FLANT
Deckhouse
Kubernetes Platform

Веб-интерфейс Deckhouse и Deckhouse Commander

Кластеры на расстоянии клика

Август 2023

+7 (495) 721-10-27

contact@deckhouse.ru deckhouse.ru

ФЛАНТ

Оглавление

Новое лицо Deckhouse

Мы рады сообщить, что работаем над веб-интерфейсами для Deckhouse Kubernetes Platform. Сейчас мы реализуем два проекта: веб-интерфейс Deckhouse и менеджер кластеров Deckhouse Commander.

Deckhouse — это инструмент управления отдельным кластером. Веб-интерфейс — это новый способ взаимодействия с Deckhouse. Веб-интерфейс будет доступен в поставке Deckhouse Enterprise Edition начиная с версии 1.51 (в начале сентября 2023 года).

Deckhouse Commander — это инструмент централизованного управления парком кластеров. Мы планируем выпустить стабильную версию этого нового инструмента в последнем квартале 2023 года в виде модуля Deckhouse для Enterprise-клиентов.

Как мы пришли к решению создать эти проекты? Благодаря обратной связи от наших клиентов мы поняли, что подход *Infrastructure as Code*, который мы исповедуем во «Фланте», удобен не для всех. Более того, у многих клиентов существуют сложившиеся привычки и ожидания от системы, которую они выбирают в качестве фундамента для IT-инфраструктуры. В числе этих ожиданий — низкий порог входа в управление системой и понятный, информативный способ наблюдать за ее состоянием.

Deckhouse — это платформа с большим набором функций, а также удобным и хорошо документированным API. Однако, чтобы управлять платформой, нужно обладать технической квалификацией и инвестировать время в изучение возможностей Deckhouse. Качественный и удобный веб-интерфейс помогает бо̀льшему количеству пользователей получать нужный бизнесу результат с Deckhouse без технических навыков работы с командной строкой и YAML-конфигурацией. Веб-интерфейс Deckhouse сочетает в себе ряд преимуществ: более информативное представление информации и очевидную структуру возможностей платформы, которые, к тому же, документированы по месту их применения. Поэтому мы ожидаем, что управление Deckhouse станет более простым и менее трудоемким для широкого круга пользователей.

Deckhouse Commander помогает управлять инфраструктурой в едином интерфейсе. С помощью шаблонизации кластеров Commander обеспечивает как унификацию, так и разделение кластеров для различных окружений и сценариев использования. Ведение каталога ресурсов и история изменений всех сущностей в Commander сделают управление инфраструктурой прозрачным. Deckhouse Commander сделает масштабирование инфраструктуры и ее централизованный контроль задачей, которая требует минимального порога входа с точки зрения необходимых навыков.

Мы поставили цель сделать управление платформой более простым и информативным, а ее статус — очевидным. «Флант» работает в постоянном диалоге с нашими конечными пользователями, чтобы реализовать не только наше видение, но и помочь пользователям достичь важных для бизнеса результатов.

Команда веб-интерфейсов Deckhouse, Флант *Август 2023 г.*

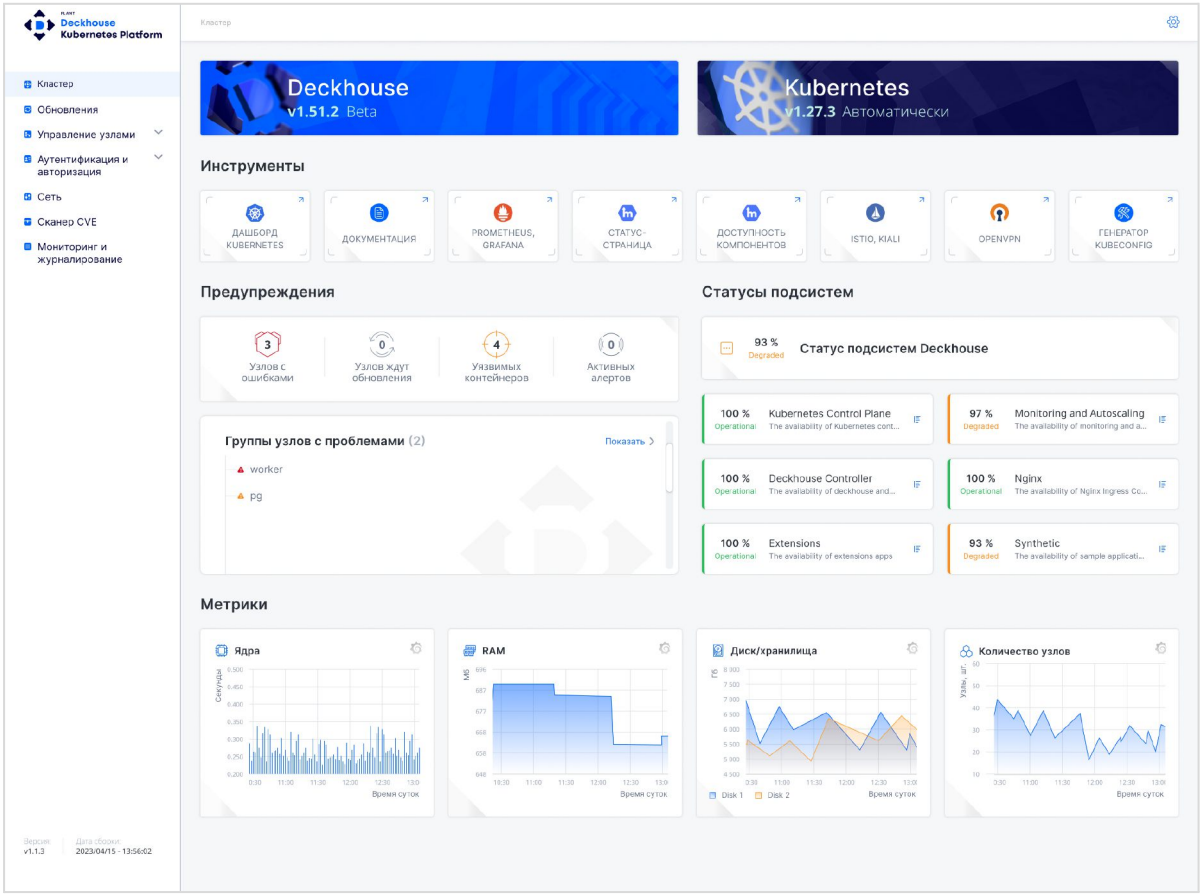
Deckhouse в браузере для типовых задач администратора

Обзор кластера (стартовый экран)

Экран находится в разработке, ожидаемая дата релиза — сентябрь 2023 г.

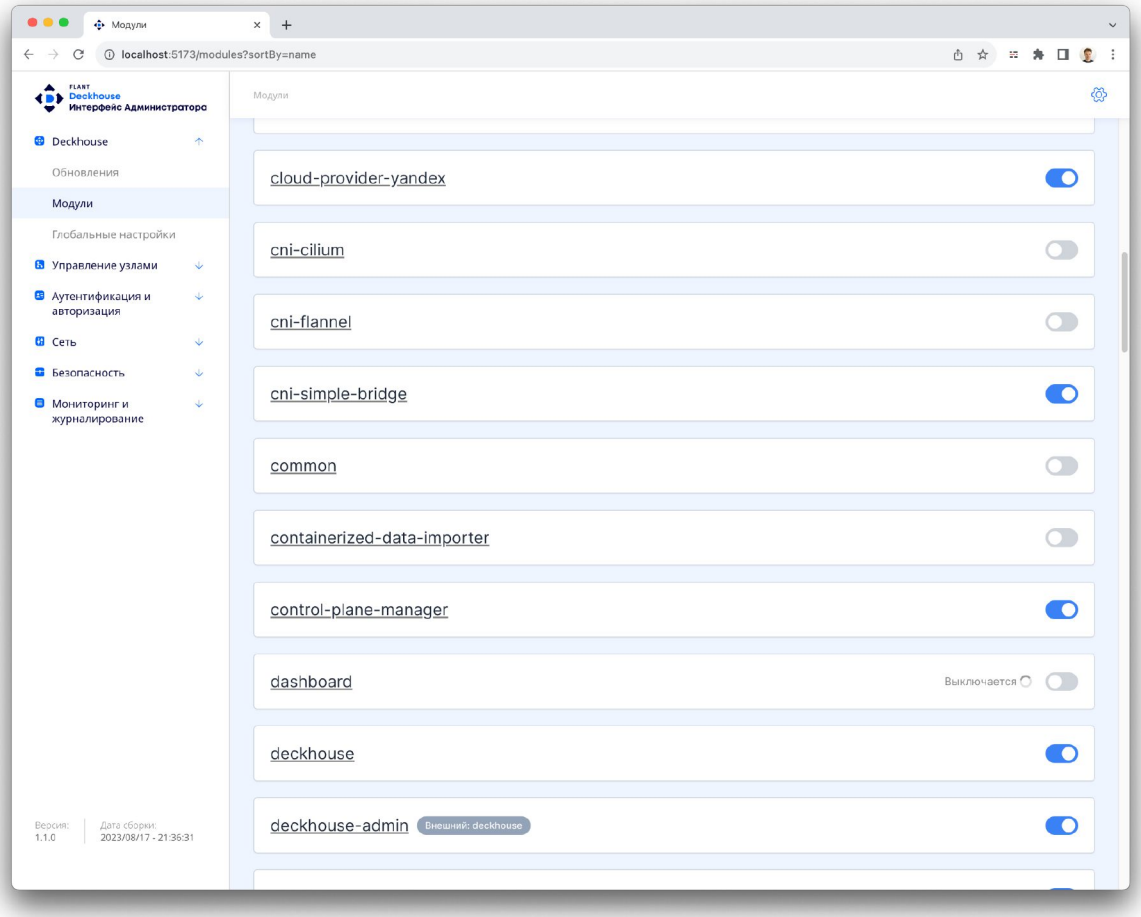
Стартовый экран состоит из нескольких логических блоков:

- **Общая информация о кластере.** Текущая версия Deckhouse и Kubernetes, наличие обновлений.
- **Инструменты.** Это набор ссылок на веб-интерфейсы всех доступных в кластере инструментов (например, Grafana или Istio).
- **Предупреждения.** Информация об ошибках и доступных обновлениях узлов, уязвимостях в контейнерах и алертах.
- **Статусы подсистем.** Информация о доступности подсистем Deckhouse (например, Prometheus, Cluster-Autoscaler, Nginx).
- **Метрики.** Графики с краткой справкой об основных ресурсах кластера и их изменениях за последние 3 часа: количество ядер, общий объем памяти, общий объем выделенных дисков, общее количество узлов кластера.

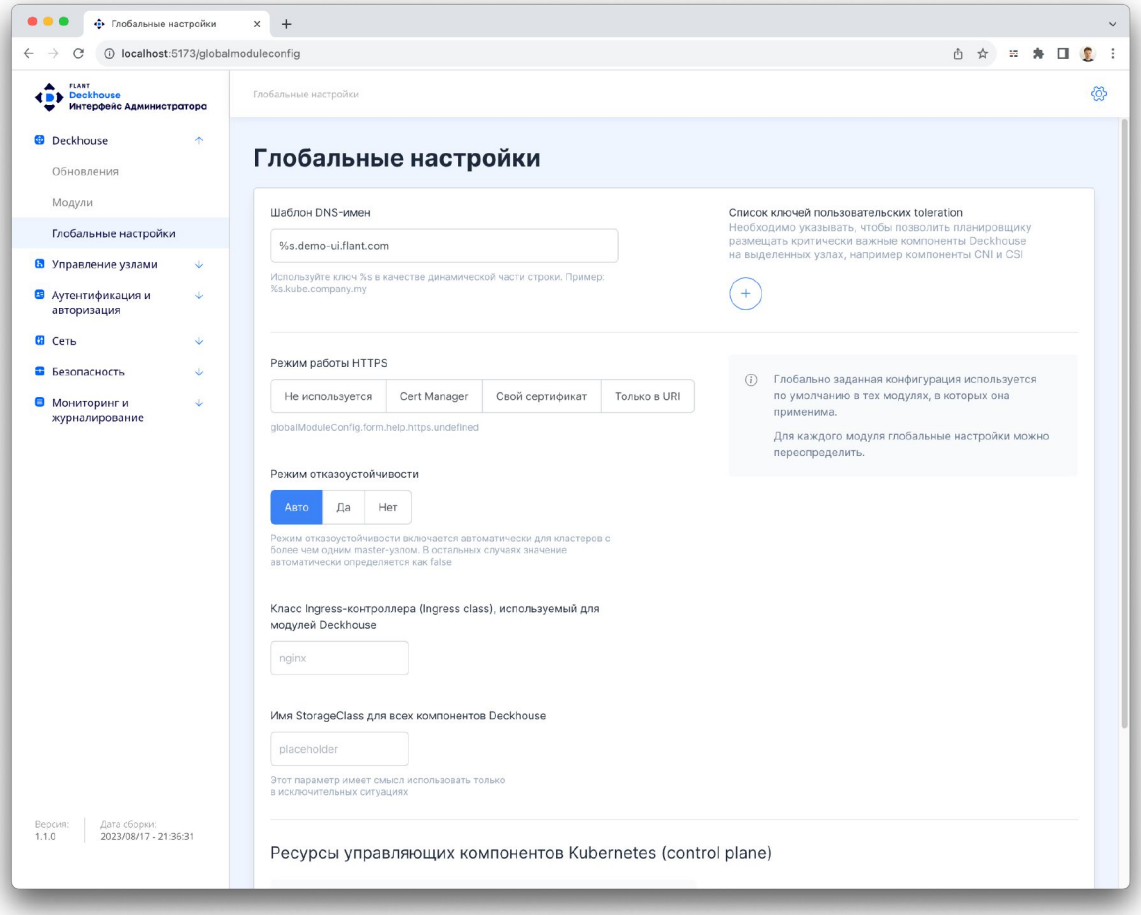


Модули Deckhouse и глобальные настройки

Функциональность Deckhouse обеспечивается модулями, которые можно включать и выключать и для которых можно переопределить настройки по умолчанию.



Для модулей Deckhouse предусмотрены глобальные настройки. Для глобальных настроек мы предусмотрели отдельный подраздел. По умолчанию эти настройки наследуются всеми модулями, в которых они могут быть применены. При этом для модулей в индивидуальном порядке эти настройки можно переопределить: например, выпуск TLS-сертификата и режим отказоустойчивости.

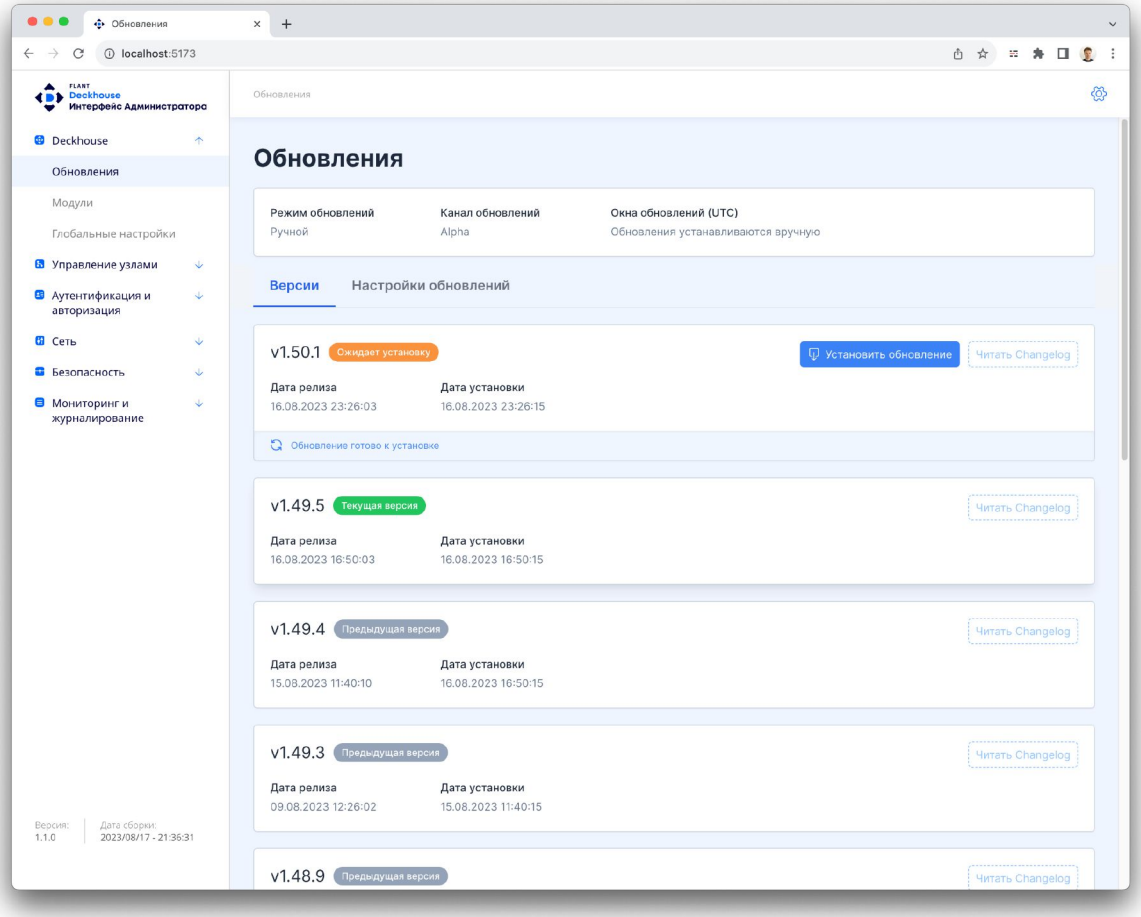


Обновления Deckhouse

Новые релизы Deckhouse выпускаются раз в две недели. Но когда именно обновлять Deckhouse, вы определяете самостоятельно.

Подраздел «Обновления» находится в разделе Deckhouse. На экране обновлений есть две вкладки: «Версии» и «Настройки обновлений».

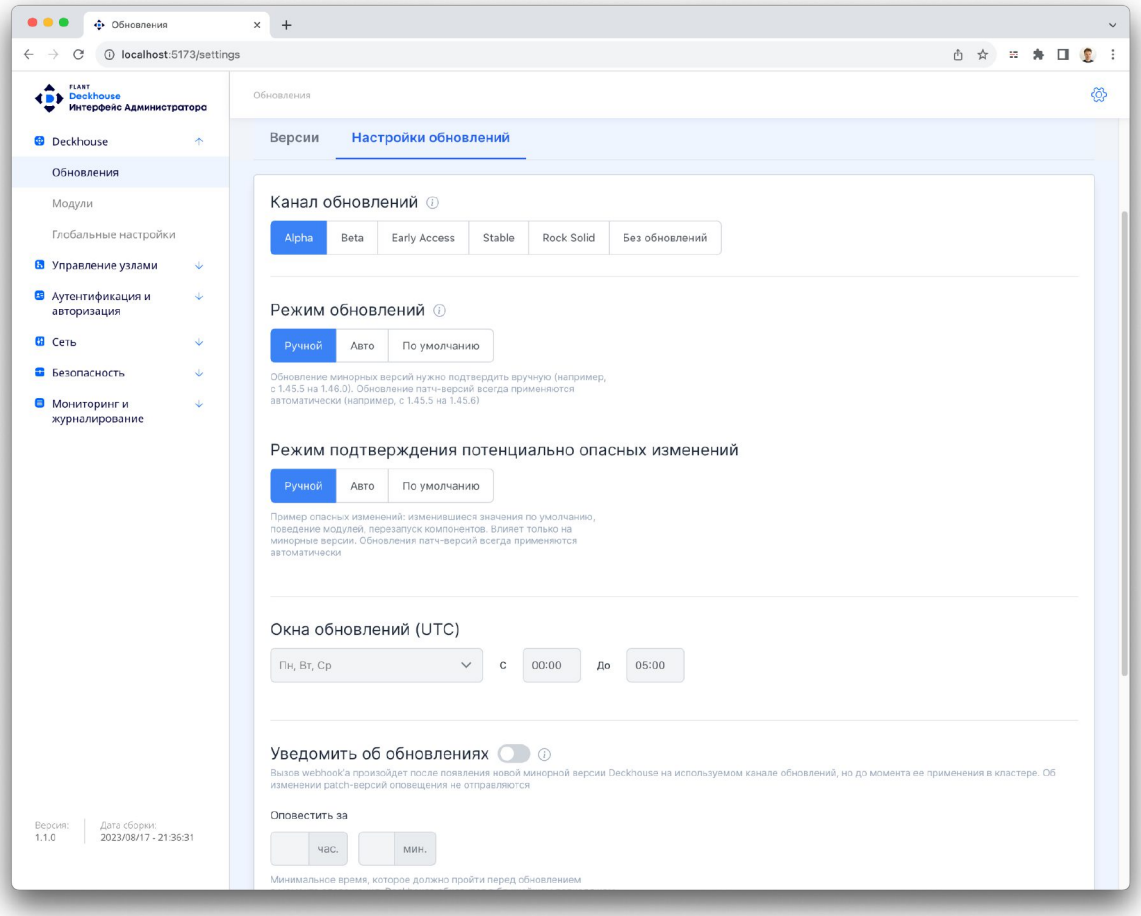
- В «Версиях» можно просмотреть новые, текущие и предыдущие версии Deckhouse.
- В «Настройках обновлений» можно задать дополнительные параметры.



Рассмотрим, как устроена вкладка «Настройки обновлений»:

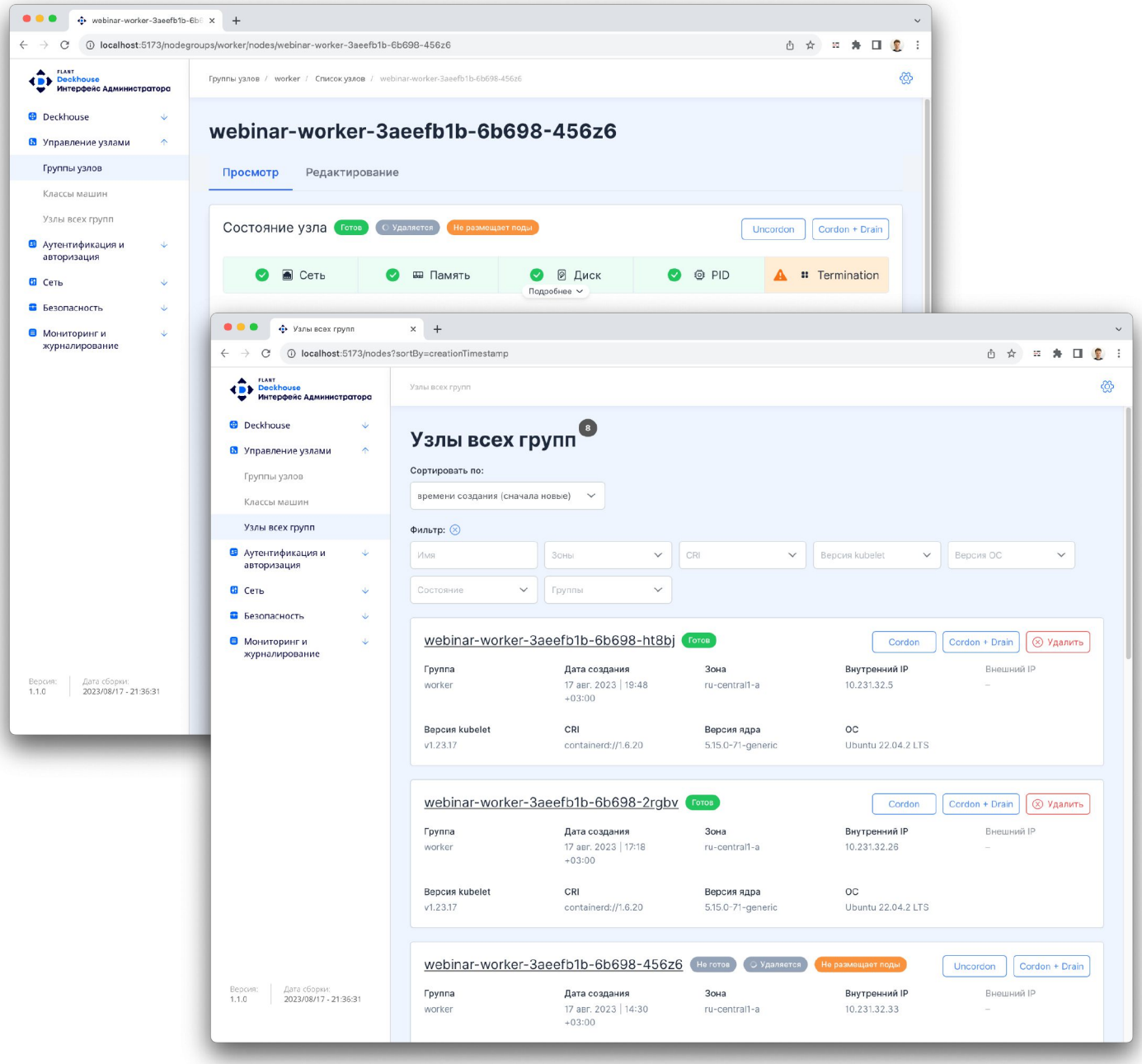
- **Канал обновлений.** Можно выбрать самые свежие фичи или самую стабильную версию. Подробнее о каналах обновлений можно узнать на нашем сайте. Если выбрать режим «Без обновлений», остальные настройки обновлений будут неактивны.
- **Режим обновлений.** В ручном режиме обновление запускает пользователь кликом по соответствующей кнопке. В автоматическом режиме Deckhouse сам запускает обновления. Ограничить время, в которое устанавливаются и применяются обновления, можно с помощью дополнительных настроек.

- **Режим подтверждения потенциально опасных изменений.** Если в релизе Deckhouse меняются настройки по умолчанию или поведение модулей, то в ручном режиме необходимо будет подтвердить обновление на новую версию нажатием на соответствующую кнопку на этой версии.
- **Окна обновлений.** Опция для автоматического режима обновлений. С ее помощью задаются интервалы времени, в которых разрешено устанавливать обновление Deckhouse. Например, вы можете выбрать для обновлений нерабочие часы с 20:00 до 5:00.
- **Уведомить об обновлениях.** Опция для автоматического режима обновлений. Позволяет задать интервал между уведомлением об обновлении и автоматическим запуском обновления. То есть обновление запустится автоматически, но не раньше, чем пройдет выбранная вами задержка между уведомлением и началом установки.

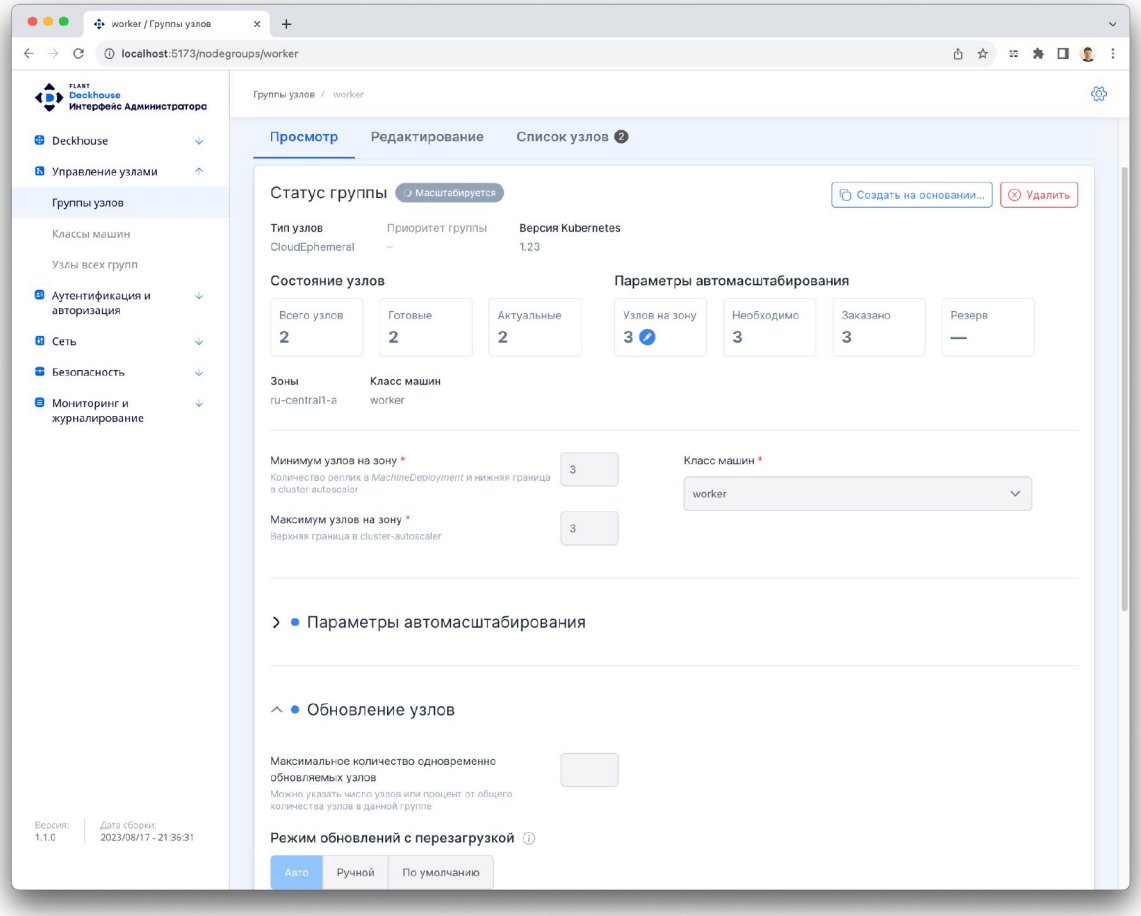


Управление узлами

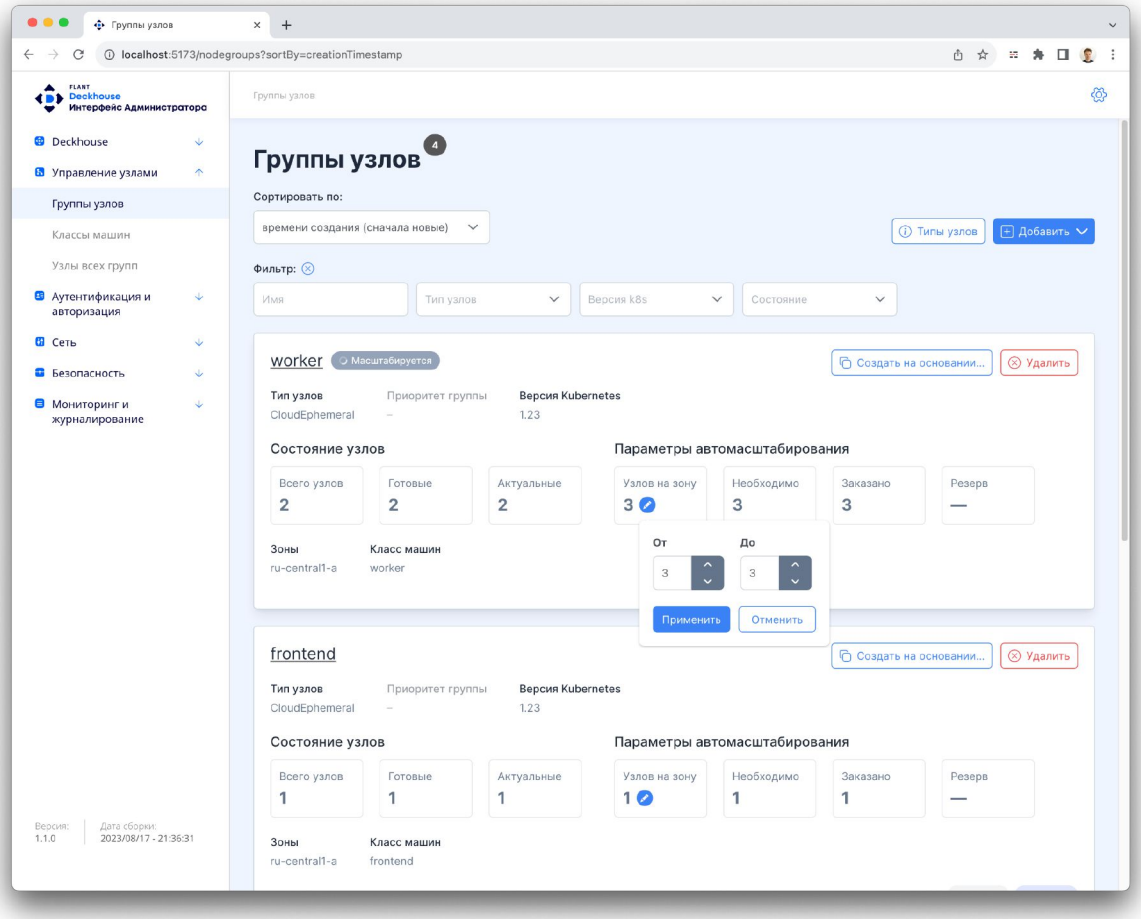
Основной ресурс кластера — это его узлы. Поэтому управление узлами является одним из важнейших разделов управления кластером. В интерфейсе предусмотрено множество механизмов работы с узлами. Пользователь может фильтровать их по имени, зонам доступности, конфигурации и состоянию. Также доступно редактирование лейблов, аннотаций и тейнтов, управление размещением подов (Cordon, Drain), а для облачных узлов — еще и удаление.



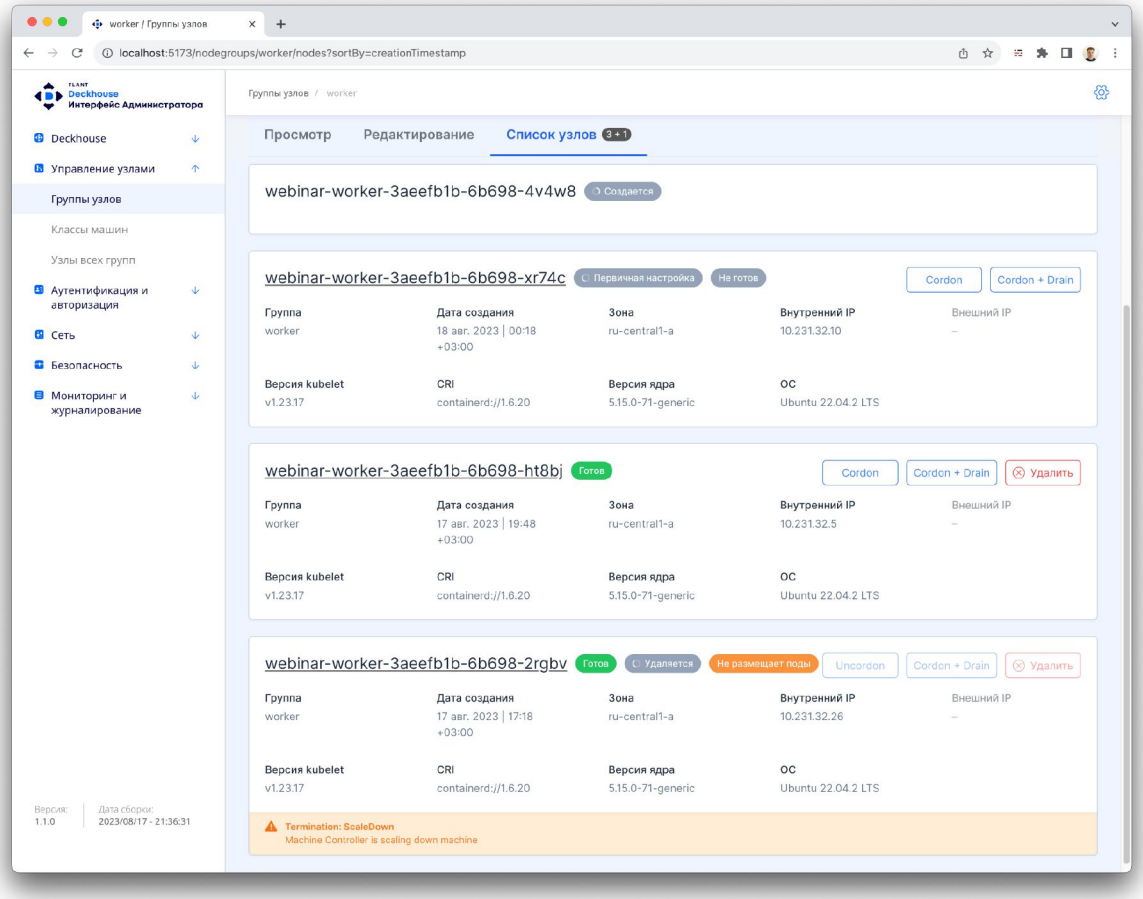
Deckhouse управляет узлами с помощью собственной наработки — *групп узлов* (Node Group). Группа узлов — это главный способ управление ресурсами кластера. Группа определяет конфигурацию узлов, их автоматического масштабирования и обновлений компонентов, а также системные параметры узлов.



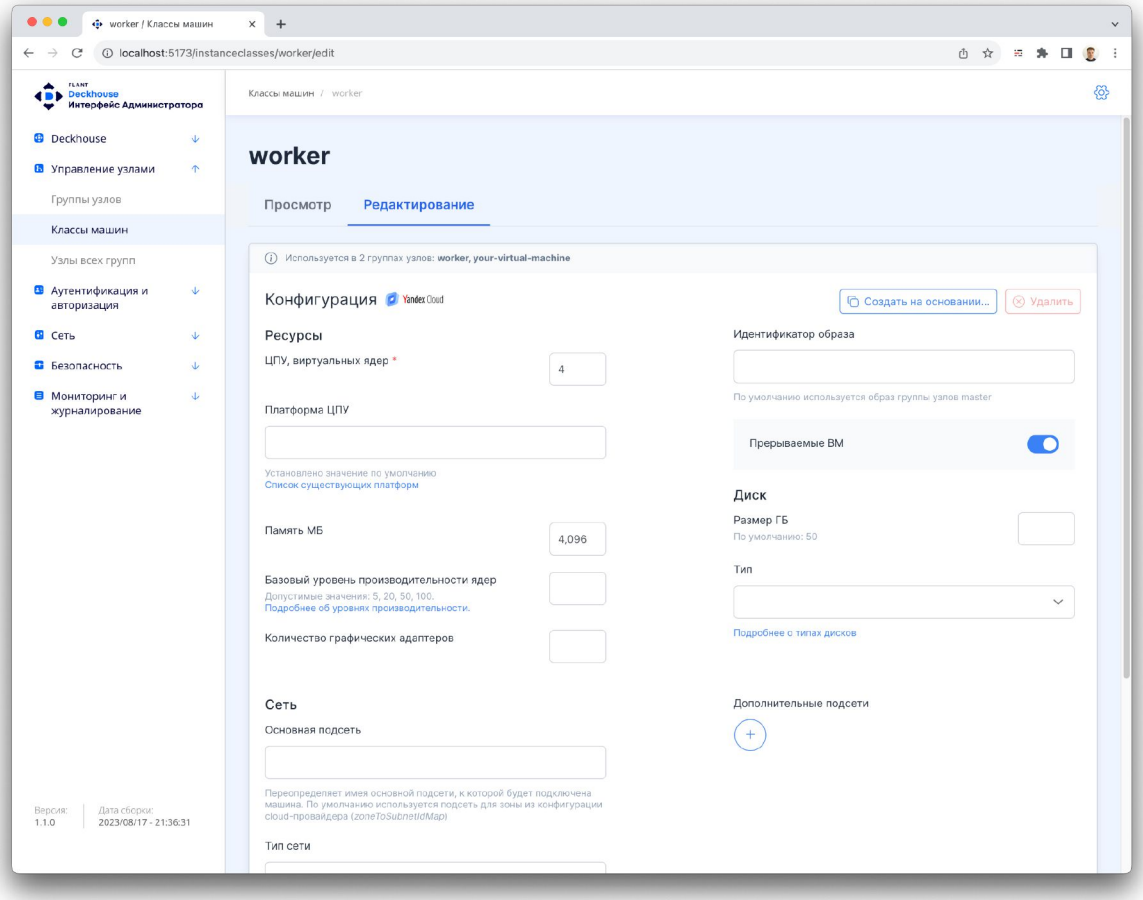
Например, для автоматического масштабирования в группе задается минимальное и максимальное количество узлов на зону доступности. В зависимости от нагрузки Deckhouse автоматически закажет новые узлы или удалит избыточные. Когда целевое количество узлов меняется, в статусе группы отображается, что происходит масштабирование.



Заказанные виртуальные машины становятся видны еще до того, как они станут узлами кластера. Вначале виртуальная машина создается в API облачного провайдера и загружает операционную систему (ОС). После загрузки ОС на машине запускается система конфигурации узлов — *bashible* — происходит первичная настройка узла. Во время этой настройки создаются необходимые конфигурационные файлы и запускаются системные компоненты, которые в конце первичной настройки регистрируют машину как узел кластера.



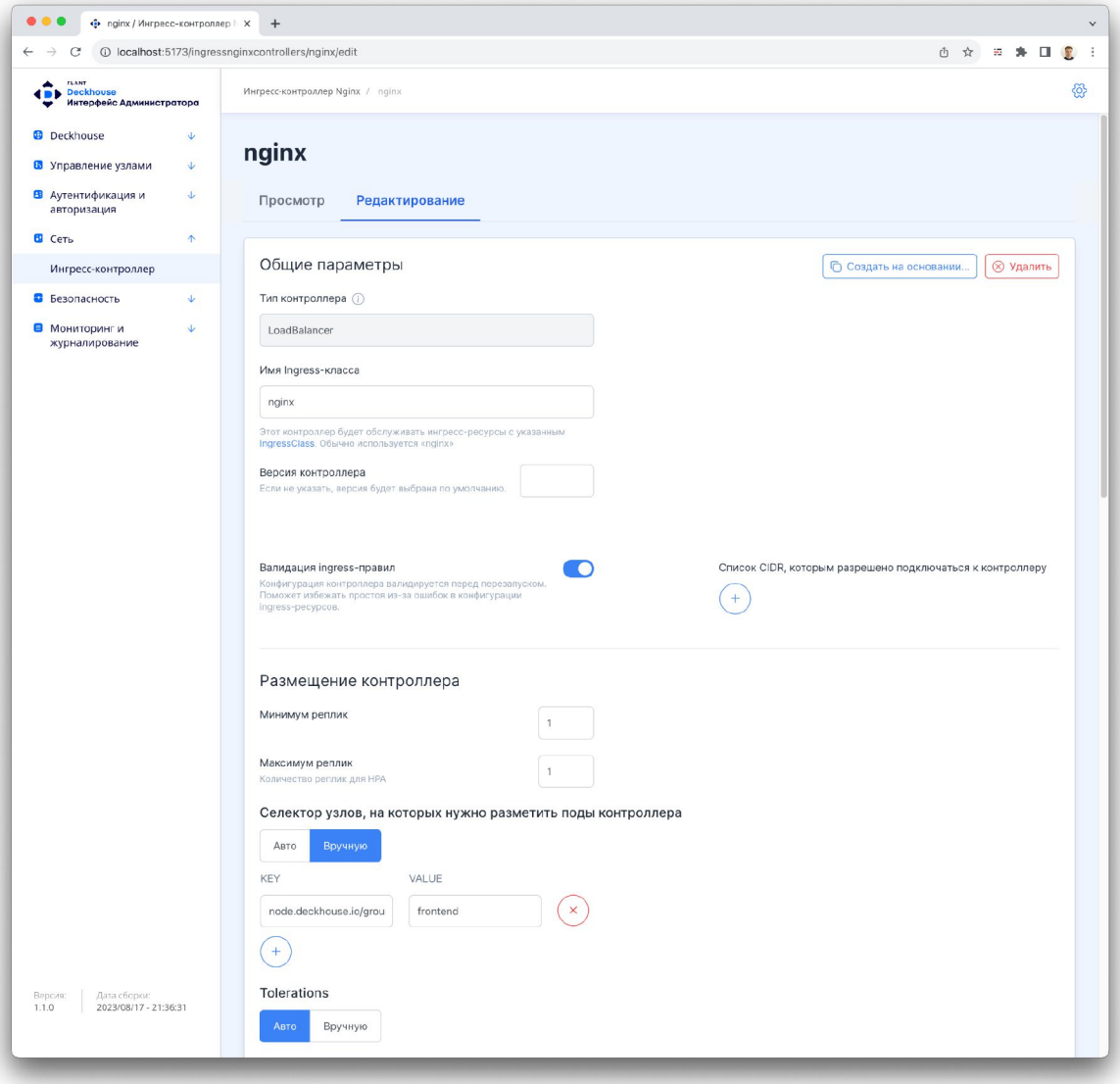
В облачном кластере группа узлов включает в себя облачную конфигурацию машин. В Deckhouse эта конфигурация задается в *классах машин*. Параметры в классах машин специфичны для каждого облачного провайдера. Например, в Yandex Cloud и VMWare ресурсы задаются в ядрах процессора и объеме памяти, а в OpenStack, AWS, GCP и Azure ресурсы определяются заранее известными типами машин.



Входящий трафик

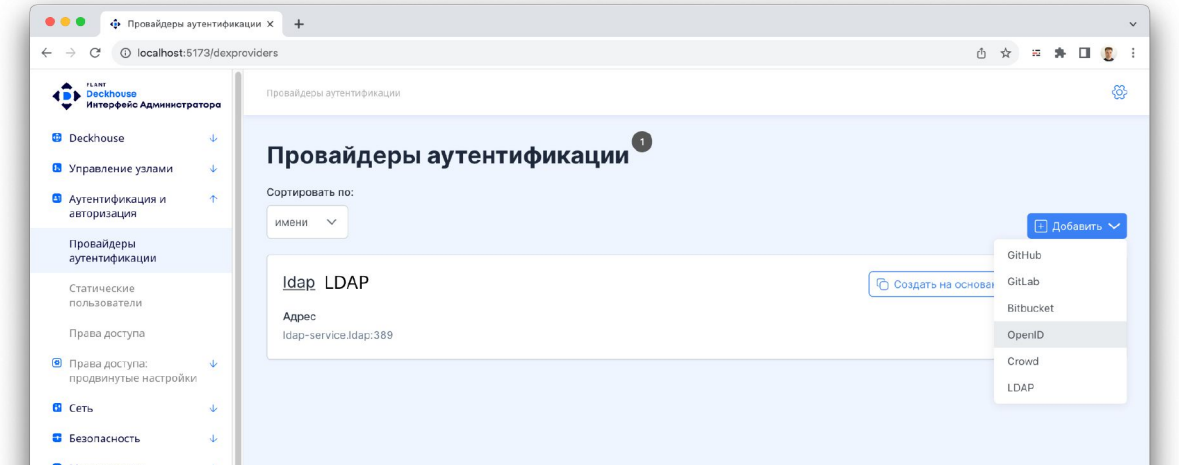
Для маршрутизации входящего трафика в Deckhouse используется Ingress-контроллер на базе Nginx. Ingress-контроллер может быть сконфигурирован для разных вариантов заведения трафика — в терминах Deckhouse они называются *inlet'ами*. Поддерживаются варианты *inlet'ов* с использованием внешнего балансировщика или портов фронтенд-узлов.

В конфигурации Ingress-контроллера доступны настройки доступа, размещения, масштабирования, GeoIP2, HSTS и многое другое.

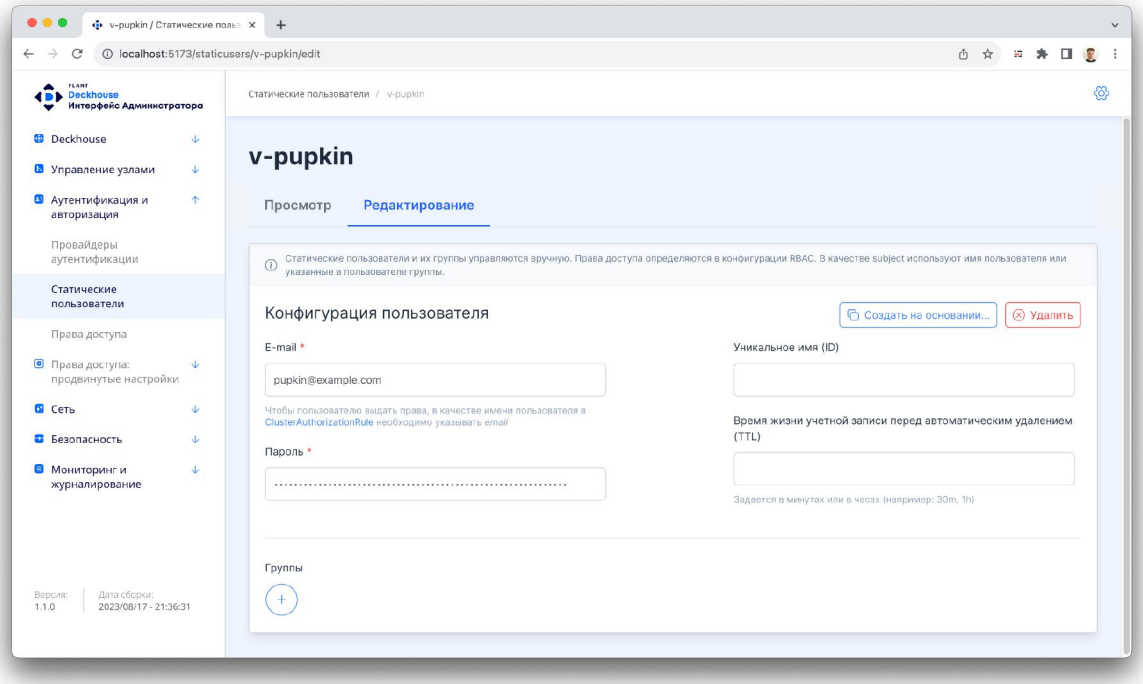


Управление доступом в кластер

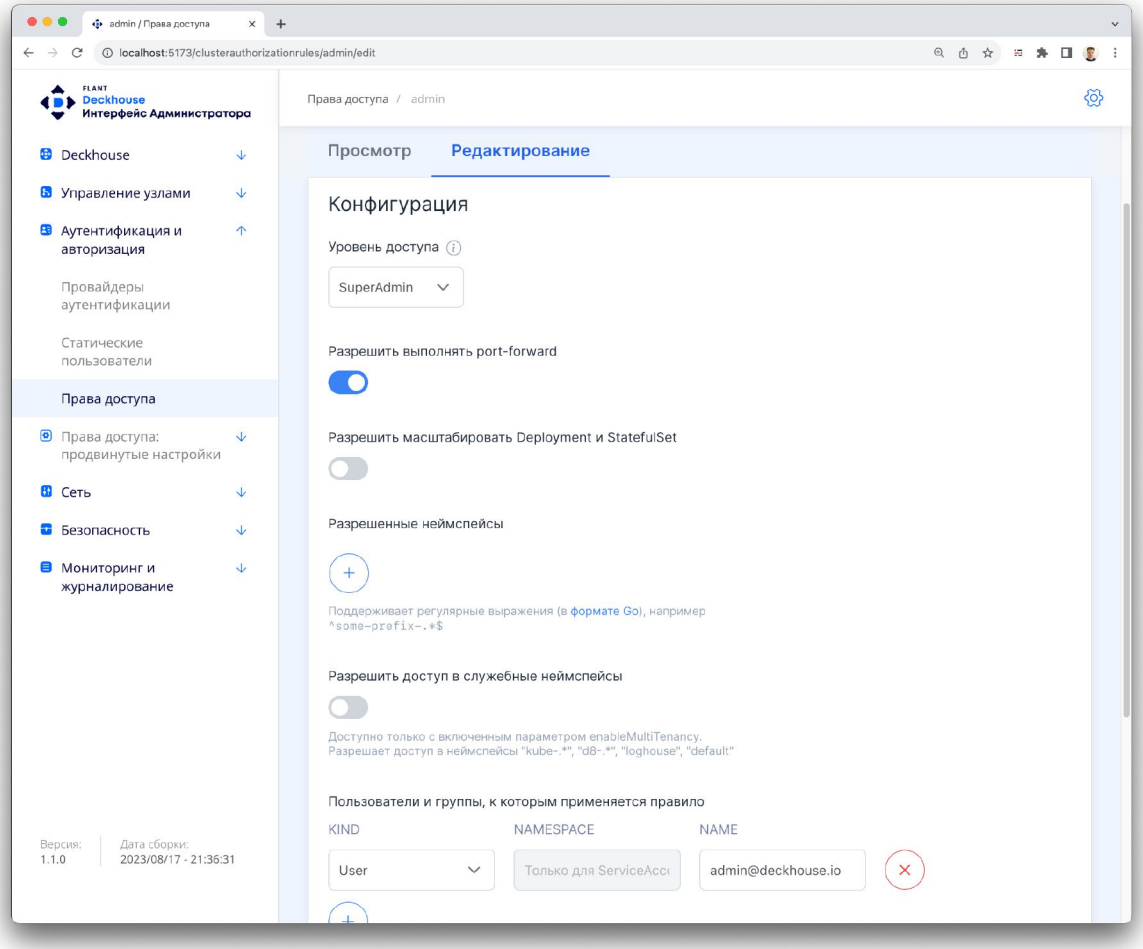
За аутентификацию пользователей в кластере может отвечать внешний провайдер. Deckhouse поддерживает шесть типов подключения к провайдерам: Github, Gitlab, Atlassian Bitbucket, Atlassian Crowd, LDAP и OpenID Connect (OIDC).



В случае, когда провайдера аутентификации нет, доступ выдают с помощью статического пользователя. Для него указываются email, пароль, а также время существования, если его необходимо ограничить.

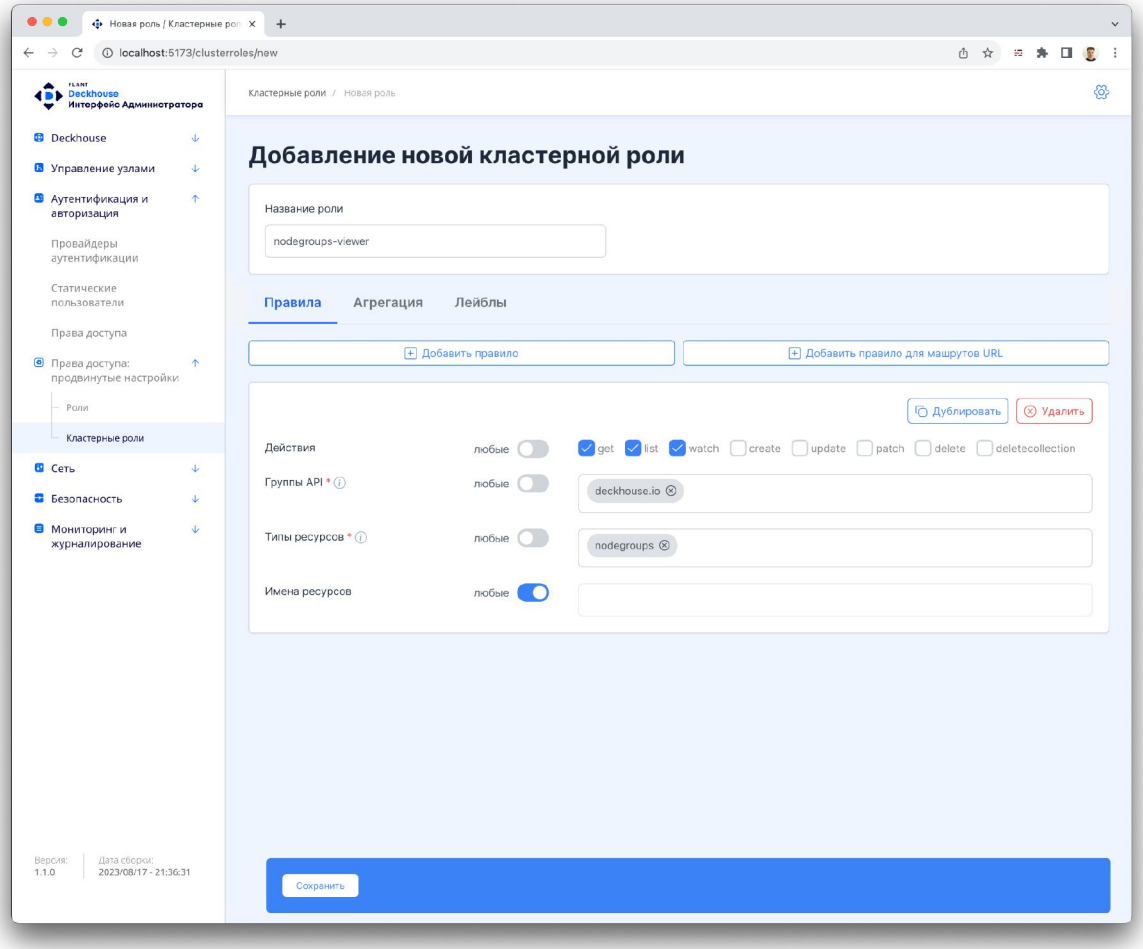


В Deckhouse есть высокоуровневый механизм управления правами доступа. В нем предусмотрено семь уровней привилегий: от доступа на чтение объектов в кластере до суперадмина. Эти уровни привилегий можно назначить отдельным пользователям, группам пользователей и сервис-аккаунтам.



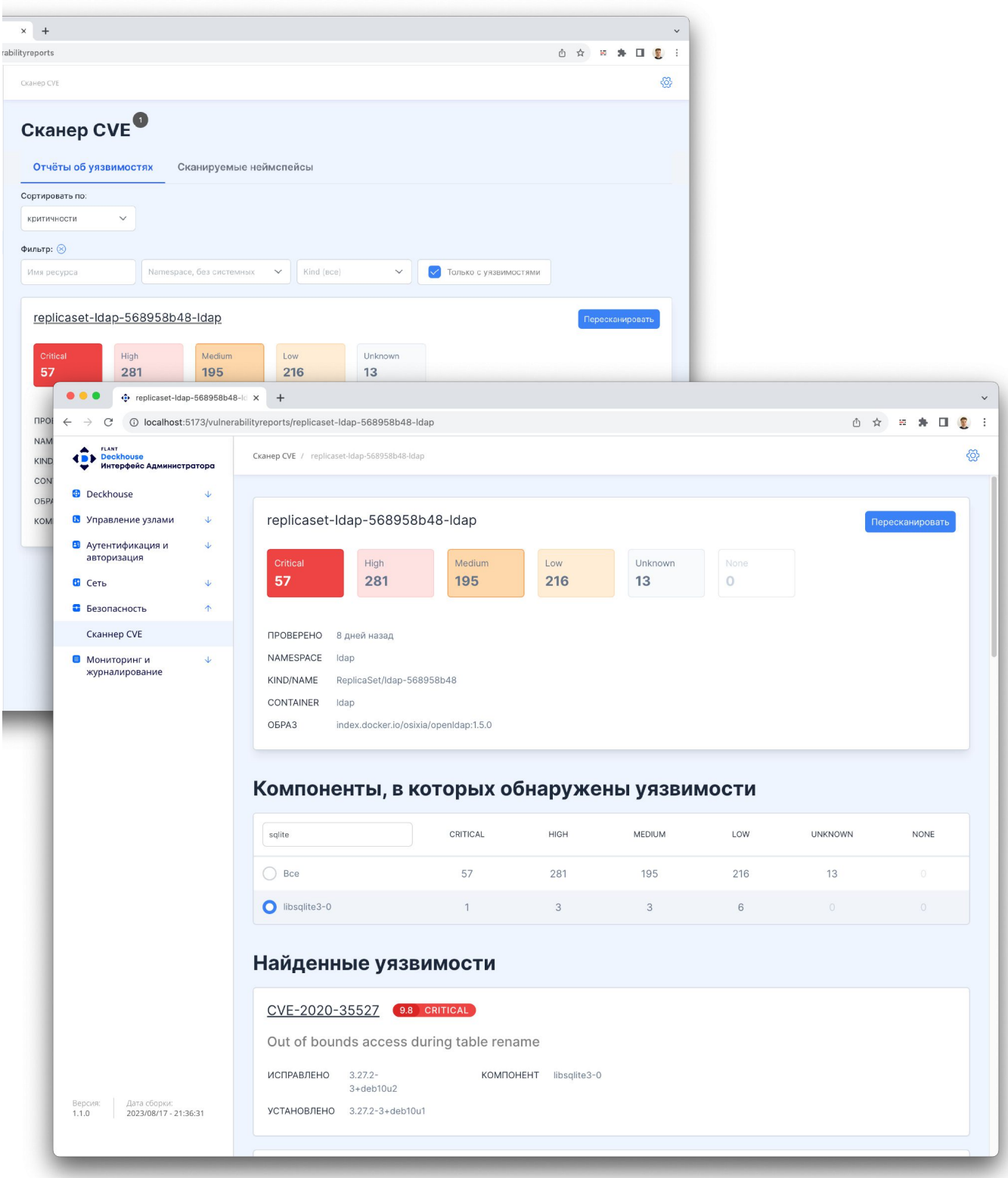
Также предусмотрены продвинутые настройки доступа, которые позволяют управлять объектами Kubernetes RBAC: ролями, кластерными ролями, привязками и кластерными привязками ролей.

Подраздел продвинутых настроек доступа находится в разработке, мы планируем завершить его в сентябре 2023 г.



Безопасность

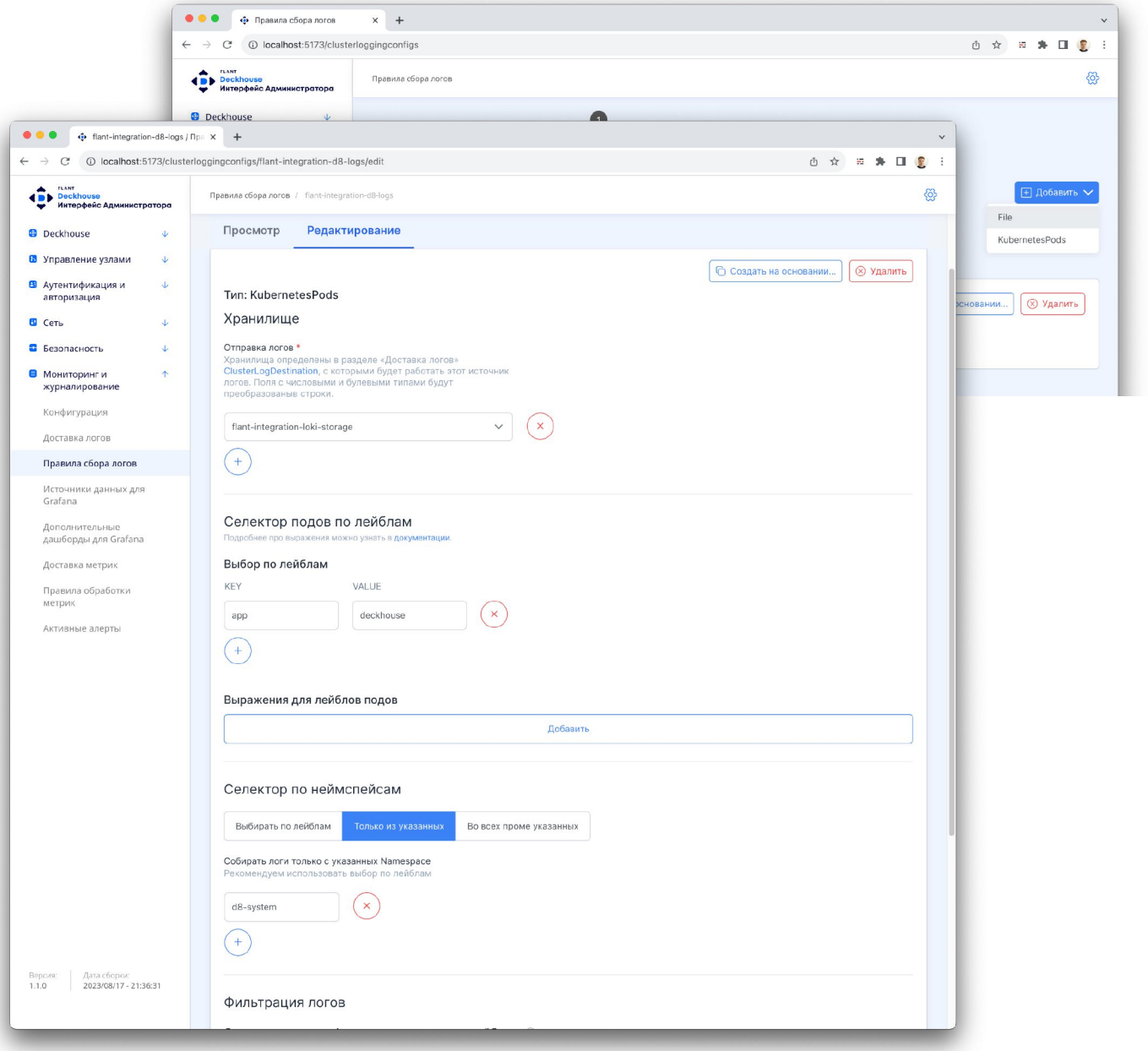
Deckhouse поможет обнаружить уязвимости в контейнерах. По найденным уязвимостям формируются отчеты — отдельно по каждому контейнеру. Отчет содержит список уязвимостей конкретного контейнера с фильтрацией по компонентам.



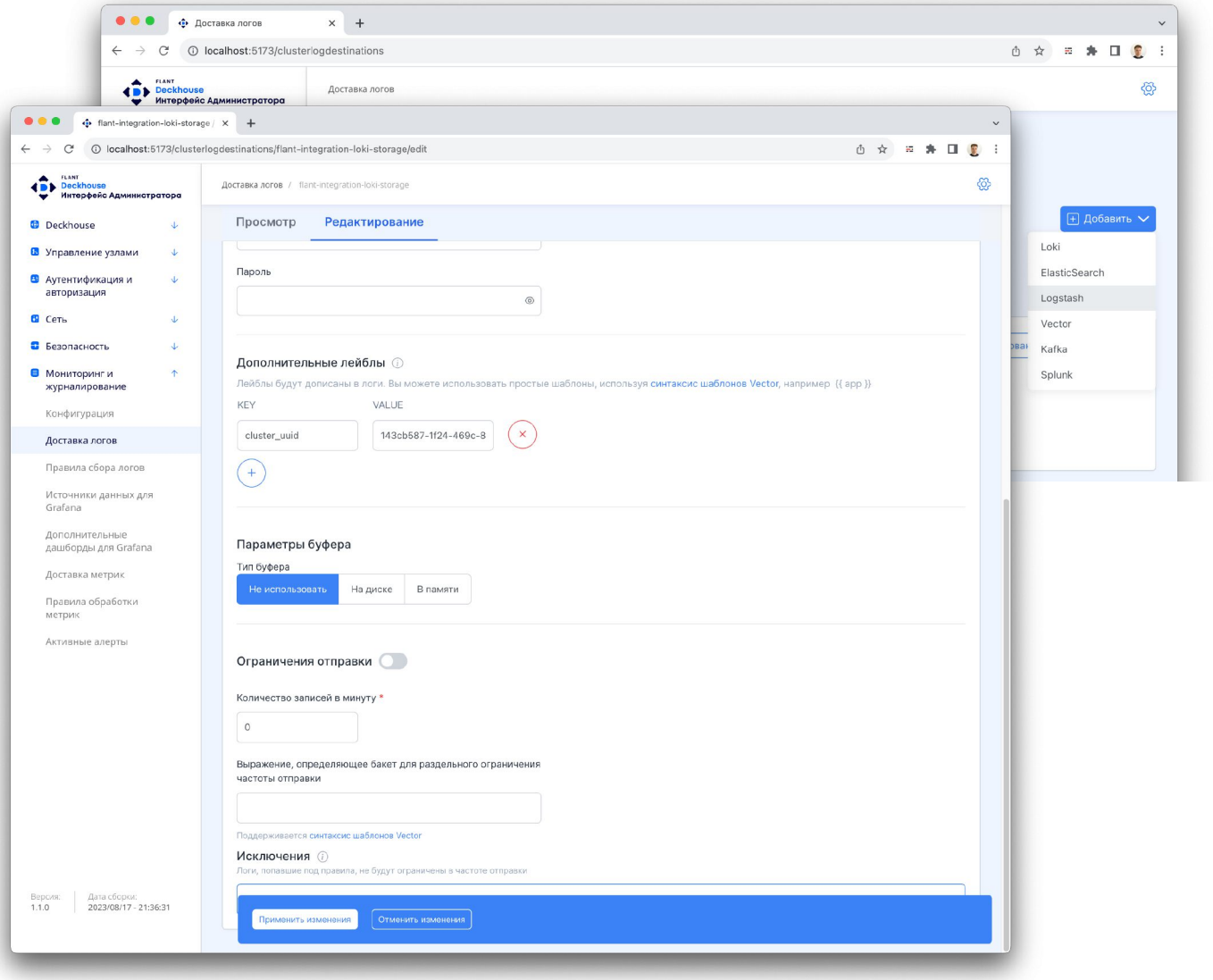
Мониторинг и журналирование

Журналирование

Deckhouse поддерживает сбор логов с подов и узлов. Для сбора логов можно выставить варианты парсинга, дополнительную фильтрацию и модификацию, а также хранилища, в которые эти логи будут отправлены.

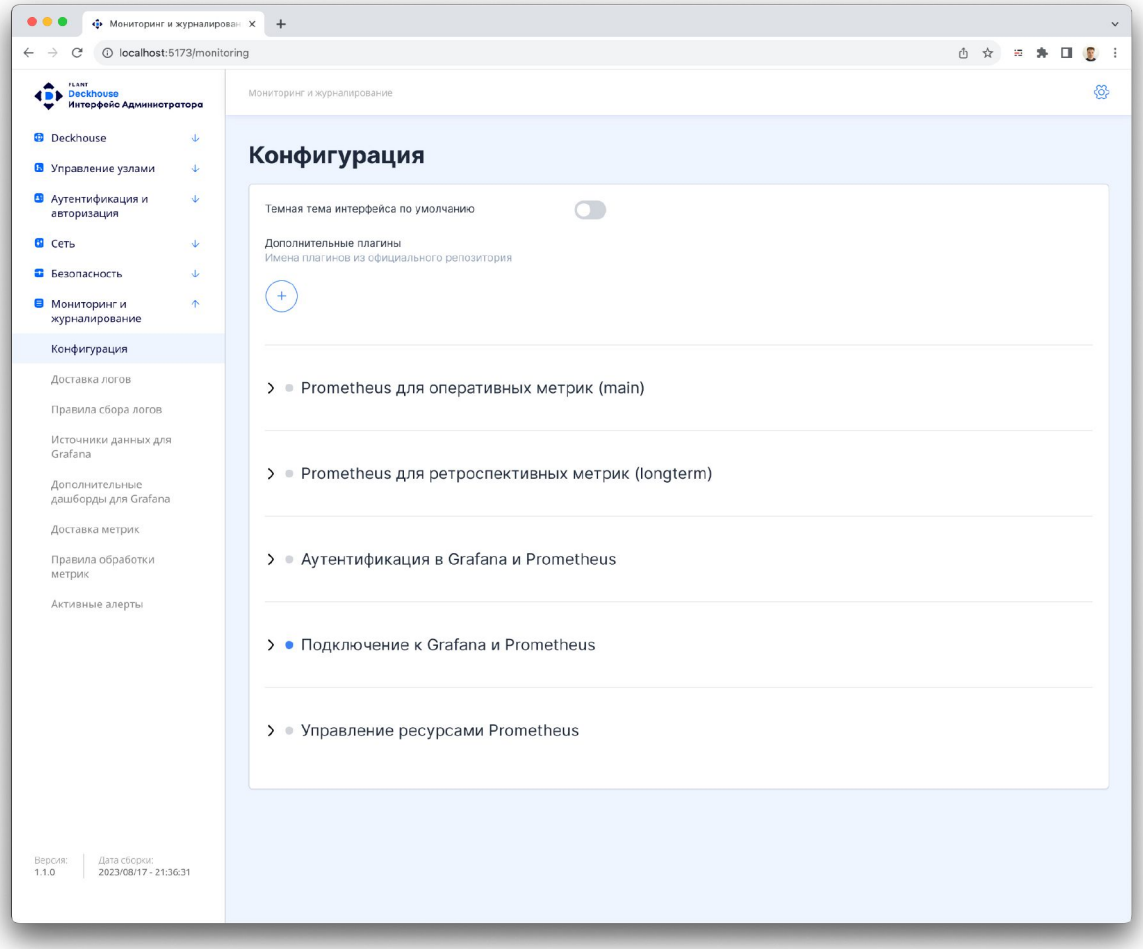


Для доставки логов поддерживается шесть типов хранилищ: Loki, Elasticsearch, Logstash, Vector, Kafka и Splunk. Перед отправкой в логи можно добавить лейблы.

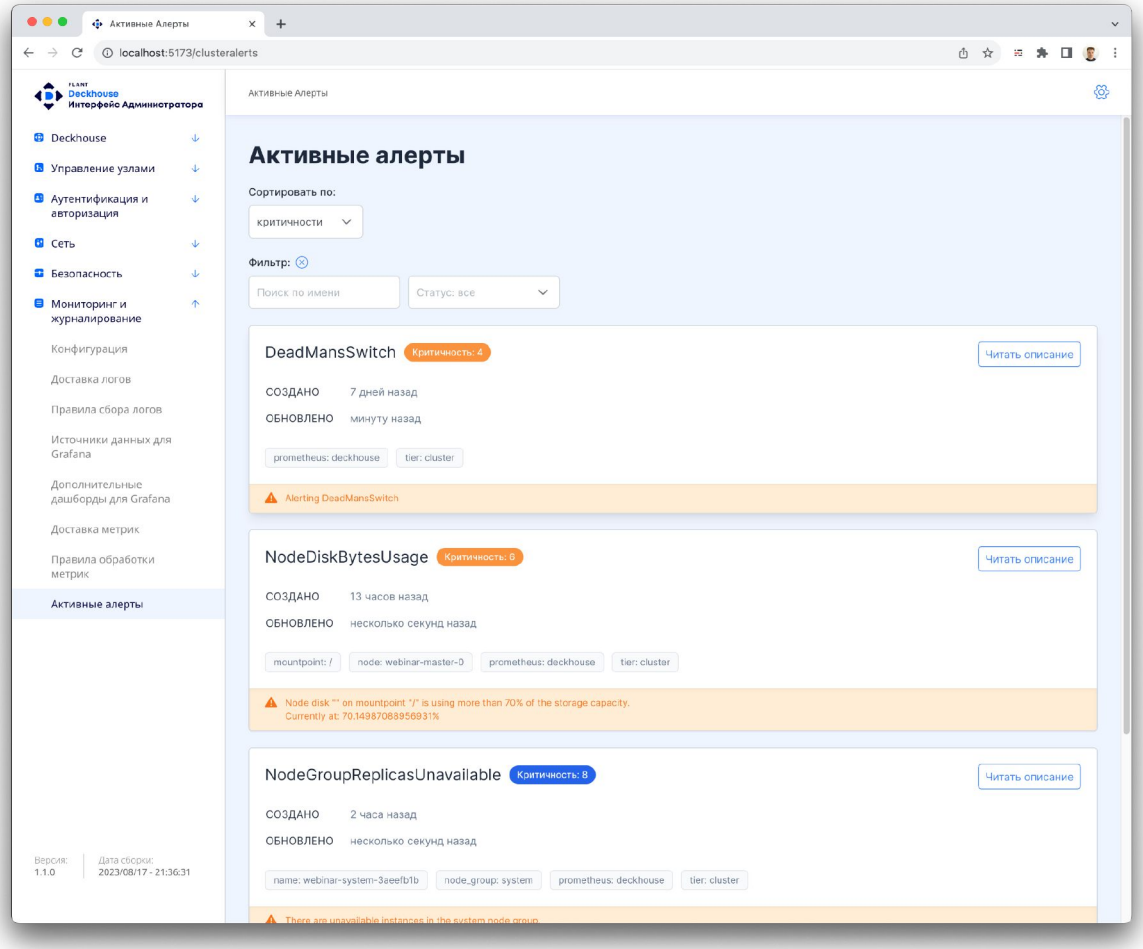


Мониторинг

Deckhouse поддерживает множество тонких настроек мониторинга. В конфигурации мониторинга доступны параметры для Prometheus и Grafana.



Есть возможность добавить в Grafana источники метрик и дашборды. Для Prometheus доступны правила обработки метрик: генерация производных метрик и алертов, а также раздел с активными алертами в кластере.



Дорожная карта

2023

1 квартал

- Новый раздел «Deckhouse»
    - Подраздел «Обновления»
      Версии Deckhouse и настройки обновлений
- Новый раздел «Управление узлами»
    - Подраздел «Группы узлов»
    - Подраздел «Все узлы
    - Подраздел «Классы машин»

2 квартал

- Глобальные настройки модулей учитываются везде, где они оказывают влияние
- Кнопка «Создать на основании...», позволяющая удобно продублировать конфигурацию
- Раздел «Deckhouse»
    - Подраздел «Обновления»: поддержка ченджлогов в истории версий Deckhouse
- Раздел «Управление узлами»
    - Подраздел «Группы узлов»: скрипты первичной настройки статических узлов
    - Виртуальные машины видны в списке еще до того, как стали узлами
- Новый раздел «Аутентификация и авторизация»
    - Подраздел «Провайдеры аутентификации»
    - Подраздел «Статические пользователи»
    - Подраздел «Права доступа»
- Новый раздел «Сеть»
    - Подраздел «Ингресс-контроллер»
- Новый раздел «Безопасность»
    - Подраздел «Сканер CVE» с отчетами об уязвимостях
- Новый раздел «Мониторинг и журналирование»
    - Подраздел «Конфигурация»
    - Подраздел «Доставка логов»
    - Подраздел «Правила сбора логов»

- Раздел «Безопасность»
    - Подраздел «Сканер CVE»: выбор неймспейсов для сканирования

3 квартал

- **Стартовый экран** с обзором кластера: предупреждениями, основными метриками и состоянием доступности подсистем Deckhouse
  (в разработке)
- Доступ в интерфейс только для администраторов
- Раздел «Deckhouse»
    - **Новый подраздел «Глобальные настройки модулей»**
      Настройки, которые наследуются модулями
    - **Новый подраздел «Модули»**
      Включение, выключение и переопределение настроек
- Раздел «Управление узлами»
    - Явное отображение процесса дренажа (draining) и его завершения (drained) в статусе узла
- Раздел «Аутентификация и авторизация»
    - **Новый подраздел «Продвинутые настройки доступа»** (Kubernetes RBAC)
        - Роли и кластерные роли
        - Привязки ролей и кластерных ролей (в разработке)
- Раздел «Мониторинг и журналирование»
    - Новый подраздел «Дополнительные дашборды для Grafana»
    - Новый подраздел «Источники данных для Grafana»
    - Новый подраздел «Активные алерты»

4 квартал

- Раздел «Deckhouse»
    - **Новый подраздел «Конфигурация кластера»**
      В этом разделе определяется версия Kubernetes (можно выбрать вариант по умолчанию или прописать конкретную версию), внутренний домен кластера и параметры прокси-сервера для исходящего трафика. Ряд параметров в этой конфигурации задается во время установки кластера и редактированию не подлежит. Например, тип кластера (облачный или статический) или подсети подов и сервисов.
    - **Новый подраздел «Конфигурация размещения»**
      В нем определяются параметры размещения в облачной инфраструктуре или на статических ресурсах. Например, можно

изменить параметры master-узлов и других узлов типа *CloudPermanent* (создаются и обновляются при помощи Terraform) для облачных кластеров, а также обновить параметры подключения к API облачного провайдера.

- Раздел «Управление узлами»
    - **Данные из мониторинга**
      В узлах и группах узлов появится информация о ключевых метриках: загрузка ядер, используемая память, используемое дисковое пространство.
    - **Лог первичной настройки узла**
      Лог первичной настройки узла будет доступен для чтения в интерфейсе. По логу можно определить проблемы, возникшие на этапе настройки.
- Раздел «Аутентификация и авторизация»
    - **Новый подраздел «Группы пользователей»**
      Управление группами пользователей было выделено в отдельный пункт конфигурации в июле 2023, поэтому для них появится свой подраздел.
- Раздел «Сеть»
    - **Новый подраздел «Сетевые политики»**
      Управление сетевыми политиками, основанное на ресурсах Kubernetes или специфическими для Cilium (если включен модуль *cilium*).
    - **Новый подраздел «Istio»**
      Управление неймспейсами, в которых включена поддержка Istio.
- Раздел «Безопасность»
    - **Ссылки на БДУ ФСТЭК в отчетах сканера уязвимостей**

2024

1 квартал

- **Новый раздел «Модули»**
    - **Настройки модулей в виде графического интерфейса**
      В первой итерации редактирование настроек модуля доступно только в виде YAML-конфигурации. Экспериментальный статус модуля указывается явно, если он есть. Также добавится управление источниками для внешних модулей.
    - Новый подраздел «Источники модулей»

- Раздел «Сеть»
    - **Статус Ingress-контроллера**
      Статус подов контроллера и отображение метрик.
    - **Новый подраздел «Keepalived»**
      Управление кластерами keepalived на фронтенд-узлах.
- Раздел «Безопасность»
    - **Новый подраздел «Аудит контейнеров»**
      Конфигурация аудита поведения контейнеров. Основан на Falco.
    - **Новый подраздел «Политики конфигурации»**
      Операционные политики создания и модификации объектов кластера. Основан на Gatekeeper.
- Новый раздел «Управление ресурсами»
    - **Новый подраздел «Descheduler»**
      Управление стратегиями Descheduler. Каждые 15 минут Descheduler вытесняет поды, которые удовлетворяют включенным в конфигурации стратегиям. Это приводит к принудительному пересозданию подов на других узлах.
    - **Новый подраздел «Приоритизация подов»**
      Доступ на чтение к встроенные классам приоритизации подов (*PriorityClasses*) и возможность добавить новые.

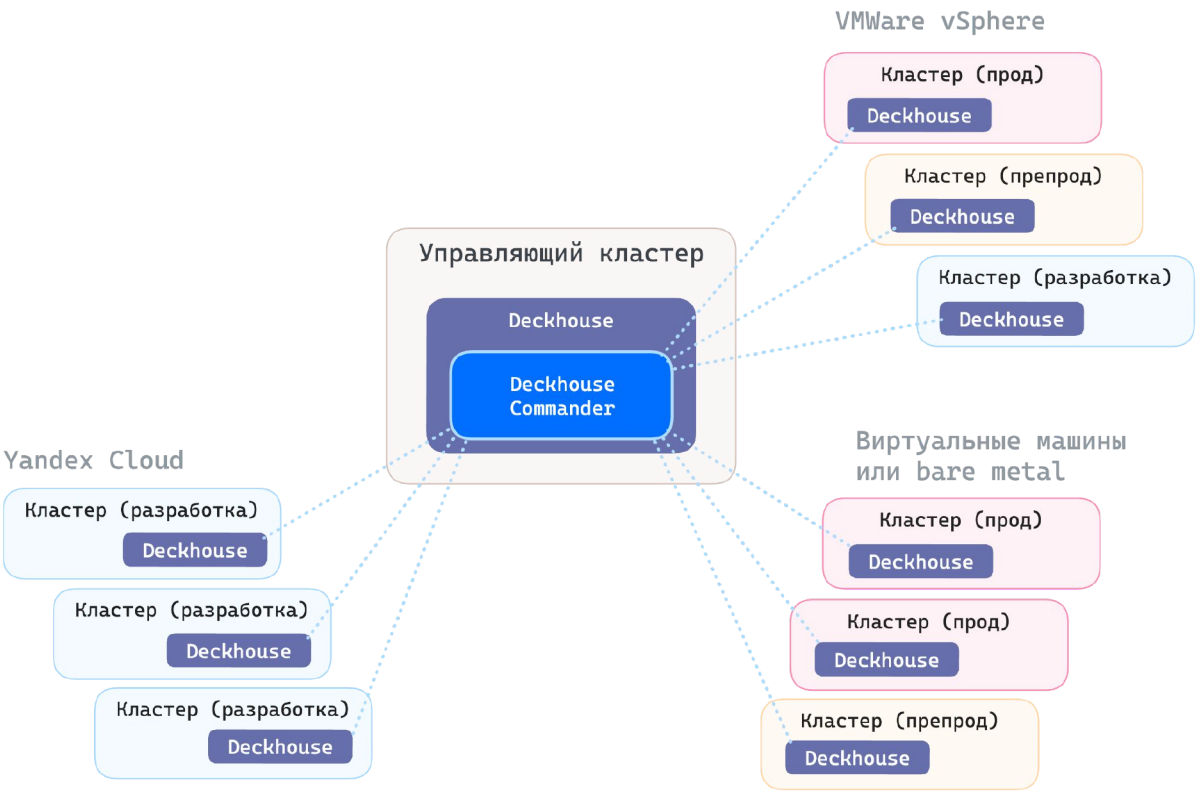
2 квартал

- Раздел «Управление доступом» («Аутентификация и авторизация»)
    - **Новый подраздел «Kubeconfig»**
      Генерирует kubeconfig-файл для локального доступа в кластер
    - **Новый подраздел «OpenVPN»**
      Управление пользовательскими сертификатами OpenVPN для доступа в подсеть подов кластера.

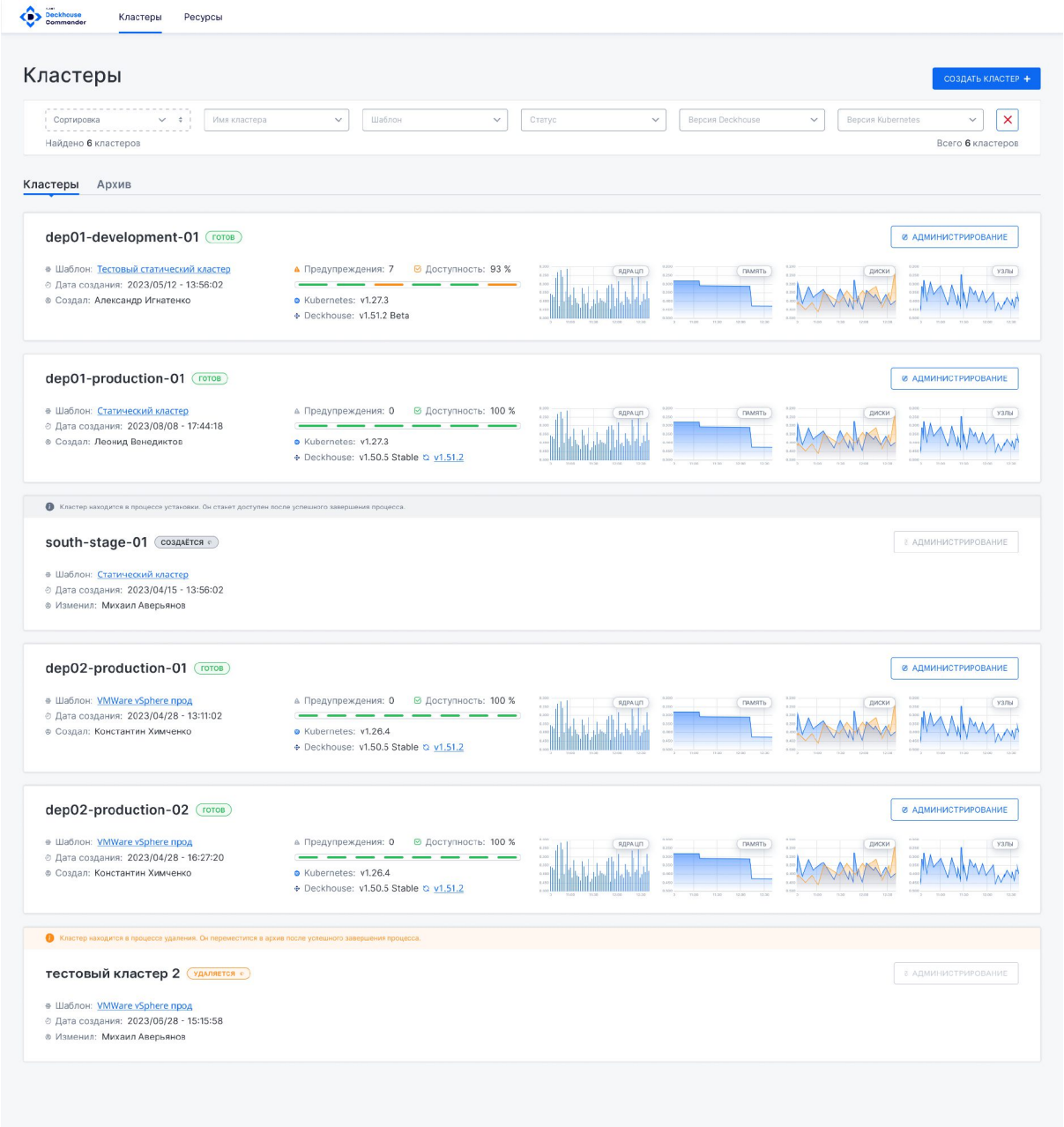
Deckhouse Commander — кластеры на кончиках пальцев

Управление кластерами

Deckhouse Commander — это менеджер кластеров. Он позволяет создавать и удалять кластеры, а также менять их конфигурацию. Создание кластеров для рабочих окружений доступно как в облаке, так и на статических ресурсах. Для Deckhouse Commander необходим управляющий кластер.



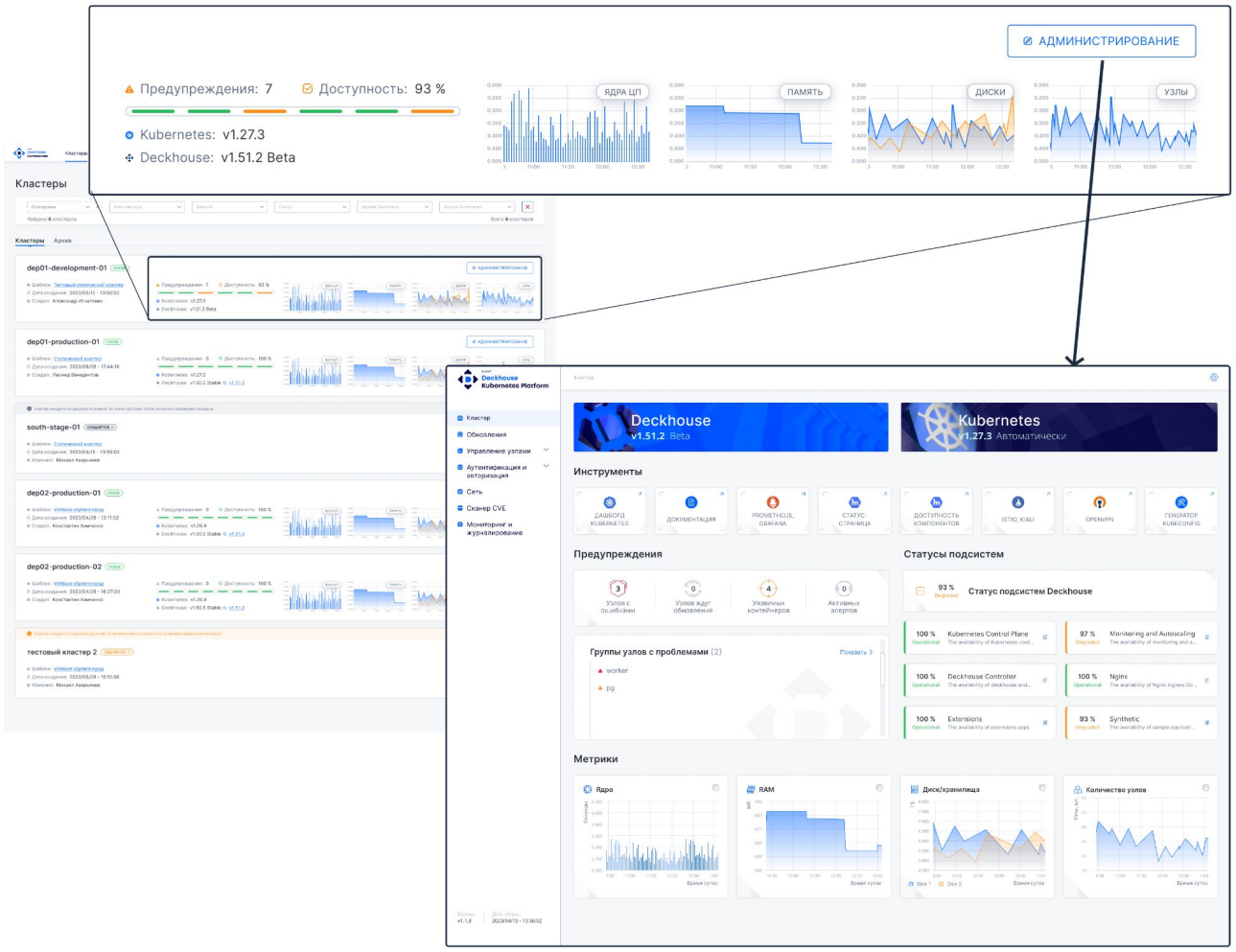
Стартовый экран Deckhouse Commander — список кластеров. Каждый элемент этого списка содержит информацию о шаблоне, по которому он был создан, о текущем состоянии кластера и о том, кем кластер последний раз редактировался.



Блок с информацией о состоянии кластера представляет собой компактный дашборд со следующей информацией:

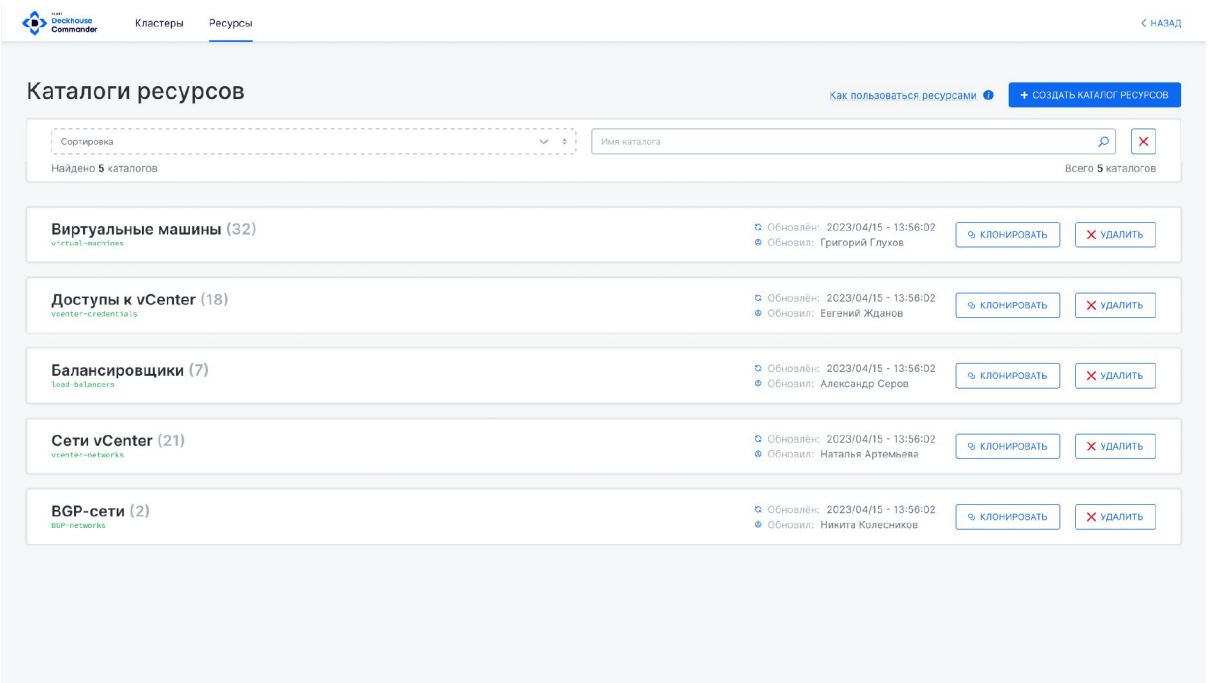
- версии Deckhouse и Kubernetes конкретного кластера и наличие для них обновлений;
- количество предупреждений (алерты, нерабочее состояние узлов или найденные уязвимости);
- статус (доступность) подсистем Deckhouse;
- метрики основных ресурсов кластера.

Ссылка «Администрирование» ведет на веб-интерфейс Deckhouse (мы описывали веб-интерфейс в первом разделе этого документа).

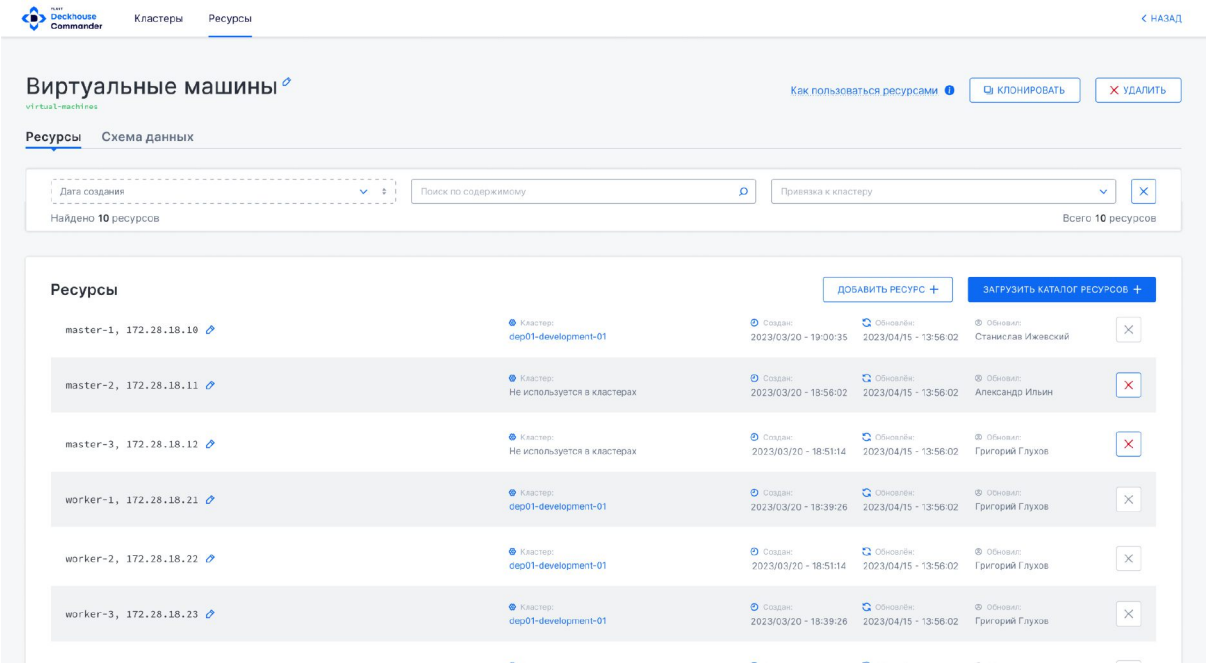


Каталоги ресурсов для кластеров

Deckhouse Commander позволяет вести учет ресурсов, доступных для использования в кластерах. Для этого используются *каталоги ресурсов*. Они представляет собой коллекцию записей об однотипных ресурсах в формате JSON/YAML и JSON-схему для валидации этих записей. Примеры ресурсов: машины для статических узлов, IP-адреса для фронтенд-узлов, BGP-сети для интеграции балансировщиков трафика, аккаунты от «разделов» на мощностях облачных провайдеров.

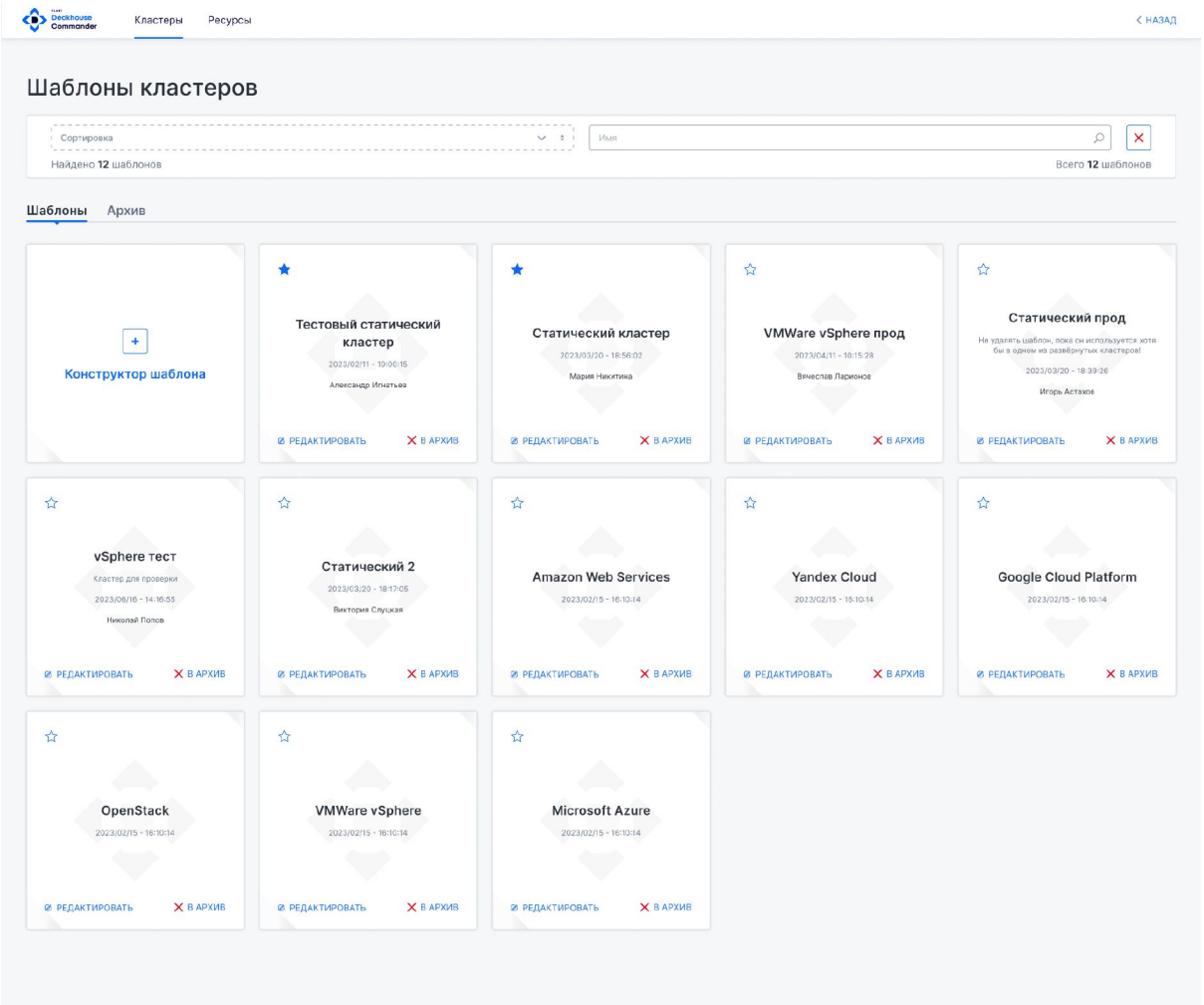


Ресурсы используются на этапе создания кластера. Когда ресурс используется кластером, в его каталоге появляется информация о привязке к кластеру.



Жизненный цикл кластера

Создание кластера включает три шага: выбор шаблона, заполнение входных параметров и непосредственно установка кластера. Кластеры создают по заранее подготовленному шаблону. Кнопка «Создать кластер» ведет на список шаблонов. Шаблоны параметризуются для разных окружений и задач. В Deckhouse Commander изначально доступны семь стандартных шаблонов: для статических кластеров и для кластеров в шести облачных провайдерах. Пользователи Deckhouse Commander также могут создать собственные шаблоны.

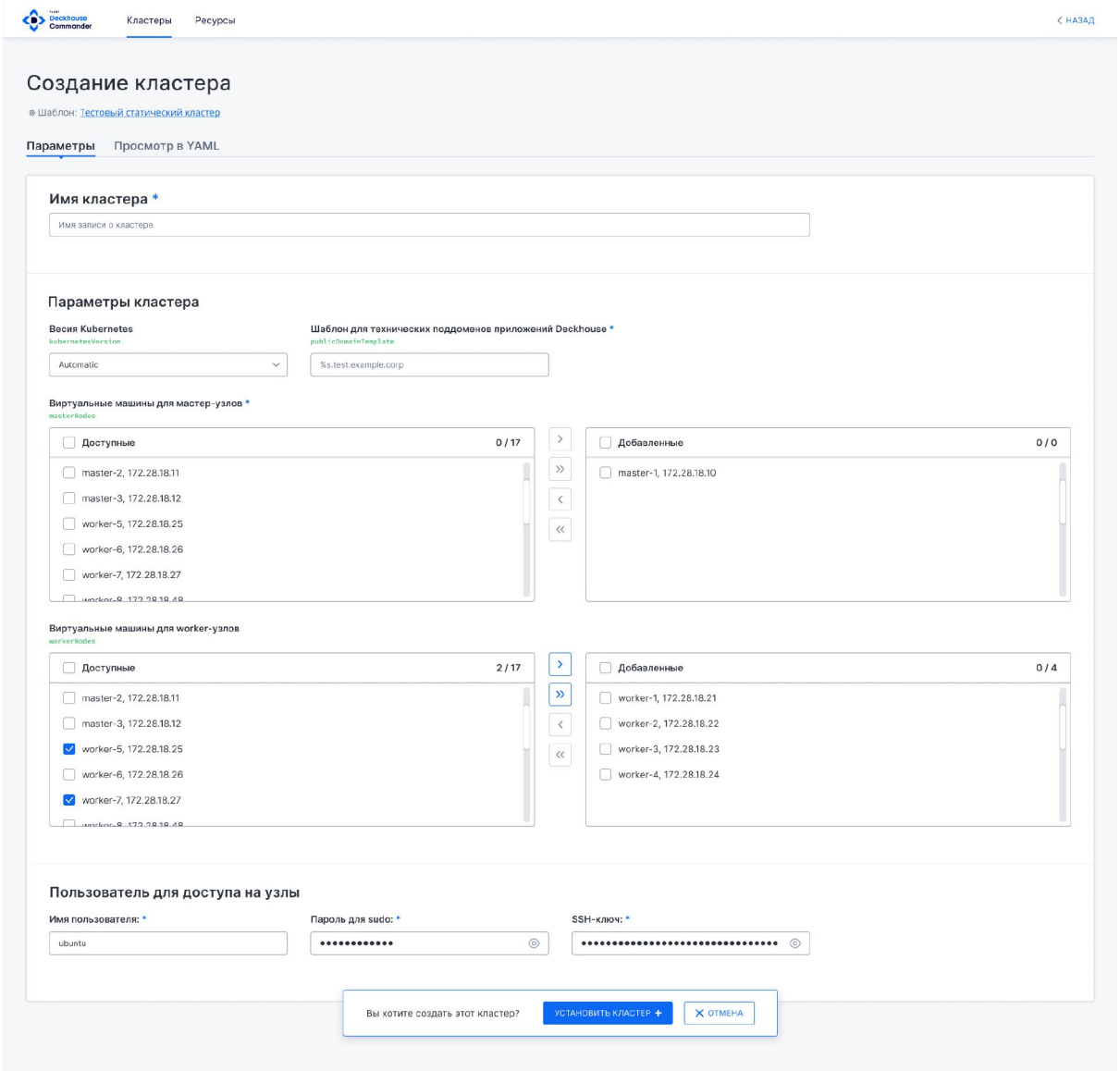


Шаблоны описывают конфигурацию, необходимую для развертывания кластера:

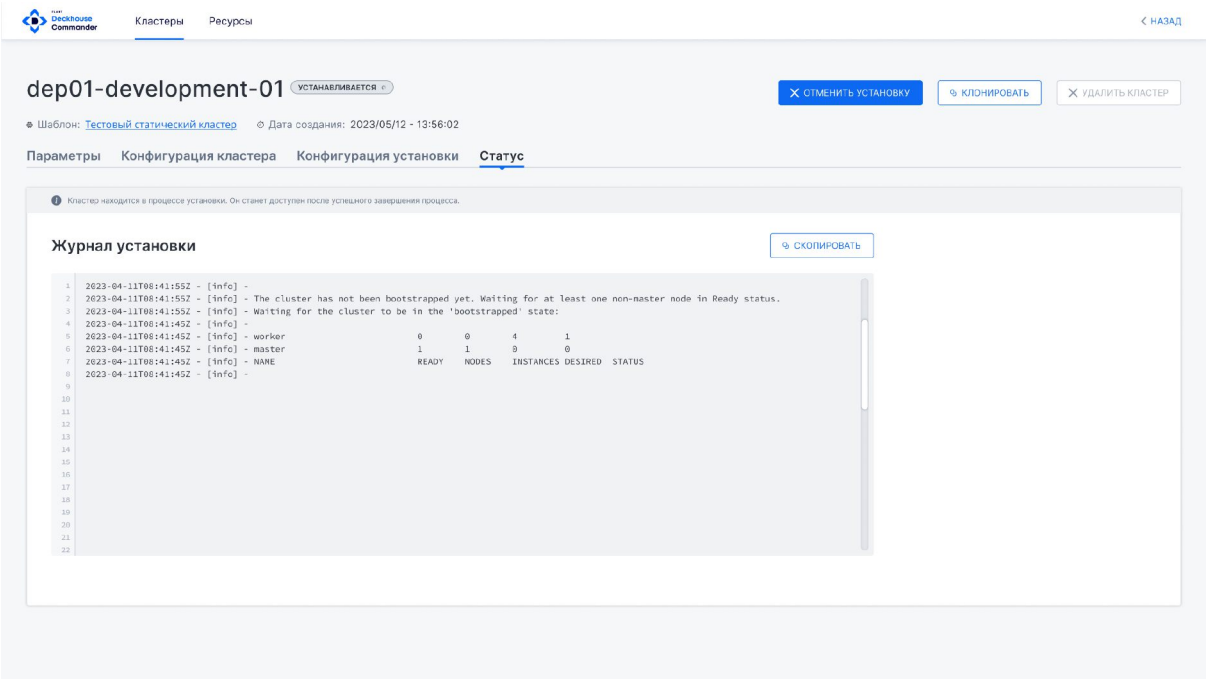
- Шаблон YAML-манифестов для установки кластера (обязательный).
- Шаблон YAML-манифестов ресурсов Kubernetes, которые будут созданы сразу после создания кластера.
- JSON-схема входных параметров для шаблонов, перечисленных в двух предыдущих пунктах.

Схема входных параметров поддерживает как произвольный ввод данных, так и использование заранее приготовленных ресурсов. Например, на рисунке ниже

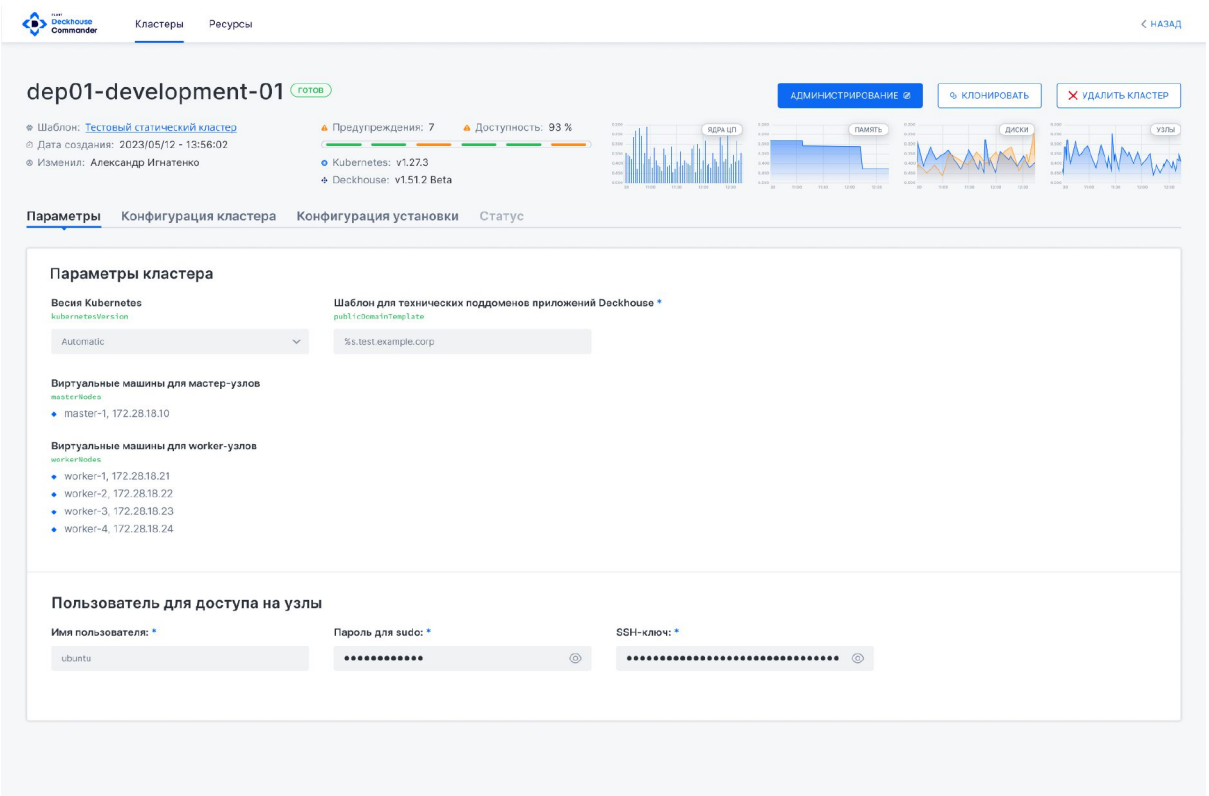
используются заранее подготовленные машины для создания статического кластера. В выбранном шаблоне нужно заполнить входные параметры, включая выбор ресурсов, после чего запустить установку кластера.



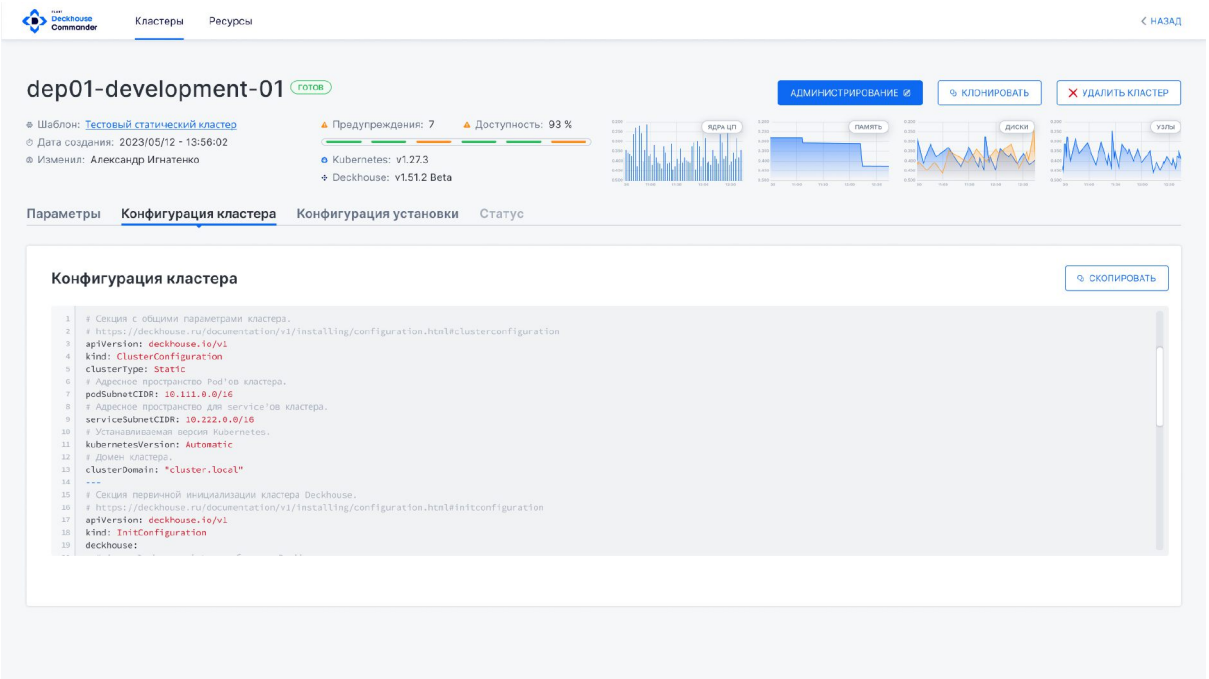
Во время установки у кластера появляется статус «Устанавливается», на экране кластера в реальном времени отображается лог установки.



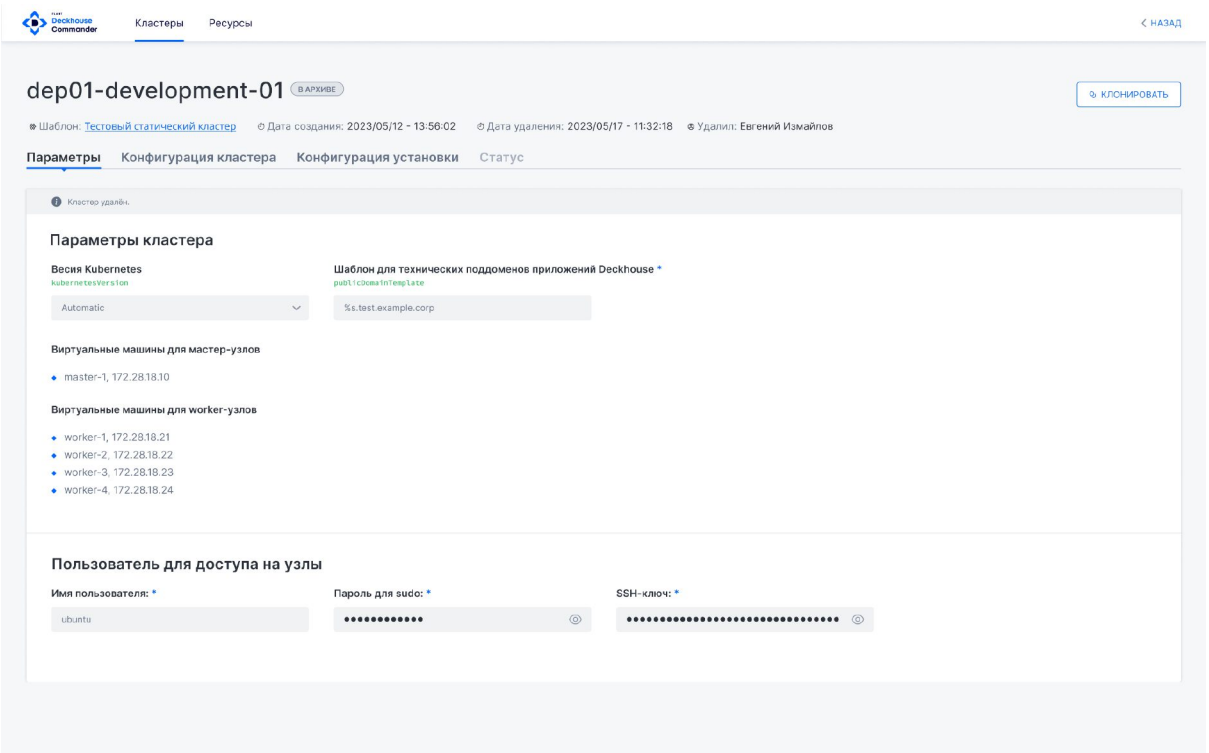
В конце установки Commander получает информацию о состоянии кластера. Также появляется возможность удалить кластер или клонировать его: создать новый кластер по тому же шаблону со скопированными входными параметрами.



Конфигурация кластера, которая использовалась во время установки, доступна на экране кластера.



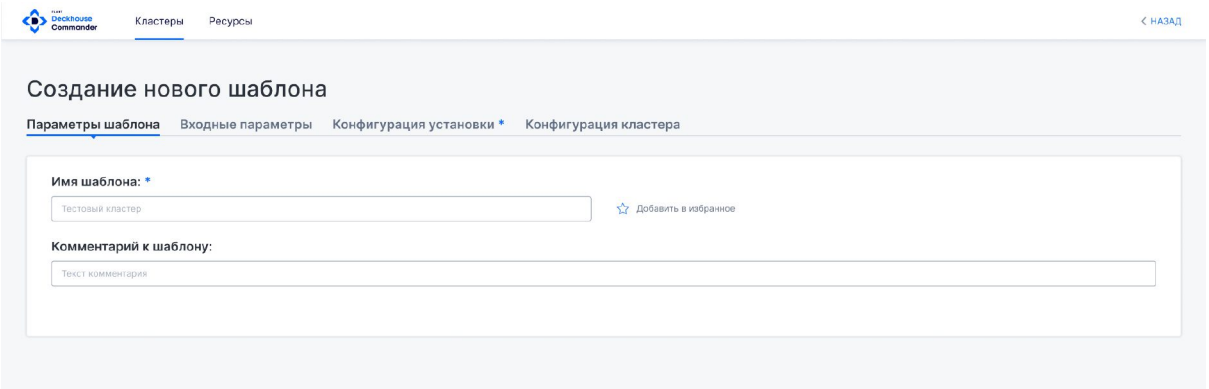
Удаление кластера запустит удаление всех объектов внутри него. После этого в Commander освободятся ресурсы, которые были заняты этим кластером. Эти ресурсы можно будет использовать для новых кластеров. Информация об удаленном кластере остается в архиве: в нее входит использованная конфигурация, входные данные и ссылка на шаблон.



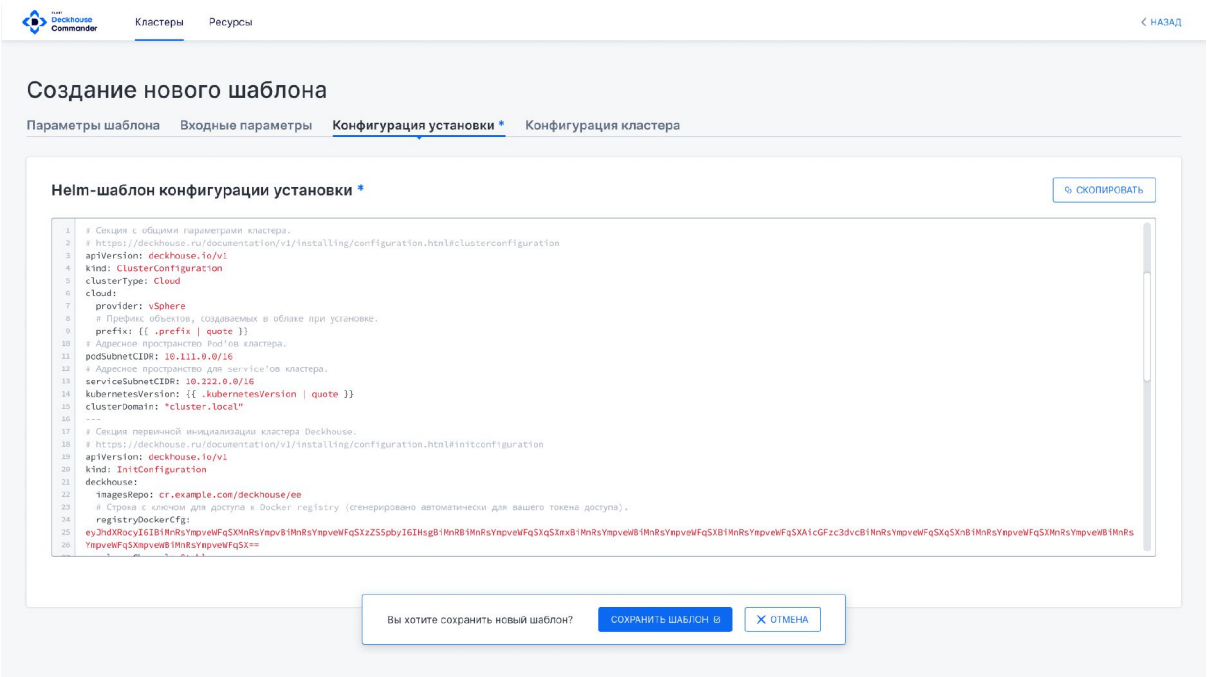
Шаблоны кластеров

Шаблоны кластеров — это одновременно и способ унификации инфраструктуры, и способ централизованной модификации работающих кластеров. Различия между кластерами выносят во входные параметры шаблона, а общую конфигурацию оставляют неизменяемой.

Возможность редактирования шаблонов и кластеров находится на стадии проектирования, поэтому она еще не отображена в макетах. Мы планируем выпустить эту функциональность в 2024 году.

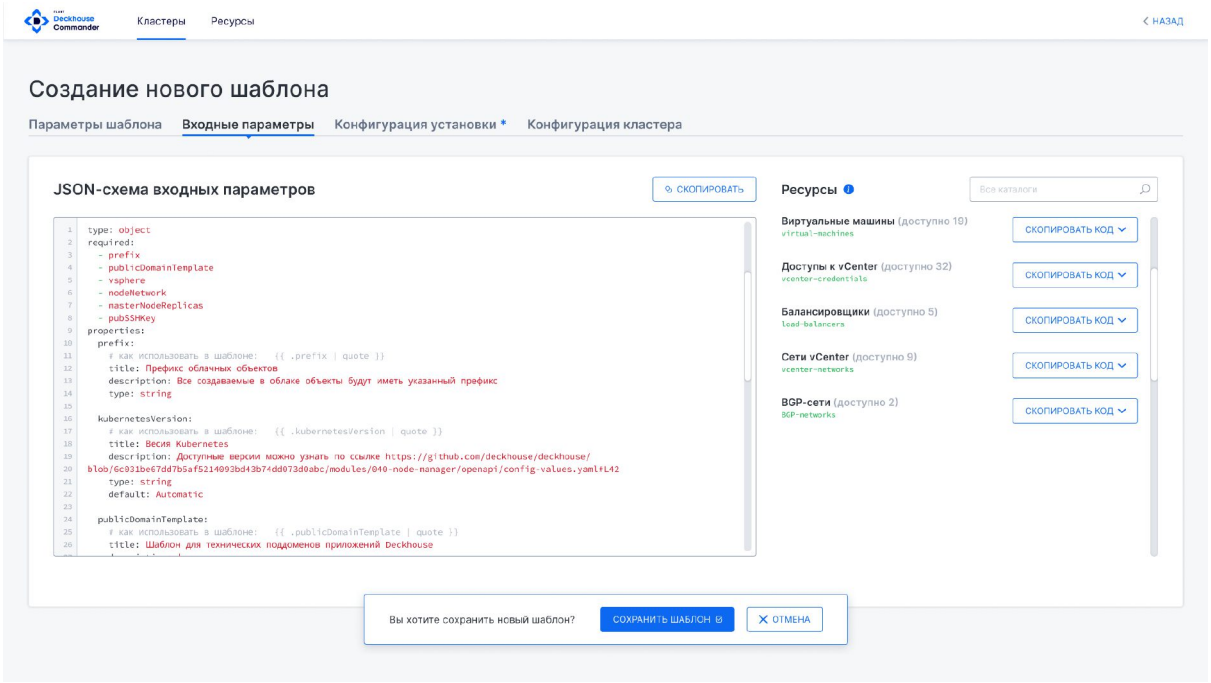


Конфигурация установки и конфигурация кластера описывается в формате YAML. Шаблонизированная часть конфигурации описана синтаксисом *go template*.



Для параметризации шаблонов необходимо составить форму входных данных. Концептуально форму входных данных можно представить как JSON-схему, в которой часть полей может быть объявлена ресурсами.

На данный момент интерфейс конструктора входных данных находится на стадии проектирования. Вместо редактора JSON-схемы мы выпустим визуальный редактор формы для входных параметров шаблона. С ним создание шаблона будет более дружелюбным к пользователю. Мы планируем выпустить редактор формы в ноябре 2023 года.



Дорожная карта

2020–2022

Первая версия Deckhouse Commander. Представляет собой веб-интерфейс для инсталлятора Deckhouse (dhctl). Включает базовую поддержку каталогов ресурсов.

2023

Август

- Начало разработки нового Deckhouse Commander

Октябрь

- Создание кластеров на основе предустановленных шаблонов
- Отображение состояния каждого кластера: предупреждения, метрики и уровень доступности

Ноябрь

- Создание пользовательских шаблонов с помощью визуальных инструментов

Декабрь

- Каталоги ресурсов

2024

- Управление доступом
    - Поддержка мультитенантности: проекты, команды, разделение прав доступа
    - История изменений кластеров, шаблонов, ресурсов
- Централизованная настройка кластеров
    - Аутентификация через единый dex в управляющем кластере
    - Мониторинг и журналирование через центральный Okmeter storage
    - Сбор алертов с кластеров в мультитенантном алерт-менеджере
    - Политики безопасности: аудит контейнеров, сетевые политики
    - Политики конфигурации кластеров. Возможность централизованно ограничить конфигурацию, которой разрешено управлять в отдельных кластерах
    - Интеграция кластеров друг с другом: мультикластерные возможности Cilium и Istio