Автоматизированная установка (IPI)

При использовании автоматизированного метода установки (IPI) нет необходимости настраивать каждый узел платформы вручную. Достаточно создать и настроить шаблон узла, который будет применяться в процессе установки. Далее узел nova-ctl самостоятельно развернет кластер, используя API поддерживаемой платформы виртуализации и частного облака, что значительно упрощает и ускоряет развертывание всей системы.

На текущий момент поддерживаются платформы виртуализации и частные облака, описанные в статье.

- Nova Container Platform на текущий момент не поддерживает IPv6.

Содержание раздела

Выберите один из следующих шагов в зависимости от планируемого метода установки платформы.

- Если планируется устанавливать платформу в среде zVirt:

  Установка в среде zVirt

- Если планируется устанавливать платформу в среде vSphere:

  Установка в среде vSphere

Подготовка сетевого окружения

1. DNS записи для встроенных сервисов

Важно: Подготовка DNS-записей должна быть выполнена до установки Nova Container Platform SE. Во избежание задержек при развертывании кластера, необходимо заранее зарезервировать и настроить DNS-имена, указывающие на infra-узлы кластера. Эти DNS-записи будут использоваться встроенными компонентами платформы.

Рекомендуемые DNS-записи для базовой установки:

- `nova-release-git-main.nova.mycompany.local`
- `nova-console.nova.mycompany.local`
- `nova-oauth.nova.mycompany.local`
- `nova-alertmanager-main.nova.mycompany.local`
- `nova-grafana-main.nova.mycompany.local`
- `nova-prometheus-main.nova.mycompany.local`

Дополнительные записи при использовании модулей OpenSearch и NeuVector:

- `nova-neuvector-ui.nova.mycompany.local`
- `nova-neuvector-api-docs.nova.mycompany.local`
- `nova-logs-main.nova.mycompany.local`

Не забудьте заменить `nova.mycompany.local` на `dnsBaseDomain`, указанный в манифесте `nova-deployment-conf.yaml`.

2. Внешние взаимодействия

Установка Nova Container Platform SE выполняется только с помощью сервера управления Nova Universe.

Сервер управления Nova Universe поддерживает использование IP-адреса, настроенного как с помощью DHCP, так и заданного статически. Рекомендуется размещать сервер управления в отдельной от кластеров Kubernetes сети.

- Если вы используете DHCP-сервер для настройки сетевого интерфейса сервера, необходимо настроить его на предоставление постоянного IP-адреса и сведений о DNS-серверах.
- Сервер управления Nova Universe на текущий момент не поддерживает IPv6.

Требования к DNS: Для установки платформы с использованием Nova Universe требуется внутренний DNS-сервер, при этом создание записей в нем является обязательным условием. При использовании внешнего DNS-сервера, например `8.8.8.8`, **невозможно** установить платформу.

Правила доступа к сети с сервером управления Nova Universe из сетей узлов Kubernetes приведены в таблице:

Ресурс	DNS-имя	Порт	IP-адрес
Хранилище образов	hub.*DNS-имя Nova Universe*	https/443	IP-адрес Nova Universe
Сервис доставки ПО	hub.*DNS-имя Nova Universe*	https/443	IP-адрес Nova Universe
Сервис настройки ПО	sun.*DNS-имя Nova Universe*	https/443	IP-адрес Nova Universe
Репозиторий пакетов	repo.*DNS-имя Nova Universe*	https/443	IP-адрес Nova Universe
Сервис загрузки обновлений	uploads.*DNS-имя Nova Universe*	https/443	IP-адрес Nova Universe

3. Внутренние взаимодействия

В данном разделе описаны требования для развертывания Nova Container Platform SE в подготовленной пользователем инфраструктуре.

3.1. Требования к межсетевому экранированию

Для корректной установки и функционирования Nova Container Platform SE убедитесь, что в пределах сетевого сегмента (сегментов), в котором располагаются узлы платформы, настроен представленный ниже перечень сетевых правил, либо ограничения по сетевому взаимодействию узлов отсутствуют.

3.1.1. Узел nova-ctl для управления платформой

Источник	Адресат	Тип трафика	Порт/Протокол	Описание
Узел `nova-ctl`	Мастер-узлы	Входящий	6443/tcp	Kubernetes API

Источник	Адресат	Тип трафика	Порт/Протокол	Описание
Узел `nova-ctl`	Мастер-узлы	Входящий	8200/tcp	StarVault API
Узел `nova-ctl`	Все узлы	Входящий	22/tcp	SSH
Узел `nova-ctl`	Инфраструктурные узлы	Входящий	80/tcp	Ingress Nginx Controller HTTP
Узел `nova-ctl`	Инфраструктурные узлы	Входящий	443/tcp	Ingress Nginx Controller HTTPS

3.1.2. Мастер-узлы кластера Kubernetes

Источник	Адресат	Тип трафика	Порт/Протокол	Описание
Все узлы, АРМ пользователей платформы	Мастер-узлы	Входящий	6443/tcp	Kubernetes API
Все узлы	Мастер-узлы	Входящий	8200/tcp	StarVault API
Все узлы	Мастер-узлы	Входящий	2379/tcp	Etcd Client Requests
Инфраструктурные узлы	Мастер-узлы	Входящий	10259/TCP	Kubernetes Scheduler metrics
Инфраструктурные узлы	Мастер-узлы	Входящий	10257/TCP	Kubernetes Controller Manager metrics
Мастер-узлы	Мастер-узлы	Двунаправленный	8201/tcp	StarVault Cluster Endpoint
Мастер-узлы	Мастер-узлы	Двунаправленный	2380/tcp	Etcd Peer Requests
Мастер-узлы	Все узлы	Исходящий	10250/TCP	Kubelet

3.1.3. Инфраструктурные узлы кластера Kubernetes

Источник	Адресат	Тип трафика	Порт/Протокол	Описание
Все узлы, АРМ пользователей платформы	Инфраструктурные узлы	Входящий	80/tcp	Ingress Nginx Controller HTTP
Все узлы, АРМ пользователей платформы	Инфраструктурные узлы	Входящий	443/tcp	Ingress Nginx Controller HTTPS

Источник	Адресат	Тип трафика	Порт/Протокол	Описание
Все узлы	Инфраструктурные узлы	Входящий	8443/tcp	Ingress Nginx Controller Validating webhook
Инфраструктурные узлы	Все узлы	Исходящий	9100/tcp	Prometheus Node Exporter
Инфраструктурные узлы	Мастер-узлы	Исходящий	10259/TCP	Kubernetes Scheduler metrics
Инфраструктурные узлы	Мастер-узлы	Исходящий	10257/TCP	Kubernetes Controller Manager metrics
Инфраструктурные узлы	Все узлы	Исходящий	10250/TCP	Kubelet
Инфраструктурные узлы	Инфраструктурные узлы	Исходящий	10249/tcp	Kube Proxy metrics

3.1.4. Узлы балансировки входящих запросов кластера Kubernetes (Ingress-узлы)

Источник	Адресат	Тип трафика	Порт/Протокол	Описание
Все узлы, APM пользователей платформы	Ingress-узлы	Входящий	80/tcp	Ingress Nginx Controller HTTP
Все узлы, APM пользователей платформы	Ingress-узлы	Входящий	443/tcp	Ingress Nginx Controller HTTPS
Все узлы	Ingress-узлы	Входящий	8443/tcp	Ingress Nginx Controller Validating webhook
Инфраструктурные узлы	Ingress-узлы	Входящий	10254/TCP	Ingress Nginx Controller metrics

Если в конфигурации кластера Nova Container Platform SE не используются выделенные Ingress-узлы, то все правила для Ingress-узлов необходимо применить к рабочим узлам (Worker).

3.1.5. Все узлы кластера Kubernetes

Источник	Адресат	Тип трафика	Порт/Протокол	Описание
Все узлы	Все узлы	Двунаправленный	179/tcp	BGP
Все узлы	Все узлы	Двунаправленный	4789/udp	VXLAN Overlay
Все узлы	Все узлы	Двунаправленный	8472/udp	VXLAN Overlay
Все узлы	Все узлы	Двунаправленный	IPIP (4)	IP in IP Protocol
Инфраструктурные узлы	Все узлы	Входящий	9100/tcp	Prometheus Node Exporter
Инфраструктурные узлы	Все узлы	Входящий	10249/tcp	Kube Proxy metrics
Инфраструктурные узлы и мастер-узлы	Все узлы	Входящий	10250/tcp	Kubelet
Все узлы	Мастер-узлы	Исходящий	2379/tcp	Etcd Client Requests
Все узлы	Мастер-узлы	Исходящий	8200/tcp	StarVault API
Все узлы	Инфраструктурные узлы	Исходящий	80/tcp	Ingress Nginx Controller HTTP (Internal)
Все узлы	Инфраструктурные узлы	Исходящий	443/tcp	Ingress Nginx Controller HTTPS (Internal)
Все узлы	Инфраструктурные узлы, Ingress-узлы	Исходящий	8443/tcp	Ingress Nginx Controller Validating webhook
Все узлы	Мастер-узлы	Исходящий	6443/tcp	Kubernetes API

Если установку Nova Container Platform SE планируется выполнять с использованием HTTP-прокси, необходимо добавить в список разрешающих правил доступ (исходящий трафик) к HTTP-прокси со всех узлов платформы.

3.1.6. АРМ пользователей платформы

Источник	Адресат	Тип трафика	Порт/Протокол	Описание
АРМ пользователей платформы	Ingress-узлы	Исходящий	80/tcp	Ingress Nginx Controller HTTP (Public)

Источник	Адресат	Тип трафика	Порт/Протокол	Описание
АРМ пользователей платформы	Ingress-узлы	Исходящий	443/tcp	Ingress Nginx Controller HTTPS (Public)
АРМ пользователей платформы	Инфраструктурные узлы	Исходящий	80/tcp	Ingress Nginx Controller HTTP (Internal)
АРМ пользователей платформы	Инфраструктурные узлы	Исходящий	443/tcp	Ingress Nginx Controller HTTPS (Internal)
АРМ пользователей платформы	Мастер-узлы	Исходящий	6443/tcp	Kubernetes API

При развертывании Nova Container Platform SE в публичных облаках за контроль сетевого взаимодействия, как правило, отвечает как функционал списков контроля доступа (Network ACL), так и функционал групп безопасности. В данном случае убедитесь, что настроенные в инфраструктуре правила не пересекаются и не блокируют друг друга. Вы также можете добавить узлы платформы в одну общую группу безопасности, в рамках которой сетевое взаимодействие не ограничивается.

3.2. Требования к сетевым балансировщикам

Для работы внутренних компонентов Nova Container Platform SE не требуется наличие внешних сетевых балансировщиков в пользовательской инфраструктуре.

Конфигурация кластера предусматривает наличие необходимых встроенных механизмов для обеспечения отказоустойчивого доступа к компонентам Kubernetes API и Ingress.

Однако, если вы хотите обеспечить внешний отказоустойчивый доступ пользователей к компонентам Kubernetes API и Ingress, следует учесть следующие требования к настройке собственных сетевых балансировщиков:

Балансировщик Kubernetes API предоставляет общую точку подключения пользователю и сервисам для работы с кластером.

- Поддерживается только Layer-4 балансировка (Raw TCP, SSL Passthrough).

Для работы с Kubernetes API не требуется настройка сохранения сессий (персистентность).

На сетевом балансировщике должны быть настроены следующие порты:

Порт	Backend-узлы	Внутренний доступ	Внешний доступ	Описание
6443	**Мастер-узлы.** Для проверки доступности узла (healthcheck) необходимо настроить HTTP-проверку, используя путь `/readyz`.	Да	Да	Kubernetes API

Балансировщики Ingress предоставляют общую точку подключения пользователям и сервисам для работы с веб-сервисами, публикуемыми через Ingress-контроллеры, а также сервисами Kubernetes, для которых используется Layer-4 балансировка средствами Ingress-контроллера.

- Поддерживается Layer-4 балансировка (Raw TCP, Raw UDP, SSL Passthrough).
- Поддерживается Layer-7 балансировка для доступа к публикуемым веб-сервисам.

Использование дополнительной Layer-7 балансировки для доступа к публикуемым веб-сервисам может привести к увеличению затрат на их настройку и поддержание стабильности сессий и подключений.

На сетевом балансировщике должны быть настроены следующие порты:

Порт	Backend-узлы	Внутренний доступ	Внешний доступ	Описание
80	***Инфраструктурные узлы***. Для проверки доступности узла (healthcheck) необходимо настроить HTTP-проверку, используя путь `/healthz`.	Да	Да	Доступ к служебным веб-сервисам Ingress по HTTP.
443	***Инфраструктурные узлы.*** Для проверки доступности узла (healthcheck) необходимо настроить HTTP-проверку, используя путь `/healthz`.	Да	Да	Доступ к служебным веб-сервисам Ingress по HTTPS.

Порт	Backend-узлы	Внутренний доступ	Внешний доступ	Описание
53	**Инфраструктурные узлы**	Да	Да	Доступ к DNS-службе, если используется внутренний или гибридный режим работы DNS.
80	**Узлы балансировки входящего трафика (Ingress).** Для проверки доступности узла (healthcheck) необходимо настроить HTTP-проверку, используя путь `/healthz`.	Да	Да	Доступ к публичным веб-сервисам Ingress по HTTP.
443	**Узлы балансировки входящего трафика (Ingress).** Для проверки доступности узла (healthcheck) необходимо настроить HTTP-проверку, используя путь `/healthz`.	Да	Да	Доступ к публичным веб-сервисам Ingress по HTTPS.

Указанный выше перечень портов может быть расширен при использовании собственных дополнительных правил TCP и UDP балансировки.

При установке Nova Container Platform SE в минимальной конфигурации роль узлов балансировки входящего трафика (Ingress) выполняют рабочие узлы, выделенные для пользовательских нагрузок.

4. Рекомендуется к выполнению

- После успешной настройки сетевого окружения перейдите к статье Подготовка узла nova-ctl для управления платформой