Глоссарий

Nova Container Platform SE - это платформа, построенная на основе Kubernetes. Поэтому, многие технологии, термины и определения являются общими.

Далее приведен глоссарий основных терминов, устоявшихся выражений, примитивов и определений, которые вы можете встретить в данной документации и при работе с платформой.

1. Общие термины и определения

Admission plugins

Специальные контроллеры Kubernetes, предназначенные для перехвата запросов к серверу Kubernetes API с целью проверки запроса или его изменения. Применяются для контроля настроек безопасности, конфигурации развертывания или количества выделяемых ресурсов.

Bootstrap

Процесс первоначального развертывания платформы Nova Container Platform SE.

Container workloads

Приложения и пользовательские сервисы, упакованные в контейнеры.

Containerd

Среда исполнения контейнеров, совместимая с Kubernetes, предоставляющая интерфейс (CRI) взаимодействия с Kubelet.

Control plane

Control Plane Nodes, Master Nodes

Control plane (плоскость управления) - служебные компоненты, предоставляющие все основные API для обеспечения жизненного цикла контейнеров в Kubernetes (например, `kube-apiserver`, `kube-scheduler`, `kube-controller-manager`). Для компонентов Control Plane, как правило, выделяются отдельные вычислительные мастер-узлы.

Custom Resource (CR)

Объект `CR` является частью какого-либо расширения Kubernetes API.

Deployment

Ресурс в среде Kubernetes, с помощью которого можно управлять жизненным циклом пользовательского приложения.

Dockerfile

Текстовый файл, описывающий конфигурацию сборки контейнера.

Config map

Объект `ConfigMap` предоставляет возможность добавлять конфигурационные данные в Pod. Такие данные можно получить внутри Pod, если к нему примонтировать том с типом `ConfigMap`, после чего приложения в Pod смогут их использовать.

Ingress

Ресурс Kubernetes, предназначенный для публикации сервиса Kubernetes на балансировщике Ingress Controller. С помощью ресурса Ingress можно обеспечить доступ пользователей к приложениями, развернутым в Kubernetes.

Installer-provisioned infrastructure (IPI)

Автоматизированный метод развертывания в инфраструктуре, подготовленной узлом `nova-ctl` для управления платформой.

Kubelet

Компонент Kubernetes (серверный агент), запускаемый на каждом узле кластера и обеспечивающий работу контейнеров в составе Pod.

Namespaces

Ресурс Namespace (пространство имен) предназначен для изоляции групп ресурсов в Kubernetes.

Node

Узел кластера Kubernetes в Nova Container Platform SE. Узел может быть как виртуально машиной, так и физическим сервером.

Pod

Один или более контейнеров с общими ресурсами, такими как тома и IP-адреса. Pod является минимальным определяемым ресурсом для запуска какого-либо приложения в Kubernetes.

Service

Ресурс сервиса Kubernetes обеспечивает единую точку доступа к Pod приложения.

User-provisioned infrastructure (UPI)

Автоматизированный метод развертывания в инфраструктуре, подготовленной пользователем.

Аутентификация

Authentication

Для контроля доступа к кластеру Nova Container Platform SE, администратор кластера может настроить параметры аутентификации пользователей. Это гарантирует доступ к

кластеру только подтвержденным пользователям. Для работы с Nova Container Platform SE необходимо пройти аутентификацию для сервера Kubernetes API с помощью OAuth-токенов или сертификатов TLS, предоставляемых в запросах к Kubernetes API.

Веб-консоль управления кластером

web console

Пользовательский интерфейс графической консоли управления Nova Container Platform SE

Вычислительные узлы

Compute nodes, Worker nodes, Nodes

Узлы кластера, не обслуживающие нагрузки Control Plane. Данные узлы отвечают за работу инфраструктурных сервисов платформы, балансировщиков нагрузки или конечных пользовательских сервисов.

Гибридные развертывания

Развертывания кластера Nova Container Platform SE, в которых часть вычислительных узлов находится в отдельной среде виртуализации, частном или публичном облаке или на физическом оборудовании.

Зеркало хранилища образов контейнеров

mirror registry

Локальное хранилище образов контейнеров, в котором размещаются контейнеры Nova Container Platform SE.

Контейнеры

Containers

Легковесные запускаемые образы, в состав которых входит некоторое ПО и его зависимости. Поскольку в контейнерах виртуализируется операционная система, вы можете запускать контейнеры одинаково в любом совместимом окружении.

Контрольные группы Linux (cgroups)

Control groups

Механизм ОС, с помощью которого для группы процессов на уровне ядра может быть установлена изоляция и ограничения потребляемых ресурсов.

Манифест Kubernetes

kubernetes manifest

Спецификация объекта Kubernetes API в формате JSON или YAML. Один манифест может содержать конфигурацию множества ресурсов Kubernetes (`deployments` , `confgmaps` , `secrets` , `statefulsets`).

Масштабирование

scaling

Увеличение или уменьшение количества ресурсов узлам или приложениям. Масштабирование может быть как горизонтальным (увеличение количества узлов или реплик Pod), так и вертикальным (увеличение количества ресурсов, выделяемых узлу или Pod).

Метаданные

metadata

Любая дополнительная информация, которая может быть указана для ресурса Kubernetes. Как правило, в метаданных находятся метки (`labels`) и аннотации (`annotations`) для ресурсов Kubernetes.

Микросервисы

microservices

Подход к разработке комплексных приложений, предполагающий разделение приложения на минимально возможные небольшие независимые компоненты (микросервисы), способные взаимодействовать по сети.

Монолитные приложения

monolithic applications

Приложение в виде единого общего модуля, в состав которого входят все его компоненты.

Оператор Kubernetes

Operator

Один из способов поставки, развертывания и управления приложениями в Kubernetes.

Отклонение конфигурации

Configuration drift

Ситуация, когда состояние объекта в кластере отличается от состояния, описанного в файле его конфигурации.

Политики доступа

access policies

Набор определенных действий, связанных с некоторыми объектами (пользователь, сущность, приложение) в кластере или за его пределами, определяющий границы их взаимодействия. Политики доступа повышают безопасность работы.

Провайдер инфраструктуры

infrastructure provider

Платформа виртуализации или облачный сервис, предоставляющие API для автоматизированного развертывания объектов инфраструктуры кластера Nova Container Platform SE.

Система управления контейнерами

container orchestration engine

ПО, предназначенное для автоматизации задач развертывания, управления, масштабирования и обеспечения сетевой связанностью контейнеров.

Управление доступом на основе ролей (RBAC)

role-based access control (RBAC)

Основной механизм управления разграничениями доступа к ресурсам кластера на основе ролей.

Хранилище

storage

Nova Container Platform SE поддерживает различные типы хранилищ. По умолчанию, для служебных нужд доступно персистентное хранилище на базе локальных директорий на инфраструктурных узлах кластера.

2. Аутентификация и авторизация

Bearer token

Bearer-токен используется для аутентификации в Kubernetes API. Токен устанавливается в HTTP-запрос в заголовок `Authorization: Bearer <token>`.

Cluster Role

Кластерная роль в RBAC Kubernetes, которая содержит набор правил, определяющих множество разрешений. Кластерная роль содержит только разрешающие правила и не может содержать запрещающих правил. Кластерная роль всегда определяет набор правил на уровне всего кластера, а не пространства имен (*Namespace*) в частности.

Cluster Role Binding

Объект *ClusterRoleBinding* (привязка кластерной роли) необходим для назначения каких-либо разрешений, определенных в роли, к пользователю или группе пользователей. В объекте *ClusterRoleBinding* содержится перечень субъектов (пользователей, групп, сервисных аккаунтов) и указание роли, которая им назначается. Объект *ClusterRoleBinding* используется только в контексте кластера и может ссылаться на любую кластерную роль.

Distinguished Name (DN)

Уникальное имя объекта, по которому данный объект может быть идентифицирован в каталоге LDAP-сервера.

Lightweight directory access protocol (LDAP)

LDAP является протоколом доступа к каталогам. С помощью данного протокола может быть запрошена информация о пользователе.

LDAPS (LDAP over SSL)

LDAP-подключения, защищенные с помощью SSL.

OpenID Connect

Протокол, позволяющий пользователю использовать единую учетную запись и сквозную аутентификацию (SSO) во множестве различных информационных систем.

Role

Роль в RBAC Kubernetes, которая содержит набор правил, определяющих множество разрешений. Роль содержит только разрешающие правила и не может содержать запрещающих правил. Роль всегда определяет набор правил на уровне пространства имен (*Namespace*).

RoleBinding

Объект *RoleBinding* (привязка роли) необходим для назначения каких-либо разрешений, определенных в роли, к пользователю или группе пользователей. В объекте *RoleBinding* содержится перечень субъектов (пользователей, групп, сервисных аккаунтов) и указание роли, которая им назначается. Объект *RoleBinding* используется только в контексте пространств имен (namespace) и может ссылаться на любую роль в том пространстве имен, в котором оно находится.

Аутентификация

Процедура проверки подлинности пользователя различными методами, например, с помощью сравнения введенного и установленного пароля. Выполняется для того, чтобы гарантировать доступ к кластеру только подтвержденным пользователям.

Авторизация

Процедура предоставления прав идентифицированному пользователю. Выполняется для того, чтобы гарантировать выполнение пользователем только тех операций, которые ему разрешены.

Группа

Набор пользователей. Группы удобно использовать, когда необходимо предоставить одинаковые привилегии нескольким пользователем одновременно.

Идентификация

Процедура проверки уникального идентификатора пользователя. Выполняется для того, чтобы однозначно определить существование пользователя в каталоге провайдера идентификации.

Клиент OAuth

Приложение или сервис, которому пользователь делегирует права доступа к своим данным на сервере OAuth. Используется для получения Bearer-токена.

Метод аутентификации

Компонент StarVault, выполняющий задачи по аутентификации пользователей в каком-либо провайдере идентификации и установке пользовательского идентификатора с набором необходимых политик.

Пользователь

Сущность, которая может выполнять запросы к API.

Провайдер идентификации

Встроенный или внешний сервис, предназначенный для хранения и управления пользовательскими идентификационными данными, необходимыми для аутентификации пользователей в Nova Container Platform.

Сервер OAuth

Компонент StarVault в Nova Container Platform имеет встроенный OAuth-сервер, который отвечает за логику работы с провайдерами идентификации и выдачу новых токенов доступа.

Системные пользователи

Пользователи, созданные автоматически в ходе установки Nova Container Platform.

Служебные аккаунты

Служебные аккаунты используются приложениями в кластере Kubernetes.

Управление доступом на основе ролей (RBAC)

Основной механизм управления разграничениями доступа к ресурсам кластера на основе ролей.

3. Управление сертификатами

Инфраструктура открытых ключей

Инфраструктура открытых ключей является набором технических средств, а также распределённых служб и компонентов, в совокупности используемых для поддержки задач шифрования на основе закрытого и открытого ключей.

Центр сертификации

Центр сертификации (удостоверяющий центр) является компонентом инфраструктуры PKI, который выдает цифровые сертификаты, осуществляет их подпись своим открытым ключом и хранит в базе данных сертификатов.

X.509

X.509 определяет стандартные форматы данных и процедуры распределения открытых ключей с помощью соответствующих сертификатов с цифровыми подписями.

Настройка идентификации и аутентификации

Идентификация и аутентификация пользователей в ПО «NOVA Container Platform Special Edition» осуществляется с учетом требований разделов 4-7 ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие положения».

Компонент StarVault в Nova Container Platform имеет встроенный OAuth-сервер, который отвечает за логику работы с провайдерами идентификации и выдачу новых токенов доступа.

После установки платформы администратор может выполнить настройку методов аутентификации в StarVault, подключив различные провайдеры аутентификации.

1. Провайдер идентификации по умолчанию

По умолчанию, после установки Nova Container Platform сконфигурирован внутренний провайдер идентификации `Username`.

Данный провайдер содержит одну учетную запись kubeadmin, находящуюся в группе `kubeadmins`.

В Kubernetes создан объект ClusterRoleBinding nova: `kubeadmins`, описывающий привязку кластерной роли cluster-admin к группе kubeadmins.

2. Поддерживаемые провайдеры идентификации

Вы можете использовать следующие провайдеры идентификации в Nova Container Platform (указаны в таблице ниже).

Поддерживаемые провайдеры идентификации

Провайдер идентификации	Описание
`Username`	Настройка выполняется с помощью метода аутентификации **userpass** (Username & Password). Используется внутреннее хранилище учетных данных StarVault

Провайдер идентификации	Описание
`Token`	Для аутентификации используется токен доступа к StarVault. Может быть создан администратором и использован в случаях, когда необходимо предоставить краткосрочный доступ к кластеру Kubernetes без создания дополнительных пользователей
`LDAP`	Настройка выполняется с помощью метода аутентификации **ldap**. В качестве служб каталогов могут использования решения, поддерживающие LDAPv3, например, FreeIPA, Microsoft Active Directory, OpenLDAP и другие
`OIDC`	В качестве провайдеров идентификации могут быть использованы решения, поддерживающие протокол OpenID Connect (OIDC), например, Keycloak, Dex, Vault, Gitlab и другие
`Okta`	Аутентификация через интеграцию с облачной службой идентификации Okta
`RADIUS`	RADIUS Аутентификация через провайдер идентификации по протоколу RADIUS
`GitHub`	Аутентификация через интеграцию с сервисом GitHub

После настройки провайдера идентификации вы можете перейти к настройке RBAC в Kubernetes.

3. Рекомендуется к ознакомлению

- Настройка централизованного управления образами контейнеров и контейнерами