

В этом разделе находятся инструкции, описывающие особенности установки ресурсов.

1. Установка портала DC Manager

1.1. Поддерживаемые операционные системы

Управляющий хост — автоматизированное или виртуальное рабочее место, с которого производится установка портала DC Manager.

Управляющий хост поддерживает ОС с минимальными версиями:

- Ubuntu 22.04
- РедОС 7.3.3
- Windows (WSL2) 10
- MacOS (Big Sur) 11

Целевой хост — виртуальная машина в инфраструктуре пользователя, на которой будет установлен модуль DC Manager.

Целевой хост поддерживает ОС с минимальными версиями:

- Astra Linux 1.7.5
- Ubuntu 22.04
- РедОС 7.3.3

1.2. Минимальные системные требования

Требования к Single Instance

Тип хоста	CPU	RAM	Диск SSD (GB)
Управляющий	4 (CPU/vCPU)	16	70
Целевой	16 (vCPU)	72	600

Требования к High Availability (HA)

Тип хоста	CPU	RAM	Диск SSD (GB)
Управляющий	4	16	70

Тип хоста	CPU	RAM	Диск SSD (GB)
Сервер (x3)	2	4	64
Агент (x3)	16	72	600
Балансировщик нагрузки (x2)	2	4	32

1.3. Подготовка окружения

1.3.1. Настройка DNS-организации

В DNS-организации необходимо выделить зону, в рамках которой будут размещаться сервисы портала, например: sample.box

Далее можно либо завести wildcard-запись, которая будет указывать на целевой хост, куда устанавливается портал (например *.sample.box и *.nexus.sample.box), либо завести каждую запись отдельно.

Для Single Instance все записи должны указывать на IP-адрес целевого сервера.

Для High Availability все записи должны указывать на IP-адрес VIP (указывается в файле **inventories/box/hosts**, см. документацию ниже).

► Список DNS записей



Проверьте разрешения следующих доменных имён с помощью `nslookup` перед запуском развёртывания (нужно указать доменные имена в явном виде):

- starvault.{{ internal_domain }}
- nexus.{{ internal_domain }}
- docker-repository.nexus.{{ internal_domain }}
- sample.box.{{ internal_domain }}

1.3.2. Требования для управляющего хоста

- Python версии 3.9 и выше;
- Docker;
- Образ deploy-manager;
- Доступ к публичным репозиториям в сети Интернет.





Доступ можно организовать разными способами: прямой доступ в сеть Интернет, прокси, установка зависимостей в ручном режиме и прочее.

1.3.3. Требования для целевого хоста

- Python версии 3.9 и выше;
- Целевой хост должен располагаться в сетевом сегменте, который реализует сетевую связность с публичной зоной безопасности.



Это обеспечит доступность пользовательского интерфейса для всех авторизованных пользователей: с управляющих консолей, публичных API-платформ виртуализации и облачных провайдеров.

1.3.4. Требования по Firewall, SELinux

Рекомендуется отключить Firewall и SELinux на целевых хостах.

1.3.5. Требования к портам

Для работы в режиме High Availability должна быть следующая сетевая доступность:

Протокол	Порт	Source	Destination	Описание
TCP	6443	Все ноды	Все ноды	оркестратор
TCP	2379-2380	Server	Server	etcd
TCP	10250	Все ноды	Все ноды	kubelet metrics
UDP	8472	Все ноды	Все ноды	flannel
TCP	80,443		LB	haproxy

1.4. Подготовка управляющего хоста

1.4.1. Дополнительные компоненты

1. Проверьте, что GNU tar установлен при помощи команды:

```
tar -- version | grep GNU
```

BASH | ↗

В выводе должно присутствовать GNU , например:

```
tar (GNU tar) 1.34
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>.
```

BASH | ↗

2. Убедитесь, что установлен Python версии не ниже 3.9 и `venv`.



На ОС Linux `venv` устанавливается с отдельным пакетом `python3-venv`.

1.4.2. Установка образа `deploy-manager` и настройка `config`



Команды выполняются на управляемом хосте.

1. Скачайте дистрибутив в архиве с расширением `.tar.gz` и распакуйте его.

2. Установите образ `deploy-manager`, который находится в распакованном архиве:

```
docker load < deploy-manager-1.8.0.tar
```

BASH | ↗

3. (Опционально) Проверьте образ на доступность:

```
docker images
```

BASH | ↗

Пример ответа, если образ доступен:

REPOSITORY	TAG	IMAGE ID	CREATED
SIZE			
docker.io/library/deploy-manager	1.8.0	243f5d6cb054	3 months ago
1.05 GB			

BASH | ↗

4. Скопируйте примеры заполненных конфигурационных файлов из каталога `sample`:

```
cp -R inventories/sample inventories/box
```

BASH | ↗



Каталог `sample` копируется, чтобы восстановить исходные данные или свериться с примерами заполнения при необходимости.

Имя каталога, в который копируются примеры, произвольное: каталог `box` можно изменить на другой.

5. Создайте SSH-ключ и скопируйте его на целевой хост:

a. Создайте ключ, если он отсутствует:

```
ssh-keygen
```

BASH | ↗

b. Скопируйте SSH-ключ на целевой хост:

```
ssh-copy-id [id пользователя]
```

BASH | ↗

```
# Команда с примером id пользователя -- ssh-copy-id astra@10.15.9.6
```

 Если авторизация по паролю на сервере запрещена, добавьте ключ вручную в **authorized_key**:

1. Выведите содержимое публичного ключа:

```
cat ~/.ssh/id_rsa.pub
```

BASH | □

2. Подключитесь на целевой хост с помощью доступных вам вариантов: ssh, vnc, novnc и так далее.
3. Добавьте содержимое публичного ключа из первого шага в файл **authorized_keys**:

```
echo 'ssh-rsa AAAAB3NzaC1yc ...' >> ~/.ssh/authorized_keys
```

BASH | □

6. Заполните файл **hosts**, расположенный в каталоге **inventories/box/**. Описание настроек находится в комментариях этого файла.

► **Вид файла hosts при установке в режиме Single Instance**

► **Вид файла hosts при установке в режиме High Availability**

7. Измените настройки в файле **config.yml**, расположенному в каталоге **inventories/box/group_vars/{}.**

1.4.3. Настройки файла config.yml

В файле **config.yml** находятся поля, которые нужно заполнить для платформы виртуализации zVirt.

Раскомментируйте строки платформы виртуализации и подставьте нужные значения. В параметре `type` необходимо указать `zvirt`.



Параметр `type` чувствителен к регистру символов, поэтому важно указать название платформы корректно.

► **Пример config.yml для zVirt**

Таблица 1. Описание параметров config.yml для платформы zVirt

Параметр	Значение	Описание

Параметр	Значение	Описание
build_cluster	false	Режим установки: High Availability или Single Instance. По умолчанию установка в режиме Single Instance. Для установки в режиме High Availability необходимо указать значение true
type	zvirt	Тип платформы — zVirt
label	zVirt	Человекочитаемое название платформы. В параметре можно указать любое удобное вам название "Zvirt-1", "Zvirt-test" и так далее.
scheme	https	Схема для доступа к zVirt API. Протокол https — это протокол по умолчанию. Рекомендуется использовать именно этот протокол.
host port	Например: host: '10.13.250.2' или host:'zvirt.sample.box' port: '443' Если иной порт не указан, то используется 443 — стандартный порт протокола https.	IP-адрес zVirt API
username password	Например, username:'root' и password:'GYHvf-5569vgds'	Учётные данные для подключения. Задайте логин и пароль для платформы.

Параметр	Значение	Описание
params	weight	Вес платформы в интерфейсе заказа продукта. Чем меньше вес, тем выше в списке. Например, weight:11, weight:102
	cluster_id	Скопируйте ID кластера в интерфейсе Zvirt. Для этого: <ol style="list-style-type: none"> Перейдите в раздел Compute → Clusters. Нажмите на название кластера. Откроется страница с подробной информацией. Скопируйте Cluster ID из соответствующего поля. Например, cluster_id: zsjhgdsdjvght6e327w3dscxdghjkjacsxdcjuu
	cluster_name	Введите название кластера. Например, cluster_name: example-cluster-1
	storage_name	Скопируйте название хранилища в интерфейсе zVirt. Для этого перейдите в раздел Storage → Domains .

Дополнительные инструкции:

- ▶ Пойск ID кластера для zVirt

1.5. Запуск развёртывания

Docker-контейнер добавляется при установке образа deploy-manager.



Перед запуском docker-контейнера необходимо создать папку `~/.kube/dcmanager`, так как эта директория монтируется в контейнер.

Запустите docker-контейнер при помощи команды:

```
docker run -it --network host --rm \
-v ${HOME}/portal-box:/apps \
-v ~/.ssh/id_rsa:/root/.ssh/id_rsa \
```

BASH | ↗

```
-v ~/.kube/dcmanager:/root/.kube/dcmanager \
deploy-manager:1.8.0 \
-i inventories/box/hosts \
-u $USER \
portal_box.yml \
--ask-vault-pass
```

Параметры команды:

- `-v /$HOME/portal-box:/apps` – отображение директории, в которой находится разархивированный архив. Слева указан путь до директории на управляющем хосте, справа указан путь до директория в образе docker - неизменяемая часть, ':' является разделителем;
- `-v ~/.ssh/id_rsa:/root/.ssh/id_rsa` – отображение файла с закрытым ключом;
- `-v ~/.kube/dcmanager:/root/.kube/dcmanager` – отображение файла, в котором будет находиться kubeconfig для подключения к кластеру;
- `deploy-manager:1.8.0` – название docker-образа;
- `-i inventories/box/hosts` – путь до файла hosts;
- `-u $USER` – пользователь, с помощью которого будет производиться подключение на удаленный хост;
- `portal_box.yml` – файл, который находится в директории portal-box;
- `--ask-vault-pass` – команда для запроса пароля в интерактивном режиме.

После запуска docker-контейнера, введите пароль для установки:

Vault password:



Данные для Vault password находятся в репозитории с дистрибутивом.

1.6. Проверка целостности дистрибутива

При необходимости вы можете проверить целостность дистрибутива zVirt DC Manager утилитой **md5sum**.

В репозитории с каждым обновлением дистрибутива размещается файл с расширением **md5**, содержащий контрольную сумму дистрибутива. Пример имени файла с контрольной суммой: **zvirt-dc-manager-1.27-20250827T192016.tar.md5**.

Для проверки целостности дистрибутива:

1. После загрузки дистрибутива запустите утилиту **md5sum** с указанием имени дистрибутива:

```
md5sum <имя_дистрибутива>.tar
```

BASH | □

Пример:

```
md5sum zvirt-dc-manager-1.27-20250827T192016.tar
```

BASH | □

После выполнения проверки будет выдано сообщение с контрольной суммой.

Пример:

```
f458058f29e5f6cbcc0618acb71a88d6 zvirt-dc-manager-1.27-20250827T192016.tar
```

BASH | □

2. Сравните значение из файла с расширением **md5** с полученным в результате проверки значением.

Проверка считается успешной с случае полного совпадения значений.

```
[root@manager dcmanager]# ls
zvirt-dc-manager-1.27-20250827T192016.tar zvirt-dc-manager-1.27-20250827T192016.tar.md5
[root@manager dcmanager]# md5sum zvirt-dc-manager-1.27-20250827T192016.tar
f458058f29e5f6cbcc0618acb71a88d6 zvirt-dc-manager-1.27-20250827T192016.tar
[root@manager dcmanager]# cat zvirt-dc-manager-1.27-20250827T192016.tar.md5
f458058f29e5f6cbcc0618acb71a88d6 zvirt-dc-manager-1.27-20250827T192016.tar
[root@manager dcmanager]# █
```

2. Настройка после установки портала



Ниже находятся примеры ссылок с доменом **sample.box**. Замените его на тот, что указан в переменной `domain_int` при настройке файла `inventories/box/hosts`.

1. После выполнения playbook будет выведена информация о подключении к Vault, оркестратору и порталу zVirt DC Manager. Сохраните учётные данные, так как они понадобятся для дальнейшей настройки `~/.kube/dcmanager`. В этой директории будет созданный config-файл оркестратора.



Также информацию можно вывести повторно, для этого необходимо выполнить playbook с тегом `info`:

```
docker run -it --network host --rm \
-v /$HOME/portal-box:/apps \
-v ~/.ssh/id_rsa:/root/.ssh/id_rsa \
-v ~/.kube/dcmanager:/root/.kube/dcmanager \
deploy-manager:1.8.0 \
-i inventories/box/hosts \
-u $USER \
portal_box.yml \
--ask-vault-pass \
--tags info
```

BASH | □

- Перейдите по адресу, указанному в результатах выполнения задачи **Portal admin credentials**.
- Скачайте корневой сертификат сайта и добавьте его в доверенные на вашем ПК. Если сертификат не будет добавлен в доверенные, могут возникнуть проблемы с открытием портала zVirt DC Manager.
- Настройте сервис NetBox (IPAM), расположенный по адресу <https://netbox.sample.box/>.



Нельзя изменять созданные на этапе установки объекты **NetBox**, такие как **site**, **tenant**, **vrf**. Если необходимо использовать собственные объекты, их необходимо создать после установки, не изменяя уже существующие.

Для этого:

- Получите учётные данные (**adminUsername** и **adminPassword**) из StarVault по адресу <https://starvault.sample.box/ui/vault/secrets/deployment/show/netbox>
- В интерфейсе NetBox перейдите на вкладку слева **IPAM → VLANs → VLANs**.

VID	Name	Site	Group
1	customer1	DC1	—
1	customer2	DC1	—
1	customer3	DC1	—
1	customer4	DC1	—
1	customer5	DC1	—

- Создайте новый VLAN, нажав **Add**, и заполните параметры:
 - ID** — цифровой идентификатор VLAN в диапазоне от 1 до 4094;
 - Name** — символьное имя VLAN, содержит только символы: "A-Z", "a-z", "0-9", "_", "-", ".", ",";
 - Status** — рабочее состояние VLAN. Имеет значения:
 - Active** — активно,

- **Reserved** — зарезервировано,
- **Deprecated** — устарело,
- **Tenant** — группа ресурсов, используемая в административных целях;
- **Assignment** — описывает группу VLAN или сайт, к которому привязана VLAN;
- **Custom virt subnet uuid** — настраиваемый идентификатор виртуальной подсети. Его можно получить запросом API (подробнее в примерах ниже).

► Пример создания VLAN для Zvirt

d. Создайте подсеть, в которой будут находиться виртуальные машины:

- В интерфейсе NetBox перейдите на вкладку слева **IPAM** → **Prefixes** → **Prefixes**.

► Пример создания подсети для zVirt

e. Зарезервируйте занятые IP-адреса в подсете:

- В интерфейсе NetBox перейдите на вкладку слева **IPAM** → **IP Addresses** → **IP Addresses** и зарезервируйте IP-адреса.

► Пример резервирования IP-адресов для zVirt



В подсистеме биллинга zVirt DC Manager стоимость всех тарифных классов равна нулю.

3. Установка Nova Universe для DC Manager

Перед тем, как заказать Nova Container Platform в модуль DC Manager, нужно развернуть контейнер на сервере управления Nova Universe.

Сервер управления Nova Universe поставляется в виде образа виртуальной машины в формате **qcow2** со следующим набором компонентов:

- хранилище образов контейнеров;
- сервис доставки ПО;
- сервис настройки ПО.

Благодаря готовым компонентам для установки кластеров Nova Container Platform не требуется самостоятельное зеркалирование образов контейнеров и настройка дополнительных артефактов.

3.1. Технические требования к серверу управления Nova Universe

3.1.1. Требования к среде размещения

Для Nova Universe рекомендуется использовать платформу виртуализации zVirt.

Формат образа виртуальной машины qcow2 является нативным для zVirt.

3.1.2. Требования к ресурсам

Для запуска сервера управления Nova Universe необходимы следующие ресурсы:

vCPU	RAM (GB)	Диск SSD (GB)	IOPS
4	16	128	300+



Компоненты сервера управления Nova Universe чувствительны к производительности диска, поэтому рекомендуется использовать более быстрое хранилище.

3.1.3. Требования к настройке сети

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 для настройки сетевого интерфейса сервера используется DHCP-сервер, то DHCP-сервер нужно настроить на предоставление постоянного IP-адреса и сведений о DNS-серверах.
- Сервер управления Nova Universe на текущий момент не поддерживает IPv6.

3.1.4. Требования к системе разрешения имен DNS

Для работы сервера управления Nova Universe необходимо создать DNS-записи:

Компонент	Пример записи	Описание
Сервер управления Nova Universe	universe.имя.домена	DNS-запись типа A разрешает адрес сервера управления
Службы Nova Universe	*.universe.имя.домена	DNS-запись типа A или CNAME разрешает адрес сервера управления при запросе его поддоменов, например, test.universe.имя.домена , hub.universe.имя.домена и так далее.

Для корректной работы сервера управления необходимо также настроить DNS-сервер в его сетевой конфигурации.

3.1.5. Требования к межсетевому экранированию

Если сервер управления Nova Universe размещается в отдельной маршрутизируемой сети, то для организации доступа к ресурсам сервера управления из сетей узлов Kubernetes, нужно настроить разрешающие правила:

Ресурс	DNS-имя	Порт	IP-адрес
Хранилище образов	hub.DNS-имя Nova Universe	https/3000	IP-адрес Nova Universe
Сервис настройки ПО	sun.DNS-имя Nova Universe	https/443	IP-адрес Nova Universe
Сервис загрузки обновлений	DNS-имя Nova Universe	https/443	IP-адрес Nova Universe
Сервис доставки ПО	hub.DNS-имя Nova Universe	https/3000	IP-адрес Nova Universe
Репозиторий пакетов	repo.DNS-имя Nova Universe	https/443	IP-адрес Nova Universe

3.2. Установка сервера управления

Для установки сервера управления выполните действия, которые описаны далее.

3.2.1. Создание виртуальной машины из образа

Создайте виртуальную машину из образа в среде виртуализации zVirt:

1. Подключитесь к web-интерфейсу управления **Hosted Engine** и перейдите в меню **Storage → Disks**.
2. Загрузите образ сервера в домен хранения, нажав **Upload → Start**.
3. Выберите файл образа сервера, целевой домен хранения и запустите процесс загрузки.
4. После окончания загрузки образа создайте новую виртуальную машину, прикрепите образ сервера и укажите его в качестве загрузочного.

3.2.2. Запуск сервера и доступ к интерфейсу управления

1. Запустите виртуальную машину сервера управления из образа и дождитесь окончания загрузки.
2. После успешной загрузки виртуальной машины выполните вход в интерфейс управления с помощью учетной записи по умолчанию.

На главной странице интерфейса управления отображается статус системных сервисов Nova Universe. При первом запуске отображается системный статус **Not Provisioned** и статус сервисов **Not Available**, поскольку инициализация сервера управления не выполнена.

3.2.3. Изменение пароля учетной записи по умолчанию

По умолчанию используется учетная запись **universe** с паролем **universe**. Его рекомендуется изменить сразу после входа.

Для этого:

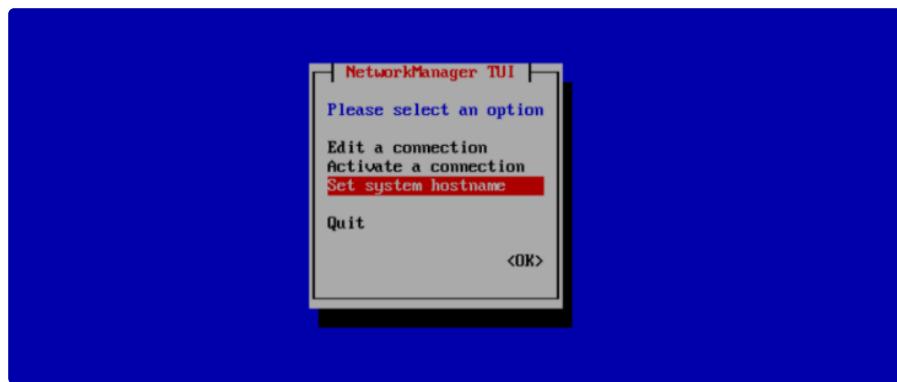
1. Перейдите в раздел **Configure**.
2. Выберите опцию **Change user password** и установите пароль согласно требованиям:
 - В пароле есть буквы разного регистра, цифры и специальные символы;
 - Длина не менее 8 символов;
 - Не используются простые и повторяющиеся слова.

3.2.4. Настройка параметров сетевого интерфейса

Вы можете настроить сетевой интерфейс сервера управления или установить дополнительные параметры сети.

Для этого:

1. Перейдите в раздел **Configure**.
2. Выберите опцию **Network configuration**. Откроется текстовая версия утилиты Network Manager (TUI).

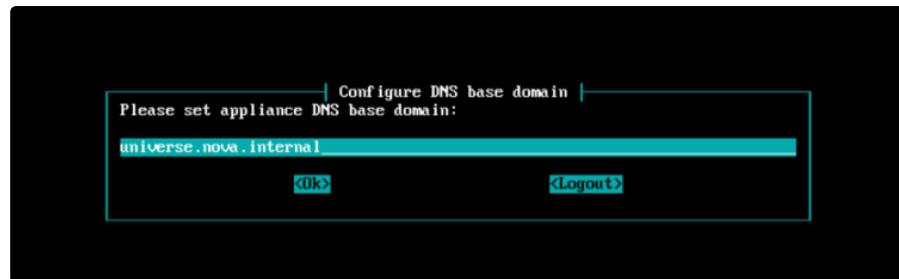


3. Сделайте настройки с помощью опций:
 - **Set system hostname** – для установки названия сервера,
 - **Edit a connection** – для изменения текущего подключения,
 - **Activate a connection** – для активации или деактивации существующего подключения.

3.2.5. Настройка базового DNS-имени

Для настройки базового DNS-имени сервера:

1. Перейдите в раздел **Configure → System configuration**.
2. Выберите опцию **Set initial configuration**.
3. Укажите базовое DNS-имя в соответствии с требованиями к системе разрешения DNS-имён.



Инициализация сервера управления

После установки параметров сетевого интерфейса и базового DNS-имени вам необходимо выполнить первичную инициализацию Nova Universe.

Для этого:

1. Перейдите в раздел **Configure → System configuration**.
2. Выберите опцию **Initialize appliance**.
3. Для подтверждения инициализации нажмите **Confirm**.

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

После успешного завершения инициализации выполните повторный вход в интерфейс управления Nova Universe и проверьте статус сервисов.



Получение реквизитов доступа к серверу управления

Реквизиты доступа к серверу управления необходимы для формирования файла конфигурации установки платформы.

Для получения реквизитов:

1. Перейдите в раздел **Configure → System configuration**.

2. Выберите опцию **Get current configuration**.
3. Сохраните значения полей hubUsername , hubToken , DNS wildcard domain . Эти значения потребуются при последующей установке портала DC Manager. Их нужно добавить в качестве значений к соответствующим переменным в файле конфигурации config.yml:

PERL | □

```
# Базовый домен, который был установлен при развертывании Nova Universe,  
например: universe.nova.internalnova_universe_base_domain: 'DNS wildcard  
domain'.  
# Учетные данные для подключения. Значения полей hubUsername и hubToken из  
конфигуратора Nova Universe.  
nova_universe_hub_username: 'hubUsername'  
nova_universe_hub_token: 'hubToken'
```

3.2.6. Получение корневого сертификата сервера управления

Корневой сертификат Nova Universe по умолчанию не будет являться доверенным на вашем ПК. В дальнейшем вы можете столкнуться с ошибками проверки подлинности сертификата хранилища образов. Рекомендуется добавить сертификат сервера управления в доверенные на вашем ПК.

Для этого:

1. Перейдите в раздел **Configure → System configuration**.
2. Выберите опцию **Get current configuration**.
3. Копируйте 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:

```
sudo curl -ko /etc/pki/ca-trust/source/anchors/universe-ca.crt  
https://repo.universe.nova.internal/ca/ca.crt  
sudo update-ca-trust
```