Подготовка сетевого окружения

1. DNS записи для встроенных сервисов

Важно: Подготовка DNS-записей должна быть выполнена до установки Nova Container Platform. 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-cilium-hubble.nova.mycompany.local`
- `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

В Nova Container Platform для установки кластера по умолчанию требуется доступ к сети Интернет.

В вашей инфраструктуре необходимо обеспечить достук к следующим ресурсам:

Ресурс	DNS-имя	Порт	IP-адреса
Хранилище образов	hub.nova-platform.io storage.cloud.croc.ru	https/443	217.73.63.211/32 217.73.63.221/32 217.73.57.4/32 185.12.28.202/32
Сервис проверки лицензии	access.nova-platform.io	https/443	217.73.63.211/32 217.73.57.4/32 185.12.28.202/32
Сервис доставки ПО	code.nova-platform.io	https/443	217.73.63.211/32 217.73.57.4/32 185.12.28.202/32
Сервис настройки ПО	sun.nova-platform.io	https/8140	217.73.63.211/32 217.73.57.4/32 185.12.28.202/32

2.1. Закрытое сетевое окружение

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

Ресурс	DNS-имя	Порт	IP-адрес
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 в подготовленной пользователем инфраструктуре.

3.1. Требования к межсетевому экранированию

Для корректной установки и функционирования Nova Container Platform 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
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

Источник	Адресат	Тип трафика	Порт/Протокол	Описание
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
Все узлы	Инфраструктурные узлы	Входящий	8443/tcp	Ingress Nginx Controller Validating webhook
Инфраструктурные узлы	Все узлы	Исходящий	9100/tcp	Prometheus Node Exporter
Инфраструктурные узлы	Все узлы	Исходящий	9962/tcp	Cilium Agent metrics
Инфраструктурные узлы	Все узлы	Исходящий	9963/tcp	Cilium Operator metrics
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 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
Все узлы	Все узлы	Двунаправленный	4240/tcp	Cilium Health Check
Все узлы	Все узлы	Двунаправленный	ICMP (8/0)	Cilium Health Check
Все узлы	Все узлы	Двунаправленный	4244/tcp	Cilium Hubble server
Все узлы	Все узлы	Двунаправленный	4245/tcp	Cilium Hubble relay
Инфраструктурные узлы	Все узлы	Входящий	9100/tcp	Prometheus Node Exporter
Инфраструктурные узлы	Все узлы	Входящий	9962/tcp	Cilium Agent metrics
Инфраструктурные узлы	Все узлы	Входящий	9963/tcp	Cilium Operator metrics

Источник	Адресат	Тип трафика	Порт/Протокол	Описание
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 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)
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)

Источник	Адресат	Тип трафика	Порт/Протокол	Описание
APM пользователей платформы	Мастер-узлы	Исходящий	6443/tcp	Kubernetes API

При развертывании Nova Container Platform 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 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).

Информация

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.

Информация

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 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

Установка сервера управления Nova Universe

В данном разделе документации вы найдете все необходимые шаги для корректной установки сервера управления Nova Universe в вашей инфраструктуре. После установки и настройки сервера управления вы сможете начать развертывание кластеров Nova Container Platform в закрытом сетевом окружении.

Для удобства копирования информации вы можете подключиться к интерфейсу управления Nova Universe по протоколу SSH, который станет доступен после настройки сетевого интерфейса.

1. Предварительные условия

- ✓ Вы ознакомились с Требованиями к установке платформы в закрытом сетевом окружении.
- ✓ Образ сервера управления Nova Universe доступен к развертыванию в вашей среде виртуализации или облачном провайдере.

2. Установка сервера управления Nova Universe

2.1. Запуск сервера и доступ к интерфейсу управления

Процедура

Запустите виртуальную машину (ВМ) сервера управления из образа и дождитесь завершения загрузки. После успешной загрузки ВМ выполните вход в интерфейс управления с помощью учетной записи по умолчанию.

Доступ к серверу управления

По умолчанию используйте учетную запись `universe` с паролем `universe`. Вы сможете изменить пароль позже в процессе настройки сервера управления.

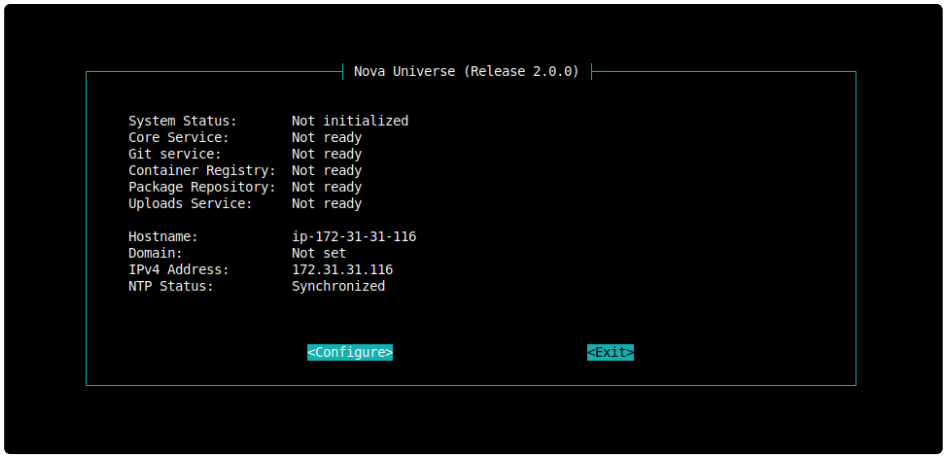

Рисунок 1. Главная страница интерфейса управления Nova Universe

На главной странице интерфейса управления отображается статус системных сервисов Nova Universe. При первом запуске общий системный статус *"Not initialized"* и статус сервисов *"Not ready"* являются нормой, поскольку инициализация сервера управления еще не выполнена.

2.2. Изменение пароля учетной записи по умолчанию

Рекомендуется изменить пароль учетной записи `universe`. Для этого выберите **Configure** на главной странице, перейдите в раздел **Settings** и выберите опцию **Change user password**. Установите новый пароль в соответствии с политикой ниже.

- Используйте сочетание букв разного регистра, цифр и специальных символов
- Не используйте простые и повторяющиеся слова
- Длина пароля должна быть не менее 8 символов

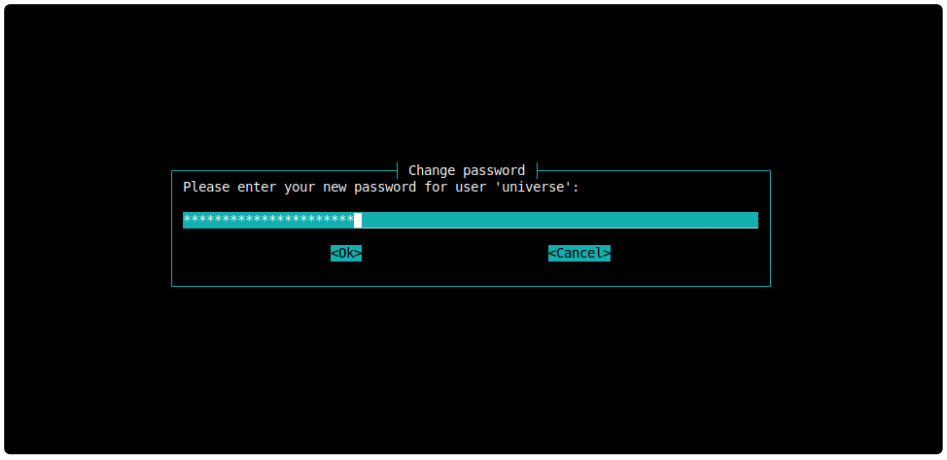

Рисунок 2. Интерфейс смены пароля учетной записи universe

2.3. Настройка параметров сетевого интерфейса

Вы можете настроить сетевой интерфейс сервера управления или установить дополнительные параметры сети. Для этого выберите **Configure** на главной странице,

перейдите в раздел **Settings** и выберите опцию **Network configuration**.

Обязательно выполните инициализацию Universe!
В противном случае сетевые настройки не сохранятся и после перезапуска виртуальной машины могу остаться ошибочные или неполные настройки сети.

Если настройки сети ошибочные или неполные — рекомендуем начать установку Universe с самого начала.

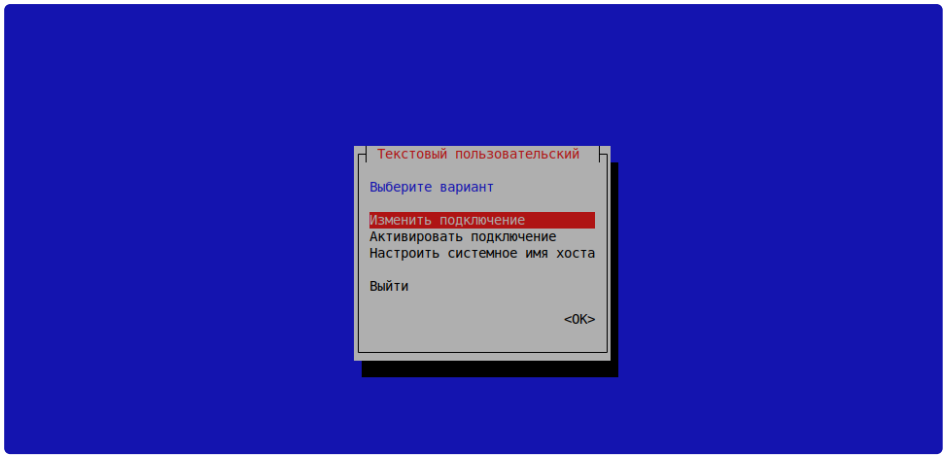

Рисунок 3. Интерфейс настройки сети Nova Universe

Для настройки сети используется текстовая версия утилиты Network Manager (TUI). С помощью Network Manager вы можете:

- установить имя сервера, используя опцию **Set system hostname**
- отредактировать существующее подключение, используя опцию **Edit a connection**
- активировать и деактивировать существующее подключение, используя опцию **Activate a connection**

После инициализации сервера управления Nova Universe изменить сетевые настройки невозможно. Для их изменения потребуется сброс к заводским настройкам и переустановка платформы, если она уже была развернута.

2.4. Настройка базового DNS-имени

Выполните настройку базового -имени сервера управления. Для этого выберите **Configure** на главной странице, перейдите в раздел **System settings** и выберите опцию **Configure DNS base domain**.

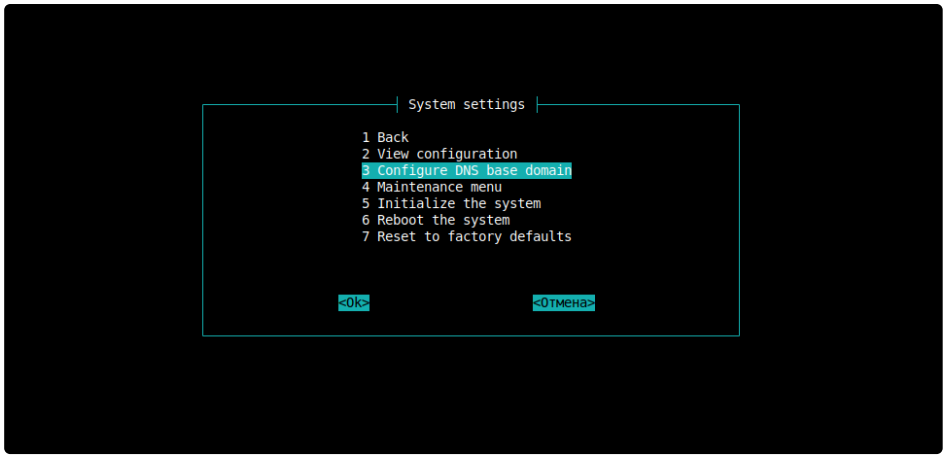

Рисунок 4. Настройка базового DNS-имени Nova Universe

Укажите базовое DNS-имя в соответствии с требованиями к системе разрешения имен DNS.

Базовое DNS-имя используется для публикации внутренних компонентов Nova Universe, таких как сервис доставки ПО, сервис настройки ПО, хранилище образов и т.д. Для удобства использования и предотвращения конфликтов разрешения имен рекомендуется использовать поддомен в вашем корпоративном домене, например, universe.mycompany.local.

`dnsBaseDomain` для Nova Universe не должен совпадать с `dnsBaseDomain` для Nova Container Platform. Если имена будут одинаковыми, сервисы Universe станут не доступны из Nova Container Platform.

Например, если DNS имя для Nova Universe установлено как `universe.mycompany.local`, то `dnsBaseDomain` для Nova Container Platform должен быть задан как `nova.mycompany.local`.

Рисунок 5. Настройка базового DNS-имени Nova Universe

После инициализации сервера управления Nova Universe изменить базовое DNS-имя невозможно. Для его изменения потребуется сброс к заводским настройкам и переустановка платформы, если она уже была развернута.

2.5. Инициализация сервера управления

После настройки параметров сетевого интерфейса и базового DNS-имени вам необходимо выполнить первичную инициализацию Nova Universe. Для этого выберите **Configure** на главной странице, перейдите в раздел **System settings** и выберите опцию **Initialize the system**. Подтвердите инициализацию, нажав кнопку **[Confirm]**.

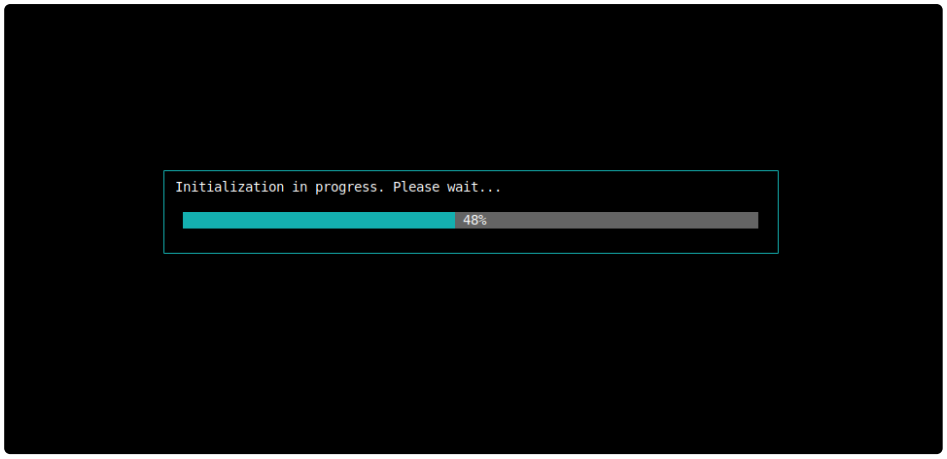

Рисунок 6. Инициализация Nova Universe

Процесс инициализации сервера управления Nova Universe может занять до 30 минут.

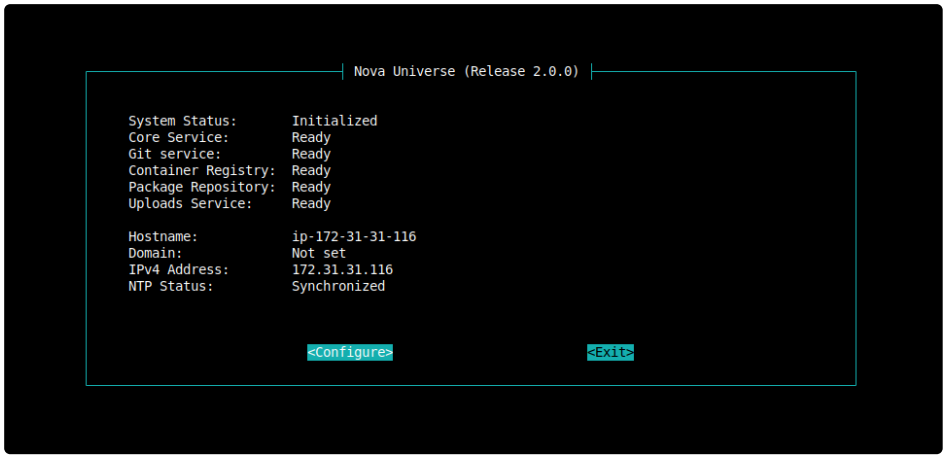

Рисунок 7. Инициализация Nova Universe

2.6. Получение реквизитов доступа к серверу управления

Реквизиты доступа к серверу управления необходимы для формирования файла конфигурации установки платформы. Для получения реквизитов доступа выберите **Configure** на главной странице, перейдите в раздел **System settings** и выберите опцию **View configuration**.

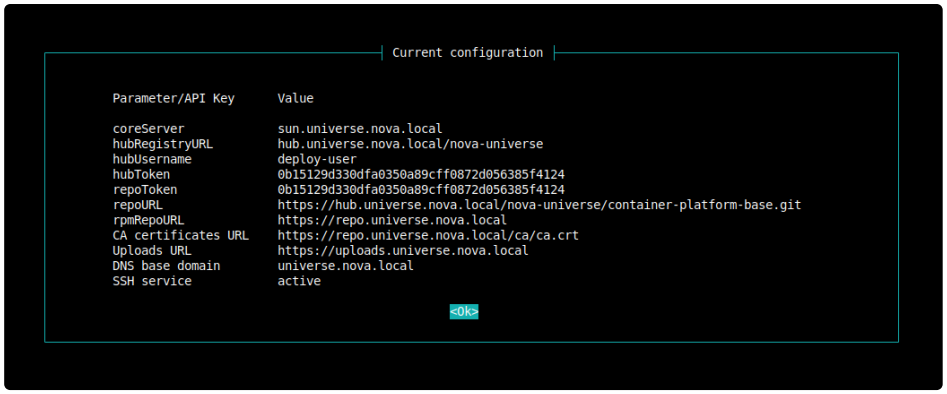

Рисунок 8. Реквизиты доступа к Nova Universe

Сохраните реквизиты доступа для установки платформы.

2.7. Получение корневого сертификата сервера управления

Корневой сертификат Nova Universe по умолчанию не будет являться доверенным на вашей локальной машине. В дальнейшем вы можете столкнуться с ошибками проверки подлинности сертификата хранилища образов, например, при установке nova-ctl. Поэтому рекомендуется добавить сертификат сервера управления в доверенные на локальной машине.

Для получения реквизитов доступа выберите **Configure** на главной странице, перейдите в раздел **System settings** и выберите опцию **View configuration**. Скопируйте значение параметра *CA certificates URL* (ссылку) и загрузите сертификат с помощью браузера или командных утилит.

Пример загрузки сертификата Nova Universe и установки в хранилище локальной машины представлен далее.

Пример

1. Скачайте сертификат.

```bash
curl -ko https://repo.universe.mycompany.local/ca/ca.crt
```

2. Переместите сертификат в директорию для хранения сертификатов и загрузите сертификат в хранилище.

```bash
sudo mv ca.crt /etc/pki/ca-trust/source/anchors/universe-ca.crt
sudo update-ca-trust
```

2.8. Дополнительные возможности раздела меню System settings и Maintenance menu

Раздел меню **System settings** предназначен для выполнения основных настроек сервера управления Nova Universe. В этом разделе доступны следующие возможности:

- получение реквизитов доступа к серверу управления после завершения инициализации
- доступ к разделу **Maintenance menu**
- выполнение перезагрузки сервера управления
- выполнение сброса сервера управления до заводских настроек

Выполнение сброса сервера управления Nova Universe до заводских настроек приведет к отключению кластеров Nova Container Platform от данного сервера без возможности переподключения после повторной инициализации.

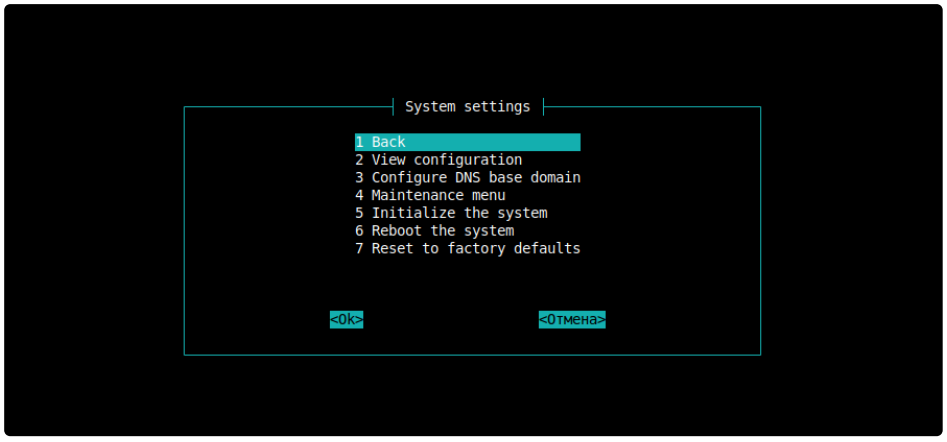

Рисунок 9. Раздел меню System settings

Раздел **Maintenance menu** предназначен для выполнения дополнительных настроек сервера управления Nova Universe. В этом разделе доступны следующие возможности:

- выключения или включения сервиса SSH
- выполнения настройки сервиса NTP

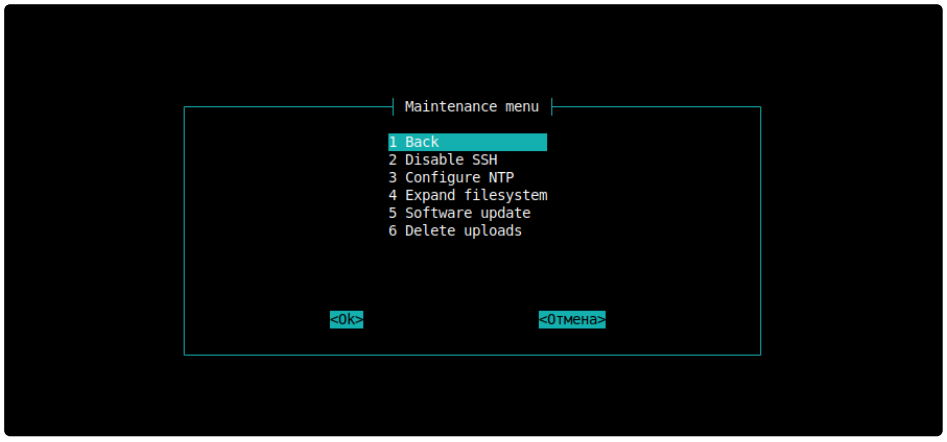

Рисунок 10. Раздел меню Maintenance menu

Соответствие версий Nova и Nova Universe: таблице указано, какие версии Nova включает в себя релиз Nova Universe.

3. Рекомендуется к выполнению

- После успешного завершения установки Nova Universe для установки платформы в закрытом контуре перейдите к статье Установка платформы

Подготовка пользовательской учетной записи

1. Подготовка пользовательской учетной записи в ОС

Для установки Nova Container Platform на каждом узле кластера необходима пользовательская учетная запись с правами администратора операционной системы. Для настройки пользовательской учетной записи выполните действия, описанные далее.

Обратите внимание, что после развертывания кластера Nova Container Platform для пользовательской учётной записи будет ограничена возможность авторизации в системе по паролю.

Процедура

1. Создайте пользователя в ОС с помощью команды:

```
useradd -m -s /bin/bash <имя_пользователя>
```

```
В качестве имени пользователя может быть выбрано любое желаемое имя.
```

Пример

```
useradd -m -s /bin/bash nova-installer
```

2. Добавьте пользователя в список `sudoers`, чтобы предоставить ему возможность выполнять привилегированные команды.

   Выполните команду:

```
cat << EOF > /etc/sudoers.d/99-nova-installer-user
nova-installer ALL=(ALL) NOPASSWD:ALL
EOF
```

2. Подготовка пары ключей SSH для доступа к узлам кластера

Во время установки Nova Container Platform вы должны использовать закрытый ключ SSH для работы утилиты установки nova-ctl. Ключ используется как один из аргументов nova-ctl и не хранится на узлах платформы или в кластере Kubernetes.

Перед запуском процесса установки кластера открытая часть ключа должна быть добавлена в список `~/.ssh/authorized_keys` для пользователя, выбранного в роли администратора ОС узлов кластера.

Процедура

1. Если у вас нет существующей пары ключей SSH на локальной машине для аутентификации на узлах кластера, создайте ее. Например, на компьютере с операционной системой Linux выполните следующую команду:

   ```bash
   ssh-keygen -f <путь>/<имя файла>
   ```

   > Вы можете указать путь и имя файла для новой пары ключей SSH, например, `~/.ssh/id_nova`.

2. Добавьте открытую часть ключа в файл `~/.ssh/authorized_keys` на каждом узле кластера:

   ```bash
   cat ~/.ssh/id_nova.pub >> ~/.ssh/authorized_keys
   ```

> **Информация**
>
> Убедитесь, что права доступа на файл `~/.ssh/authorized_keys` соответствуют значению 0600. Если значение отличается, то измените права с помощью команды `chmod 600 ~/.ssh/authorized_keys`.

3. Рекомендуется к выполнению

- Установка платформы