



В этом разделе находятся инструкции, описывающие особенности установки ресурсов.

1. Установка портала Cloudlink

1.1. Поддерживаемые операционные системы

Manager-хост — хост, с которого производится установка портала Cloudlink.

Поддерживаемые ОС с минимальными версиями:

- Ubuntu 22.04
- Alma Linux 9.3
- Windows (WSL2) 10
- MacOS 11

Target-хост — хост на котором будет запущен портал Cloudlink.

Поддерживаемые ОС с минимальными версиями:

- Alma Linux 9.3
- Astra Linux (Orel) 2.12.45
- Ubuntu 22.04

1.2. Минимальные системные требования

Требования к Single instance

Тип хоста	CPU	RAM	Диск SSD (GB)
Manager	4	8	64
Target	16	72	600

Требования к High Availability (HA)

Тип хоста	CPU	RAM	Диск SSD (GB)
Manager	4	8	64
Server (x3)	2	4	64
Agent (x3)	16	72	600
LB(x2)	2	4	32

1.3. 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 target-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 target-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):

- `vault.{{ internal_domain }}`
- `nexus.{{ internal_domain }}`
- `docker-repository.nexus.{{ internal_domain }}`
- `sample.box.{{ internal_domain }}`

1.3.1. Требования для Manager

- Docker
- Образ `deploy-manager`

1.3.2. Требования для Target

- Python не ниже 3.9
- Доступ к репозиториям ОС. Его можно организовать разными способами: прямой доступ в интернет, прокси, установка зависимостей в ручном режиме и прочее.
- Необходимо включить IPv6 на Target-хосте (без доступа к IPv6 сборка портала может сломаться)

1.3.3. Требования по Firewall, SELinux

Для работы в режиме High Availability на target-хостах рекомендуется отключить Selinux и Firewall. Эта рекомендация распространяется на работу в режиме Single Instance.

1.3.4. 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	k3s
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. Установка образа `cloudlink-manager` и настройка `config`

i Команды выполняются на manager-хосте.

1. Скачайте дистрибутив в архиве с расширением `tar.gz` и распакуйте его.
2. В случае установки с помощью `manage-tool` пропустите этот шаг, иначе:
 - a. Установите образ `deploy-manager`, который находится в распакованном архиве. Пример установки версии 1.5.0:

```
docker load < deploy-manager-1.5.0.tar
```

BASH | 📄

- b. (Опционально) Проверьте образ на доступность:

```
docker images
```

BASH |

Пример ответа в случае, если образ доступен:

REPOSITORY	SIZE	TAG	IMAGE ID
deploy-manager	1.01GB	1.5.0	35ca14ec55b4

BASH |

3. Скопируйте пример inventory:

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

BASH |

Измените данные подключения к порталу и в файле **hosts**, расположенном в каталоге **inventories/box/**. Описание настроек находится в комментариях к этому файлу.

4. Создайте SSH-ключ и скопируйте его на target-хост(ы):

a. Создайте ключ, если он отсутствует:

```
ssh-keygen
```

BASH |

b. Скопируйте SSH-ключ на target-хост:

```
ssh-copy-id [id пользователя]  
# Команда с примером id пользователя -- ssh-copy-id root@192.168.0.1
```

BASH |



Если авторизация по паролю на сервере запрещена добавьте ключ вручную:

1. Выведите содержимое публичного ключа:

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

BASH |

2. Подключитесь на target хост(ы) с помощью доступных вам вариантов (ssh, vnc, povnc и т.п.).

3. Добавьте содержимое публичного ключа из первого шага:

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

BASH |

5. Заполните файл **hosts**.

Файл должен находиться по пути **inventories/box/hosts**.

► Вид файла **hosts** при установке **Single instance**

► Вид файла **hosts** при установке **High Availability instance**

6. Измените настройки в файле **config.yml**, расположенном к каталоге **inventories/box/group_vars/k3s/config.yml**.

1.4.1. Настройки файла **config.yml**

В файле **config.yml** находится описание полей, которые нужно заполнить для выбранной/выбранных платформ виртуализации. Для этого нужно раскомментировать строки платформы виртуализации и подставить значения. Заполнить файл **config.yml** можно как вручную, так и через пользовательский интерфейс, запустив команду:

```
manage-tool --ui
```

BASH |

Поддерживаются следующие типы платформ: zVirt, vSphere, Openstack, vCloud, Hyper V, Yandex Cloud. Название этих платформ нужно указать в параметре **type**.

Типы платформ должны быть строго выбраны из списка: `zvirt`, `vsphere`, `openstack`, `vcloud`, `hyper_v`, `yandex_cloud`. Параметр `type` чувствителен к регистру символов, поэтому важно указать названия платформ корректно.

► Пример `config.yml` для `zVirt`

Таблица 1. Описание параметров `config.yml` для платформы `zVirt`

Параметр	Значение	Описание
<code>type</code>	<code>zvirt</code>	Тип платформы. Зависит от того, какую платформу вы устанавливаете. Могут быть следующие типы: <code>zvirt</code> , <code>vsphere</code> , <code>openstack</code> , <code>vcloud</code> , <code>hyper_v</code> , <code>yandex_cloud</code>
<code>label</code>	<code>zVirt</code>	Человеко читаемое название платформы. В этом параметре можно указать любое удобное вам название "Zvirt-1", "Zvirt-test" и т.д
<code>scheme</code>	<code>https</code>	Схема для доступа к <code>zVirt</code> API. Протокол <code>https</code> является протоколом по умолчанию. Рекомендуется использовать именно этот протокол.
<code>host</code> <code>port</code>	Например: <code>host: '10.13.250.2'</code> или <code>host: 'zvirt.sample.box'</code> . <code>port: '443'</code> Если иной порт не указан, то используется 443 — стандартный порт протокола <code>https</code> .	IP-адрес <code>zVirt</code> API.
<code>username</code> <code>password</code>	Например, <code>username: 'root'</code> и <code>password: 'GYHvf-5569vgds'</code>	Учётные данные для подключения. Задайте логин и пароль для платформы
<code>params</code>	<code>weight</code>	Вес платформы в интерфейсе заказа продукта. Чем меньше вес, тем выше в списке. Например, <code>weight: 11</code> , <code>weight: 102</code>
	<code>cluster_id</code>	Скопируйте ID кластера в интерфейсе <code>Zvirt</code> . Для этого: 1. Перейдите в раздел Compute → Clusters . 2. Нажмите на название кластера. Откроется страница с подробной информацией. 3. Скопируйте Cluster ID из соответствующего поля. Например, <code>cluster_id: zsjhgsdsjbvght6e327w3dscxdghjkjacsxdcjuu</code>
	<code>cluster_name</code>	Введите название кластера. Например, <code>cluster_name: example-cluster-1</code>
	<code>storage_name</code>	Скопируйте название хранилища в интерфейсе <code>zVirt</code> . Для этого перейдите в раздел Storage → Domains .

► Пример `config.yml` для `vSphere`

Таблица 2. Описание параметров `config.yml` для платформы `vSphere`

Параметр	Значение	Описание
----------	----------	----------

Параметр	Значение	Описание
type	vsphere	Тип платформы. Зависит от того, какую платформу вы устанавливаете. Могут быть следующие типы: <code>zvirt</code> , <code>vsphere</code> , <code>openstack</code> , <code>vcloud</code> , <code>hyper_v</code> , <code>yandex_cloud</code>
version	6.7 или 7.0	Данный параметр указывает версию для платформы VMware vSphere.
label	vSphere	Человеко читаемое название платформы. В этом параметре можно указать любое удобное вам название "vSphere-1", "vSphere-test" и т.д
scheme	https	Схема для доступа к vSphere API. Протокол https является протоколом по умолчанию. Рекомендуется использовать именно этот протокол.
host	Например: <code>host: '10.13.250.2'</code> или <code>host: 'vpshere.cloudlink.local'</code>	IP-адрес или FQDN vSphere API.
port	443	Номер порта для подключения к интерфейсу API. По умолчанию используется 443 — стандартный порт протокола https.
username	Например, <code>username: 'root'</code> и	Учётные данные для подключения. Задайте
password	<code>password: 'GYHvf-5569vgds'</code>	логин и пароль для платформы.

Параметр	Значение	Описание
params	weight	Вес платформы в интерфейсе заказа продукта. Чем меньше вес, тем выше в списке. Например, <code>weight:11</code> , <code>weight:102</code>
	cluster_name	Скопируйте имя кластера в интерфейсе VSprehe Client. Для этого: 1. Перейдите в раздел Hosts and Clusters → Clusters . 2. Скопируйте Cluster name из соответствующего поля.
	domain_id	Введите название кластера. Для этого: 1. Перейдите в раздел Hosts and Clusters в интерфейсе VSprehe Client. 2. Нажмите по необходимому кластеру и скопируйте из URL значение параметра <code>ClusterComputeResource</code> . Например, URL - <code>https://vc.cloudlink.local/ui/app/cluster;nav=h/urn:vmomi:ClusterComputeResource:domain-c7005:111111/summary</code> значение параметра <code>domain_id</code> в данном случае domain-c7005 .
	datastore_id	Введите идентификатор хранилища (<code>datastore id</code>) в интерфейсе VSprehe Client. Для этого: 1. Перейдите в раздел Storage . 2. Нажмите по необходимому хранилищу и скопируйте из URL значение параметра <code>Datastore</code> . Например, URL - <code>https://vc.cloudlink.local/ui/app/datastore;nav=s/urn:vmomi:Datastore:datastore-11:123123/summary</code> значение параметра <code>datastore_id</code> в данном случае datastore-11 .
	tenant_prefix	Укажите имя директории (Folder), в которой будут создаваться директории Проектов.
	template_inventory	Укажите имя директории (Folder), в которой находятся шаблоны для развертывания ВМ. По умолчанию директория для версии VMware vSphere 6.7 <code>templates/cloudlink</code> По умолчанию директория для версии VMware vSphere 7.0 <code>library/templates</code>

► Пример config.yml для Openstack

Таблица 3. Описание параметров config.yml для платформы Openstack

Параметр	Значение	Описание
type	openstack	Тип платформы. Зависит от того, какую платформу вы устанавливаете.
label	OpenStack	Человеко читаемое название платформы. В этом параметре можно указать любое удобное вам название "OpenStack-1", "Open-Stack-test" и т.д
scheme	https	Протокол https является протоколом по умолчанию. Рекомендуется использовать именно этот протокол.

Параметр	Значение	Описание
host	Например: host: '10.13.250.2' или host: 'openstack.cloudlink.local'	IP-адрес или FQDN хоста.
port	5000	Номер порта для подключения к интерфейсу API. По умолчанию используется 5000.
username	Например, username: 'root' и password: 'GYHvf-5569vgds'	Учётные данные для подключения. Задайте логин и пароль для платформы
params	weight	Вес платформы в интерфейсе заказа продукта. Чем меньше вес, тем выше в списке. Например, weight:11, weight:102
	region	Укажите название региона.
	domain_name	Укажите название домена OpenStack.
	tenant_prefix	Человеко читаемый префикс. Подставляется перед именем проекта OpenStack при создании заказа в проекте Cloudlink.

Дополнительные инструкции:

► Поиск ID кластера для zVirt

► Поиск ID кластера для Vmware

► Поиск ID кластера для RedVirt

► Поиск ID кластера для OpenStack

1.4.2. Запуск развертывания

1. Если используются параметры по умолчанию, выполните команду:

```
./PATH/manage-tool --install
```

BASH |

2. Если используются другие пути до инвентаря и ssh-ключа, выполните команду:

```
./PATH/manage-tool.sh --inventory inventories/myinventory/hosts --ssh-private-key ~/.ssh/mykeys/dev --install
```

BASH |



Подробно ознакомиться с утилитой manage-tool.sh можно с помощью команды `manage-tool --help`.

1.4.3. Альтернативный вариант запуска развертывания

Команда для запуска docker контейнера (был добавлен в 1 шаге).



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

```
docker run -it --network host --rm \
  -v /$HOME/portal-box:/apps \
  -v ~/.ssh/id_rsa:/root/.ssh/id_rsa \
  -v ~/.kube/cloudlink:/root/.kube/cloudlink \
  deploy-manager-1.5.0 \
```



```
-i inventories/box/hosts \  
-u $USER \  
portal_box.yml \  
--ask-vault-pass
```

Параметры команды:

`-v /$HOME/portal-box:/apps` — маппинг директории в которой находится разархивированный архив. Слева указан путь до директории на manager хосте, справа указан путь до директория в образе docker - НЕИЗМЕНЯЕМАЯ, разделителем является ':')

`-v ~/.ssh/id_rsa:/root/.ssh/id_rsa` — маппинг файла с закрытым ключом.

`-v ~/.kube/cloudlink:/root/.kube/cloudlink` — маппинг файл, в котором после будет находится kubernetes config для подключения к кластеру.

`deploy-manager-1.5.0` — название docker-образа.

`-i inventories/box/hosts` — путь до файла inventory.

`-u $USER` — пользователь, с помощью которого будет производиться подключение на удаленный хост.

`portal_box.yml` — файл, находящийся в portal-box директории.

`--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 репо.

1.5. 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**, **k3s** и portalу Cloudlink. Сохраните учётные данные, так как они понадобятся для дальнейшей настройки `~/.kube/cloudlink`. В этой директории будет созданный kubernetes config файл.



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

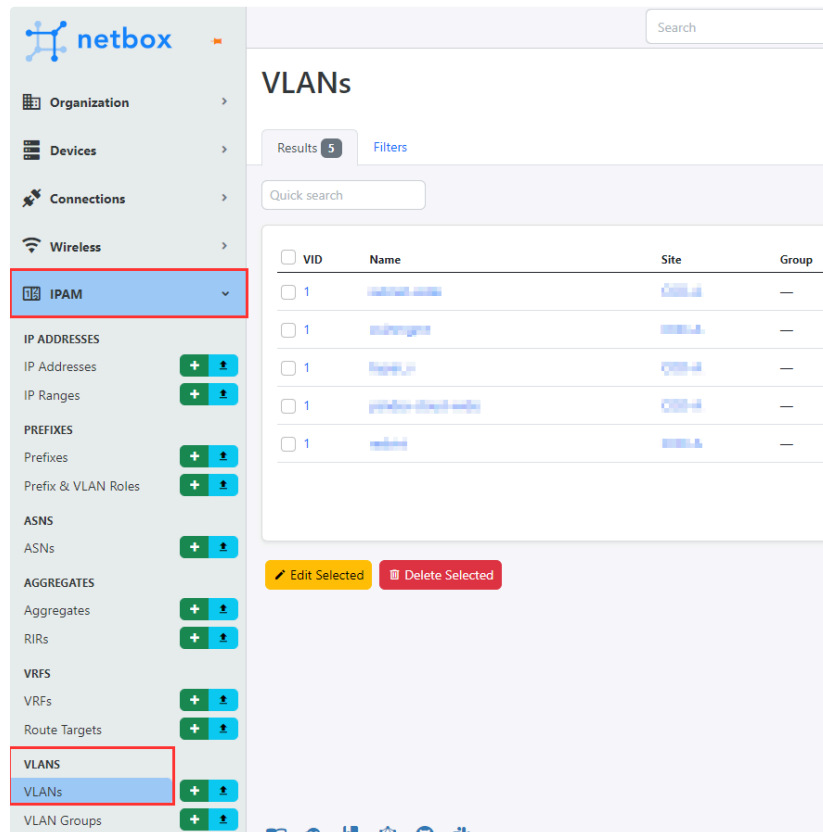
```
docker run -it --network host --rm \  
-v /$HOME/portal-box:/apps \  
-v ~/.ssh/id_rsa:/root/.ssh/id_rsa \  
-v ~/.kube/cloudlink:/root/.kube/cloudlink \  
deploy-manager-1.5.0 \  
-i inventories/box/hosts \  
-u $USER \  
portal_box.yml \  
--ask-vault-pass \  
--tags info
```

2. Перейдите по адресу, указанному в результатах выполнения задачи **Portal admin credentials**.
3. Скачайте корневой сертификат сайта и добавьте его в доверенные на вашем ПК. В случае, если сертификат не добавлен в доверенные, могут возникнуть проблемы с открытием портала Cloudlink.
4. 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 Vault по адресу <https://vault.sample.box/ui/vault/secrets/deployment/show/netbox>
- В интерфейсе NetBox перейдите на вкладку слева **IPAM** → **VLANs** → **VLANs**.



c. 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** — представляет собой группу ресурсов, используемую 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 vSphere**

► **Пример создания VLAN для Zvirt**

- Создайте подсеть, в которой будут находиться виртуальные машины. Для этого в интерфейсе NetBox перейдите на вкладку слева **IPAM** → **Prefixes** → **Prefixes**.
- Зарезервируйте занятые IP-адреса в подсети:

- (Не рекомендуется для нескольких IP по порядку) В интерфейсе NetBox перейдите на вкладку слева **IPAM** → **IP Addresses** → **IP Addresses** <https://netbox.sample.box/ipam/ip-addresses/> и зарезервируйте IP-адреса.

В примере показана резервация IP-адреса сетевого шлюза:

```
Address = 10.15.8.1/24
Status = Reserved
VRF = DEV_DEV (dev_dev)
Description = Gateway
Tenant = BOX
```

BASH |

- (Рекомендуется для нескольких IP по порядку) В интерфейсе NetBox перейдите на вкладку слева **IPAM** → **IP Addresses** → **IP Ranges** <https://netbox.sample.box/ipam/ip-ranges/> и зарезервируйте IP-адреса.

Для примера взят диапазон первых 123 IP-адресов в подсети 10.15.8.0.24

```
VRF = DEV_DEV (dev_dev)
Start address = 10.15.8.1/24
End address = 10.15.8.123/24
Status = Reserved
Description = [vSphere] Reserved
Tenant = BOX
```

BASH |

5. Зачислите деньги для организации через контрольную панель <https://control.sample.box/>. Для этого:

- Авторизуйтесь под пользователем admin-box.
- Перейдите в раздел **Биллинг** → **Пополнение счета**.
- Выберите организацию, счет отправителя и получателя, сумму, описание.
- Нажмите **Подтвердить**.
- Перейдите в орг.структуру портала <https://portal.sample.box/management/org-structure>.
- Нажмите на [:] напротив названия организации и выберите **Перевести**.
- Выберите счет получателя, сумму, укажите описание.
- Нажмите **Перевести**.

1.6. Обновление портала

Вы можете обновиться до целевой версии портала с любой версии, начиная с указанной минимальной версии и заканчивая той, что предшествует целевой. Подробнее о минимальной и целевой версиях портала в таблице ниже.

Пример: До версии 1.23 можно обновиться с версий 1.6 - 1.22.

Версия портала	Минимальная версия
1.1 - 1.6	1.0
1.7 - 1.24	1.6
1.25 - 1.26	1.21
1.27 и новее	1.25

Чтобы обновить портал, выполните следующие действия:

1. Разархивируйте новую версию дистрибутива в **отдельную директорию**.
2. Скопируйте **inventory/sample** в **inventories/box** (аналогично процессу установки с нуля). Это будет новый inventory для обновленного портала.
3. Перенесите значения из старых файлов **config.yml** и **hosts** в соответствующие разделы нового inventory.

Не копируйте старые файлы целиком: структура нового файла конфигурации могла измениться, поэтому совместимость не гарантируется.

4. Продолжите процесс обновления портала после заполнения нового inventory значениями. Процесс аналогичен установке портала с нуля.
5. Выполните действия после обновления, если они есть. При обновлении через несколько версий (например, с 1.10 до 1.12), выполняйте действия для каждой промежуточной версии по порядку (1.10, 1.11, 1.12 и т.д.). Если действий для какой-то версии нет, пропустите её.

1.7. Установка патчей для портала

Для установки патча выполните следующие шаги:

1. Скопируйте архив с патчем.
2. Выполните команду, где `PATH_TO_PATCH_ARCHIVE` — путь до файла архива:

```
manage-tool --update-services PATH_TO_PATCH_ARCHIVE
```

BASH |

3. После сообщения об успешном обновлении запустите команду развертывания, чтобы применить обновления.

1.8. Миграция данных между разными инсталляциями

Установщик Cloudlink поддерживает миграцию данных между различными инсталляциями, начиная с версии 1.9.



Миграцию рекомендуется проводить между одинаковыми версиями портала.

Для выполнения миграции:

1. Разверните инсталляции source и destination, используя стандартный процесс установки.
2. Укажите путь к `kubeconfig` для обеих инсталляций (source и destination) в файле **migration.yml**.
3. Запустите playbook с помощью команды:

```
ansible-playbook migration.yml -vv
```

BASH |



Это действие деструктивно для destination-кластера — все его объекты будут заменены данными из source-кластера.

4. Разверните destination-кластер повторно, используя стандартный процесс установки.

1.9. Действия после обновления

1.9.1. Описание для подготовки к выполнению команд

Для выполнения обновления после обновления версии, требуется:

1. Подключение к хостам по SSH. Для этого:

```
ssh root@${IP/DNS}
# или команда:
ssh ${USERNAME}@${IP/DNS}
sudo su
```

BASH |

2. Root-права

3. Получение списка подов (имен):

```
kubectl get pods -n portal-box
# или команда:
```

BASH |

```
# kubectl get pods -n portal-box | grep ${SERVICE_NAME}
```

- `${SERVICE_NAME}` — название сервиса (к примеру "lucrum-back", "auditor" и т.д.)

После получения имени пода выполните команду:

```
kubect -n portal-box exec -it ${POD_NAME} -- ${COMMAND}
```

BASH |

1.9.2. Release 1.15

С е р в и с	Команда	kubectl	О п и с а н и е и к о м м е н т а р и и

о r d e r- m a n a g e r	<p>Запуск Rails консоли: rails c</p> <p>Выполнение команды внутри Rails консоли:</p> <p>Platform.without_deleted.update_all(disable_reservation: true, disable_reservation_for_action: true)</p>	<p>kubect -n portal-box exec -it \${POD_NAME} - rails runner 'Platform.without_deleted.update_all(disable_reservation: true, disable_reservation_for_action: true)'</p>	О т к л ю ч е н и е р е з е р в а ц и и д л я в с е х п л а т ф о р м . К о м а н д у н е о б х о д и м о в ы п о л н я т ь т о л ь
---	--	---	--

1.9.3. Release 1.20

Сервис	Команда	kubectl	Описание и комментарии
order-manager	bundle exec rake init_data:add_orders_to_iam	kubect -n portal-box exec -it \${POD_NAME} – bundle exec rake init_data:add_orders_to_iam	<p>Выполнить задачу по добавлении информации о существующих заказах.</p> <p>Команду нужно выполнять в main поде, если производится обновление портала. В иных случаях не требуется.</p>
order-manager	bundle exec rake update_data:orders:rename_simple_mode	kubect -n portal-box exec -it \${POD_NAME} – bundle exec rake update_data:orders:rename_simple_mode	<p>Выполнить задачу по добавлении информации о существующих заказах.</p> <p>Команду нужно выполнять в main поде, если производится обновление портала. В иных случаях не требуется.</p>

Сервис	Команда	kubectl	Описание и комментарии
calculator	python manage.py fix_manual_deleted	kubect -n portal-box exec -it \${POD_NAME} - python manage.py fix_manual_deleted	Выполнить задачу, она пересчитывает поврежденные ручным удалением объекты. # Команду нужно выполнять, если производится обновление портала. В иных случаях не требуется.#
calculator	python manage.py calc_not_calculated_prices	kubect -n portal-box exec -it \${POD_NAME} - python manage.py calc_not_calculated_prices	Выполнить задачу, она пересчитывает пропущенные/не посчитанные заказы. Команду нужно выполнять, если производится обновление портала. В иных случаях не требуется.

1.9.4. Release 1.22

Сервис	Команда	kubectl	Описание и комментарии
netbox			Изменились теги для префиксов (Prefixes) сетей в Netbox для zVirt и redvirt. Новые теги основанные на cluster_id создаются автоматически, но необходимо заменить cluster_name на cluster_id вручную во вкладке Prefixes по ссылке https://netbox.{hostname}/ipam/prefixes .

1.10. Контрольные суммы

Версия	MD5
1.21	9f61fc0cd11706d7eec28cd71541a599
1.22	f68e04cc580390d09c62fbb55e3743ca

2. Установка Nova Universe для Cloudlink

Перед тем, как заказать Nova Container Platform в Cloudlink, 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.

2.1. Технические требования к серверу управления Nova Universe

2.1.1. Требования к среде размещения

Для Nova Universe рекомендуются использовать платформы виртуализации zVirt и VMware vSphere.

Формат образа виртуальной машины qcow2 является нативным для zVirt.

Для размещения сервера управления в vSphere, следует провести дополнительные действия. Подробнее о них — в разделе создания виртуальной машины из образа в среде виртуализации VMware vSphere.

2.1.2. Требования к ресурсам

Для запуска сервера управления Nova Universe необходимо следующее количество ресурсов:

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.

2.1.3. 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.

2.1.4. Требования к системе разрешения имен DNS

Для работы сервера управления Nova Universe нужно создать следующие 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 т.д.

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

2.1.5. 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 следующие 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

2.2. Установка сервера управления

Для установки сервера управления выполните следующие действия.

2.2.1. Создание VM из образа

Создайте виртуальную машину из образа в среде виртуализации zVirt или VMware vSphere:

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 и 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.

VMware vSphere

1. Перед созданием виртуальной машины из образа, конвертируйте образ из формата qcow2 в vmdk:
 - a. Откройте терминал в своей системе.
 - b. Выполните следующую команду для конвертации:


```
qemu-img convert -p -f qcow2 -O vmdk universe.qcow2 universe.vmdk
```

BASH | 

- `universe.qcow2` — название исходного образа в формате qcow2.
- `universe.vmdk` — название, которое нужно присвоить конвертированному образу в формате vmdk.

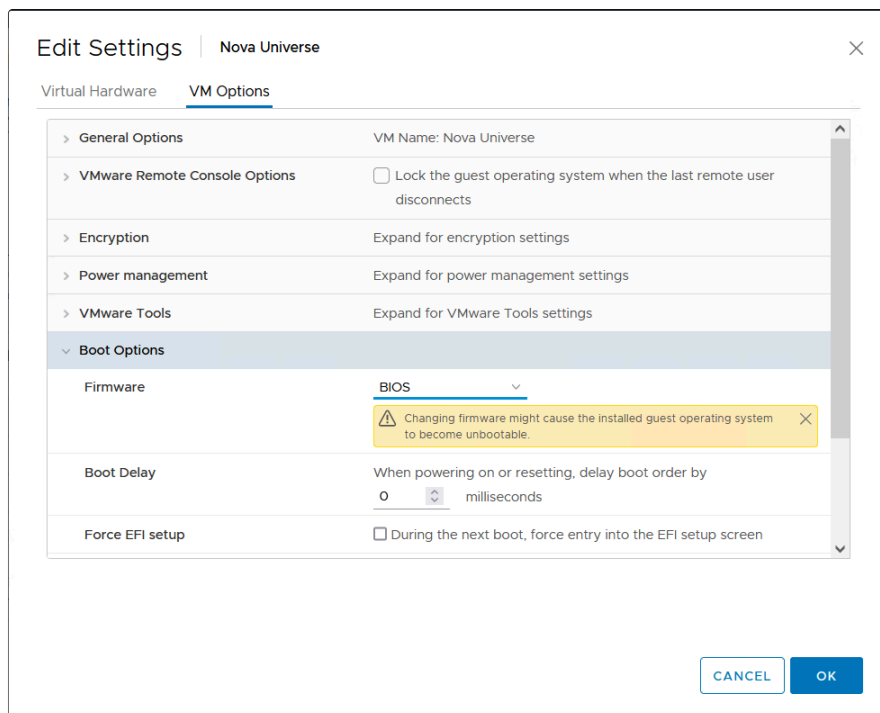
2. Загрузите образ на хост ESXi и выполните следующую команду для создания тонкого диска (thin provisioned) из конвертированного образа:

```
vmkfstools -i universe.vmdk -d thin converted_universe.vmdk
```

BASH | 

- `universe.vmdk` — название конвертированного образа в формате vmdk.
- `converted_universe.vmdk` - название, которое нужно присвоить созданному тонкому диску.

3. Создайте новую виртуальную машину в соответствии с требованиями и прикрепите образ сервера `converted_universe.vmdk`.
4. Измените режим загрузки виртуальной машины на BIOS:
 - a. В интерфейсе управления VMware ESXi откройте настройки вашей виртуальной машины: **VM → Actions → Edit settings → VM Options**.
 - b. Перейдите в раздел **Boot Options** и в параметрах **Firmware** выберите **BIOS**.



2.2.2. Запуск сервера и доступ к интерфейсу управления

Запустите VM сервера управления из образа и дождитесь окончания загрузки. После успешной загрузки VM 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.

2.2.3. Изменение пароля учетной записи по умолчанию

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

Для этого:

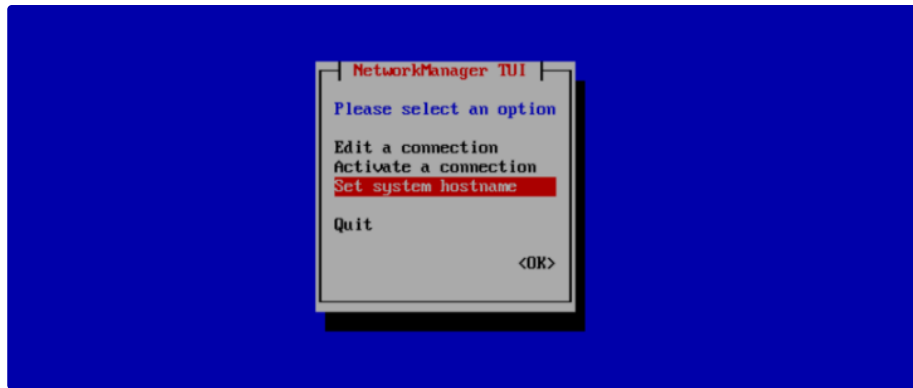
1. Перейдите в раздел **Configure**.
2. Выберите опцию **Change user password** и установите пароль согласно требованиям:
 - В пароле есть буквы разного регистра, цифры и специальные символы.
 - Длина не менее 8 символов.
 - Не используются простые и повторяющиеся слова.

2.2.4. 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).



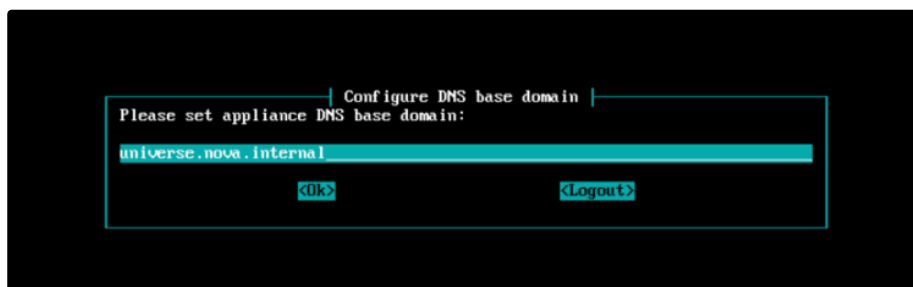
3. Сделайте настройки с помощью опций:

- **Set system hostname** — для установки названия сервера.
- **Edit a connection** — для изменения текущего подключения.
- **Activate a connection** — для активации или деактивации существующего подключения.

2.2.5. 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 имен DNS.



Инициализация сервера управления

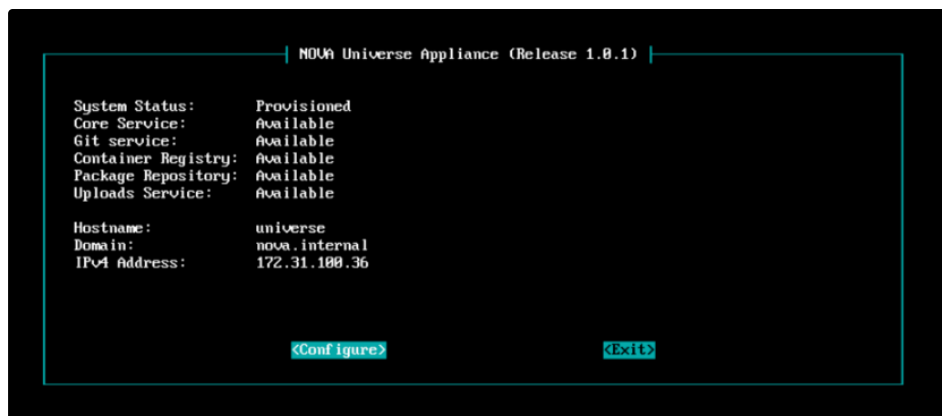
После установки параметров сетевого интерфейса и базового DNS-имени вам необходимо выполнить первичную инициализацию Nova Universe.

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 Cloudlink. Их нужно добавить в качестве значений к соответствующим переменным в файле конфигурации `config.yml`:

```
# Базовый домен, который был установлен при разворачивании 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'
```

PERL I

2.2.6. 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. Рекомендуется добавить сертификат сервера управления в доверенные на локальной машине.

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
```