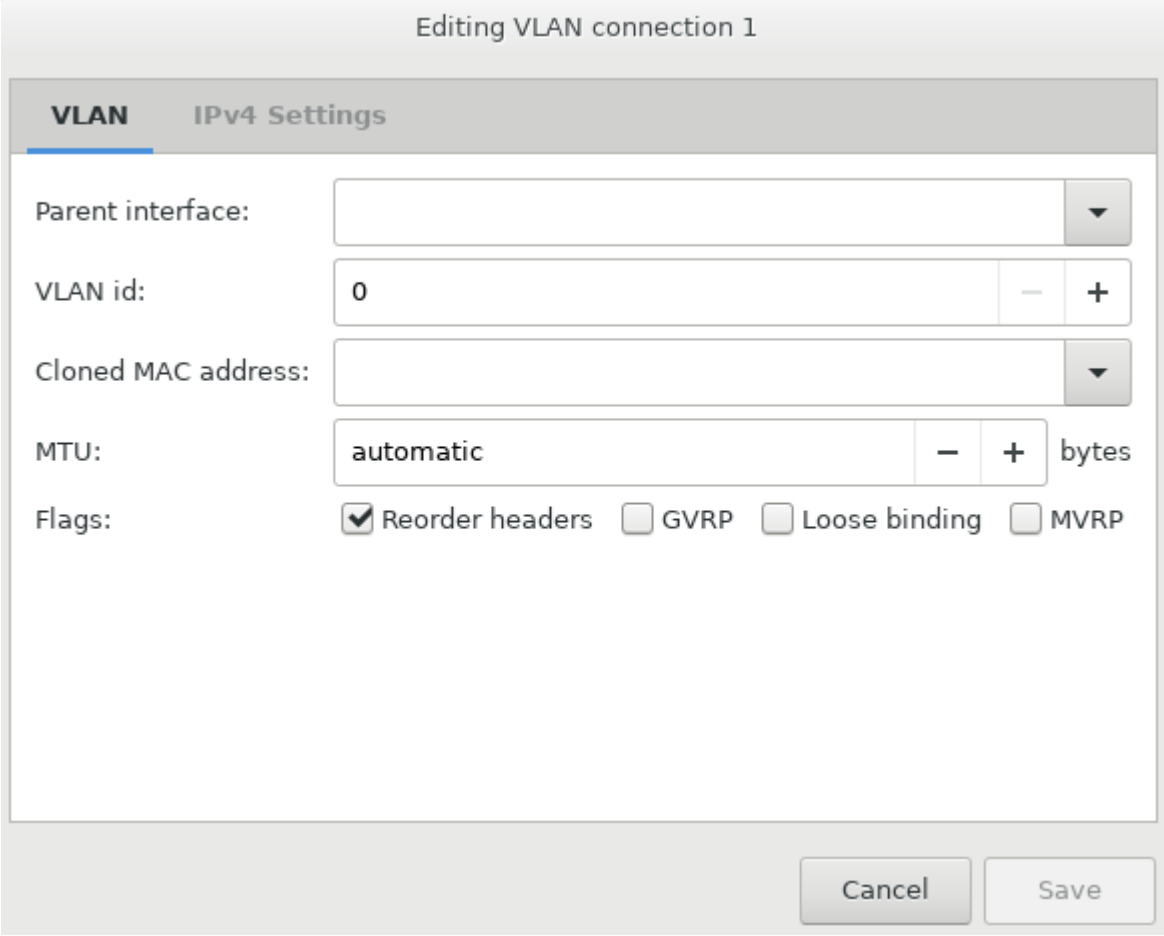
1. Чтобы добавить новый адаптер VLAN, нажмите кнопку «плюс» внизу страницы, выберите **VLAN** из раскрывающегося списка и нажмите **Добавить**.



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

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

2.2. Укажите идентификатор адаптера VLAN в поле **VLAN ID**. Значение должно находиться в диапазоне 1–4094.



3. При необходимости настройте параметры IPv4 и нажмите кнопку **Сохранить**.

Адаптер VLAN появится в списке на странице **Network and hostname** (Сеть и имя хоста).

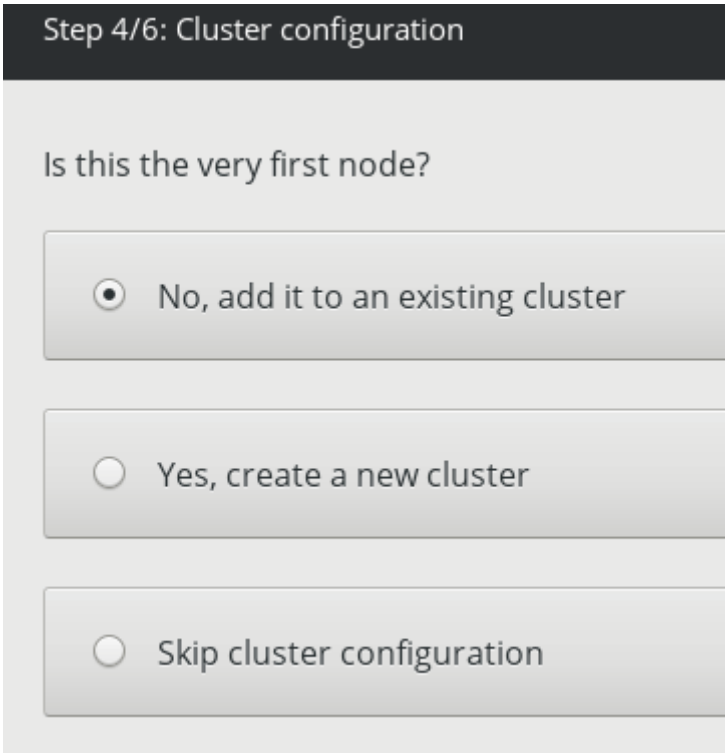
3.6 Шаг 3. Выбор часового пояса

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

3.7 Шаг 4. Настройка кластера хранилища

На этом шаге необходимо указать тип устанавливаемого сервера.

- Выберите **No, add it to an existing cluster** (Нет, добавить в существующий кластер), если это подчиненный сервер, который нужно добавить в существующий кластер хранилища. Такие серверы будут использоваться для сервисов, связанных с хранением данных, и будут добавлены в инфраструктуру во время установки.
- Выберите **Yes, create a new cluster** (Да, создать новый кластер), если вы только начинаете настройку продукта Acronis Инфраструктура и хотите создать новый кластер хранилища. На этом главном сервере, также называемом сервером управления, будут размещены сервисы управления кластером и панель администратора. Он также будет служить в качестве сервера хранения данных. Только главный сервер является необходимым для установки.
- Выберите **Skip cluster configuration** (Пропустить настройку кластера), если вы хотите позже вручную зарегистрировать развернутый сервер на панели администратора (см. раздел Re-adding unassigned nodes).

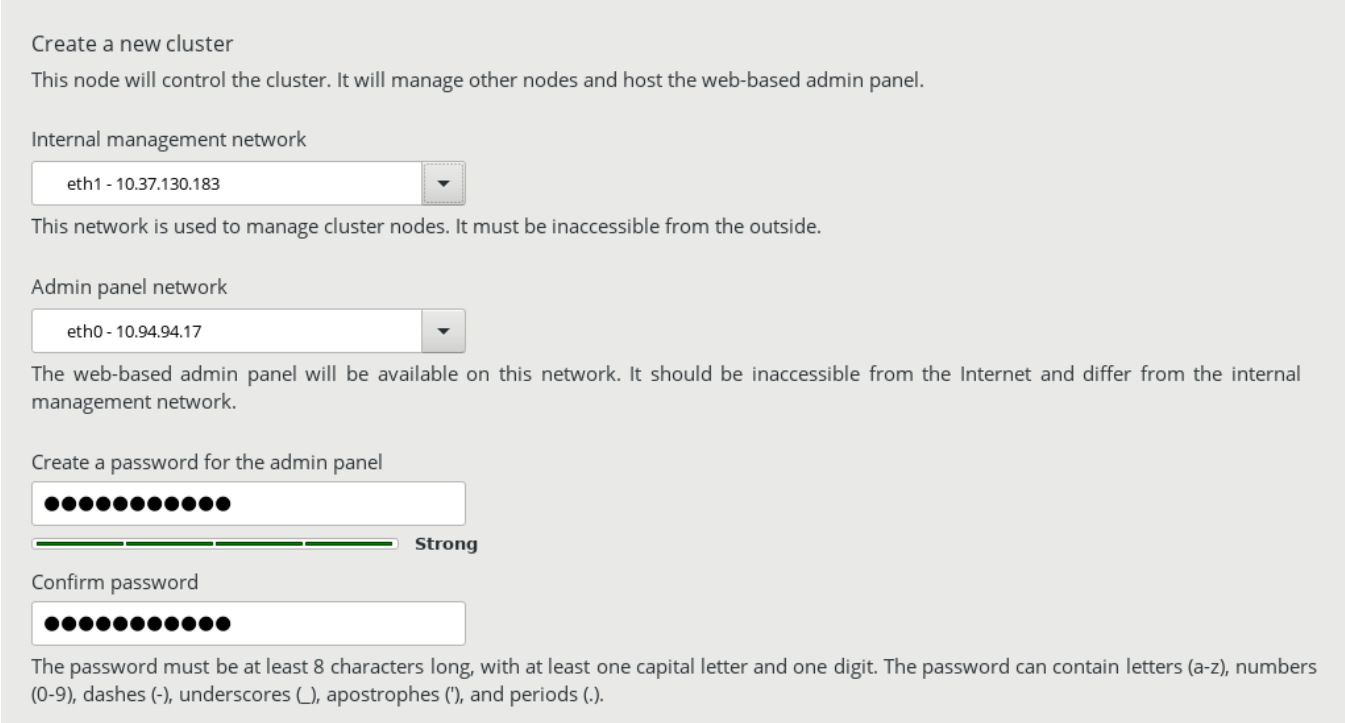


Нажмите **Далее**, чтобы перейти к следующему дополнительному шагу, который зависит от выбранного варианта.

3.7.1 Развертывание главного сервера

Если вы выбрали развернуть главный сервер, сделайте следующее.

1. В раскрывающемся списке **Internal management network** (Сеть управления системными сервисами) выберите сетевой интерфейс для управления системными сервисами и настройки.
2. В раскрывающемся списке **Admin panel network** (Сеть панели администратора) выберите сетевой интерфейс для доступа к панели управления.
3. Создайте и подтвердите пароль для учетной записи суперадминистратора панели управления.
4. Нажмите кнопку **Далее**.



3.7.2 Развертывание подчиненных серверов

Если вы выбрали развернуть подчиненный сервер, потребуется указать IP-адрес сервера управления и маркер, который можно получить только в панели администратора кластера. Один маркер можно использовать для параллельного развертывания нескольких подчиненных серверов.

Чтобы получить маркер и адрес сервера управления, сделайте следующее.

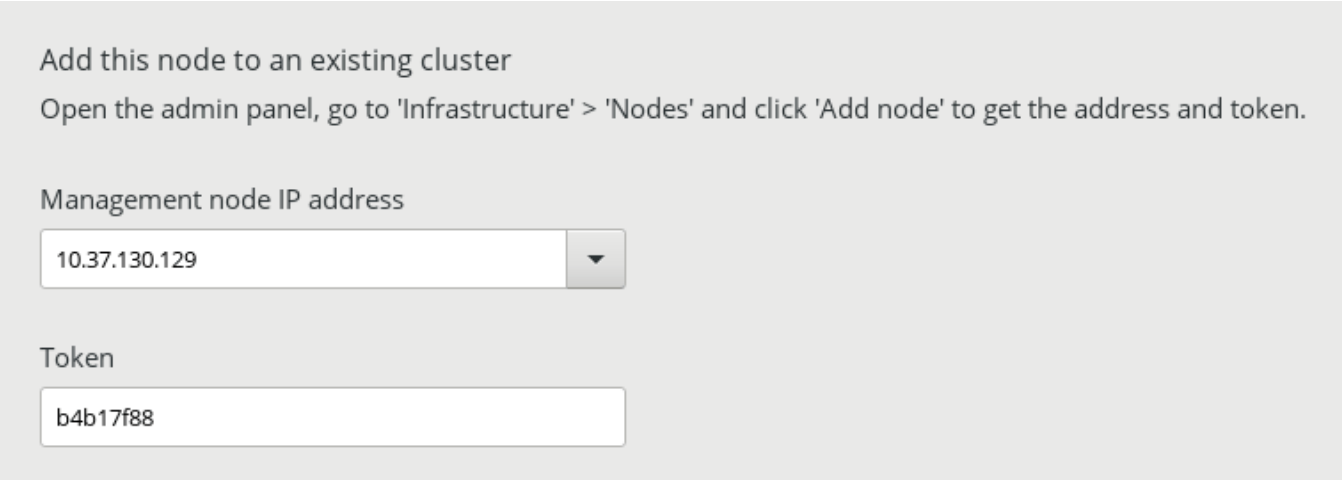
1. Выполните вход на панель администратора через порт 8888. IP-адрес панели отображается в консоли после развертывания главного сервера. Используйте имя пользователя по умолчанию, указанное на экране входа в систему, и пароль привилегированного пользователя главного сервера.

   При появлении запроса добавьте сертификат безопасности в исключения браузера.

2. На панели администратора откройте раздел **Инфраструктура** > **Серверы** и нажмите **Подключить сервер**, чтобы вызвать страницу с адресом сервера управления и маркером.

Примечание: При необходимости можно создать новый маркер, при этом старый маркер станет недействительным.

Вернувшись на страницу установки, введите адрес сервера управления и маркер и нажмите **Далее**.

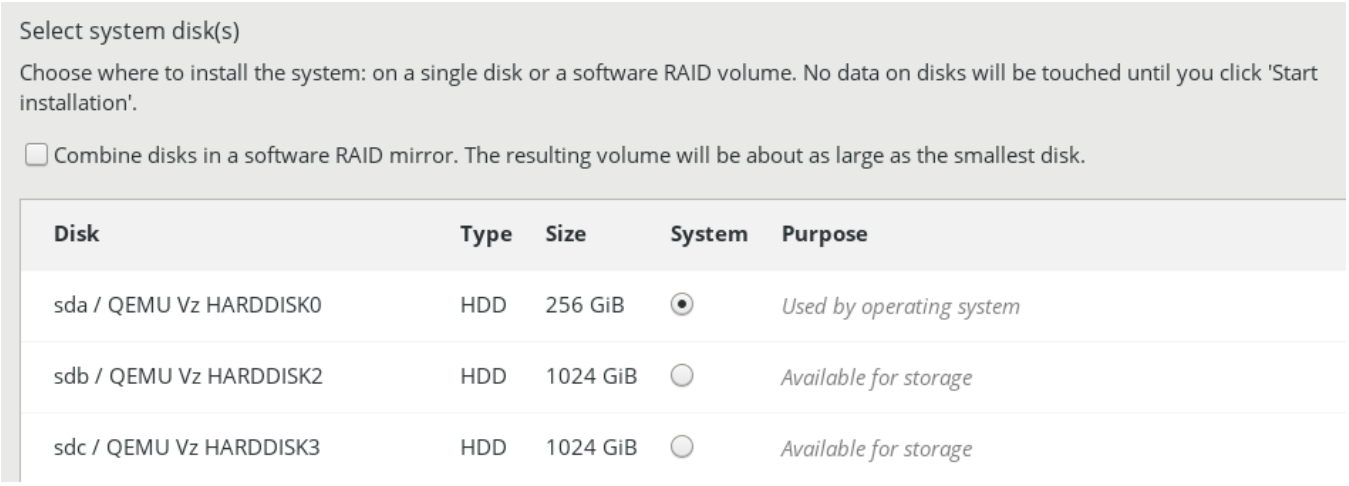


Сервер может появиться на экране **Инфраструктура** > **Серверы** со статусом **Без назначения** сразу после проверки маркера. Однако его можно будет присоединить к кластеру хранилища только после завершения установки.

3.8 Шаг 5. Выбор системного раздела

На этом шаге необходимо выбрать диск для операционной системы. Диску будет назначена дополнительная роль **Система**, хотя его можно будет настроить для хранения данных в панели администратора.

Также можно создать программный массив RAID1 для системного диска, чтобы обеспечить его высокую производительность и доступность. Для этого установите флажок RAID1 и выберите как минимум два диска.



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

Нажмите кнопку **Далее**.

Важно: Вся информация на дисках, распознанных программой установки, будет стерта.

3.9 Шаг 6. Установка пароля привилегированного пользователя

На последнем шаге введите и подтвердите пароль для учетной записи привилегированного пользователя и нажмите **Start installation** (Начать установку).

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

3.10 Завершение установки

После развертывания главного сервера можно приступить к развертыванию нужного количества подчиненных серверов, как описано в разделе *Развертывание подчиненных серверов* (страница 55). Убедитесь, что все серверы отображаются на панели администратора на странице **Инфраструктура** > **Серверы** со статусом **Без назначения**.

Если вы пропустили настройку кластера на шаге 4 и хотите добавить сервер без назначения вручную, см. инструкции в разделе Re-adding unassigned nodes.

Когда все нужные серверы будут отображаться со статусом **Без назначения**, можно приступать к созданию кластера хранилища, как описано в руководстве администратора.

ГЛАВА 4

Установка с помощью PXE

В этой главе описывается установка продукта Acronis Инфраструктура по сети с помощью сервера Preboot eXecution Environment (PXE).

Потребуется сделать следующее.

1. Получить образ дистрибутива, как описано в разделе *Получение образа дистрибутива* (страница 44).
2. Настроить серверы TFTP, DHCP и HTTP (или FTP).
3. Загрузить сервер, на котором будет установлен продукт Acronis Инфраструктура, по сети и запустить программу установки Acronis Инфраструктура.
4. Задать параметры установки вручную или передать их автоматически с помощью файла kickstart и завершить установку.

4.1 Подготовка среды

В этом разделе описывается настройка среды для установки по сети.

4.1.1 Установка компонентов PXE

Для настройки среды PXE потребуются следующие компоненты.

- TFTP-сервер. Это машина, которая позволяет вашим серверам загрузиться и установить продукт Acronis 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 Acronis Инфраструктура по сети.

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

Самым простым способом будет настройка всех серверов на одной физической машине:

```
# 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.

4.1.2 Настройка TFTP-сервера

В этом разделе описывается настройка TFTP-сервера для систем на базе BIOS. Для получения сведений о настройке сервера для установки продукта Acronis Инфраструктура в системах на базе EFI см. Руководство по установке Red Hat Enterprise Linux.

Сделайте следующее.

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 Acronis 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/`.

4.1.3 Настройка DHCP-сервера

Чтобы настроить DHCP-сервер для установки продукта Acronis Инфраструктура по сети, 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.

4.1.4 Настройка HTTP-сервера

После настройки серверов TFTP и DHCP необходимо сделать файлы дистрибутива продукта Acronis Инфраструктура доступными для установки по сети. Для этого сделайте следующее.

1. Настройте HTTP-сервер (или измените конфигурацию существующего).
2. Скопируйте содержимое установочного DVD-продукта Acronis Инфраструктура в произвольный каталог на HTTP-сервере (например, `/var/www/html/distrib`).
3. На PXE-сервере укажите путь к установочным файлам продукта Acronis Инфраструктура 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
   ```

4.2 Установка по сети

После подготовки всех серверов можно установить продукт Acronis Инфраструктура по сети следующим образом.

1. Загрузите сервер продукта Acronis Инфраструктура по сети. Должно отобразиться созданное **меню загрузки**.
2. В меню загрузки выберите **Установить продукт Acronis Инфраструктура**.
3. На главной странице программы установки задайте параметры установки, как описано в разделе *Установка с помощью графического интерфейса* (страница 44), и нажмите **Начать установку**.

Чтобы установить продукт Acronis Инфраструктура в автоматическом режиме, потребуется сделать следующее.

1. Создать файл kickstart, как описано в разделе *Создание файла kickstart* (страница 63).
2. Добавить расположение файла kickstart в меню загрузки, как описано в разделе *Использование файла kickstart* (страница 69).
3. Загрузить сервер по сети и выбрать **Установить продукт Acronis Инфраструктура** в меню загрузки.

   Установка должна начаться автоматически.

4.3 Создание файла kickstart

Если планируется автоматическая установка продукта Acronis Инфраструктура, можно использовать файл kickstart. Он автоматически отправит в программу установки Acronis Инфраструктура параметры, которые выбираются вручную при обычной установке. Acronis 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 и инструкции по использованию созданного файла kickstart.

4.3.1 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 Acronis 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 хэш пароля, полученный с помощью алгоритма, указанного в параметре `--passalgo`. Например, чтобы создать из пароля хэш SHA-512, выполните команду `python -c 'import crypt; print(crypt.crypt("  _  "))'`.

`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!

4.3.2 Сценарии kickstart

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

4.3.2.1 Установка пакетов

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

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

4.3.2.2 Установка компонентов панели администратора и хранилища

Требуется только одна панель управления, которую следует установить только на первом сервере. Для развертывания всех остальных серверов необходимо будет получить маркер из работающей панели администратора. Дополнительные сведения см. в разделе *Развертывание подчиненных серверов* (страница 55).

Чтобы установить на сервере компоненты панели администратора и хранилища, не раскрывая пароля суперадминистратора и маркера хранилища в файле kickstart, выполните следующие действия.

1. Добавьте сценарий `%addon com_vstorage` в файл kickstart:

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

2. После завершения установки выполните на сервере следующую команду, чтобы настроить компонент панели администратора:

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

   где:

   - `<superadmin_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 внешней сети (который вы бы выбрали для сети панели администратора при ручной установке).

3. Запустите сервис панели администратора:

```
# systemctl start vstorage-ui-backend
```

4. Если вы также установили на сервере компонент хранилища, выполните следующую команду:

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

Чтобы установить компоненты без последующего запуска сценариев с риском раскрытия пароля и маркера, укажите интерфейсы для публичной (внешней) и частной (внутренней) сетей и пароль учетной записи суперадминистратора панели управления в файле kickstart. Например:

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

4.3.2.3 Установка только компонента хранилища

Компонент хранилища без панели администратора устанавливается по умолчанию и не требует сценариев в файле kickstart, за исключением случаев, когда вы хотите указать маркер.

Если вы не хотите раскрывать маркер в файле kickstart, после установки выполните на сервере следующую команду, чтобы зарегистрировать сервер в панели администратора:

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

где:

- `<token>` — маркер, который можно получить в панели администратора.
- `<MN_IP_address>` — IP-адрес интерфейса частной сети на сервере с панелью администратора.

Чтобы установить компонент хранилища без последующего запуска сценариев с риском раскрытия маркера, укажите маркер и IP-адрес сервера с панелью администратора в файле kickstart. Например:

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

4.3.3 Пример файла kickstart

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

Важно: 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 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
# Disable SELinux.
selinux --disabled
```

```
# Enable time synchronization via NTP.
services --enabled="chronyd"
# Set the system time zone.
timezone America/New_York

# 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
```

4.3.3.1 Создание системного раздела на программном массиве RAID1

Чтобы создать системный раздел на томе программного массива RAID1, вместо использования параметра `autopart` потребуется сделать следующее.

1. Разбить диски на разделы.
2. Создать том RAID1.
3. Создать том подкачки и корневой том LVM.

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

Следующий пример для сервера на базе BIOS разбивает на разделы диски `sda` и `sdb`, собирает программный массив RAID1 и создает расширяемый том подкачки и корневой том 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
```

4.4 Использование файла kickstart

Чтобы установить продукт Acronis Инфраструктура с помощью файла kickstart, сначала необходимо сделать этот файл доступным по сети. Для этого выполните следующие действия.

1. Скопируйте файл kickstart в тот же каталог на HTTP-сервере, где расположены установочные файлы продукта Acronis Инфраструктура (например, в `/var/www/html/astor`).
2. 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/astor/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/astor \
   inst.ks=http://198.123.123.198/astor/ks.cfg
   ```

ГЛАВА 5

Дополнительные режимы установки

В этой главе описываются дополнительные режимы установки, которые могут понадобиться в зависимости от ваших потребностей.

5.1 Установка через VNC

Чтобы установить продукт Acronis Инфраструктура через VNC, загрузите экран приветствия и выполните следующие действия.

1. Выберите основной вариант установки и нажмите клавишу **E** для внесения изменений.
2. 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
   ```
3. Нажмите **Ctrl+X**, чтобы начать загрузку с выбранным вариантом установки.
4. При появлении запроса, предлагающего запустить VNC или продолжить в текстовом режиме, нажмите клавишу **1**.
5. Введите пароль VNC по запросу.
6. В выходных данных найдите имя хоста или IP-адрес и порт VNC для подключения, например `192.168.0.10:1`.
7. Подключитесь к этому адресу в клиенте VNC. Откроется обычная страница **Installation Summary** (Сводка установки).

Сам процесс не отличается от установки в стандартном графическом режиме (см. раздел *Установка с помощью графического интерфейса* (страница 44)).

ГЛАВА 6

Поиск и устранение неисправностей установки

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

6.1 Установка в базовом графическом режиме

Если программе установки не удается загрузить нужный драйвер для графического адаптера, можно попробовать установить продукт Acronis Инфраструктура в базовом графическом режиме. Чтобы включить этот режим, на экране приветствия выберите **Troubleshooting** (Поиск и устранение неисправностей) –> **Install in basic graphics mode** (Установить 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 (см. раздел *Установка с помощью графического интерфейса* (страница 44)).

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 Acronis Инфраструктура подключается в каталог `/mnt/sysimage`. Можно перейти в этот каталог и внести необходимые изменения в систему.

Для входа в режим аварийного восстановления сделайте следующее.

1. Загрузите систему из образа дистрибутива продукта Acronis Инфраструктура.
2. На экране приветствия нажмите **Troubleshooting** (Поиск и устранение неисправностей) –> **Rescue system** (Восстановить систему).
3. После того, как Acronis 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 Acronis Инфраструктура в режиме чтения и записи в каталог `/mnt/sysimage`.
   - Подключение только для чтения (нажмите **2**): подключение установленного продукта Acronis 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, когда 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 Acronis 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.