Nova Container Platform

Nova Container Platform - это комплексная платформа на базе Kubernetes для доставки, развертывания и масштабирования приложений в контейнерах.

В Nova Container Platform привычные технологии Kubernetes дополнены множеством различных инструментов и решений для построения единой среды размещения приложений.

Преимущества использования приложений в контейнерах

Использование приложений в контейнерах обеспечивает ряд существенных преимуществ по сравнению с традиционными подходами к развертыванию. Вместо установки и настройки приложений внутри операционной системы на отдельной виртуальной машине, контейнер позволяет упаковать приложение вместе со всеми необходимыми зависимостями в единый переносимый образ. Такой образ можно запускать в любой среде — в облачной инфраструктуре, в среде виртуализации или на локальном сервере — без необходимости внесения изменений в конфигурацию.

Ключевые преимущества контейнерного подхода:

- Простота создания образа контейнера по сравнению с ВМ.
- Возможность настройки процессов непрерывной интеграции и доставки.
- Возможность быстрого отката версии приложения.

Операционные системы

Контейнеры используют небольшие дистрибутивы ОС семейства Linux без ядра. Их файловая система, сетевая подсистема, контрольные группы (cgroups) изолированы от хостовой ОС. Вы можете развертывать на одном сервере множество разных контейнеров с приложениями, требующими разные ОС или несовместимые зависимости.

Развертывание и масштабирование

С помощью инструментов Kubernetes вы легко можете применять практику непрерывного обновления (rolling update) для вашего приложения без влияния на пользователей. Вы также можете развертывать новую версию приложения в целях тестирования совместно с основной версией.

Поскольку все программные зависимости для приложения находятся внутри контейнера, вы можете использовать любую подходящую под ваши требования ОС. В редких случаях из-за особенности нагрузки вам может потребоваться дополнительная конфигурация ОС на узлах, выделенных под работу вашего приложения.

Для возможности масштабирования приложений в контейнерах Nova Container Platform предлагает как встроенные инструменты Kubernetes, так и дополнительные инструменты. Они позволяют изменять как количество реплик приложений, так и объем потребляемых ими ресурсов на основе оценки данных из пользовательских метрик в системе мониторинга. Это позволяет не только масштабировать требуемые сервисы при росте нагрузке, но и в зависимости от различных параметров (например, бизнес-метрик).

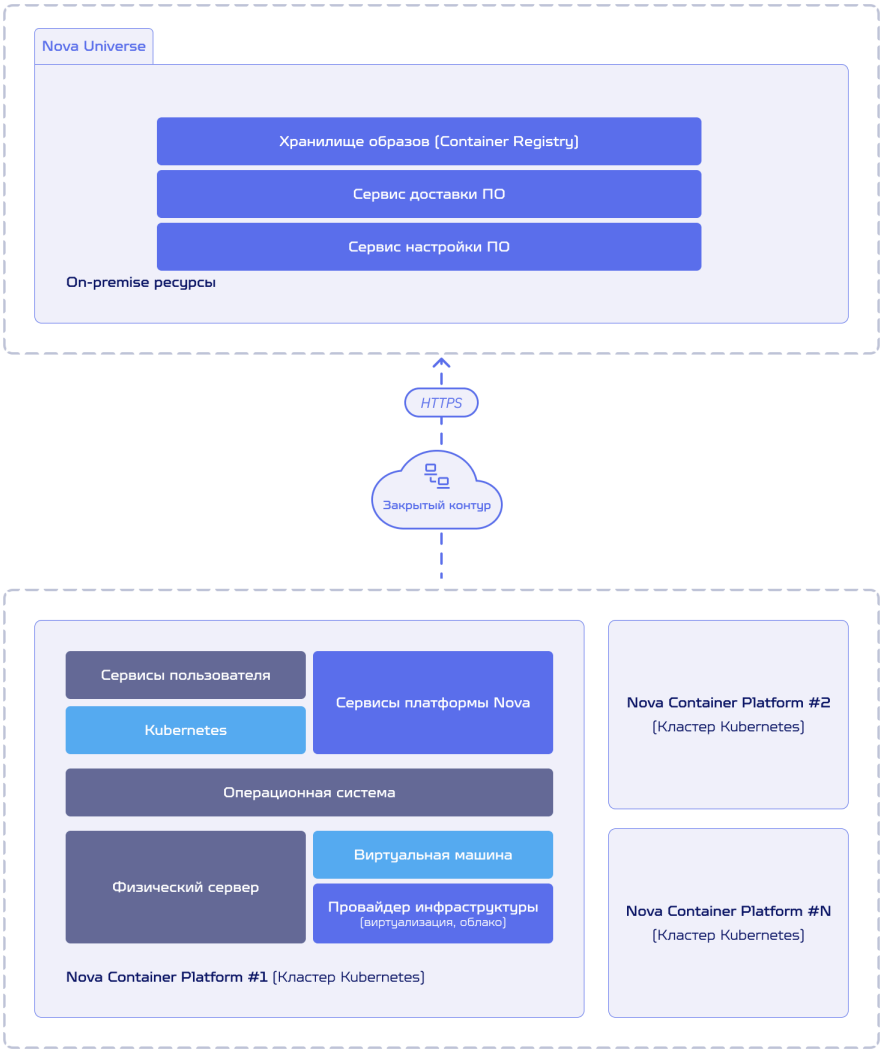
Архитектура платформы

Nova Container Platform состоит из множества компонентов, набор и размещение которых различается в зависимости от метода установки платформы. Компоненты Nova Container Platform могут быть **внешними** и **внутренними**.

В рамках решения zVirt Containers платформа может быть развернута только в закрытом сетевом контуре без доступа к сети Интернет (оффлайн - установка). Для выполнения этой процедуры используется отдельная служебная виртуальная машина Nova Universe, в которой размещаются все необходимые сервисы для установки и дальнейшей эксплуатации кластеров Nova Container Platform.

Внешние компоненты

На схеме ниже приведен Nova Universe, как основной внешний компонент Nova Container Platform, в котором хранятся все необходимые образы для установки и обновления платформы.



- **Хранилище образов**. Отвечает за хранение контейнерных образов, используемых при установке и обновлении компонентов платформы. Обеспечивает доступ к актуальным версиям пакетов.
- **Сервис доставки ПО**. Представляет собой Git-репозиторий, содержащий сценарии и манифесты для развертывания компонентов Nova Container Platform. Используется на этапе автоматической установки.
- **Сервис настройки ПО (Nova Configuration Manager)** Отвечает за генерацию и подготовку конфигураций для установки и обновления платформы. Обеспечивает автоматизацию параметризации среды.
- **Сервер управления (Nova Universe)** Выполняет роль центрального управляющего узла при установке и обслуживании платформы. Обеспечивает автономную работу всех сервисов без подключения к внешним источникам.

Внутренние компоненты

На схеме ниже приведены внутренние компоненты Nova Container Platform.

Внутренние компоненты разделены на модули. Модулем называется ПО (или группа ПО), которое может быть установлено в Nova Container Platform после этапа установки самой платформы. При этом, по-прежнему, в зависимости от среды и метода развертывания платформы, набор компонентов внутри модуля может меняться.

Модули в Nova Container Platform имеют две категории:

- **Базовый модуль**: Устанавливается всегда в любой вариант платформы и содержит ПО для обеспечения ключевого функционала платформы (например, система мониторинга, веб-консоль Nova и т.п.).
- **Дополнительный модуль**: Устанавливается при необходимости только после этапа установки платформы. В дополнительном модуле, как правило, находится ПО, установка которого требует выполнения подготовительных действий (например, планирования ресурсов кластера, архитектуры решения и т.п.). Далее перечислены дополнительные модули платформы. Более подробно можно ознакомиться с ними по ссылкам:
  - NeuVector. Дополнительный модуль, который устанавливается в кластер Kubernetes с целью обеспечить дополнительную безопасность и защиту контейнеров во время их работы.
  - OpenSearch. Дополнительный модуль, позволяющий настроить автоматический сбор логов кластера.
  - Velero. Дополнительный модуль, отвечающий за процессы создания резервной копии компонентов платформы Nova, а также последующее восстановление данных компонентов из этой копии в случае ошибки.
  - Longhorn. Распределенная система хранения данных, разработанная для использования в контейнерных средах, таких как Kubernetes. Представляет из себя блоковое хранилище и обладает рядом функций:
    - **Простота установки и управления**: легко устанавливается в кластер Kubernetes и управляется с помощью стандартных инструментов оркестрации.
    - **Резервное копирование и восстановление**: поддерживает создание резервных копий данных, что упрощает управление данными и позволяет

быстро восстанавливать их в случае сбоя.

- **Масштабируемость**: масштабирует хранилище в зависимости от потребностей, добавляя новые узлы.
- **Высокодоступное хранилище**: обеспечивает репликацию данных и устойчивость к сбоям, что позволяет сохранять данные в случае выхода узлов из строя.

Дистрибутивы всех модулей Nova Container Platform включены в сервер управления Nova Universe. Пользователь платформы может в любой момент времени установить или удалить любой дополнительный модуль.

Обзор компонентов платформы

Кластер Kubernetes

В таблице представлено описание ключевых компонентов кластера Kubernetes в Nova Container Platform:

Компонент	Описание
Containerd	Среда исполнения контейнеров, используемая в Nova Container Platform, совместимая с Kubernetes, предоставляющая интерфейс (CRI) взаимодействия с Kubelet.
Calico CNI	Один из плагинов для сетевых интерфейсов контейнеров (CNI), доступный для установки в Nova Container Platform.
Cilium CNI	Один из плагинов для сетевых интерфейсов контейнеров (CNI), доступный для установки в Nova Container Platform. К данному плагину дополнительно устанавливается ПО Cilium Hubble для отслеживания сетевого взаимодействия контейнеров в реальном времени.
NGINX Ingress	Основной балансировщик нагрузки и сервис-прокси, устанавливаемый в платформу на узлы с ролью `infra` и `ingress`. В Nova Container Platform балансировщики NGINX Ingress имеют два отдельных `DaemonSet`, разделяя нагрузку на служебные и пользовательские сервисы. Тем самым повышается независимость и доступность публикуемых служебных и пользовательских сервисов.
Scheduler	Стандартный компонент Kubernetes, задача которого состоит в определении подходящих узлов для вновь создаваемых `Pod`.
Controller Manager	Стандартный компонент, обеспечивающий основные циклы управления Kubernetes. Controller Manager отслеживает конфигурации в Etcd в кластере и вносит необходимые изменения для достижения указанного состояния какого-либо компонента.

Компонент	Описание
API Server	Стандартный компонент, который предоставляет интерфейс взаимодействия (API) компонентам кластера и пользователям, проверяет и обслуживает их REST-запросы.
Descheduler	Компонент кластера Kubernetes в Nova Container Platform, задача которого поддерживать баланс размещения `Pod` на узлах кластера. Поскольку стандартный Kubernetes Scheduler определяет подходящие узлы для размещения только новых `Pod`, то в динамичной инфраструктуре кластера может возникать разбалансировка ресурсов (например, когда добавляется или удаляется узел кластера, или узел кластера неутилизирован). Descheduler имеет несколько стратегий по оптимизации распределения нагрузки в кластере, а также возможность конфигурации дополнительных стратегий пользователем.
etcd	Основное хранилище данных Kubernetes в формате “ключ-значение”.
Local Path CSI	Компонент кластера Kubernetes в Nova Container Platform, который позволяет утилизировать локальное хранилище на инфраструктурных узлах кластера. Локальное хранилище используется для временного хранения метрик системы мониторинга и данных платформы безопасности Neuvector.
StarVault	Компонент Nova Container Platform для реализации глобального внешнего хранилища секретов, внешней инфраструктуры PKI и OAuth-провайдера аутентификации.
StarVault CSI	Компонент кластера, который позволяет использовать хранилище секретов StarVault в качестве провайдера секретов `SecretProviderClass` для компонента Secrets Store CSI. StarVault CSI позволяет синхронизировать `Secrets` в Kubernetes с хранилищем секретов StarVault. В Nova Container Platform вся чувствительная информация (учетные данные, параметры подключения к OAuth, PKI) хранится в StarVault. Информация, которая должна быть доступна в Kubernetes в виде ресурса `Secret`, передается в кластер с помощью StarVault CSI и Secrets Store CSI и синхронизируется с StarVault на постоянной основе.
StarVault PKI	Инфраструктура PKI, организованная в рамках хранилища секретов StarVault. В Nova Container Platform управление центрами сертификации, а также управление конечными сертификатами Kubernetes интегрировано со StarVault. На узлах кластера не хранятся приватные ключи центров сертификации. Узлы кластера взаимодействуют со StarVault через API для получения или обновления своих сертификатов.
StarVault OAuth	Реализация доступа к ресурсам Nova Container Platform и в частности к Kubernetes API по протоколу OAuth с помощью StarVault OIDC Provider. StarVault позволяет использовать внешних поставщиков аутентификации (например, Active Directory, LDAP, OIDC, Github, Octa), а также имеет собственный каталог пользователей. В Nova Container Platform интеграция с StarVault OAuth также поддерживается и для утилиты `kubectl`.

Компонент	Описание
Secrets Store CSI	Компонент Nova Container Platform, который позволяет с помощью провайдера секретов переносить ключи, секреты или сертификаты в кластер Kubernetes, сохранять их в объектах `Secret` или `ConfigMap` и монтировать в `Pod` в виде тома. В Nova Container Platform поставщиком секретов является хранилище StarVault.
Metrics Server	Компонент Nova Container Platform, отвечающий за предоставление метрик контейнеров. Metrics Server не хранит метрики локально, используется для быстрой оценки использования ресурсов `Pod` и интегрируется через Metrics API со службами автоматического горизонтального масштабирования (Horizontal Pod Autoscaler) и автоматического вертикального масштабирования (Vertical Pod Autoscaler).
Prometheus Adapter	Адаптер Prometheus для Kubernetes Metrics API, позволяющий использовать пользовательские метрики в сценариях автоматического масштабирования.
HPA	Служба автоматического горизонтального масштабирования `Pod` (Horizontal Pod Autoscaler).
VPA	Служба автоматического вертикального масштабирования `Pod` (Vertical Pod Autoscaler).

Сервисы платформы

В таблице ниже представлено описание базовых сервисов платформы, предустанавливаемых в кластер Kubernetes в Nova Container Platform:

Компонент	Описание
Prometheus	Система мониторинга и оповещения в Nova Container Platform.
Grafana	Система визуализации данных мониторинга в Nova Container Platform.
Alertmanager	Компонент системы мониторинга в Nova Container Platform, задача которого обрабатывать поступающие предупреждения, дедуплицировать их, группировать и маршрутизировать получателям согласно установленной конфигурации.
Thanos Query	Масштабируемый компонент системы мониторинга, предназначенный для осуществления запросов в несколько экземпляров Prometheus. Thanos Query устанавливается в кластер, когда количество инфраструктурных узлов три и более.
Logging Operator	Оператор Kubernetes для автоматического развертывания и конфигурации сбора логов с помощью агентов Fluentd или Fluentbit. После установки Nova Container Platform пользователь может сразу настроить сбор логов в кластере и их экспорт во внешнюю систему хранения. Кроме этого, поддерживается интеграция с модулем Opensearch, если пользователь планирует размещать систему хранения логов в кластере Kubernetes.

Компонент	Описание
Opensearch	Масштабируемая платформа с открытым исходным кодом для реализации задач поиска информации, аналитики и визуализации данных. Opensearch является ответвлением коммерческого продукта Elasticsearch. В Nova Container Platform Opensearch может быть установлен опционально для хранения логов компонентов платформы. Поставляется вместе с компонентом Opensearch Dashboards (аналог Elasticsearch Kibana) для визуализации данных.
Fluentd	Аналогичный Fluenbit производительный обработчик логов, предназначенный для сбора данных и их передачи в различные системы. Имеет преимущество перед Fluenbit в количестве доступных плагинов для сбора информации. В Nova Container Platform Fluentd может быть настроен с помощью Logging Operator, а передача данных - в платформу Opensearch.
Neuvector	Комплексная платформа для управления безопасностью в Nova Container Platform. Осуществляет постоянный мониторинг платформы, процессов, файловых систем, поведенческий анализ работы контейнеров. С помощью Neuvector пользователь может выполнять сканирование образов контейнеров в различных хранилищах, проводить аудит безопасности узлов и контейнеров, а также оценивать риски информационной безопасности в различных аспектах.
Secrets Webhook	Webhook для Kubernetes, который широко используется в Nova Container Platform для передачи секретов “на лету” из хранилища StarVault в запускаемое приложение. Перед запуском приложения, Webhook изменяет его манифест и добавляет специальный init-контейнер, который получает из StarVault необходимую информацию (например, данные какой-либо учетной записи) и сохраняет ее в память, доступную для чтения только данному процессу. Таким образом, конфиденциальная информация не хранится ни на узлах кластера, ни в хранилище etcd. Приложения получают доступ только к своим секретам в StarVault на основе Kubernetes RBAC и механизмов безопасности StarVault.
CertManager	Компонент в кластере для управления X.509 сертификатами. В Nova Container Platform CertManager полностью интегрирован с StarVault PKI, и может автоматически выпускать и обновлять сертификаты для конечных приложений.
Gitea	Компонент Nova Container Platform для хостинга и управления Git-репозиториями. Gitea используется для зеркалирования релизного репозитория с конфигурациями сервисов платформы. Gitea является единым источником конфигураций всех сервисов платформы и используется службой непрерывной доставки FluxCD.
FluxCD	Служба непрерывной доставки в Nova Container Platform. Используется для установки и поддержания консистентности конфигураций всех сервисов платформы и дополнительных модулей, размещаемых в Kubernetes. Подробную информацию об архитектуре данной службы можно получить в разделе Непрерывное развертывание и доставка.
Automation Tools (Reflector)	Компонент Nova Container Platform, который выполняет задачи копирования объектов `Secret` и `ConfigMap` между `Namespace` в случаях, когда это необходимо (например, при распространении цепочки доверенных сертификатов).

Компонент	Описание
Automation Tools (Reloader)	Компонент Nova Container Platform, который может выполнять процесс перезапуска (`rollout restart`) объектов `Deployment` , `DaemonSet` , `StatefulSet` при изменении монтируемого ими файла конфигурации в `ConfigMap` или `Secret` .
Nova DNS	Компонент Nova Container Platform на основе CoreDNS, который отвечает за обслуживание DNS-зоны по умолчанию для Ingress-ресурсов. Пользователь также может осуществлять перенаправление запросов с собственных DNS-серверов на инфраструктурные узлы с Nova DNS в случаях, когда не планирует обслуживание DNS-зоны самостоятельно.
Nova Console	Графический веб-интерфейс управления Nova Container Platform, который позволяет выполнять большинство задач по администрированию платформы. Также веб-интерфейс предоставляет отдельный режим для работы пользователей, с помощью которого можно оперативно развертывать приложения и получать данные мониторинга.

О способах установки

Установка Nova Container Platform в рамках решения zVirt Containers поддерживает различное количество конфигураций и сценариев, которые рассмотрены в данном разделе документации.

Инструмент для установки

Решение zVirt Containers предполагает автоматическое развертывание Nova Container Platform и управление платформой через интерфейс Hosted Engine внутри инфраструктуры zVirt. С помощью UI пользователь в интерактивном режиме может указать все необходимые настройки для развертывания кластеров Nova.

Инфраструктура для установки

Установка платформы может быть выполнена двумя методами:

- **Installer-provisioned infrastructure (IPI)**: Автоматизированный метод развертывания в инфраструктуре, подготовленной узлом `nova-ctl` для управления платформой. Данный метод может применяться в средах виртуализации и облачных средах. За счет взаимодействия `nova-ctl` с API провайдера инфраструктуры необходимые узлы платформы (виртуальные машины) могут быть подготовлены автоматически.
- **User-provisioned infrastructure (UPI)**: Автоматизированный метод развертывания в инфраструктуре, подготовленной пользователем. Данный метод обеспечивает полный контроль и кастомизацию инфраструктурного слоя. Перед установкой платформы

пользователь самостоятельно подготавливает необходимые узлы платформы согласно представленным в документации требованиям. Данный метод подходит для развертывания в средах, где взаимодействие узла `nova-ctl` для управления платформой с API провайдера инфраструктуры недоступно, а также в случае развертывания платформы на узлах без использования средств виртуализации.

В таблице ниже приведен сравнительный анализ методов установки:

	IPI	**UPI**
Развертывание с настройками по умолчанию	✅	✅
Возможность кастомизации кластера на этапе установки	✅	✅
Автоматическая подготовка BM	✅	
Привязка шаблонов ОС к группам узлов кластера	✅	
Установка в закрытом сетевом окружении с помощью Universe	✅	✅
Переиспользование существующей сетевой инфраструктуры	✅	✅
Автоматизированное вертикальное масштабирование узлов кластера	✅	
Автоматизированное горизонтальное масштабирование узлов кластера	✅	✅
Автоматизированная установка и настройка компонентов CSI	✅	

Сетевое окружение

В рамках решения zVirt Containers установка платформы может быть выполнена **только в офлайн-режиме**. Установка выполняется в полностью закрытом сетевом окружении. Для установки используется предварительно настроенный **сервер управления Nova Universe**, который предоставляет все необходимые репозитории. Дальнейшее обновление Nova

Container Platform выполняется также с использованием Nova Universe без доступа к сети Интернет.

Узлы платформы

Об узлах платформы

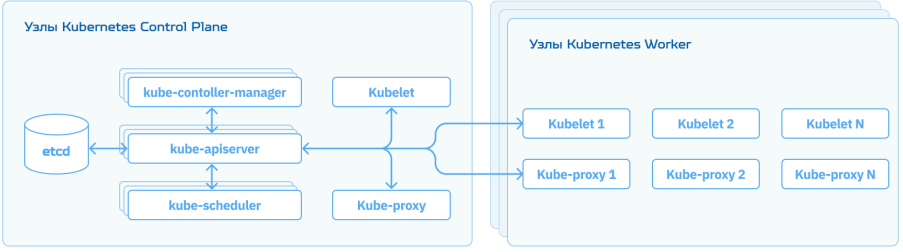
Узлом в Nova Container Platform является виртуальная машина или физический сервер, на котором размещаются компоненты платформы и среды Kubernetes, а также пользовательские приложения. Для стабильной работы приложений важно следить за состоянием узлов, их метриками, своевременно реагировать на возникающие ошибки.

В Nova Container Platform можно получить информацию об узле, его конфигурации и событиях через объект Node в Kubernetes. Для этого можно использовать как утилиту `kubectl`, так и веб-консоль Nova.

Следующие компоненты каждого узла непосредственно обеспечивают работу Pod в среде Kubernetes:

- **Среда исполнения контейнеров (Container Runtime)**: обеспечивает работу контейнеров в ОС. В Nova Container Platform используется среда Containerd, однако, существуют и альтернативные решения, например, cri-o, Docker.
- **Kubelet**: Kubelet работает на каждом узле платформы, выполняет роль агента и промежуточного звена между Kubernetes и службами ОС, обрабатывает запросы на запуск, удаление или изменение контейнеров в составе Pod, контролирует состояние контейнеров, обслуживает задачи на настройке сетевых политик и форвардинга портов. Kubelet управляет только теми контейнерами, создание которых было выполнено через Kubernetes.
- **Kube-proxy**: основной задачей компонента является отслеживание изменений объектов Service и Endpoints в Kubernetes API и трансляция изменений в сетевые правила ОС. В Nova Container Platform компонент Kube-proxy работает в режиме IPVS.

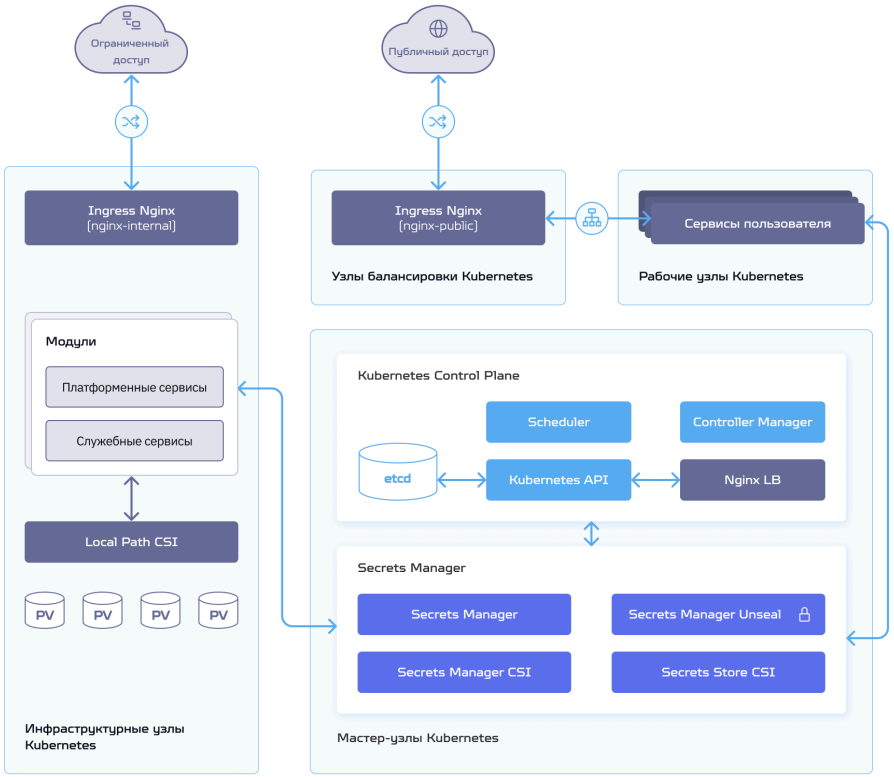
На диаграмме ниже схематично отображены компоненты Kubelet и Kube-proxy.



Роли узлов

В Nova Container Platform предусмотрено использование преднастроенных ролей, определяющих назначение узла в архитектуре кластера и набор компонентов, которые на него устанавливаются. Назначение роли задается при создании или масштабировании кластера и влияет на структуру размещаемых служб.

- `control-plane` — мастер-узлы, обеспечивающие работу управляющих компонентов Kubernetes и платформенных сервисов Nova. Отвечают за планирование, оркестрацию и общее управление кластером.
- `infra` — инфраструктурные узлы, предназначенные для размещения служебных компонентов платформы (например, мониторинг, авторизация, телеметрия).
- `ingress` — узлы, выделенные под обработку входящего сетевого трафика. Включают Ingress-контроллер (по умолчанию — Nginx), выполняющий маршрутизацию запросов к сервисам внутри кластера.
- `worker` — рабочие узлы, на которых размещаются пользовательские приложения, сервисы и любая вычислительная нагрузка.



Преимущества Nova Container Platform

Nova Container Platform дополняет Kubernetes решениями, необходимыми для промышленной эксплуатации кластера, и имеет ключевые преимущества по сравнению с обычным дистрибутивом Kubernetes:

- Автоматизированное обновление компонентов платформы, в том числе компонентов Kubernetes.

- Поддержка сертифицированных российских ОС.
- Интеграция процессов развертывания и управления жизненным циклом с платформами виртуализации.
- Интеграция компонентов с открытым исходным кодом из экосистемы Kubernetes.
- Работа в экосистеме ОРИОН: поддержка платформы виртуализации zVirt Безопасность среды согласно лучшим практикам сообщества Kubernetes и CIS (Center for Internet Security).
- Наличие интегрированных в платформу решений для мониторинга, оповещения, сбора диагностической информации, сбора событий ИБ с инфраструктуры Kubernetes.
- Наличие встроенных инструментов контроля отклонений от желаемой конфигурации как на уровне компонентов кластера, так и на уровне сервисов платформы.
- Наличие полноценного графического веб-интерфейса управления платформой.
- Наличие встроенных инструментов для организации процессов непрерывного развертывания и обновления приложений в кластер Kubernetes.
- Наличие встроенных балансировщиков сетевого трафика для публикации приложений.

Решение zVirt Containers предполагает автоматическое развертывание Nova Container Platform и управление платформой, упрощает запуск, сопровождение и масштабирование контейнерной среды внутри инфраструктуры zVirt.