## Учреждение образования

## Белорусский государственный технологический университет

Кафедра информационных систем и технологий

**ЛАБОРАТОРНАЯ РАБОТА 5**

по дисциплине «Облачные технологии»

Выполнил студент

Бобрович Г.С.

Минск 2024

**Настройка совместной работы управляющего и рабочего узлов облака**

**I. Настройка совместной работы управляющего и рабочего узлов.**

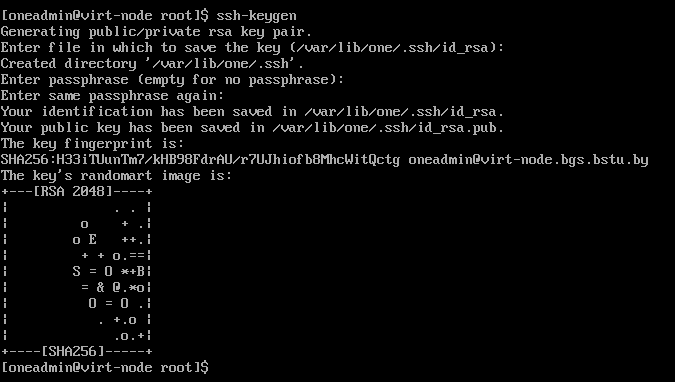
**1. Настройка и проверка беспарольного доступа между упраляющим и рабочими узлами в облаке OpenNebula.**

**1.1 Настройка беспарольного доступа между узлами кластера виртуализации вручную.**

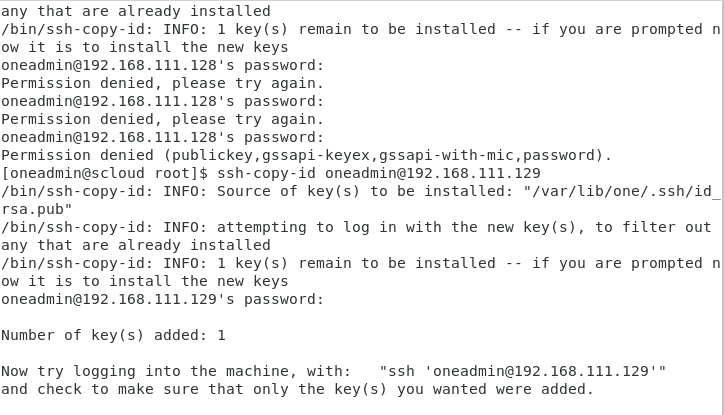
1) необходимо выполнить:

# ssh-keygen





По этой команде будет создана новая пара ключей публичный/личный.



**1.1.1 Проверка существующих ключей rsa на узлах.**

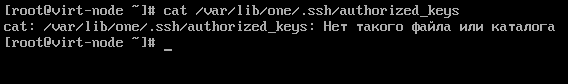
Когда пакеты ПО OpenNebula установлены на управляющем узле (фронт-енд), то это значит, что ключи SSH уже были сгенерированы и занесены в файл authorized\_keys.

a) На УУ проверить это можно с помощью команды:

# cat /var/lib/one/.ssh/authorized\_keys

 б) Проверяем наличие ключей на УВ (узле виртуализации):

[root@virt-node ~]# cat /var/lib/one/.ssh/authorized\_keys



На УУ ключ rsa для пользователя oneadmin@scloud.tgl.bstu.by имеется. На УВ ключей rsa для пользователя oneadmin пока нет, т.к. на этом узле нет рабочего каталога пользователя oneadmin.

**1.1.2 Создание файл known\_hosts на управляющем узле**

Для создания файла known\_hosts на управляющем узле необходимо выполнить:

а) Перейти в уч.запись oneadmin:

# su oneadmin

$

Проверяем результат:

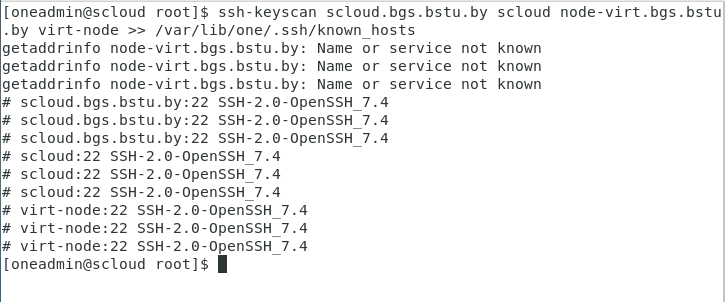
$ whoami

oneadmin

$

б) **из-под учетной записи oneadmin** выполнить следующую команду, указав в ней имена всех узлов (управляющего и виртуализации в качестве параметров). Эта команда просканирует все узлы, соберет с них ключи и поместит их в файл **known\_hosts** на управляющем узле:

$ ssh-keyscan scloud.tgl.bstu.by scloud node-virt.tgl.bstu.by



в) Проверяем результат

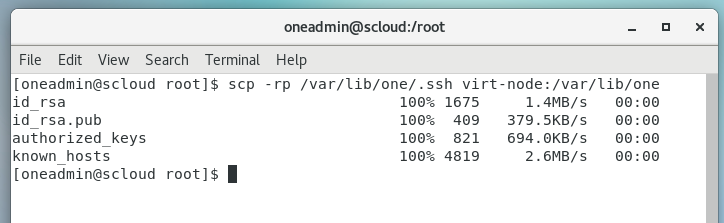
- на УУ:

Файл known\_hosts действительно создан, и в нем хранятся ключи узлов virt-node.tgl.bstu.by и scloud.tgl.bstu.by.

**1.1.3 Синхронизация содержимого каталог /var/lib/one/.ssh между управляющим и рабочим узлами**

б) Копирование осуществляется с помощью команды scp (копирование по ssh) (**выполняется на УУ c правами root,** т.к. у пользователя oneadmin на virt-node нет пароля, он не назначен):

# scp -rp /var/lib/one/.ssh virt-node:/var/lib/one/

Копирование прошло успешно.

в) На узле virt-node проверяем результат из под уч.записи oneadmin.

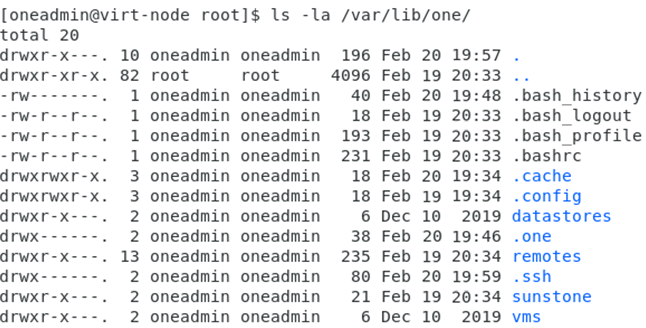
- Смотрим содержимое файла known\_hosts

$ cat /var/lib/one/.ssh/known\_hosts



- Смотрим список файлов в домашнем каталоге пользователя oneadmin

$ ls -la /var/lib/one/



Примечание. Файл начинающийся с точки "." в ОС Linux(Unix) является скрытым. Скрытые файлы не показываются комадой ls (показать список файлов) для просмотра скрытых файлов используеися ключ –a.

Из-за того, что копирование каталога .ssh с УУ на УВ выполнялось из под root некоторые файлы в качестве владельца и группы владельца имеют root, это надо поправить.

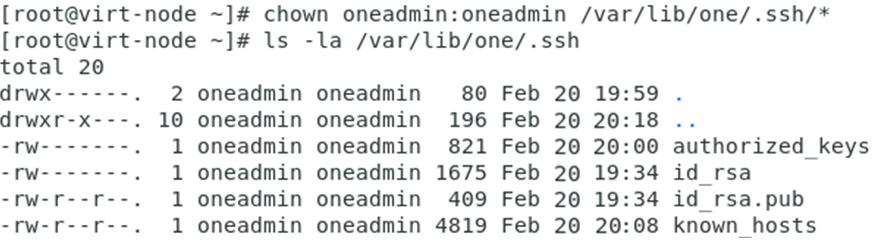
Изменить владельца каталога .ssh с помощью команд:

$ su root

Пароль:

#

# chown oneadmin:oneadmin /var/lib/one/.ssh



**1.1.4 Проверка беспарольных подключений между узлами по SSH**

Надо проверить возможность беспарольных подключений под учетной записью oneadmin в следующих направлениях:

* с управляющего узла (УУ) на узлы виртуализации (УВ);
* с УУ на сам УУ;
* с УВ на УУ.

Для этого выполним команды:

а) Начинаем с УУ (scloud):

Переключаемся в уч. запись oneadmin

[root@scloud ~]# su oneadmin

[oneadmin@scloud root]$ whoami

oneadmin

[oneadmin@scloud root]$

Выполняем подключение с УУ на УУ:

[oneadmin@scloud root]$ ssh scloud.tgl.bstu.by

Warning: Permanently added the ECDSA host key for IP address '192.168.231.132' to the list of known hosts.

Last login: Fri Feb 10 18:59:47 2023

[oneadmin@scloud ~]$

Успешно.

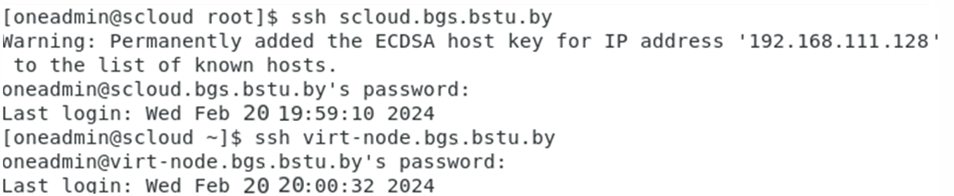
С УУ на УВ:

[oneadmin@scloud ~]$ ssh virt-node.tgl.bstu.by

Last login: Fri Feb 10 19:31:18 2023

[oneadmin@virt-node ~]$

Успешно.



С УВ на УВ:

[oneadmin@virt-node ~]$ ssh virt-node.tgl.bstu.by

Last login: Fri Feb 10 19:33:28 2023 from scloud

[oneadmin@virt-node ~]$

Успешно.

С УВ на УУ:

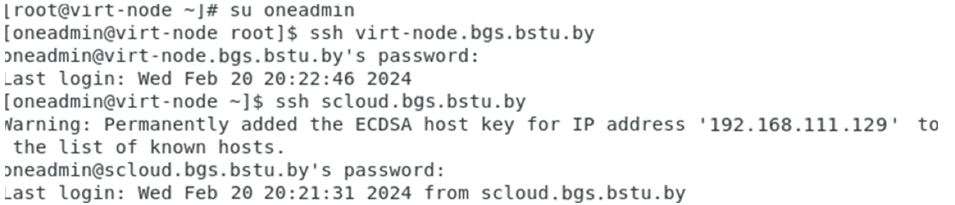
[oneadmin@virt-node ~]$ ssh scloud.tgl.bstu.by

Warning: Permanently added the ECDSA host key for IP address '192.168.231.132' to the list of known hosts.

Last login: Fri Feb 10 19:32:00 2023 from scloud

[oneadmin@scloud ~]$

Успешно.



**2 Создание моста на узле виртуализации.**

**2.1 Настройка сетевых интерфейсов на узле виртуализации**

в) Отредактируем файл ifcfg-br0

# nano /etc/sysconfig/network-scripts/ifcfg-br0

Если для назначения IP адреса на интерфейсе ens33 используется протокол dhcp, то файл ifcfg-br0 должен содержать следующие строки:

DEVICE=br0

NAME=br0

TYPE=Bridge

ONBOOT=yes

BOOTPROTO=dhcp

DEFROUTE=yes

IPV4\_FAILURE\_FATAL=no

IPV6INIT=yes

IPV6\_AUTOCONF=yes

IPV6\_DEFROUTE=yes

IPV6\_FAILURE\_FATAL=no

IPV6\_ADDR\_GEN\_MODE=stable-privacy

IPV6\_PRIVACY=no

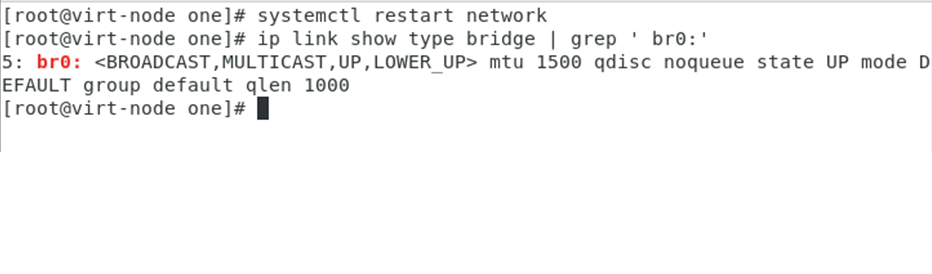


Примечание. Если в файле ifcfg-br0 содержатся и другие строки, то их можно либо оставить, либо закомментировать, т.е. поставить знак '#' в первую позицию строки. Обратите внимание, что строки не должны содержать пробелов.

**2.2 Перезапустить на узле виртуализации сервис network.**

а) Чтобы изменения в настройке сети на УВ вступили в силу необходимо перестаровать сервис network c помощью следующей команды:

# systemctl restart network

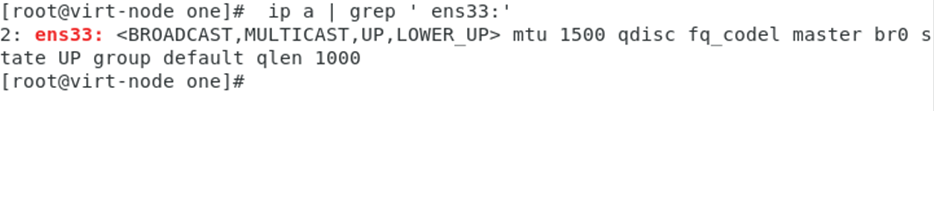


в) Проверяем состояние интерфейса ens33:

[root@virt-node network-scripts]# ip a | grep ' ens33:'

2: ens33: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc fq\_codel master br0 state UP group default qlen 1000

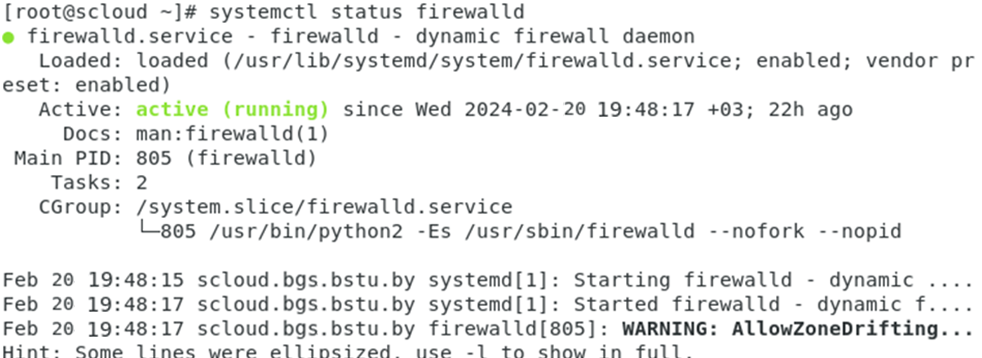
[root@virt-node network-scripts]#



**3. Открыть порты VNC на узле виртуализации**

Для этого необходимо внести в брэндмауэр firewalld, правило разрешающее доступ к этому узлу по портам TCP 5900-5999, предназначенным, для доступа к рабочему столу (если ВМ использует GUI) или консоли (если на ВМ используется CLI) УВ c помощью VNC (Virtual Network Computing).

а) Проверим состояние сервиса firewalld:



б) Просмотрим какие правила установлены в системе:



Видим, что разрешен только доступ по SSH и сервис dhcpv6-client.

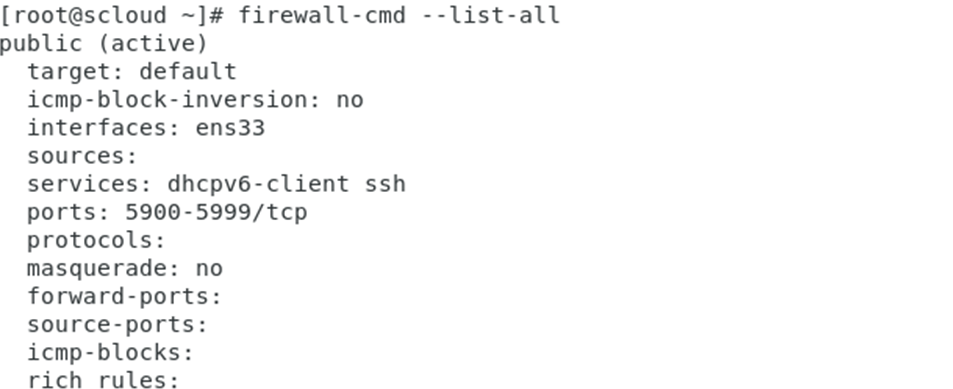
в) Откроем порты 5900-5999



г) Перезагрузим конфигурацию firewalld



ж)Просмотрим результат

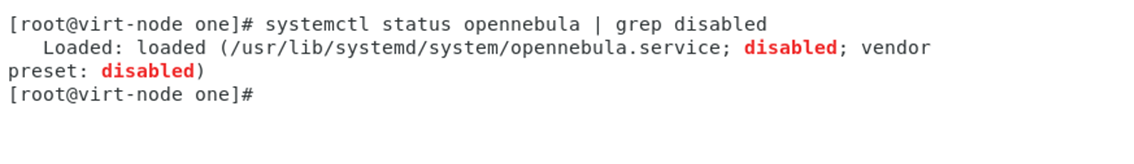


Теперь наши узлы управления и виртуализации готовы к подключению к облаку OpenNebula УВ, в качестве узла, на котором буду размещаться виртуальные машины.

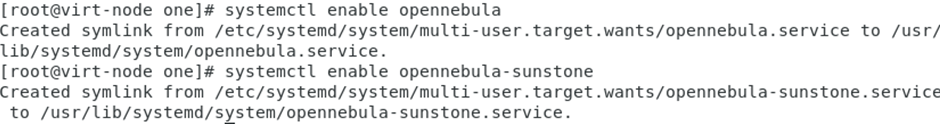
**4. Настройка запуска сервисов OpenNebula при перезагрузке системы:**

**3.1 на УУ:**

а) Проверяем настройки сервисов opennebula:

Обеим сервисам opennebule запрещено стартовать при загрузке системы:

б) Разрешаем запуск сервисов opennebula при загрузке ОС:



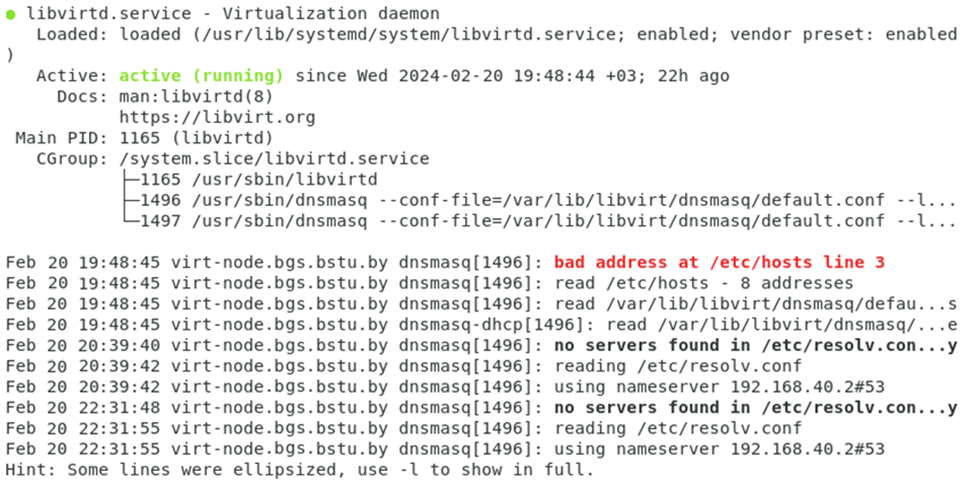
Старт сервисов opennebula при загрузке ОС разрешен

**4.1 на УВ:**

На УВ OpenNebula использует сервисы виртуализации libvirtd

а) Проверим настройки, касающиеся запуска этого сервиса при загрузке системы:

[root@virt-node ~]# systemctl status libvirt\*

Старт при загрузке ОС разрешен.

**4.2 Проверка поведения сервисов OpenNebula при перезагрузке ОС**

а) Выпоняем на обоих узлах команды:

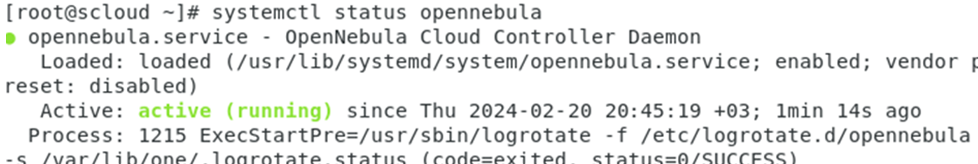
# su root

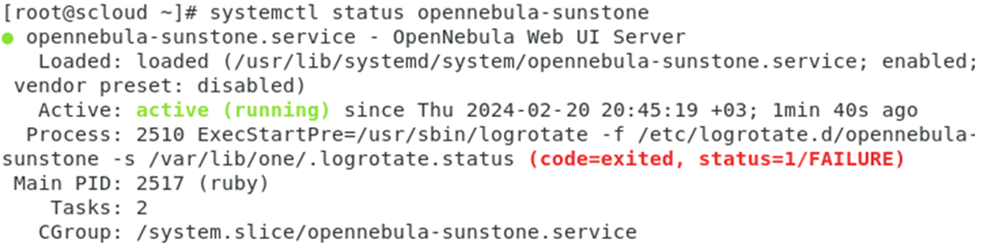
# reboot

б) После перезагрузки выполняем на управляющем узле

- проверяем состояние сервисов opennebula

[root@scloud ~]# systemctl status opennebula

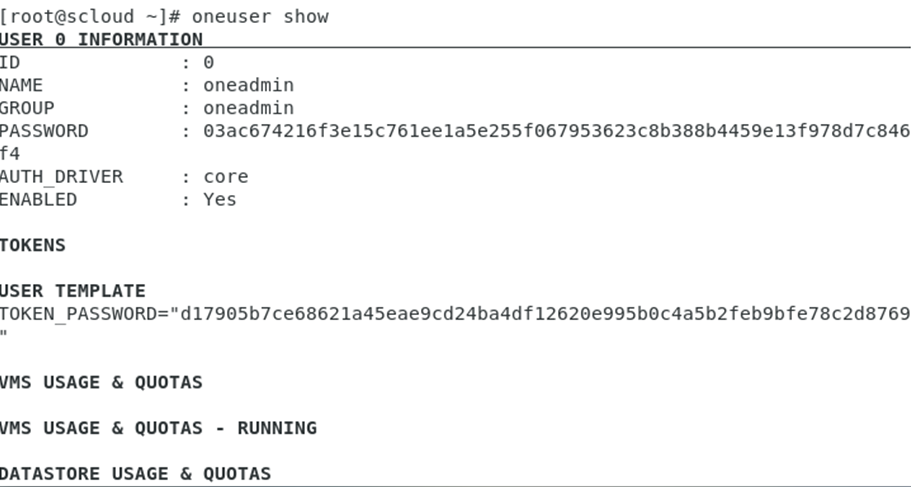




Оба сервиса после перезагрузки запустились успешно.

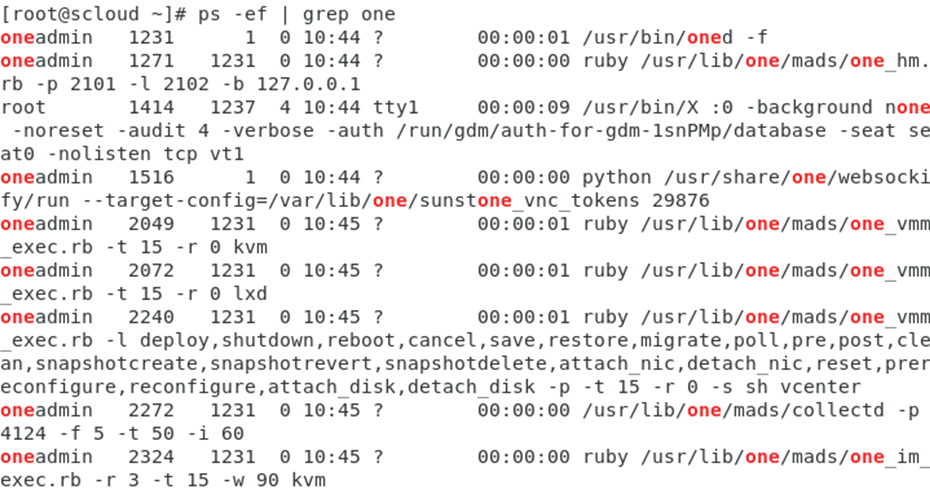
- проверяем работоспособность демонов one:

[root@scloud ~]# oneuser show



Смотрим процессы запущенные в системе от имени пользователя oneadmin

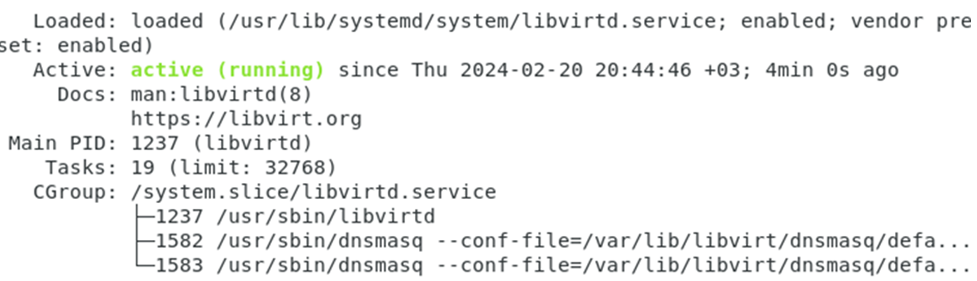
[root@scloud ~]# ps -ef | grep one

Сервисы OpenNebula успешно стартуют при перезапуске ОС.

в) После перезагрузки выполняем на узле виртуализации:

- проверяем состояние сервиса libvirtd

[root@virt-node ~]# systemctl status libvirt\*

- преключаемся на учетную запись oneadmin

[root@virt-node ~]# su oneadmin

[oneadmin@virt-node root]$

**5. Подключение рабочего узла к управляющему**

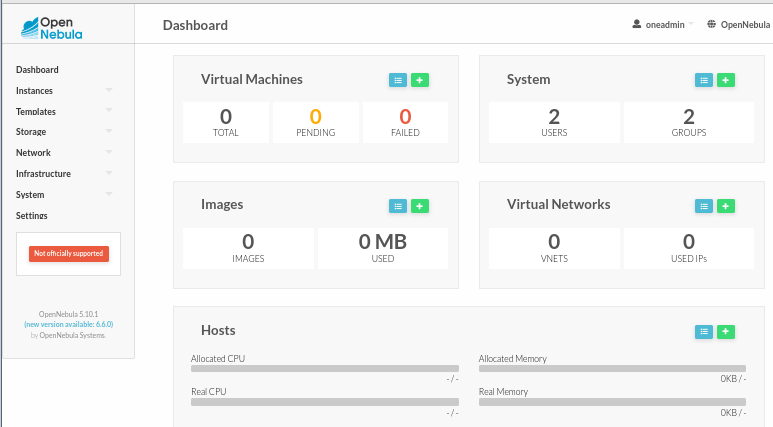
**5.1 С помощью GUI Sunstone (Web интерфейс)**

Теперь необходимо подключить созданный рабочий узел к облачному сервису. Выполняется на управляющем узле.

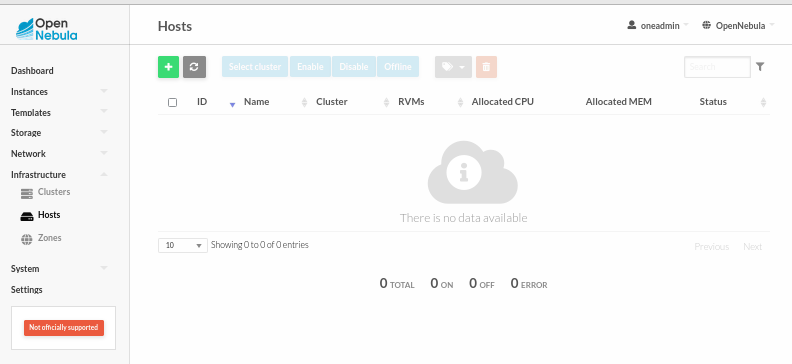
а) Для этого открываем браузер на управляющем узле, подключаемся к sunstoune (<http://localhost:9869/>



Кликаем Login



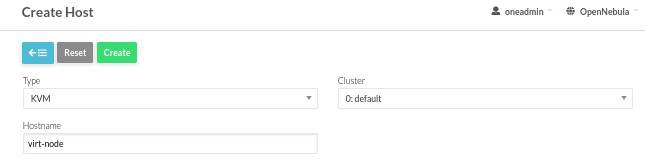
В левой панели окна разворачиваем строку Infrastructure, и кликаем строку Hosts. Откроется страница управления Hosts



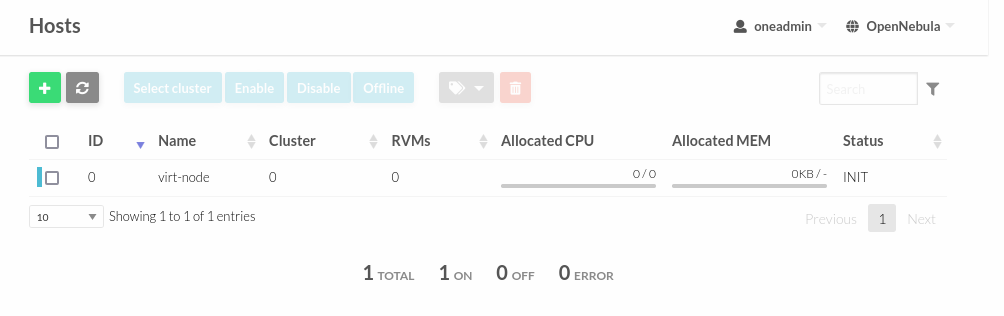
Для добавления УВ в инфраструктуру облака нажимаем значек добавить 

Откроется страница Create Host.

Будет выполнен переход на страницу «Create Host»



Здесь необходимо выбрать тип гипервизора и ввести имя (vipt-node) или IP адрес, подключаемого хоста виртуализации, затем кликнуть значек Create. Будет выполнен возврат в окно хостов, где появятся данные о подключенном рабочем узле виртуализации.



**5.2 Добавление хоста с помощью CLI**

Для добавления узла к облаку необходимо выполнить следующую команду от имени oneadmin **на управляющем узле**.

б) Проверка подключения узла виртуализации

[oneadmin@scloud root]$ onehost list



Если хост переходит в состояние err вместо on, то надо обратиться к журналу /var/log/one/oned.log. Возможно, что эта проблема связана с SSH.

**Итоги**

Проведена проверка работоспособности развернутых элементов облака OpenNebula 5.10. на управляющем узле под LinuxСentOS 7.

Проведена проверка работоспособности развернутых элементов облака на узле виртуализации под LinuxСentOS 7.

Настроен беспарольный доступ по SSH между УУ и УВ облака OpenNebula.

Узел виртуализации подключен к управляющему узлу ОН.