



Платформа Deckhouse как сервис из облака



Артём Кожокин

Директор по стратегическому
развитию Deckhouse



DECKHOUSE

**Kubernetes
Platform**

О компании Deckhouse

15+

лет опыта
в Open Source

С 2017

года используем
Kubernetes в production

300+

сотрудников

№1

контрибьютор
Kubernetes в России

>150

компаний-
пользователей



Реестр
российского ПО



ФСТЭК



Аккредитация
Минцифры



2023 год — объединение с Express 42.
Подразделение по DevOps-консалтингу



Deckhouse Kubernetes Platform в цифрах

>7

лет эксплуатации.
Первая российская
K8s-платформа

150+

клиентов
из различных
индустрий

>1 млн

контейнеров
в Deckhouse-
кластерах

600+

кластеров под
управлением

7000+

приложений в
production прямо
сейчас

9000+

узлов в кластерах

74000+

vCPU в кластерах

99,99%

фактический SLA
по всем кластерам



Deckhouse console

Аутентификация

Мониторинг
и алертинг

Service mesh

Журналирование

Управление
сертификатами

Балансировка
трафика

Безопасность

Инструментарий
для CI/CD

Резервное
копирование

Запуск
legacy-
приложений

Программно-
определяемое
хранилище

Программно-
определяемая
сеть

Managed-
сервисы *

Подсистемы платформы

Оператор
платформы

Механизм модулей

Маркетплейс *

Kubernetes

Инфраструктурно-независимый фундамент платформы

Инфраструктура

openstack

vmware
vSphere

Selectel

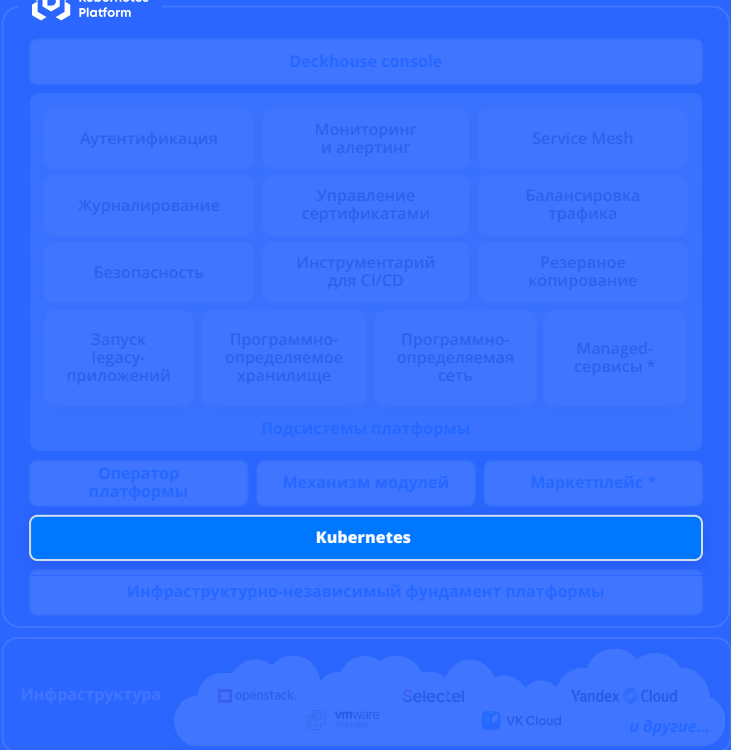
VK Cloud

Yandex Cloud

и другие...

Архитектура Deckhouse Kubernetes Platform

* В планах



Настраивает и управляет компонентами Kubernetes

- Control plane Kubernetes полностью **под управлением Deckhouse**, что обеспечивает отказоустойчивость и управление жизненным циклом кластера.
- Все **ручные операции автоматизированы**: создание и ротация сертификатов, масштабирование и восстановление кластера.
- Поддержка **четырёх версий Kubernetes** в каждой версии платформы — обновляйтесь, когда вам удобно.
- Каждая версия **сертифицирована CNCF**, что гарантирует совместимость приложений.



Deckhouse console

Аутентификация

Мониторинг
и алертинг

Service Mesh

Журналирование

Управление
сертификатами

Балансировка
трафика

Безопасность

Инструментарий
для CI/CD

Резервное
копирование

Запуск
legacy-
приложений

Программно-
определяемое
хранилище

Программно-
определяемая
сеть

Managed-
сервисы *

Подсистемы платформы

Оператор
платформы

Механизм модулей

Маркетплейс *

kubernetes

Инфраструктурно-независимый фундамент платформы

Инфраструктура

openstack

vmware

Selectel

VK Cloud

Yandex Cloud

и другие...

Обеспечивает автоматизацию пятого уровня

Уровень 1

Уровень 2

Уровень 3

Уровень 4

Уровень 5

Только
установка

- Подготовка инфраструктуры
- Настройка ОС
- Развёртывание кластера
- Начальная настройка

Бесшовное
обновление

- Обновление управляющего слоя
- Обновление компонентов
- Обновление Kubernetes control plane
- Управление обновлениями

Управление
жизненным
циклом

- Бэкапы и восстановление
- Режим высокой доступности
- Глобальные настройки и глубокая связанность всех компонентов
- Мультиарендность и управление ресурсами через проекты

Полная
наблюдаемость

- Готовые метрики для компонентов платформы и приложений
- Продуманные алерты с разным уровнем критичности
- Группировка и дедупликация уведомлений
- Предиктивные уведомления для предотвращения сбоев

Автопилот

- Автомасштабирование под нагрузкой
- Автоконфигурация
- Автообнаружение и реагирование на угрозы
- Автопланировщик ресурсов

Другие решения

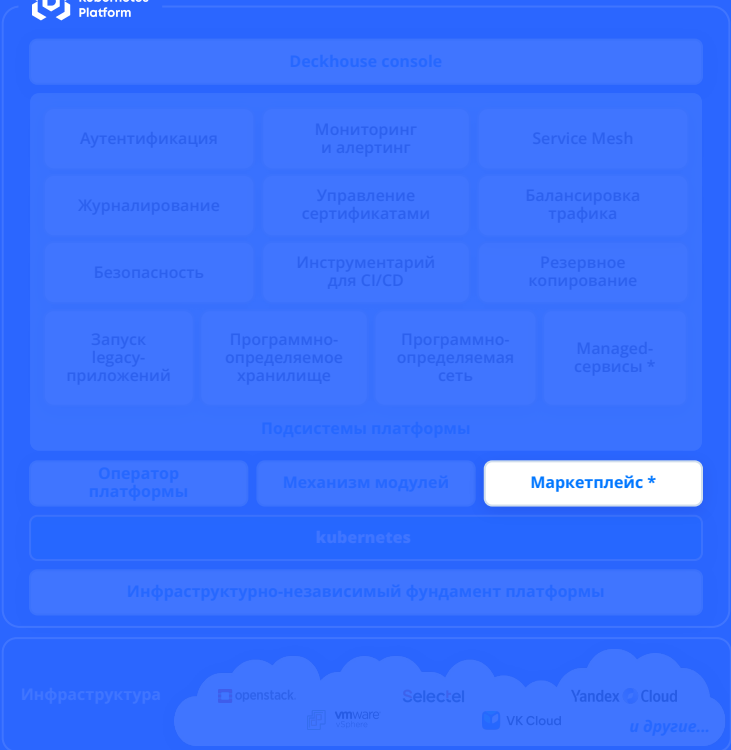




Расширяет возможности платформы

- Простой фреймворк для написания **собственных модулей к платформе**: унифицированное описание и полная валидация конфигурации.
- Постоянный **контроль и приведение состояния модуля к желаемому** исключают внесение ручных изменений.
- Пять каналов стабильности дают **гибкие возможности доставки** модуля в кластер.
- Автоматическое **отображение документации** модуля в кластере.
- Простое добавление модуля во **внутренний маркетплейс** в кластере с возможностью включения/отключения модуля одной кнопкой.





Упрощает доставку и обновление прикладного ПО, гарантирует совместимость

- Каталог приложений как **для бизнеса**, так и **для инфраструктуры**.
- Удобный **механизм доставки**, в том числе в закрытый контур: каналы стабильности, окна обновлений, установка «по кнопке».
- **Гарантированная совместимость** всего ПО с платформой.
- Продуманный **механизм обновления** для закрытых окружений из единого реестра образов.
- Простой и быстрый способ доставки **ваших модулей во все кластеры**.

* В планах



Deckhouse console

Аутентификация

Мониторинг
и алертинг

Service Mesh

Журналирование

Управление
сертификатами

Балансировка
трафика

Безопасность

Инструментарий
для CI/CD

Резервное
копирование

Запуск
legacy-
приложений

Программно-
определяемое
хранилище

Программно-
определяемая
сеть

Managed-
сервисы *

Подсистемы платформы

Оператор
платформы

Механизм модулей

Маркетплейс *

Kubernetes

Инфраструктурно-независимый фундамент платформы

Инфраструктура

openstack

vmware

Selectel

VK Cloud

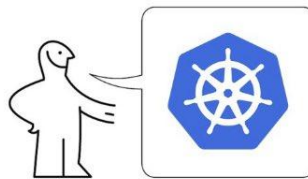
Yandex Cloud

и другие...

Одного Kubernetes недостаточно!

В состав Kubernetes **не входят** многие компоненты, необходимые для запуска продуктивных нагрузок.

KÜBERNETES



Всё, чего не хватает в Kubernetes



Deckhouse console

Аутентификация

Мониторинг
и алертинг

Service mesh

Журналирование

Управление
сертификатами

Балансировка
трафика

Безопасность

Инструментарий
для CI/CD

Резервное
копирование

Запуск
legacy-
приложений

Программно-
определяемое
хранилище

Программно-
определяемая
сеть

Managed-
сервисы *

Подсистемы платформы

Оператор
платформы

Механизм модулей

Маркетплейс *

kubernetes

Инфраструктурно-независимый фундамент платформы

Инфраструктура

openstack

vmware
vSphere

Selectel

VK Cloud

Yandex Cloud

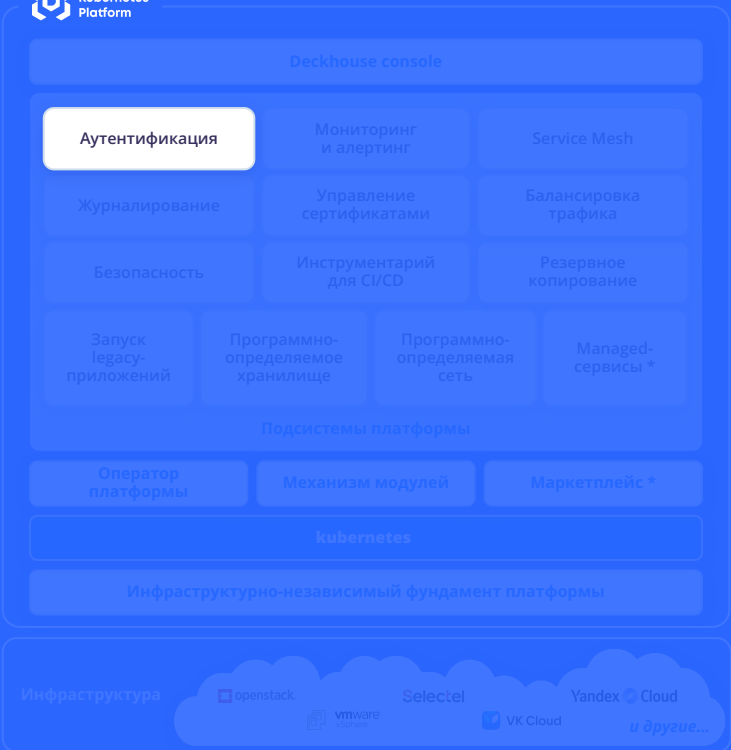
и другие...

* В планах



Единый центр аутентификации

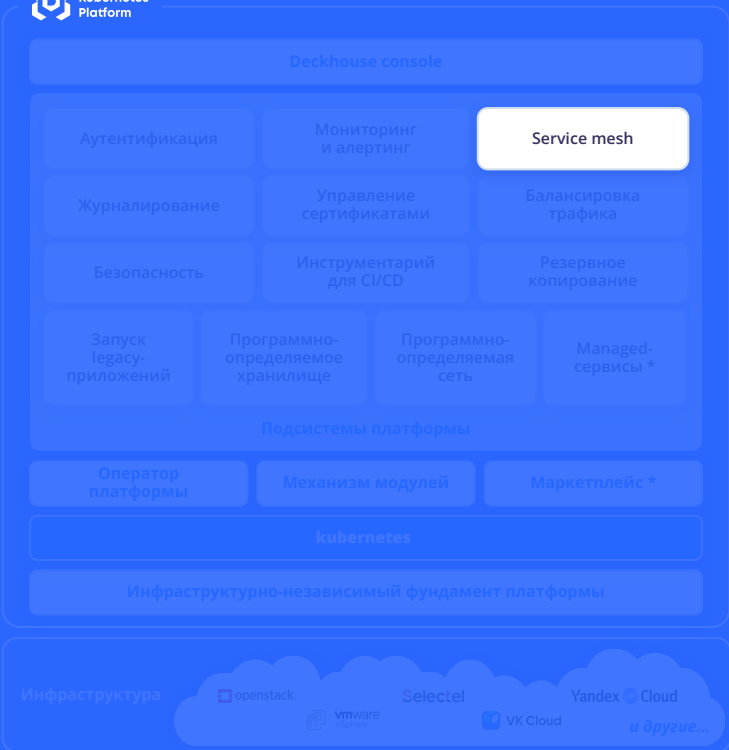
- Обеспечивает **безопасный доступ** к API кластера, всем веб-интерфейсам и пользовательским приложениям.
- Возможность создания **локальных пользователей и групп**. Простая выдача конфигурации подключения.
- Интеграция с **внешними провайдерами аутентификации** (LDAP, Active Directory, OIDC и другие).
- Контроль доступа к ресурсам платформы, настройка **правил авторизации и ограничения доступа** к любым системам по IP и группам пользователей.
- Аутентификация для сторонних приложений.





Сквозная наблюдаемость

- Готовые метрики, алерты и дашборды визуализации для всех компонентов платформы «из коробки» с любой степенью детализации.
- Все возможности для мониторинга пользовательских приложений.
- Встроенное хранилище метрик высокой детализации (30 секунд) и долгосрочное хранилище метрик низкой детализации (5 минут).
- Возможность отправки метрик и алертов во внешние системы.
- Кэширование запросов к Prometheus.



Service mesh на базе Istio

- Организация отказо- и катастрофоустойчивой инфраструктуры за счёт **объединения кластеров** в режиме федерации или мультикластера.
- **Авторизация доступа** между сервисами.
- Взаимная достоверная **аутентификация сервисов и шифрование трафика (mTLS)**.
- Возможность реализовать **canary-deployment** и **A/B-тестирование**.
- Управление **балансировкой запросов** между эндпоинтами сервиса: Circuit Breaker, Sticky Sessions, Locality Failover.
- **Визуализация** состояния связей между сервисами и состояния служебных компонентов Istio с помощью Kiali.



Журналирование

- Система **сбора, парсинга и фильтрации журналов** для распределённых систем.
- Встроенное **хранилище журналов**.
- Возможность **отправки журналов** во внешние хранилища.
- **Отправка оповещений** на основе данных журналов.
- Удобный **просмотр и визуализация журналов** в реальном времени.





Управление сертификатами

- Заказ, отслеживание сроков действия и автоматическое обновление SSL-сертификатов.
- Интеграция с различными **CA-сервисами**, такими как Let's Encrypt, Vault, или **корпоративным центром сертификации**.
- Сертификаты могут использоваться как для **защиты связи между службами** внутри платформы, так и для **обеспечения безопасного доступа** пользователей к приложениям через TLS/SSL.
- Параметры заказа сертификатов могут быть настроены **на уровне всей платформы** или **индивидуально** для каждого приложения.



Балансировка трафика

- Обеспечивает **управление маршрутизацией** HTTP- и HTTPS-трафика.
- Позволяет определять **правила маршрутизации** на основе путей URL и хостов.
- Обеспечивает **балансировку нагрузки** и **терминацию SSL/TLS** для защиты трафика.
- Заказ балансировщика и настройка правил производятся **в режиме самообслуживания** через единый API Kubernetes, упрощая управление и контроль доступа к приложениям.
- Глубокая интеграция с платформой мониторинга и проработанные панели графиков позволяют **быстро находить и диагностировать проблемы** в работе приложений.



Deckhouse console

Аутентификация

Мониторинг
и алертинг

Service Mesh

Журналирование

Управление
сертификатами

Балансировка
трафика

Безопасность

Инструментарий
для CI/CD

Резервное
копирование

Запуск
legacy-
приложений

Программно-
определяемое
хранилище

Программно-
определяемая
сеть

Managed-
сервисы *

Подсистемы платформы

Оператор
платформы

Механизм модулей

Маркетплейс *

kubernetes

Инфраструктурно-независимый фундамент платформы

Инфраструктура

openstack

vmware

Selectel

Yandex Cloud

VK Cloud

и другие...

Преднастроенная безопасность

1

Управление и контроль доступа к кластерам

Подключение

Аутентификация

Авторизация

ЗАДАЧИ

РЕШЕНИЕ

ФУНКЦИОНАЛ

Централизованная
сквозная аутентификация

Разделение прав доступа
в платформе

Функционал проектов,
мультитенантность



Deckhouse console

Аутентификация

Мониторинг
и алертинг

Service Mesh

Журналирование

Управление
сертификатами

Балансировка
трафика

Безопасность

Инструментарий
для CI/CD

Резервное
копирование

Запуск
legacy-
приложений

Программно-
определяемое
хранилище

Программно-
определяемая
сеть

Managed-
сервисы *

Подсистемы платформы

Оператор
платформы

Механизм модулей

Маркетплейс *

kubernetes

Инфраструктурно-независимый фундамент платформы

Инфраструктура

openstack

vmware

Selectel

VK Cloud

Yandex Cloud

и другие...

Преднастроенная безопасность

1

Управление и контроль доступа к кластерам

ФУНКЦИОНАЛ

Централизованная
сквозная аутентификация

Разделение прав доступа
в платформе

Функционал проектов,
мультитенантность

- Множество провайдеров (LDAP, Active Directory, OIDC и другие).
- Аутентификация для сторонних приложений.
- Простая выдача конфигурации подключения.



Deckhouse console

Аутентификация

Мониторинг
и алертинг

Service Mesh

Журналирование

Управление
сертификатами

Балансировка
трафика

Безопасность

Инструментарий
для CI/CD

Резервное
копирование

Запуск
legacy-
приложений

Программно-
определяемое
хранилище

Программно-
определяемая
сеть

Managed-
сервисы *

Подсистемы платформы

Оператор
платформы

Механизм модулей

Маркетплейс *

kubernetes

Инфраструктурно-независимый фундамент платформы

Инфраструктура

openstack

vmware

Selectel

VK Cloud

Yandex Cloud

и другие...

Преднастроенная безопасность

1

Управление и контроль доступа к кластерам

ФУНКЦИОНАЛ

Централизованная
сквозная аутентификация

Разделение прав доступа
в платформе

Функционал проектов,
мультитенантность

- Стандартный RBAC.
- Семь преднастроенных ролей.
- Кастомные роли.
- Упрощённый режим мультитенантности с разделением доступа по пространствам имён.



Deckhouse console

Аутентификация

Мониторинг
и алертинг

Service Mesh

Журналирование

Управление
сертификатами

Балансировка
трафика

Безопасность

Инструментарий
для CI/CD

Резервное
копирование

Запуск
legacy-
приложений

Программно-
определяемое
хранилище

Программно-
определяемая
сеть

Managed-
сервисы *

Подсистемы платформы

Оператор
платформы

Механизм модулей

Маркетплейс *

kubernetes

Инфраструктурно-независимый фундамент платформы

Инфраструктура

openstack

vmware

Selectel

VK Cloud

Yandex Cloud

и другие...

Преднастроенная безопасность

1

Управление и контроль доступа к кластерам

ФУНКЦИОНАЛ

Централизованная
сквозная аутентификация

Разделение прав доступа
в платформе

Функционал проектов,
мультитенантность

- Автоматическое назначение прав доступа.
- Сетевые политики с визуализацией.
- Контроль и квотирование ресурсов.
- Распределение проектов по выделенным узлам.



Deckhouse console

Аутентификация

Мониторинг
и алертинг

Service Mesh

Журналирование

Управление
сертификатами

Балансировка
трафика

Безопасность

Инструментарий
для CI/CD

Резервное
копирование

Запуск
legacy-
приложений

Программно-
определяемое
хранилище

Программно-
определяемая
сеть

Managed-
сервисы *

Подсистемы платформы

Оператор
платформы

Механизм модулей

Маркетплейс *

kubernetes

Инфраструктурно-независимый фундамент платформы

Инфраструктура

openstack

vmware

Selectel

VK Cloud

Yandex Cloud

и другие...

Преднастроенная безопасность

1

Управление и контроль доступа к кластерам

2

Контроль и безопасность рабочих нагрузок

Аудит Runtime

Аутентификация

Внедрение
и унификация политик

ЗАДАЧИ

РЕШЕНИЕ

ФУНКЦИОНАЛ

Сканирование образов
и аудит событий

Контроль конфигурации
всех сущностей кластера

Готовый мониторинг
и журналирование



Преднастроенная безопасность

1

Управление и контроль доступа к кластерам

2

Контроль и безопасность рабочих нагрузок

ФУНКЦИОНАЛ

Сканирование образов и аудит событий

Контроль конфигурации всех сущностей кластера

Готовый мониторинг и журналирование

- Сканирование образов на предмет уязвимостей.
- Поиск и предотвращение угроз безопасности.



Deckhouse console

Аутентификация

Мониторинг
и алертинг

Service Mesh

Журналирование

Управление
сертификатами

Балансировка
трафика

Безопасность

Инструментарий
для CI/CD

Резервное
копирование

Запуск
legacy-
приложений

Программно-
определяемое
хранилище

Программно-
определяемая
сеть

Managed-
сервисы *

Подсистемы платформы

Оператор
платформы

Механизм модулей

Маркетплейс *

kubernetes

Инфраструктурно-независимый фундамент платформы

Инфраструктура

openstack

vmware

Selectel

VK Cloud

Yandex Cloud

и другие...

Преднастроенная безопасность

1

Управление и контроль доступа к кластерам

2

Контроль и безопасность рабочих нагрузок

ФУНКЦИОНАЛ

Сканирование образов
и аудит событий

**Контроль конфигурации
всех сущностей кластера**

Готовый мониторинг
и журналирование

- Политики безопасности Pod Security Standards.
- Возможность создавать собственные политики.
- Регулярные проверки на соответствие CIS benchmark.



Deckhouse console

Аутентификация

Мониторинг
и алертинг

Service Mesh

Журналирование

Управление
сертификатами

Балансировка
трафика

Безопасность

Инструментарий
для CI/CD

Резервное
копирование

Запуск
legacy-
приложений

Программно-
определяемое
хранилище

Программно-
определяемая
сеть

Managed-
сервисы *

Подсистемы платформы

Оператор
платформы

Механизм модулей

Маркетплейс *

kubernetes

Инфраструктурно-независимый фундамент платформы

Инфраструктура

openstack

vmware

Selectel

Yandex Cloud

VK Cloud

и другие...

Преднастроенная безопасность

1

Управление и контроль доступа к кластерам

2

Контроль и безопасность рабочих нагрузок

ФУНКЦИОНАЛ

Сканирование образов
и аудит событий

Контроль конфигурации
всех сущностей кластера

Готовый мониторинг
и журналирование

Обеспечение лучших практик через централизованные политики



Разрешить только
доверенные registry



Обязательно
прописывать ресурсы



Использовать
пробы



Ограничить
количество ревизий



Указывать
priorityClass



Запретить
использовать ter latest



Deckhouse console

Аутентификация

Мониторинг
и алертинг

Service Mesh

Журналирование

Управление
сертификатами

Балансировка
трафика

Безопасность

Инструментарий
для CI/CD

Резервное
копирование

Запуск
legacy-
приложений

Программно-
определяемое
хранилище

Программно-
определяемая
сеть

Managed-
сервисы *

Подсистемы платформы

Оператор
платформы

Механизм модулей

Маркетплейс *

kubernetes

Инфраструктурно-независимый фундамент платформы

Инфраструктура

openstack

vmware

Selectel

VK Cloud

Yandex Cloud

и другие...

Преднастроенная безопасность

1

Управление и контроль доступа к кластерам

2

Контроль и безопасность рабочих нагрузок

ФУНКЦИОНАЛ

Сканирование образов
и аудит событий

Контроль конфигурации
всех сущностей кластера

Готовый мониторинг
и журналирование

- Гибкий сбор логов аудита, их обработка и доставка в SIEM-системы.
- Встроенные метрики и возможность собирать любые пользовательские метрики.
- Удобная настройка оповещений о событиях ИБ в кластерах.



Инструменты для построения DevSecOps-конвейера

- Возможность реализовывать **гибкие CI/CD-сценарии** с применением широкого спектра систем.
- **Доставка приложений** из хранилища артефактов прямо в кластер Deckhouse с помощью Argo CD и механизма werf bundles.
- Автоматический **контроль за состоянием ресурсов** в процессе развёртывания.
- Удобная **доставка в изолированных средах** (air-gapped).



Deckhouse console

Аутентификация

Мониторинг
и алертинг

Service Mesh

Журналирование

Управление
сертификатами

Балансировка
трафика

Безопасность

Инструментарий
для CI/CD

Резервное
копирование

Запуск
legacy-
приложений

Программно-
определяемое
хранилище

Программно-
определяемая
сеть

Managed-
сервисы *

Подсистемы платформы

Оператор
платформы

Механизм модулей

Маркетплейс *

kubernetes

Инфраструктурно-независимый фундамент платформы

Инфраструктура

openstack

vmware
vSphere

Selectel

VK Cloud

Yandex Cloud

и другие...

Графический интерфейс

API-based графический интерфейс администратора и пользователя платформы.

