**Облачные технологии**

Лабораторная работа № 5

**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.**

Управляющий узел OpenNebula связывается с хостами гипервизоров с помощью SSH. Для работы УУ с узлами виртуализации и наоборот необходимо обеспечить прозрачный доступ по SSH в следующих направлениях:

от УУ (Front-end) к УУ (Front-end),

от УУ (Front-end) к хостам гипервизора (УВ),

от УУ (Front-end) к узлу гипервизора (УВ) и далее к другому узлу (УВ) (для выполнения операций миграции),

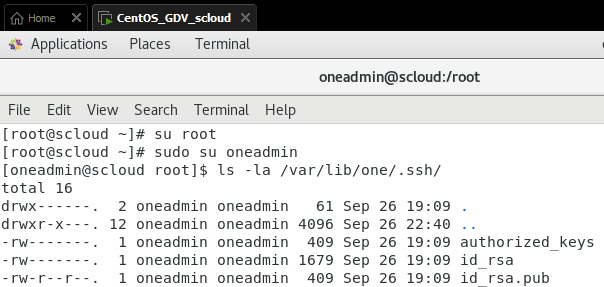
от Front-end к УВ (хоста гипервизора) и далее от УВ к УУ (Front-end) (для обратного копирования данных).

**Важно** Необходимо убедиться, что УУ и все УВ (хосты) могут подключаться друг к другу по SSH без ручного вмешательства.

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

При попытке подключения по SSH на обоих узлах (машинах), пытающихся установить SSH соединение генерируются ключи rsa, которые сохраняются в файлах id\_rsa и id\_rsa.pub, размещаемых в каталоге .ssh, находящемся в рабочем каталоге пользователя. Для пользователя oneadmin это каталог /var/lib/one/.ssh/

[oneadmin@scloud one]$ ls -la /var/lib/one/.ssh/



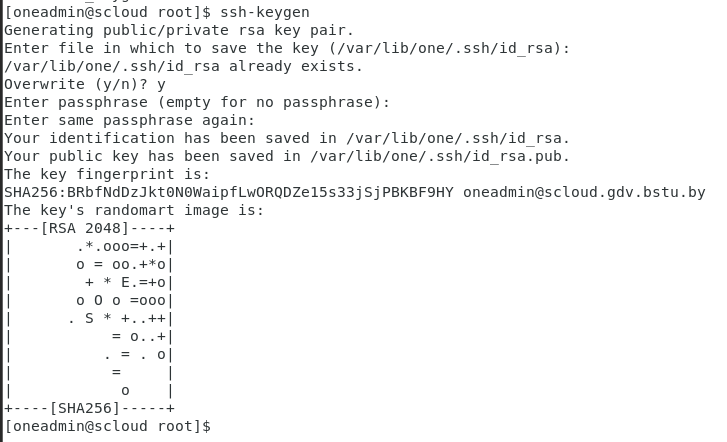
Для организации парольного доступа по SSH между узлами OpenNebula (УУ и УВ) необходимо распространить публичный ключ пользователя oneadmin с УУ на все остальные машины (УВ), поместив его в файл /var/lib/one/.ssh/authorized\_keys на всех машинах (УУ и УВ). Имеется много методов по выполнению распространения ключей SSH, в конце концов, администратор сам выбирает подходящий ему метод. Ниже описывается порядок распространения SSH ключей по узлам вручную с помощью команды scp.

Для создания ключей на управляющем узле:

1) необходимо выполнить:

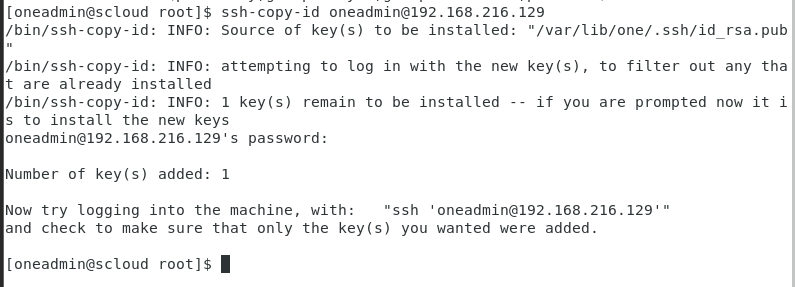
# ssh-keygen

По этой команде будет создана новая пара ключей публичный/личный. Кодовую фразу вводить не надо.



2) Затем, необходимо скопировать публичный ключ с управляющего на рабочий сервер с помощью команды:

# ssh-copy-id oneadmin@IP\_адрес\_сервера



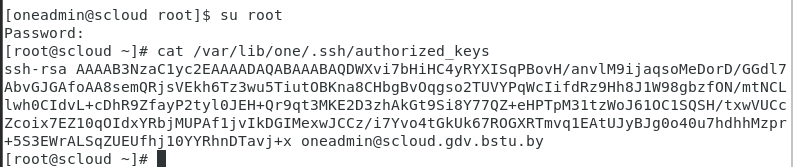
**1.1.1 Проверка существующих ключей rsa на узлах.**

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:

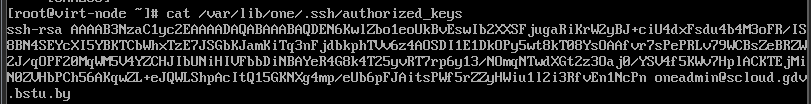
# cat /var/lib/one/.ssh/authorized\_keys

[root@scloud ~]# 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



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

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

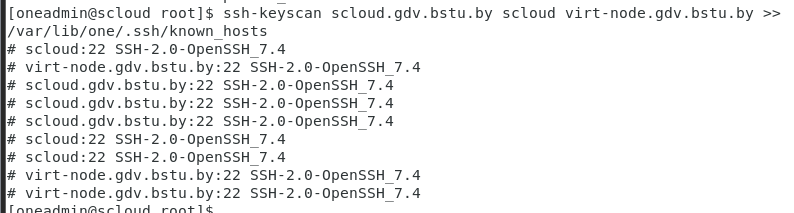
а) Перейти в уч.запись oneadmin:

# su oneadmin

Проверяем результат:

$ whoami

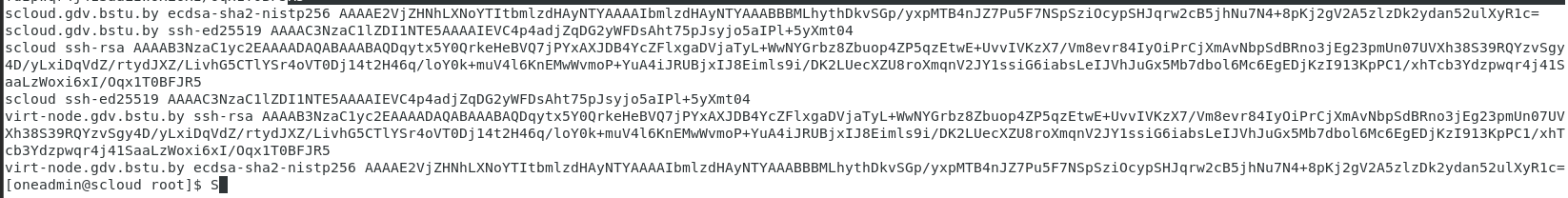
б) **из-под учетной записи oneadmin** выполнить следующую команду, указав в ней имена всех узлов (управляющего и виртуализации в качестве параметров). Эта команда просканирует все узлы, соберет с них ключи и поместит их в файл **known\_hosts** на управляющем узле:



в) Проверяем результат

- на УУ:





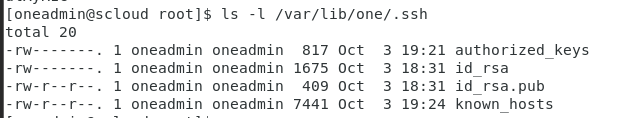
Файл known\_hosts действительно создан, и в нем хранятся ключи узлов virt-node.gdv.bstu.by и scloud.gdv.bstu.by.

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

Выполним синхронизацию содержимого файла known\_hosts управляющего узла с аналогичными файлами на всех узлах гипервизорах. Для этого требуется скопировать каталог /var/lib/one/.ssh с управляющего узла на все узлы виртуализации.

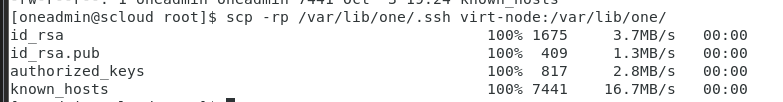
а) Перед выполнением копирования посмотрим содержание этого каталога на узлах виртуализации:

# ls -l /var/lib/one/.ssh

Каталога /var/lib/one/.ssh на узле виртуализации пока еще нет.

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/



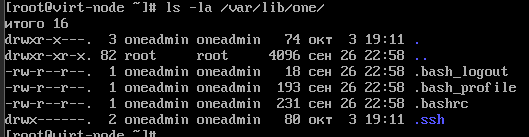
Копирование прошло успешно.

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

- Смотрим содержимое файла known\_hosts



- Смотрим список файлов в домашнем каталоге пользователя oneadmin



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

Проверяем:

# ls -la /var/lib/one/

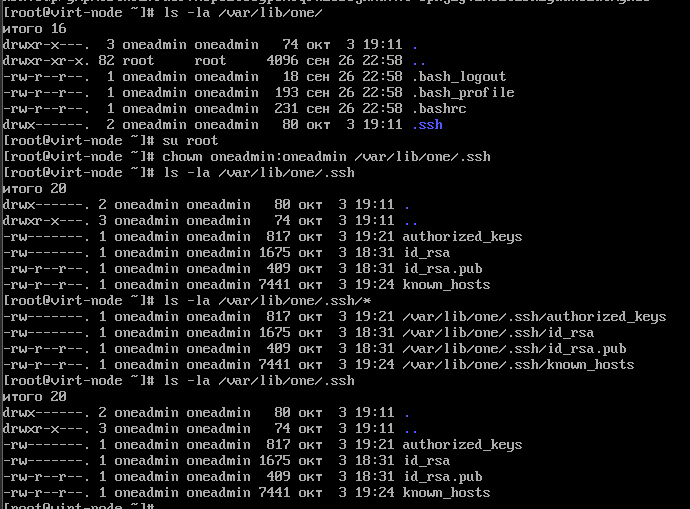
Смотрим содержимое файла .ssh, котрый был скопирован с УУ.

Видим что, так как мы копировали из под root, поэтому надо изменить владельца скопированных файлов:

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

Проверяем

[root@virt-node one]# ls -la /var/lib/one/.ssh



Все файлы имеет владельца и группу владельца: oneadmin oneadmin

Теперь необходимо проверить работу беспарольных подключений для учетной записи oneadmin

**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

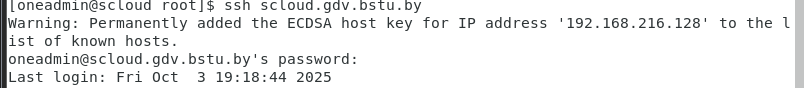
[oneadmin@scloud root]$ whoami

oneadmin

[oneadmin@scloud root]$

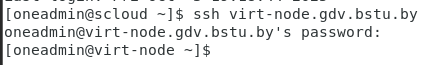
Выполняем подключение с УУ на УУ:

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



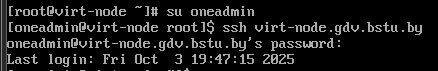
Успешно.

С УУ на УВ:



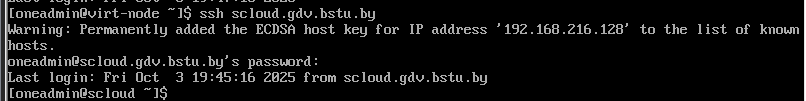
Успешно.

С УВ на УВ:



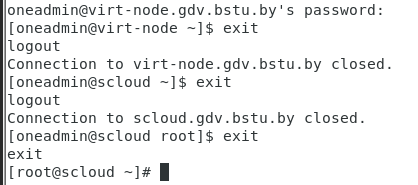
Успешно.

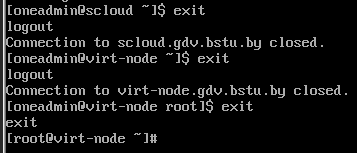
С УВ на УУ:



Успешно.

Закроем созданные ssh подключения: exit





**2 Создание моста на узле виртуализации.**

Для включения узла виртуализации в инфраструктуру облака, необходимо, чтобы сетевой интерфейс узла виртуализации был подключён к мостовому соединению. Здесь приводится пример с названием сетевого интерфейса ens33, но название интерфейса может быть любым, оно определяется при запуске системы. Opennebula требует, чтобы название моста было одинаковым на сетевых картах (интерфейсах) на всех рабочих узлах (на управляющем узле мост не создается).

Примечание. Рекомендуется сделать копии всех файлов конфигурации сетевых интерфейсов, перед их изменением!

Для этого можно выполнить команду:

# cp /etc/sysconfig/network-scripts/ifcfg-ens33 /etc/sysconfig/network-scripts/ifcfg-ens33.bak





**2.1 Настройка сетевых интерфейсов на узле виртуализации**

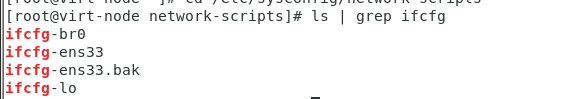
Мостовой интерфейс, также как и основной сетевой интерфейс (сетевая карту) настраивается с помощью файла.

а) Создадим файл настройки моста, назовем его br0, из файла настройки интерфейса ens33, путем копирования последнего:

# cp /etc/sysconfig/network-scripts/ifcfg-ens33 /etc/sysconfig/network-scripts/ifcfg-br0



Проверяем результат:

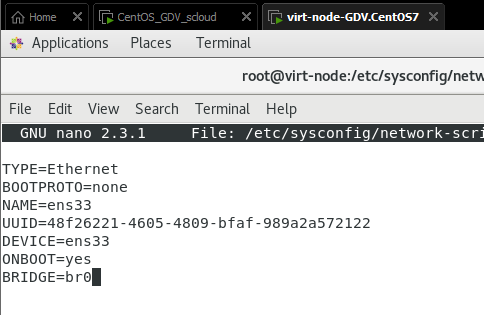


Видим, что имеютcя: файл бекапа, а также два файла конфигурации интерфейса и моста. Теперь следует отредактировать файлы конфигурации.

б) Изменим содержание файла /etc/sysconfig/network-scripts/ifcfg-ens33 путем его редактирования с помощью nano.

# nano /etc/sysconfig/network-scripts/ifcfg-ens33

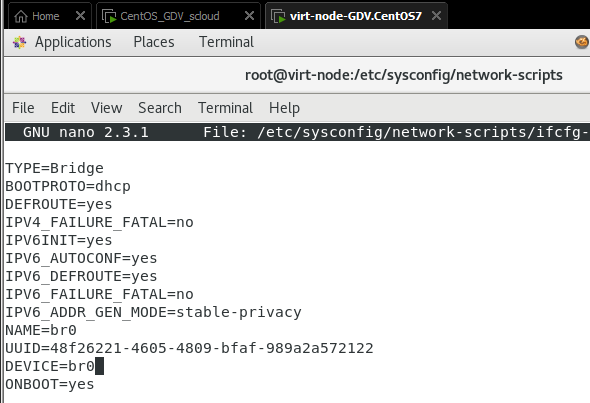
Редактирование сводится к удалению отдельных строк с помощью комбинации клавиш Ctr+K и изменения содержания некоторых строк. После редактирования файл ifcfg-ens33 должен содержать следующие строки:



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:

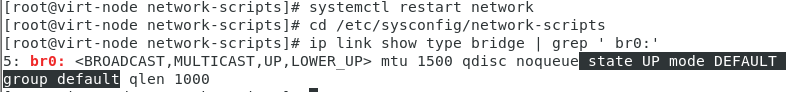


**2.2 Перезапустить на узле виртуализации сервис network.**

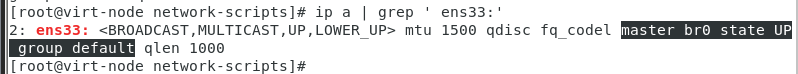
а) Чтобы изменения в настройке сети на УВ вступили в силу необходимо перестаровать сервис network c помощью следующей команды:

# systemctl restart network

б) Проверяем состояние моста с помощью команды:



в) Проверяем состояние интерфейса ens33:

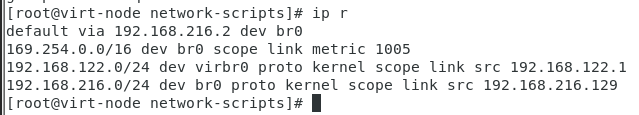


Примечание. Обратите внимание, что ни у интерфейса ens33, ни у моста br0 нет IP адреса, но оба находятся в состоянии UP.

г) Проверяем доступность сети с узла виртуализации

- проверяем маршрутизацию

# ip r



- проверяем доступность внешних ресурсов с узла виртуализации:

$ ping one

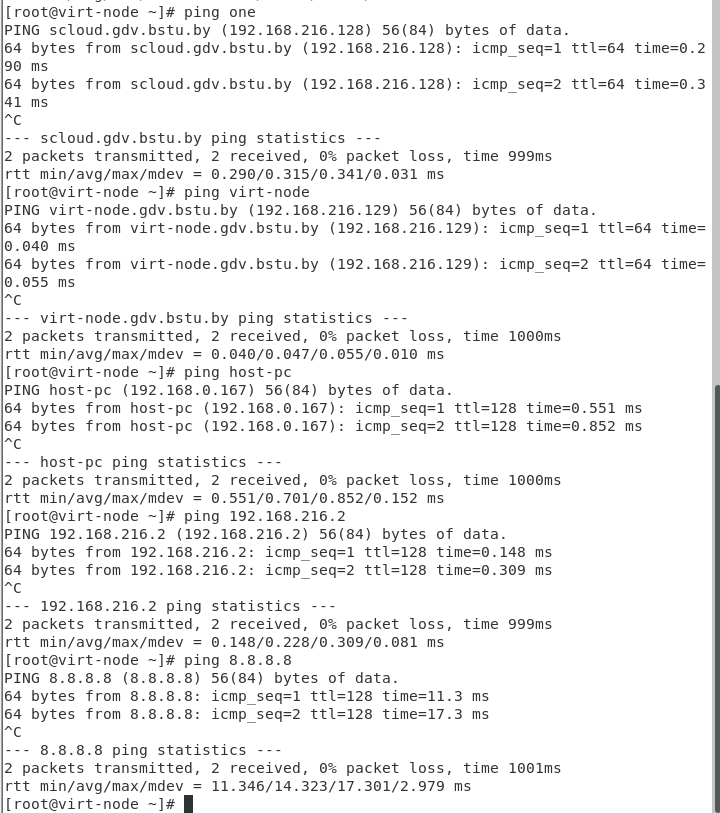
$ ping virt-node

$ ping gw

$ ping host-pc

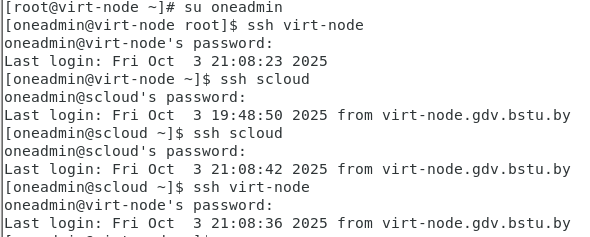
$ ping vmnet8

$ ping 8.8.8.8



д) Проверка беспарольного доступа между узлами

Выполняется из под учетной записи oneadmin на УВ:



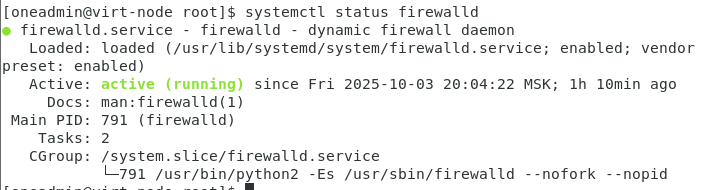
ОК!

Выполняем возврат (закрытие открытых SSH сессий):

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

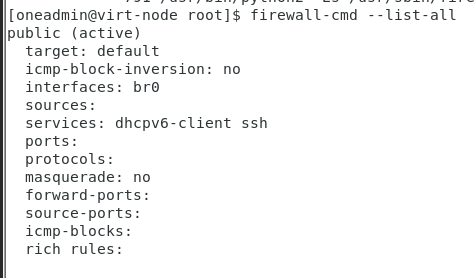
Для этого необходимо внести в брэндмауэр firewalld, правило разрешающее доступ к этому узлу по портам TCP 5900-5999, предназначенным, для доступа к рабочему столу (если ВМ использует GUI) или консоли (если на ВМ используется CLI) УВ c помощью VNC (Virtual Network Computing).

а) Проверим состояние сервиса firewalld:



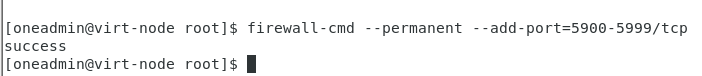
Сервис работает.

б) Просмотрим какие правила установлены в системе:



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

в) Откроем порты 5900-5999

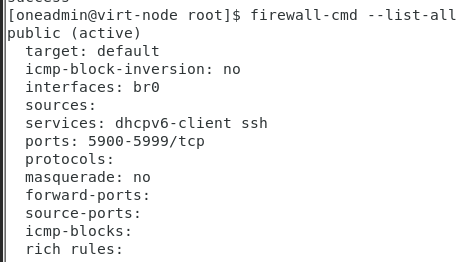


г) Перезагрузим конфигурацию firewalld



ж)Просмотрим результат

[root@virt-node ~]# firewall-cmd --list-all



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

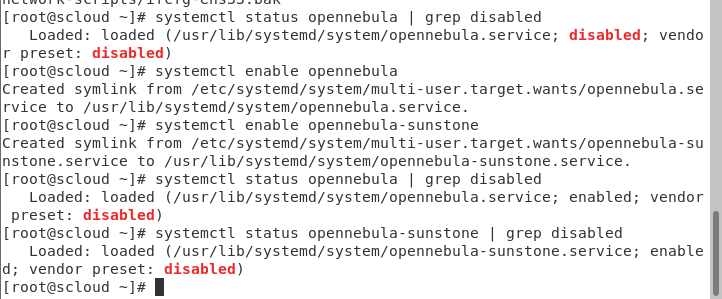
**3.1 на УУ:**

а) Проверяем настройки сервисов opennebula:

Обеим сервисам opennebule запрещено стартовать при загрузке системы.

б) Разрешаем запуск сервисов opennebula при загрузке ОС:

в) Проверяем:

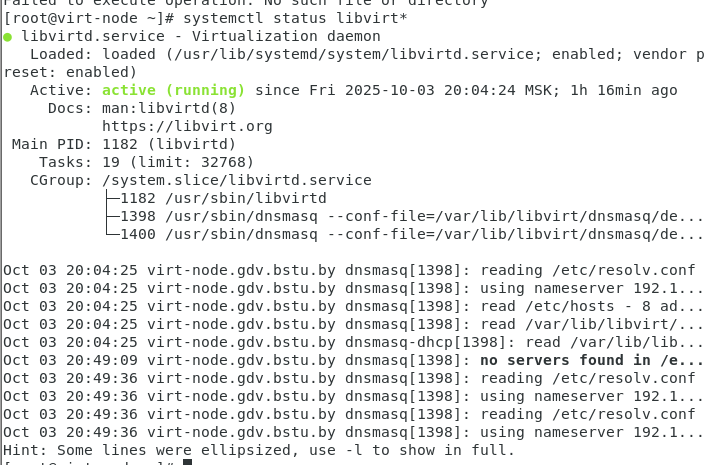
Старт сервисов opennebula при загрузке ОС разрешен

**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:

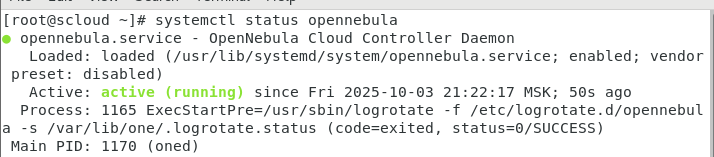
# su root

# reboot

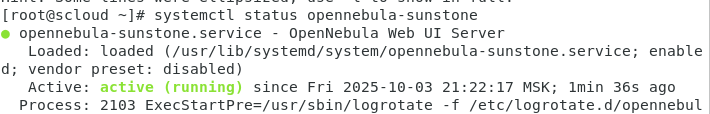
б) После перезагрузки выполняем на управляющем узле

- проверяем состояние сервисов opennebula

[root@scloud ~]# systemctl status opennebula



[root@scloud ~]# systemctl status opennebula-sunstone



Оба сервиса после перезагрузки запустились успешно.

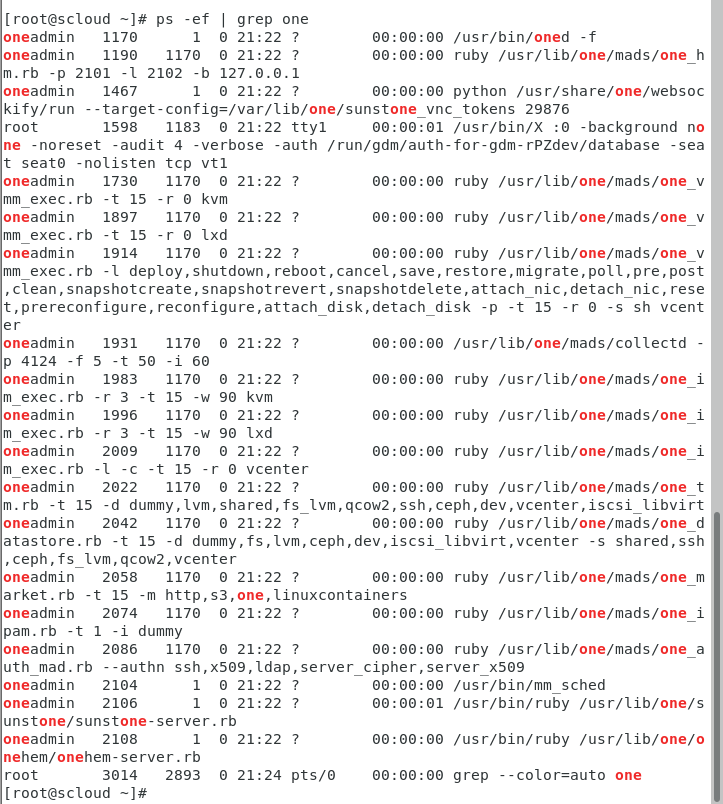
- проверяем работоспособность демонов one:

[root@scloud ~]# oneuser show



Смотрим процессы запущенные в системе от имени пользователя oneadmin

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

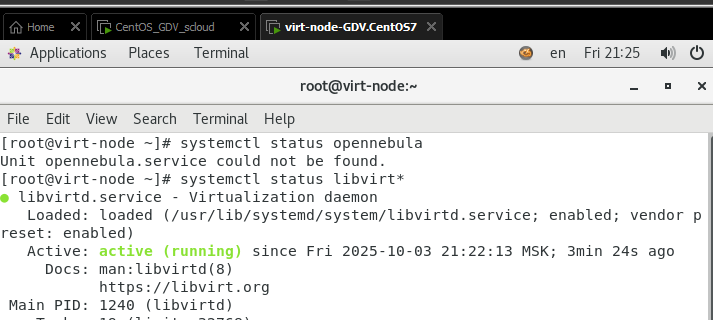


Сервисы OpenNebula успешно стартуют при перезапуске ОС.

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**

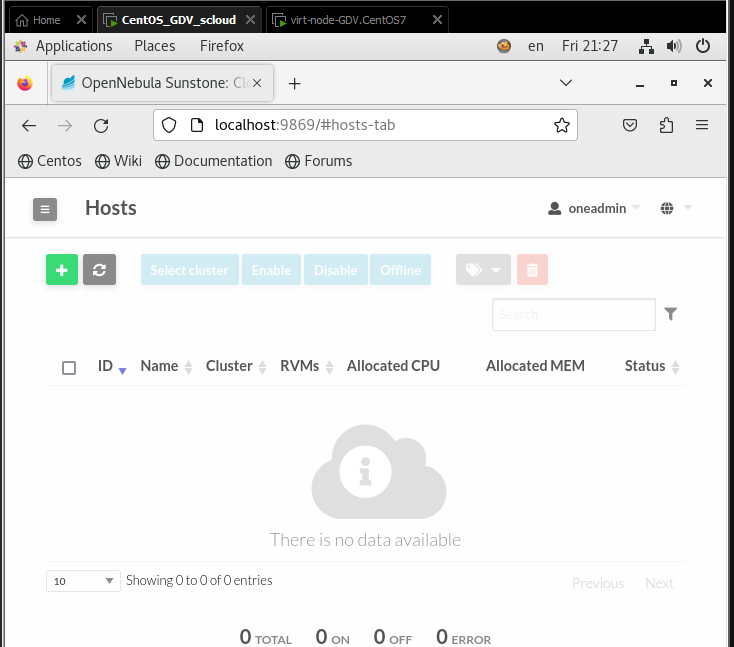
**5.1 С помощью GUI Sunstone (Web интерфейс)**

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

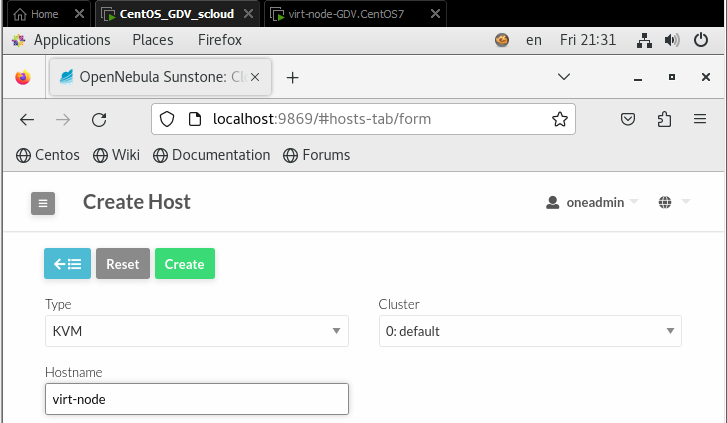
В левой панели окна разворачиваем строку Infrastructure, и кликаем строку Hosts. Откроется страница управления Hosts



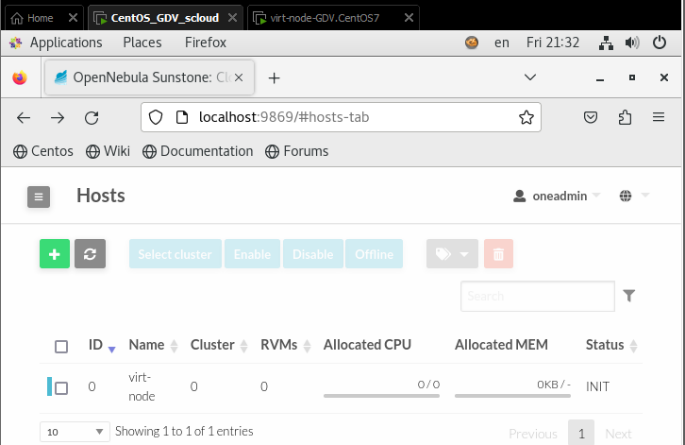
Для добавления УВ в инфраструктуру облака нажимаем значек добавить 

Откроется страница Create Host.

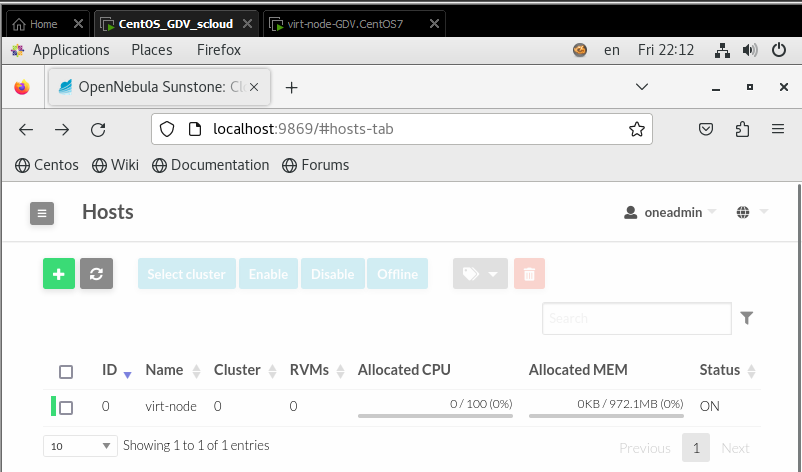
Будет выполнен переход на страницу «Create Host»



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.

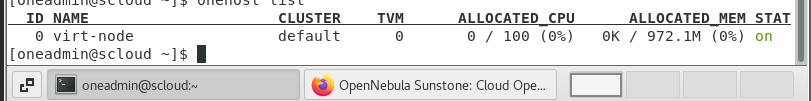


Состояние узла в случае удачного подключении будет INIT.



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.

**IV. Подготовка отчета**

**1. Подготовить отчет о выполнении данной работы.**

1.1 В отчет включите описание всех выполненных действий (раздел Выполнение работы).

1.2. Также в отчет необходимо включить ответы на контрольные вопросы (раздел Контрольные вопросы).

**V. Контрольные вопросы**

Данный раздел находится на стадии разработки

**VI. Защита отчета**

**1. Предъявите отчет преподавателю для защиты.**