Архитектура DNS в Nova Container Platform SE

Nova Container Platform SE предлагает несколько возможных конфигураций системы разрешения имен (DNS) в кластере Kubernetes. В данном разделе представлена детальная информация о конфигурациях и рекомендации по их выбору.

1. О DNS в Kubernetes

Система DNS является неотъемлемой частью среды Kubernetes и предназначена для управления DNS-записями объектов *Service* и *Pod*. Пользователь Kubernetes может обратиться к данным объектам, используя постоянные DNS-имена вместо внутренних IP-адресов. Для обслуживания DNS-зон и процессов Service Discovery применяется решение CoreDNS.

Kubernetes автоматически управляет системой DNS и публикует информацию об объектах *Pod* и *Service*. Компонент *Kubelet* вносит настройки DNS в *Pod*, после чего контейнеры внутри *Pod* могут разрешать запросы как в пределах кластера Kubernetes, так и за его пределами.

Всем объектам *Service* в кластере Kubernetes присваивается постоянное DNS-имя, которое разрешается либо во внутренний IP-адрес самого объекта *Service*, либо в IP-адреса объектов *Pod*, которые составляют данный сервис. По умолчанию, домены поиска каждого объекта Pod содержат свое собственное пространство имен, а также кластерный DNS-домен по умолчанию.

Подробную информацию об устройстве системы DNS в Kubernetes вы можете получить в разделе официальной документации DNS for Services and Pods.

2. О Nova DNS

В Nova Container Platform SE по умолчанию используется дополнительный компонент Nova DNS, который расширяет систему разрешения имен и решает ряд конфигурационных задач в различных аспектах.

В основе Nova DNS также используется решение CoreDNS. Компонент тесно интегрирован с DNS-службой Kubernetes и решает следующие задачи:

- Обслуживает DNS-зону базового DNS-домена.

- Перенаправляет запросы к записям зоны базового DNS-домена, когда зона обслуживается инфраструктурными (пользовательскими) DNS-серверами.
- Принимает запросы от инфраструктурных (пользовательских) DNS-серверов и разрешает записи зоны базового DNS-домена.

Таким образом, компонент Nova DNS позволяет использовать следующие подходы к организации системы разрешения имен:

- Полностью обслуживать DNS-зону базового DNS-домена средствами кластера Kubernetes.
- Обеспечить интеграцию с инфраструктурными (пользовательскими) DNS-серверами через организацию перенаправления запросов к базовому DNS-домену.
- Обеспечить интеграцию с инфраструктурными (пользовательскими) DNS-серверами через организацию приема запросов к базовому DNS-домену от инфраструктурных (пользовательских) DNS-серверов.

3. Зона DNS по умолчанию

DNS-зона по умолчанию (или базовый домен) необходимы в Nova Container Platform SE для разрешения имен платформенных сервисов. DNS-зона по умолчанию обязательна, однако ее размещение и характер взаимодействия с ней могут быть изменены пользователем на этапе установки платформы.

Перед установкой платформы пользователь указывает в конфигурационном манифесте параметр dnsBaseDomain, который определяет базовый домен и соответствующую wildcard-запись для разрешения имен платформенных сервисов.

Пример имен платформенных сервисов, доступных после установки платформы, используя параметр `dnsBaseDomain` со значением `nova.internal`:

- nova-release-git-main.nova.internal
- nova-console.nova.internal
- nova-oauth.nova.internal
- nova-alertmanager-main.nova.internal
- nova-grafana-main.nova.internal
- nova-prometheus-main.nova.internal

В примере, представленном выше, все имена платформенных сервисов находятся в DNS-зоне `nova.internal`, а wildcard-запись, с помощью которой разрешаются данные имена, имеет вид `*.nova.internal`.

DNS-имена платформенных сервисов предопределены в Nova Container Platform SE и не могут быть изменены.

Обслуживание DNS-зоны по умолчанию осуществляется компонентом Nova DNS. Поскольку доступ к платформенным сервисам осуществляется через балансировщики нагрузки, расположенные на инфраструктурных узлах, то запись `*.nova.internal` должна разрешаться в IP-адреса инфраструктурных узлов платформы.

4. Режимы работы DNS

Nova Container Platform SE поддерживает три режима работы компонента Nova DNS.

В диаграммах, представленных далее, IP-адреса и конфигурации DNS-серверов приведены в качестве примера и могут отличаться в зависимости от вашей инфраструктуры и используемого ПО.

4.1. Внутренний режим

Внутренний режим используется, когда в пользовательской инфраструктуре полностью отсутствует какая-либо служба DNS либо доступ к ней невозможен. Если вам не требуется интеграция с вашими DNS-серверами, а обслуживание DNS-зоны достаточно осуществлять только в пределах кластера Kubernetes, то используйте данный режим.

При использовании внутреннего режима Nova DNS для доступа к веб-интерфейсам платформенных сервисов необходимо использовать статические записи *hosts* в вашей ОС.

Ниже на схеме представлен принцип работы DNS во внутреннем режиме.

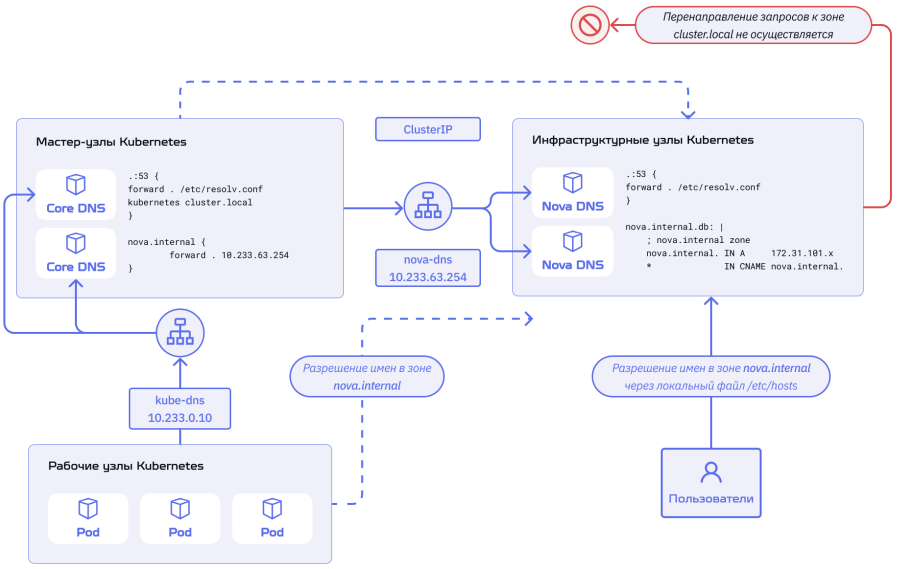

Рисунок 1. Внутренний режим работы Nova DNS в Nova Container Platform SE

1. Пользовательские сервисы (объекты *Pod*) настроены на использование DNS-сервера по умолчанию - `kube-dns`. Объект *Service* с типом *ClusterIP* предоставляет единый IP-адрес для балансировки запросов к объектам *CoreDNS Pod*.
2. Объекты *CoreDNS Pod* обслуживают основную зону Kubernetes `kubernetes.local`, все запросы к зоне `nova.internal` направляют в IP-адрес сервиса `nova-dns`, а остальные запросы направляют в хостовые DNS-серверы, указанные в файле `/etc/resolv.conf`.
3. Объекты *Nova DNS Pod* принимают и обрабатывают запросы к зоне `nova.internal`.
4. Для разрешения имен платформенных сервисов пользователи добавляют в локальный файл `/etc/hosts` необходимые записи, указывающие на IP-адреса инфраструктурных узлов.

Внутренний режим Nova DNS устанавливается по умолчанию, если блок конфигурации extraOptions не заполнен в конфигурационном манифесте.

4.2. Внешний режим

Внешний режим используется, когда DNS-зона и другие записи обслуживаются только инфраструктурными (пользовательскими) серверами DNS. Если вы планируете управлять DNS-зоной самостоятельно, то воспользуйтесь данным режимом. В данном режиме компонент Nova DNS не разворачивается в кластере Kubernetes.

Ниже на схеме представлен принцип работы DNS во внешнем режиме.

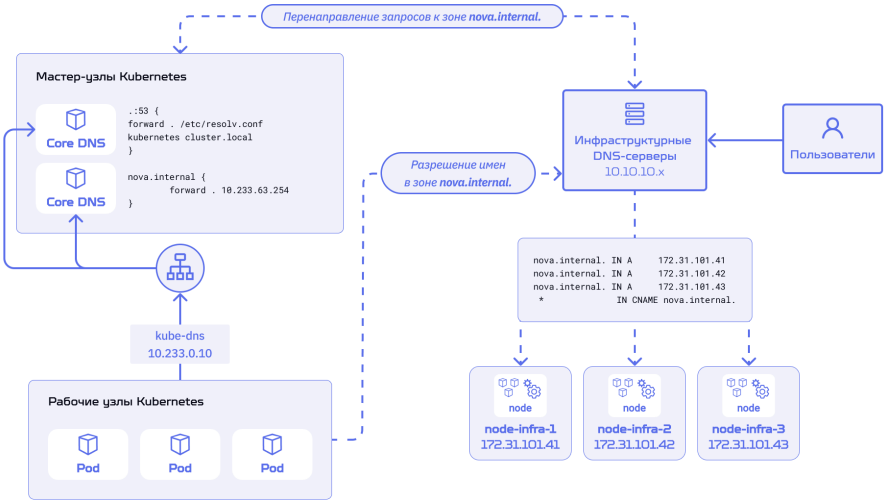

Рисунок 2. Внешний режим работы Nova DNS в Nova Container Platform SE

1. Пользовательские сервисы (объекты *Pod*) настроены на использование DNS-сервера по умолчанию - `kube-dns`. Объект *Service* с типом *ClusterIP* предоставляет единый IP-адрес для балансировки запросов к объектам *CoreDNS Pod*.
2. Объекты *CoreDNS Pod* обслуживают основную зону Kubernetes `kubernetes.local`, все запросы к зоне `nova.internal` направляют в IP-адреса инфраструктурных DNS-серверов, а остальные запросы направляют в хостовые DNS-серверы, указанные в файле `/etc/resolv.conf`.
3. Для разрешения имен платформенных сервисов пользователи используют стандартные настройки DNS в собственной инфраструктуре.

Для настройки внешнего режима Nova DNS на этапе установки платформы вы можете использовать пример конфигурационного манифеста ниже.

YAML

```yaml
apiVersion: "config.nova-platform.io/v1alpha3"
kind: "Infrastructure"
metadata:
  name: "cluster"
spec:
  clusterConfiguration:
    extraOptions:
      dns:
        customerDns:
          enable: true
          forwardZones:
          - name: nova.internal
            server: 10.0.0.1
          - name: acme.corp
            server: 10.0.0.2
```

Если в списке DNS-зон *forwardZones* присутствует базовая DNS-зона, то компонент Nova DNS в кластере не устанавливается.

Пример выше описывает конфигурацию, в результате которой системный компонент *CoreDNS* будет иметь две дополнительные зоны `nova.internal` и `acme.corp` с перенаправлением запросов на пользовательские серверы `10.0.0.1` и `10.0.0.2` соответственно.

4.3. Гибридный режим

Гибридный режим используется, когда вам необходимо сохранить обслуживание базовой DNS-зоны компонентом Nova DNS в пределах кластера Kubernetes, но инфраструктурные (пользовательские) серверы DNS должны перенаправлять DNS-запросы на серверы Nova DNS.

Доступ к DNS-серверам Nova DNS осуществляется по стандартным портам и протоколам `tcp/53` и `udp/53` через инфраструктурные узлы. Публикация данных портов осуществляется с помощью TCP/UDP балансировки компонента Ingress Controller.

Информация

Для перехода из внутреннего режима в гибридный вам достаточно на собственных DNS-серверах настроить перенаправление запросов к DNS-зоне по умолчанию на инфраструктурные узлы Nova Container Platform SE. Переход из внутреннего или гибридного режима во внешний не поддерживается.

Ниже на схеме представлен принцип работы DNS в гибридном режиме.

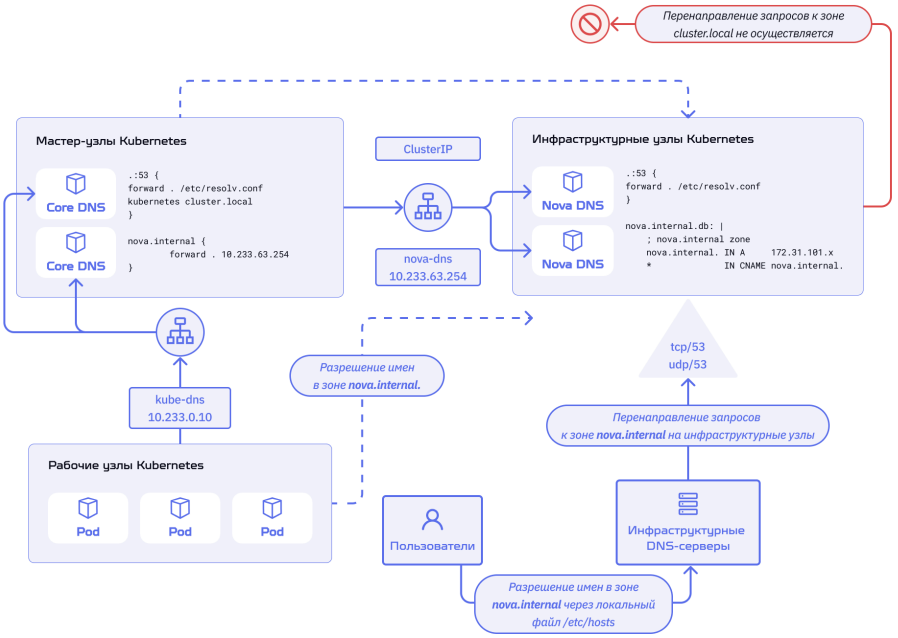

Рисунок 3. Гибридный режим работы Nova DNS в Nova Container Platform SE

1. Пользовательские сервисы (объекты *Pod*) настроены на использование DNS-сервера по умолчанию - `kube-dns`. Объект *Service* с типом *ClusterIP* предоставляет единый IP-адрес для балансировки запросов к объектам *CoreDNS Pod*.
2. Объекты *CoreDNS Pod* обслуживают основную зону Kubernetes `kubernetes.local`, все запросы к зоне `nova.internal` направляют в IP-адрес сервиса `nova-dns`, а остальные запросы направляют в хостовые DNS-серверы, указанные в файле `/etc/resolv.conf`.
3. Объекты *Nova DNS Pod* принимают и обрабатывают запросы к зоне `nova.internal`.
4. Инфраструктурные (пользовательские) DNS-серверы перенаправляют запросы пользователей к зоне `nova.internal` на инфраструктурные узлы платформы (сервисы Nova DNS).
5. Для разрешения имен платформенных сервисов пользователи используют стандартные настройки DNS в собственной инфраструктуре.

Гибридный режим Nova DNS аналогичен внутреннему и устанавливается по умолчанию, если блок конфигурации extraOptions не заполнен в конфигурационном манифесте.

5. Дополнительные параметры DNS

Кроме выбора режимов работы DNS в Nova Container Platform SE вы также можете указать дополнительные параметры и DNS-имена некоторых служебных компонентов на этапе установки платформы:

- DNS-зона кластера Kubernetes
- DNS-имя сервера Kubernetes API

- Дополнительные DNS-имена и IP-адреса Kubernetes API
- Пользовательские DNS-серверы

5.1. DNS-зона кластера Kubernetes

По умолчанию, в Nova Container Platform SE используется DNS-зона `cluster.local`. Однако, при необходимости, вы можете изменить ее, используя параметр k8sDefaultDnsZone

5.2. Kubernetes API

По умолчанию, в Nova Container Platform SE не используется отдельное публичное DNS-имя для API-сервера Kubernetes. В веб-консоли Nova, а также в конфигурациях `kubeconfig` вам будет доступен IP-адрес первого мастер-узла кластера Kubernetes.

Однако, для удобства вы можете установить DNS-имя по умолчанию для Kubernetes API, используя параметр k8sAPIDefaultFqdn на этапе установки платформы.

Если вам необходимо добавить дополнительные DNS-имена и IP-адреса Kubernetes API, например, для доступа по альтернативным именам или с сетевых балансировщиков, то воспользуйтесь параметром k8sAPIAdditionalSANs.

5.3. Пользовательские серверы DNS по умолчанию

Если вам необходимо добавить список собственных DNS-серверов, которые должны использоваться по умолчанию в среде Kubernetes, то воспользуйтесь параметром servers. В данном случае служба CoreDNS будет перенаправлять все запросы именно на ваш список серверов вместо записей в хостовом файле `/etc/resolv.conf`.

Интеграция с инфраструктурными провайдерами

Nova Container Platform SE поддерживает различные провайдеры инфраструктуры. Для взаимодействия с ними установщик платформы `nova-ctl` использует *Terraform* и его плагины (инфраструктурные провайдеры).

В плагине *Terraform* реализованы механизмы управления инфраструктурными объектами через API. Утилита `nova-ctl` имеет в составе все поддерживаемые инраструктурные провайдеры, а для их работы не требуется иметь доступ в Интернет. Все операции с инфраструктурными провайдерами выполняются прозрачно для пользователя.

Провайдеры инфраструктуры *Terraform* разрабатываются сообществом и ОРИОН для совместимости с Nova Container Platform SE.

1. Поддерживаемые интеграции

Вы можете получить актуальный перечень поддерживаемых провайдеров инфраструктуры в разделе Перечень матриц совместимости и протестированных интеграций.

2. Использование в Nova Container Platform SE

Перед установкой платформы пользователь может получить предзаполненные установочные манифесты (шаблоны конфигураций) с помощью `nova-ctl init`. Далее nova-ctl в интерактивном режиме запрашивает у пользователя тип инфраструктуры, в которой планируется установка, и предоставляет шаблон с блоком конфигурации необходимого провайдера инфраструктуры.

Заполнение установочного манифеста выполняется строго в соответствии с параметрами объекта *Infrastructure* в API-группе *config.nova-platform.io*. `nova-ctl` обрабатывает полученные из манифеста данные и автоматически подготавливает конфигурационные файлы Terraform. Пользователь также дополнительно уведомляется об изменениях, которые будут внесены в инфраструктуру, например, создание необходимого количества ВМ, дисков, сетевых интерфейсов и т.п.

Процесс использования провайдеров инфраструктуры в Nova Container Platform SE на этапе развертывания представлен на схеме ниже.

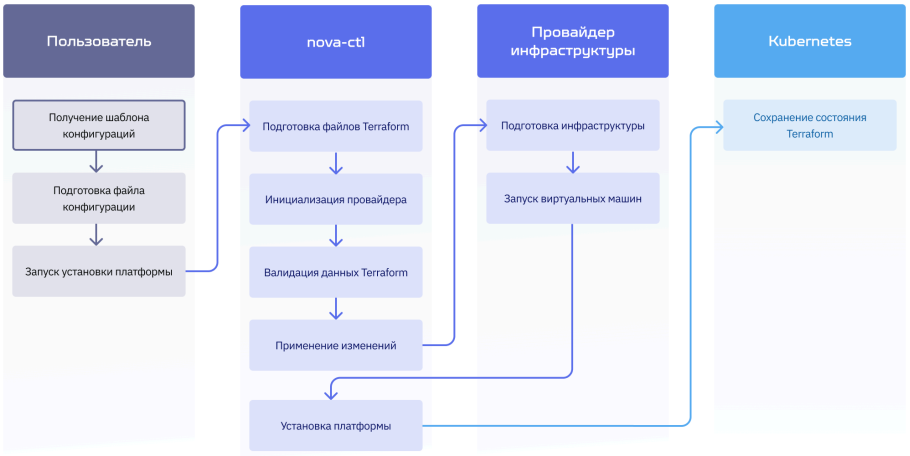

Рисунок 1. Процесс использования провайдеров инфраструктуры в Nova Container Platform SE

До инициализации кластера Kubernetes `nova-ctl` хранит состояние объектов *Terraform* локально, а после его инициализации сохраняет состояние в кластер Kubernetes в объект *ConfigMap*. При масштабировании кластера Kubernetes `nova-ctl` также работает с блокировками Terraform, которые управляются автоматически объектом *TerraformLock* в API-группе *config.nova-platform.io* в Kubernetes.

Схема, представленная ниже, демонстрирует процесс масштабирования кластера в контексте взаимодействия `nova-ctl` и пользователя с кластером Kubernetes.

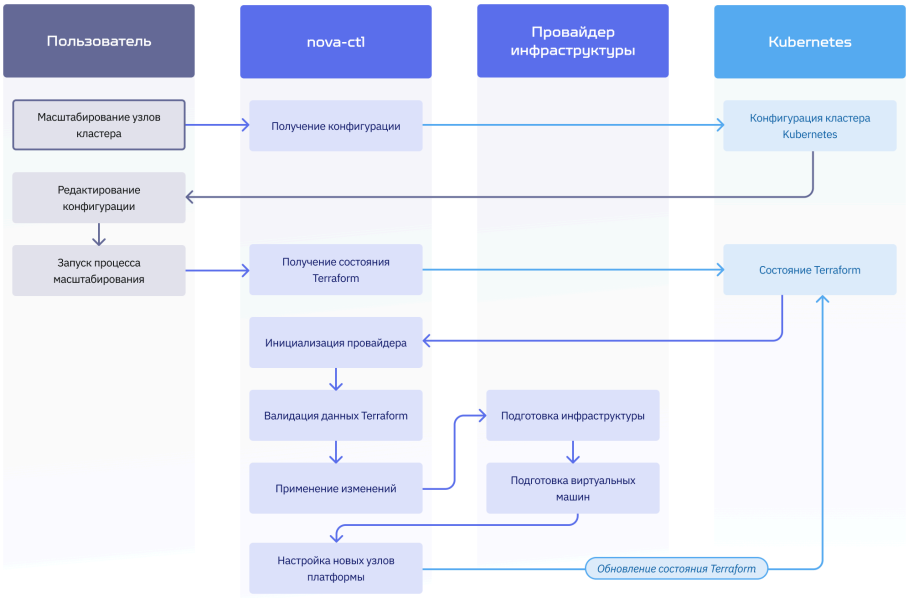

Рисунок 2. Процесс масштабирования кластера Nova Container Platform SE