**Облачные технологии**

Лабораторная работа № 5

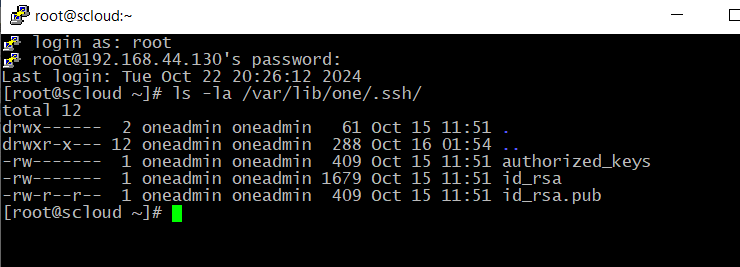
**Настройка совместной работы управляющего и рабочего узлов облака**

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

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

**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/



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.

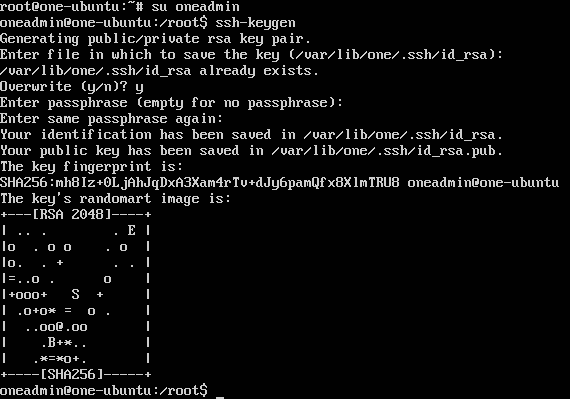
Замечание. Если на УУ или УВ отсутствуют ключи для пользователя oneadmin то их следует создать

Например, 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

После ввода пароля скопированный ключ будет добавлен в файл .ssh/authorized\_keys на рабочем сервере.

Для создания публичного ключа на узле виртуализации и его копирования на УУ, необходимо повторить п.п. 1), 2) на УВ.

Примечание. Файл known\_hosts используется для организации беспарольного (прозрачного) подключения (доступа) узлов друг к другу по SSH. Этот файл должен быть синхронизирован на всех узлах кластера OpenNrbula. Как выполняется настройка прозрачного доступа описывается ниже.

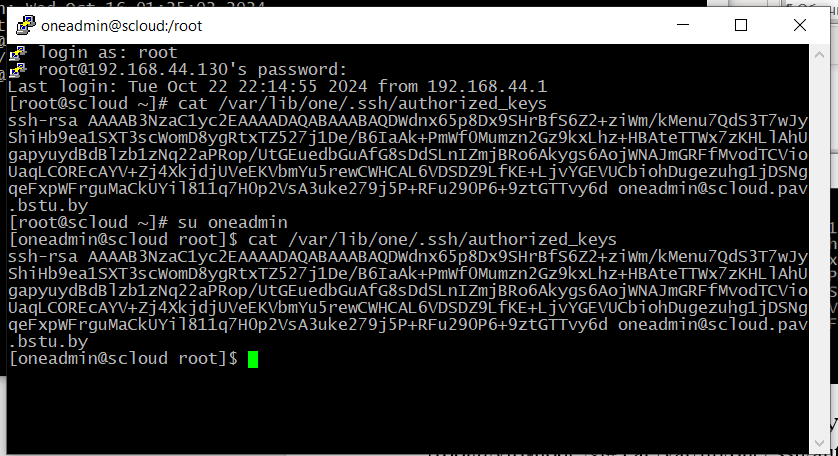
**1.1.1 Проверка существующих ключей rsa на узлах.**

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

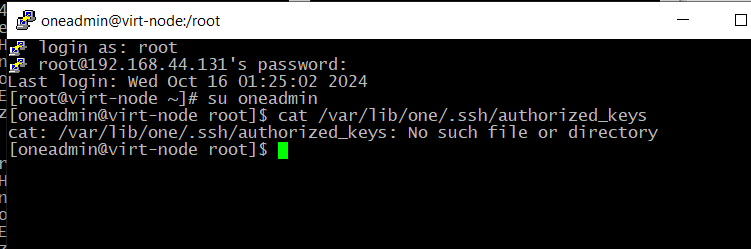
[root@scloud ~]# cat /var/lib/one/.ssh/authorized\_keys

ssh-rsa 

[root@scloud ~]#

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

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

 [root@virt-node ~]#

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:

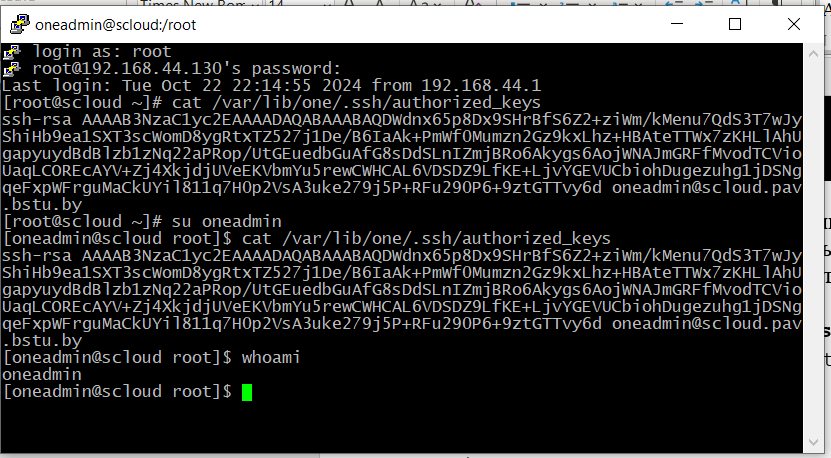
# su oneadmin

$

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 virt-node >> /var/lib/one/.ssh/known\_hosts

# virt-node.tgl.bstu.by:22 SSH-2.0-OpenSSH\_7.4

# virt-node.tgl.bstu.by:22 SSH-2.0-OpenSSH\_7.4

# virt-node.tgl.bstu.by:22 SSH-2.0-OpenSSH\_7.4

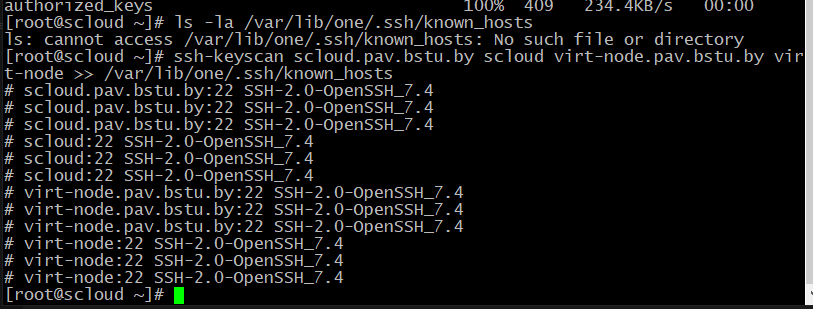
# scloud.tgl.bstu.by:22 SSH-2.0-OpenSSH\_7.4

# scloud.tgl.bstu.by:22 SSH-2.0-OpenSSH\_7.4

# scloud.tgl.bstu.by:22 SSH-2.0-OpenSSH\_7.4

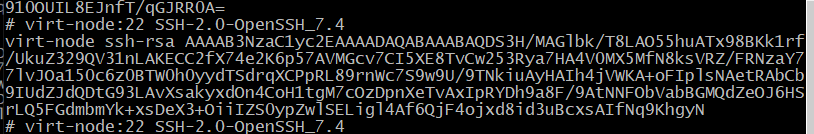
$

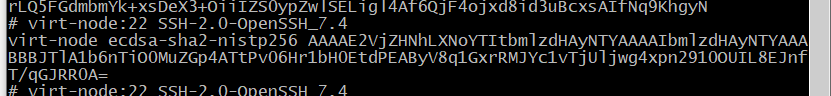


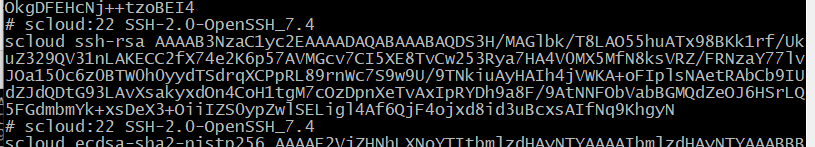


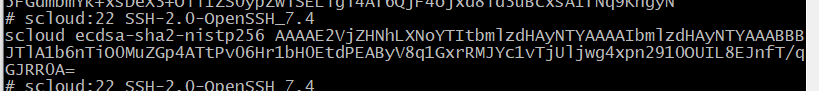
в) Проверяем результат

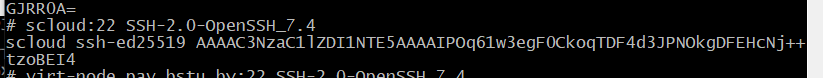
- на УУ:

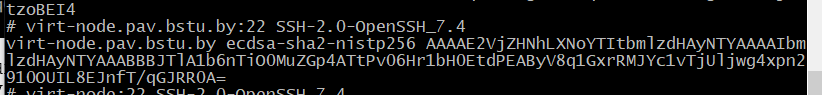
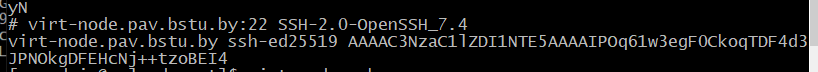
virt-node ecdsa-sha2-nistp256



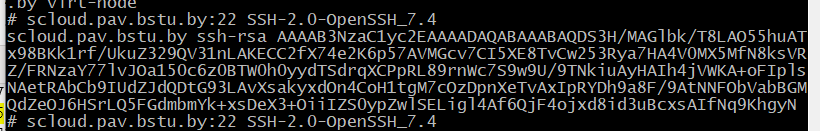
scloud ssh-rsa 

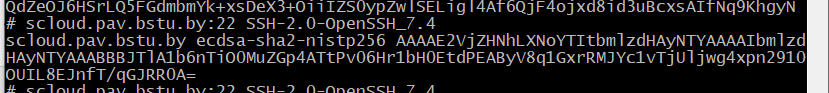
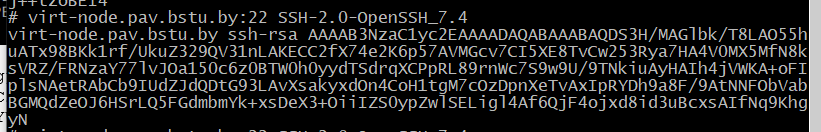
scloud ecdsa-sha2-nistp256 

scloud ssh-ed25519 

virt-node.tgl.bstu.by ecdsa-sha2-nistp256 virt-node.tgl.bstu.by ssh-ed25519 

scloud.tgl.bstu.by ssh-rsa



scloud.tgl.bstu.by ecdsa-sha2-nistp256 virt-node.tgl.bstu.by ssh-rsa 

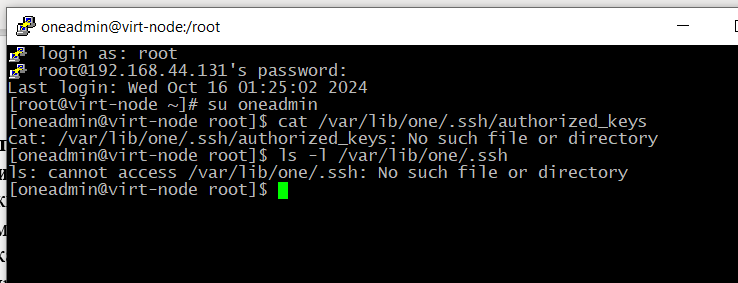
[root@scloud one]#

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**

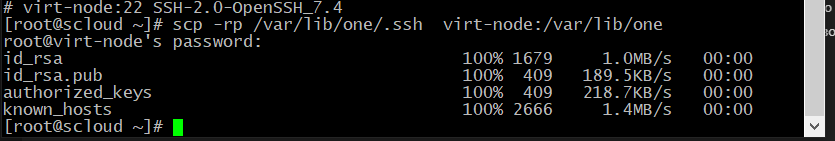
Выполним синхронизацию содержимого файла known\_hosts управляющего узла с аналогичными файлами на всех узлах гипервизорах. Для этого требуется скопировать каталог /var/lib/one/.ssh с управляющего узла на все узлы виртуализации.

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



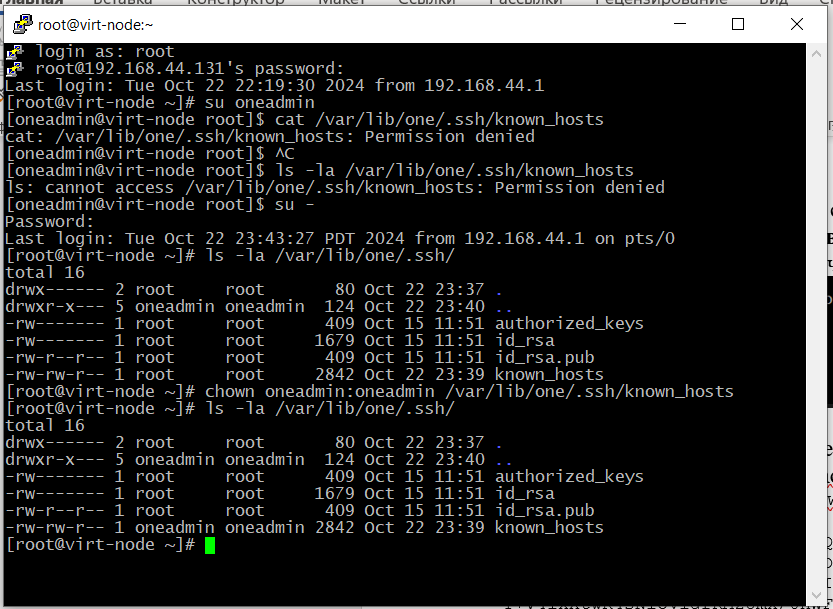
Каталога /var/lib/one/.ssh на узле виртуализации пока еще нет.

Простейшим способом выполнения этой задачи является копирование директории /var/lib/one/.ssh на узел виртуализации с управляющего узла. В результате будет выполнена установка пароля oneadmin с УУ (фронт-енд) на узлы виртуализации, а также будет создан файл known\_hosts полностью синхронизированный с аналогичным файлом УУ. 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):



Копирование прошло успешно.

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

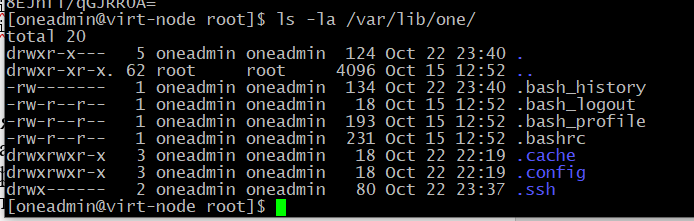




- Смотрим содержимое файла known\_hosts

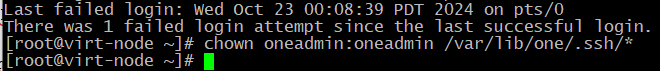
$ cat /var/lib/one/.ssh/known\_hosts

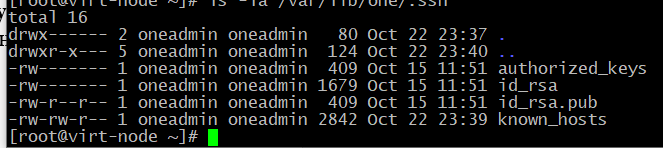
- Смотрим список файлов в домашнем каталоге пользователя oneadmin

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.

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

Проверяем

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**

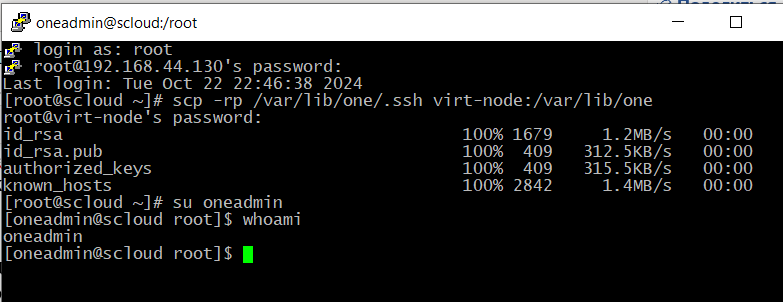
Надо проверить возможность беспарольных подключений под учетной записью oneadmin в следующих направлениях:

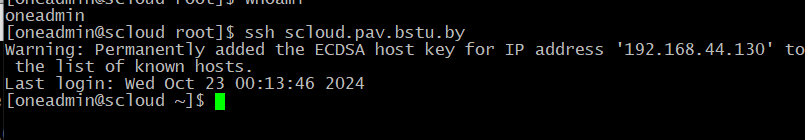
* с управляющего узла (УУ) на узлы виртуализации (УВ);
* с УУ на сам УУ;
* с УВ на УУ.

Для этого выполним команды:

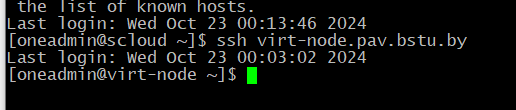
а) Начинаем с УУ (scloud):

Переключаемся в уч. запись oneadmin

Выполняем подключение с УУ на УУ:

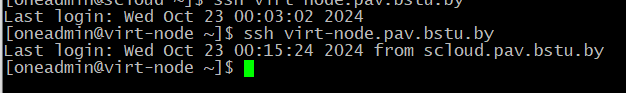
Успешно.

С УУ на УВ:

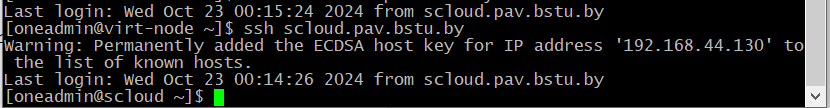


Успешно.

С УВ на УВ:

Успешно.

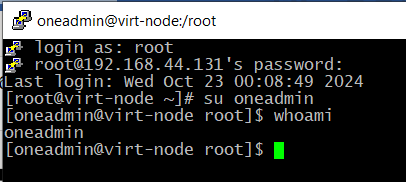
С УВ на УУ:

Успешно.

Закроем созданные ssh подключения:

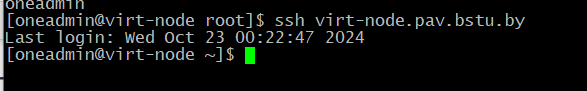
б) Перходим на УВ (virt-node):

Переключаемся в уч. запись oneadmin



Успешно.

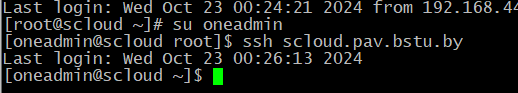
Выполняем подключение с УВ на УВ:

Успешно.

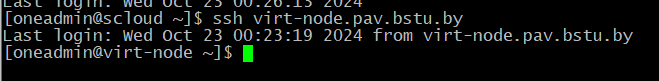
С УВ на УУ:

Успешно.

С УУ на УУ:

Успешно.

С УУ на УВ:

Успешно.

Закроем созданные ssh подключения:

[oneadmin@virt-node ~]$ exit

logout

Connection to virt-node closed.

[oneadmin@scloud ~]$ exit

logout

Connection to scloud closed.

[oneadmin@scloud ~]$ exit

logout

Connection to scloud closed.

[oneadmin@virt-node ~]$ exit

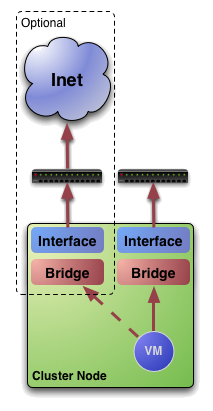
logout

Connection to virt-node closed.

[oneadmin@virt-node ~]$

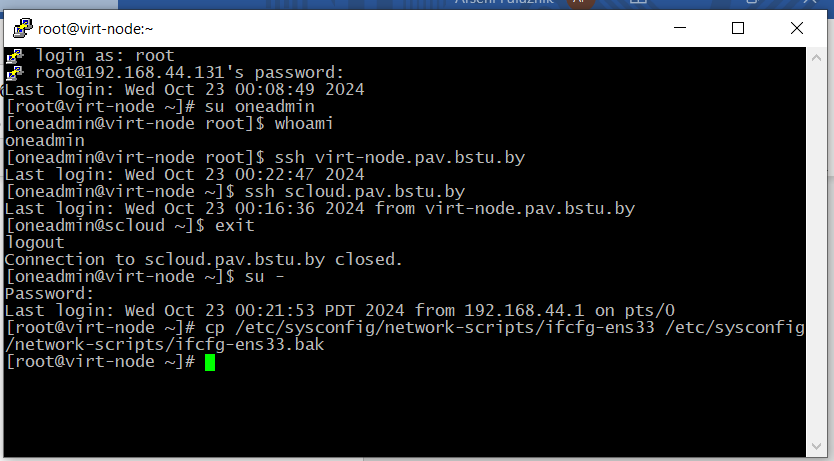
**2 Создание моста на узле виртуализации.**

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!

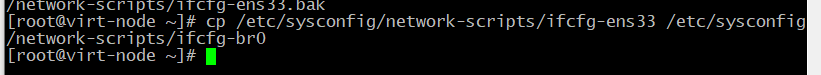
Для этого можно выполнить команду:



**2.1 Настройка сетевых интерфейсов на узле виртуализации**

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

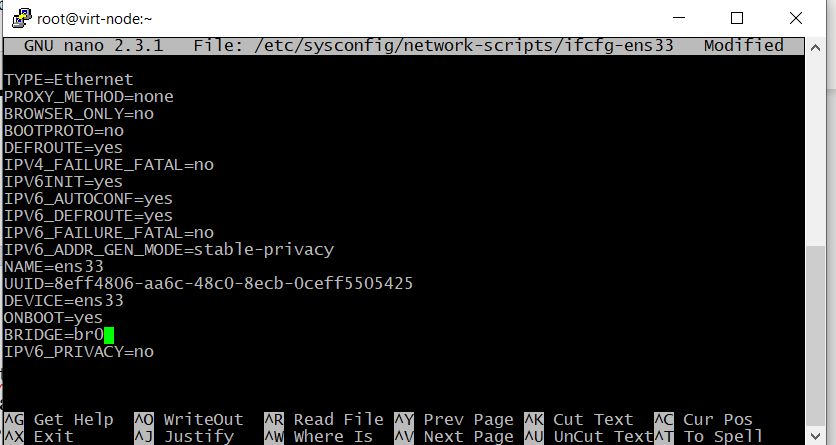
а) Создадим файл настройки моста, назовем его br0, из файла настройки интерфейса ens33, путем копирования последнего:

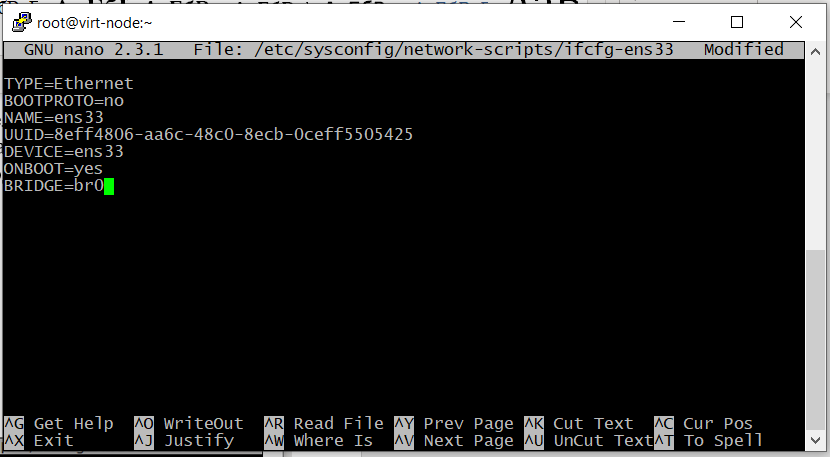


б) Изменим содержание файла /etc/sysconfig/network-scripts/ifcfg-ens33 путем его редактирования с помощью nano.

# 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:



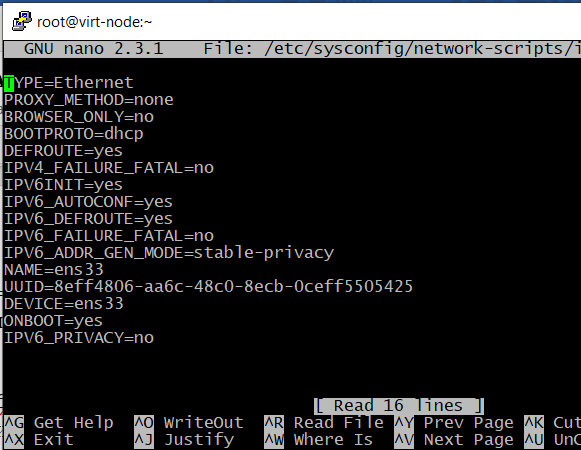


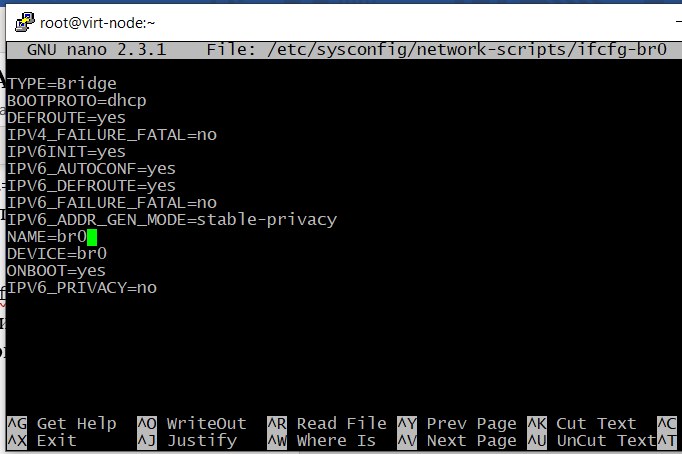
Примечание. Строку UUID оставить без изменения (не редактировать). Если в файле ifcfg-ens33 содержатся и другие строки, то их следует либо закомментировать, либо удалить. Строку BRIDGE=br0, надо добавить. Обратите внимание, что строки не должны содержать пробелов.

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:



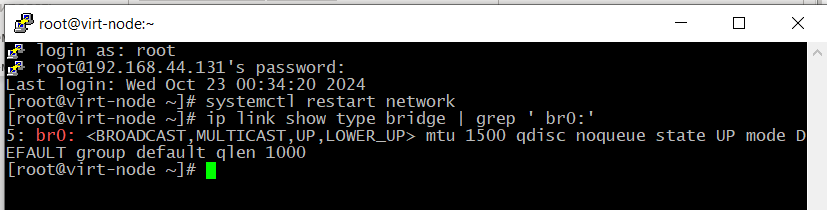


Примечание. Если в файле ifcfg-br0 содержатся и другие строки, то их можно либо оставить, либо закомментировать, т.е. поставить знак '#' в первую позицию строки. Обратите внимание, что строки не должны содержать пробелов.

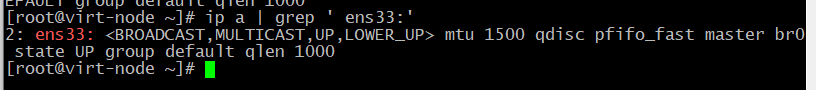
**2.2 Перезапустить на узле виртуализации сервис network.**

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

б) Проверяем состояние моста с помощью команды:



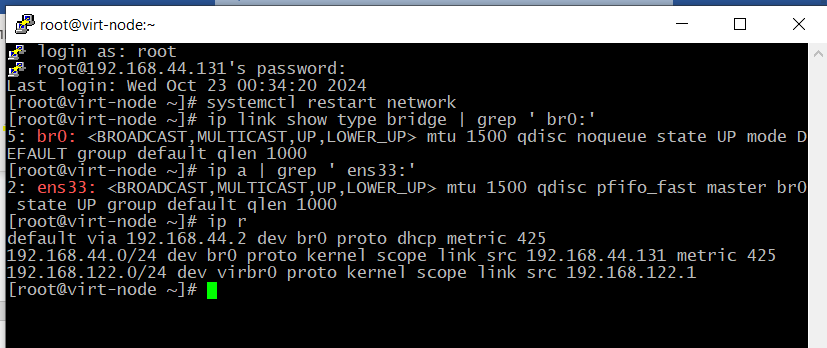
в) Проверяем состояние интерфейса ens33:



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



- проверяем доступность внешних ресурсов с узла виртуализации:

$ ping one

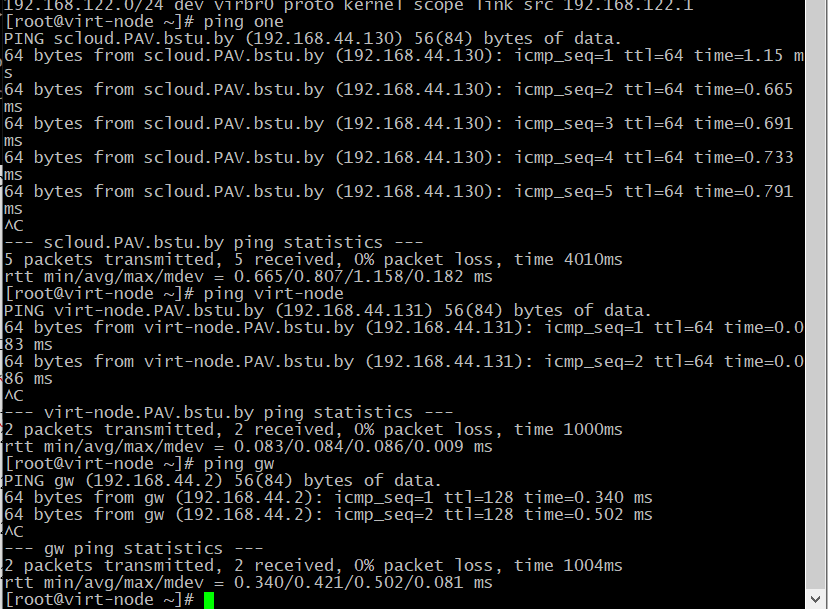
$ ping virt-node

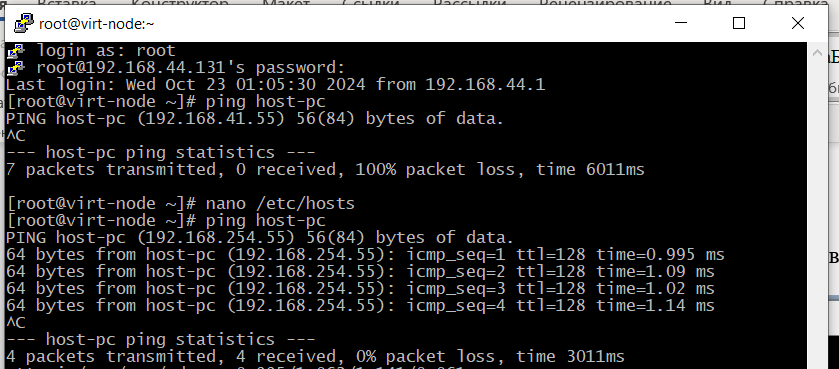
$ ping gw

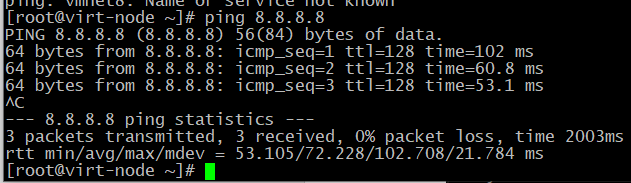
$ ping host-pc

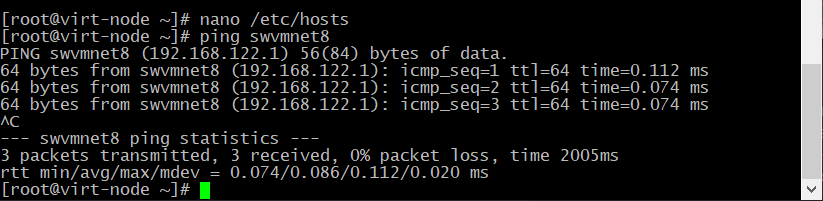
$ ping swvmnet8

$ ping 8.8.8.8



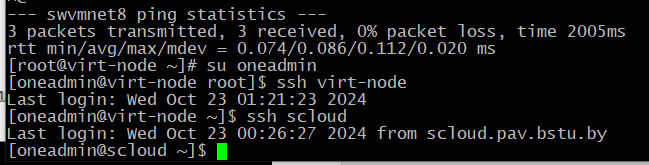


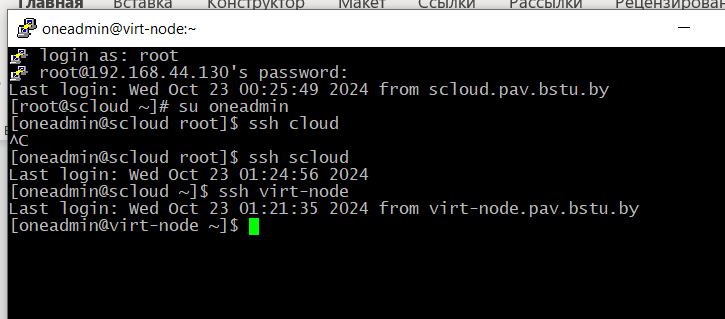




д) Проверка беспарольного доступа между узлами

Выполняется из под учетной записи oneadmin на УВ:





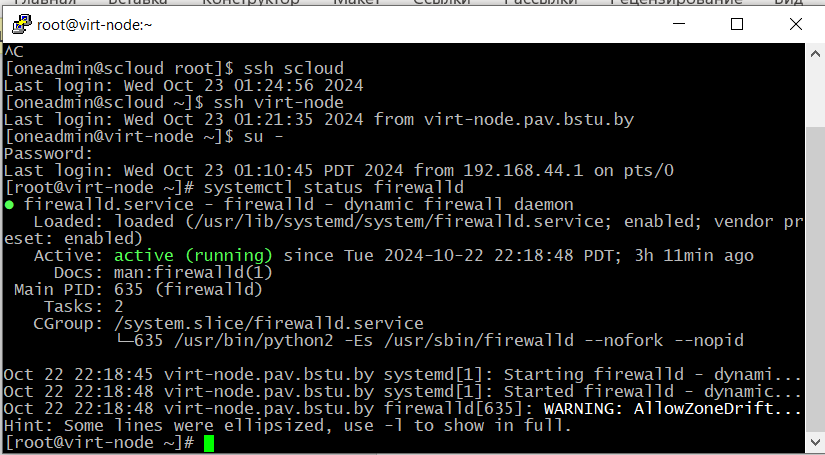
ОК!

Выполняем возврат (закрытие открытых SSH сессий):

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

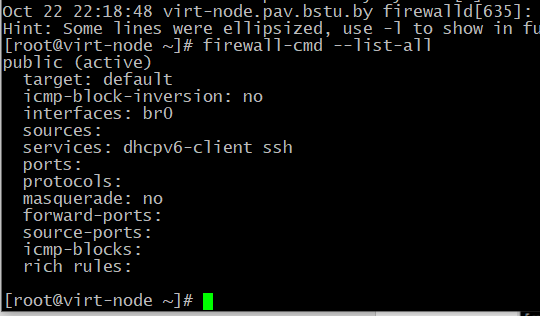
Для этого необходимо внести в брэндмауэр firewalld, правило разрешающее доступ к этому узлу по портам TCP 5900-5999, предназначенным, для доступа к рабочему столу (если ВМ использует GUI) или консоли (если на ВМ используется CLI) УВ c помощью VNC (Virtual Network Computing).

а) Проверим состояние сервиса firewalld:

Сервис работает.

б) Просмотрим какие правила установлены в системе:

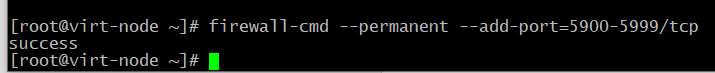
[root@virt-node ~]# firewall-cmd --list-all



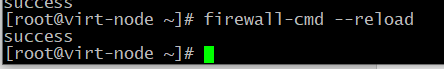
[root@virt-node ~]#

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

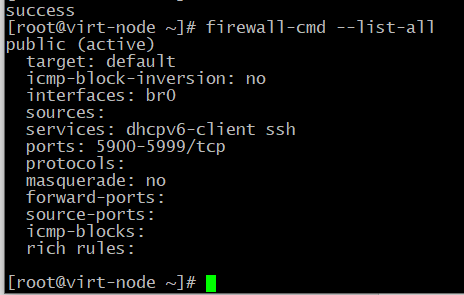
в) Откроем порты 5900-5999



г) Перезагрузим конфигурацию firewalld



ж)Просмотрим результат



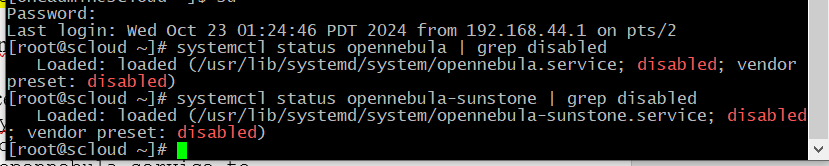
Теперь наши узлы управления и виртуализации готовы к подключению к облаку OpenNebula УВ, в качестве узла, на котором буду размещаться виртуальные машины.

Но прежде, чем мы "соберем" облако OpenNebula, необходимо убедиться, что настройки, выполненные в лаб.работах 1-5 на обоих узлах сохраняются после перезагрузки узлов:

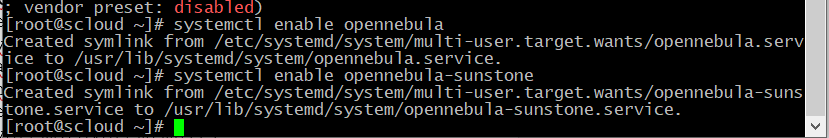
**4. Настройка запуска сервисов OpenNebula при перезагрузке системы:**

**3.1 на УУ:**

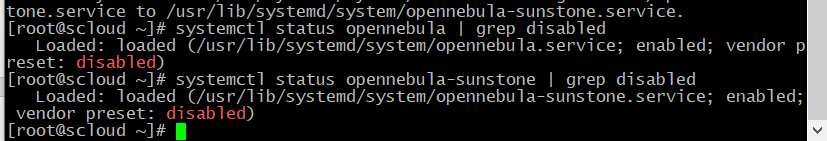
а) Проверяем настройки сервисов opennebula:

Обеим сервисам opennebule запрещено стартовать при загрузке системы:

б) Разрешаем запуск сервисов opennebula при загрузке ОС:



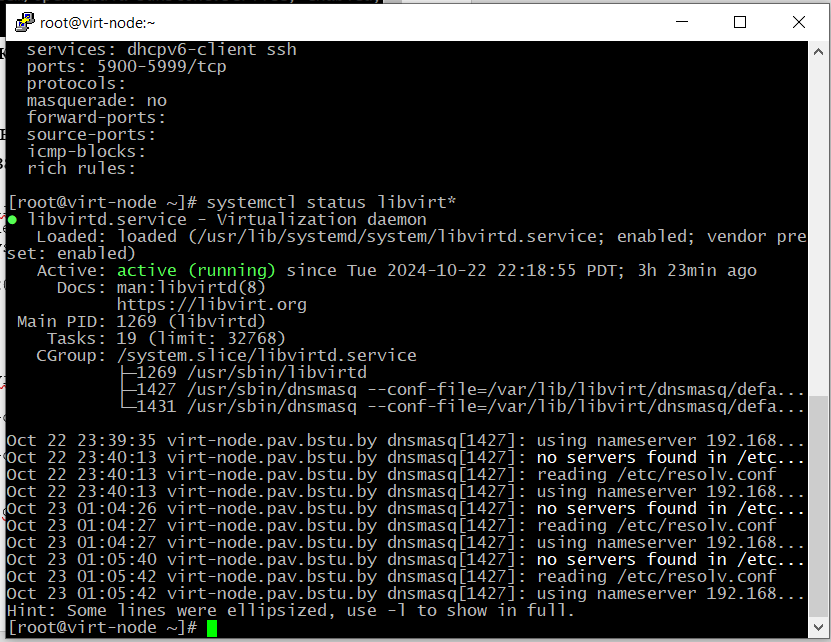
в) Проверяем:

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:

Старт при загрузке ОС разрешен.

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

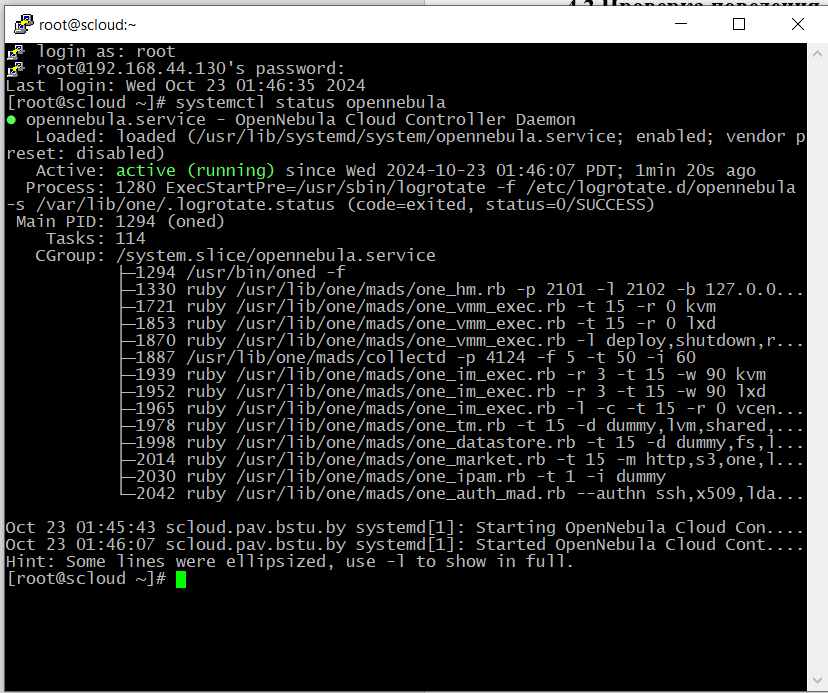
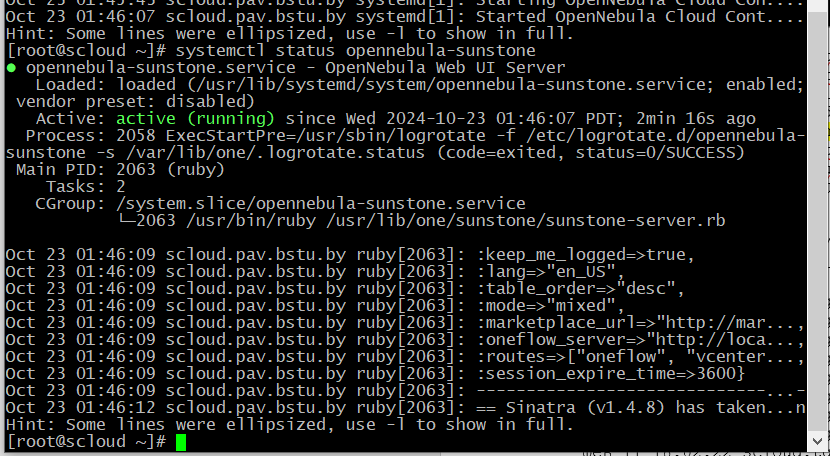
а) Выпоняем на обоих узлах команды:

# su root

# reboot

б) После перезагрузки выполняем на управляющем узле

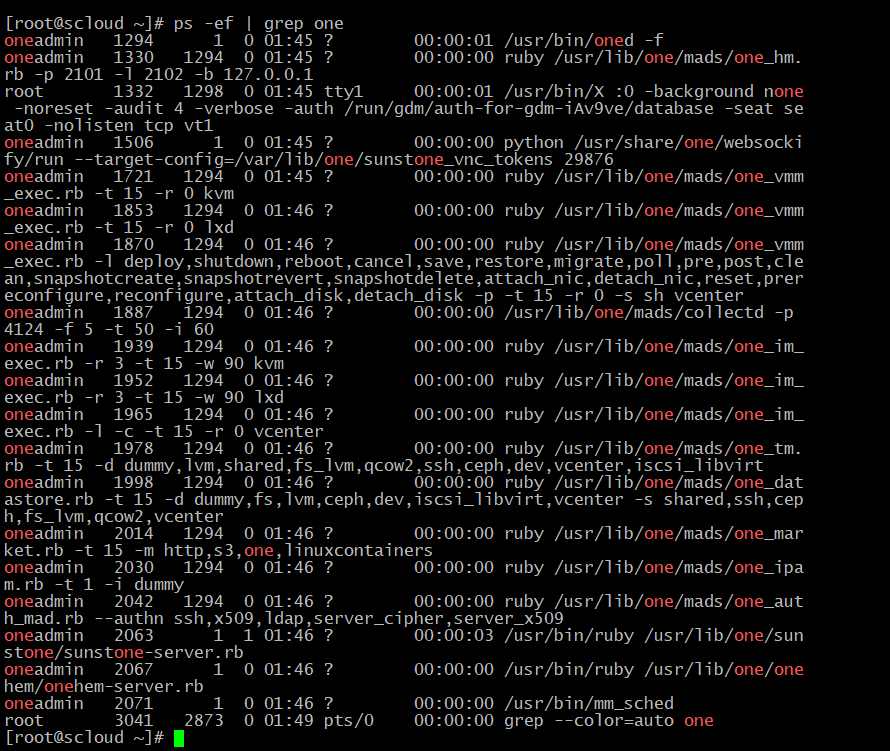
- проверяем состояние сервисов opennebula

 Оба сервиса после перезагрузки запустились успешно.

- проверяем работоспособность демонов one:

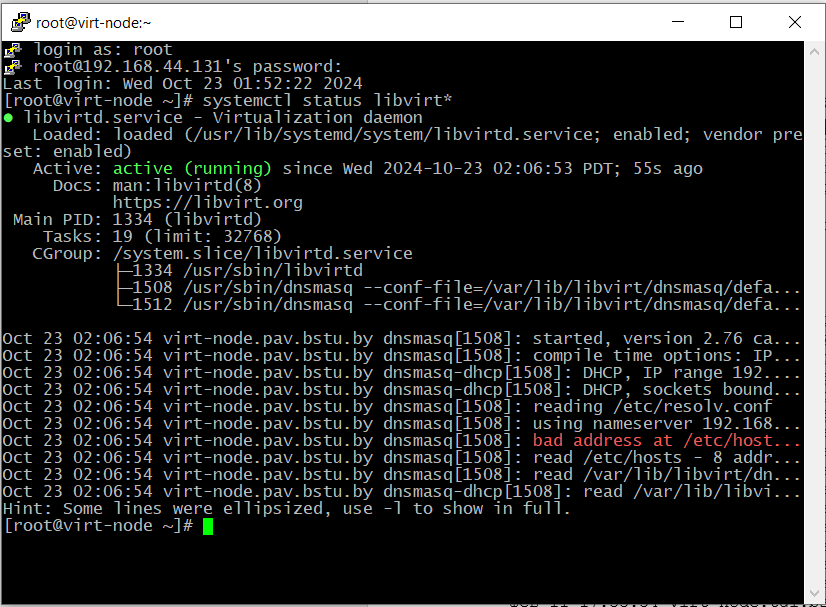


Смотрим процессы запущенные в системе от имени пользователя oneadmin

Сервисы OpenNebula успешно стартуют при перезапуске ОС.

в) После перезагрузки выполняем на узле виртуализации:

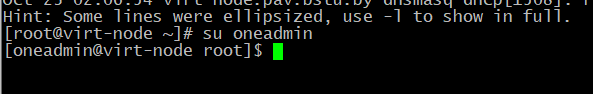
- проверяем состояние сервиса libvirtd



- 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)**

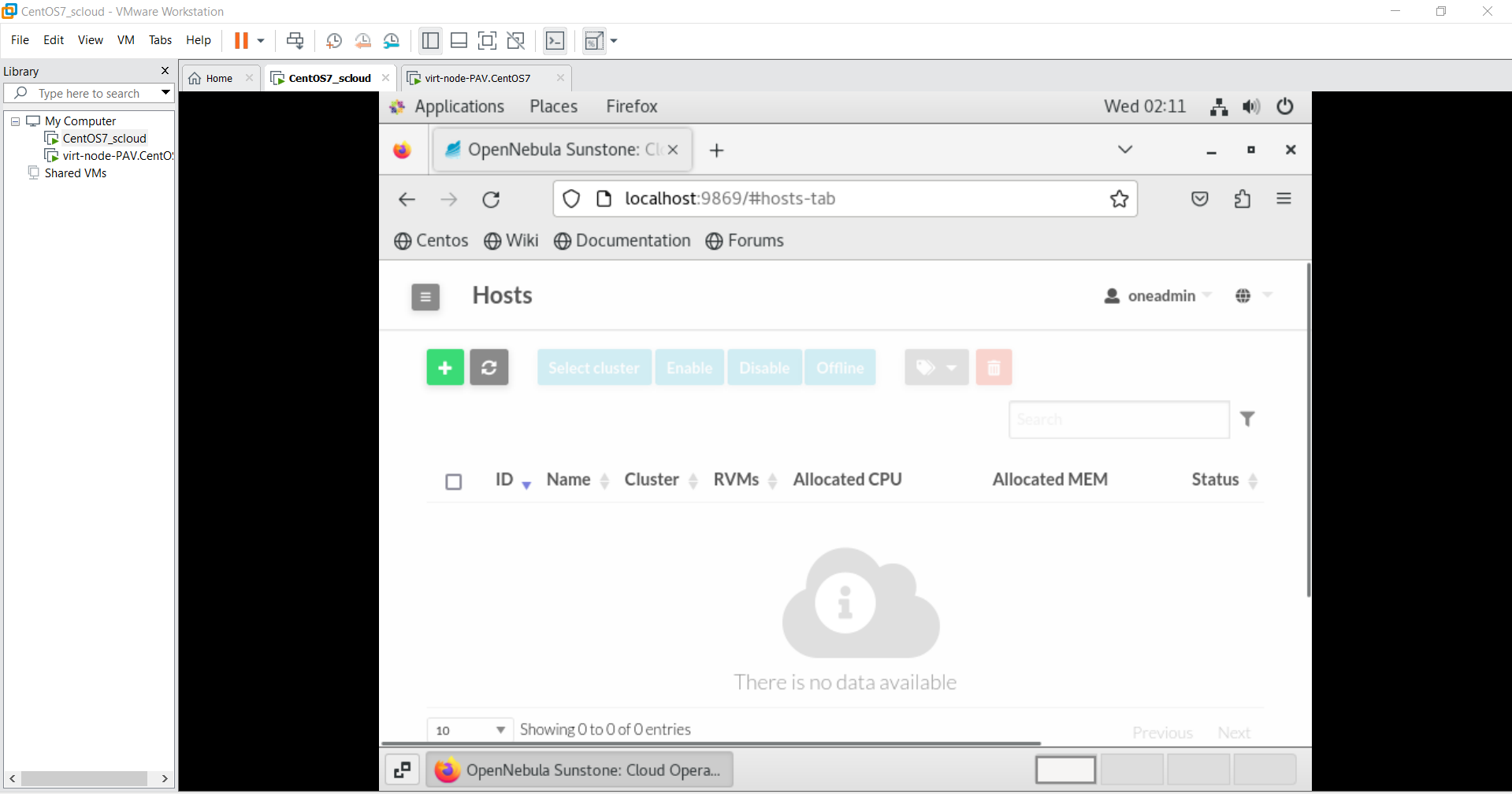
Теперь необходимо подключить созданный рабочий узел к облачному сервису. Выполняется на управляющем узле.

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



Кликаем Login

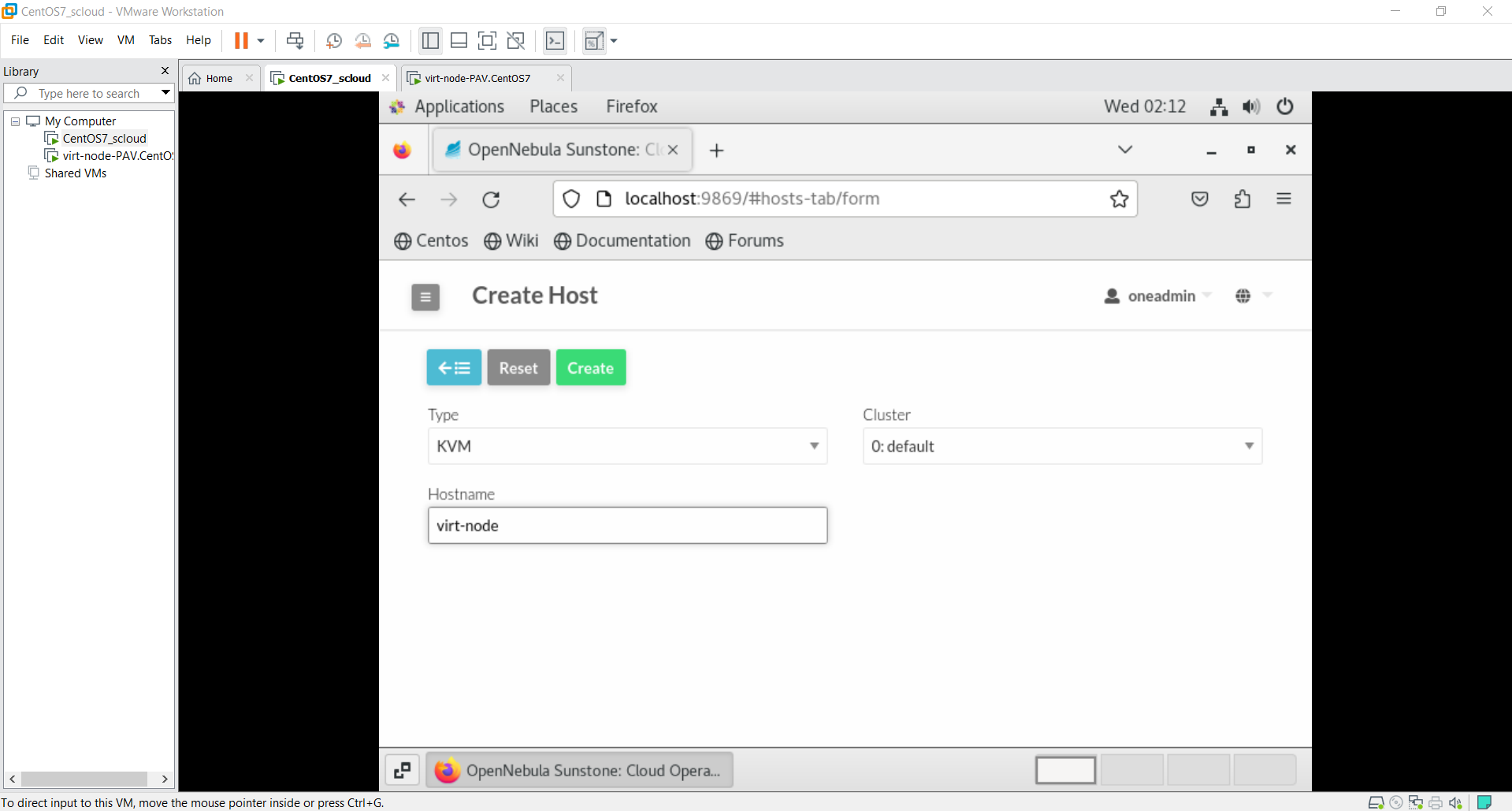
В левой панели окна разворачиваем строку Infrastructure, и кликаем строку Hosts. Откроется страница управления Hosts



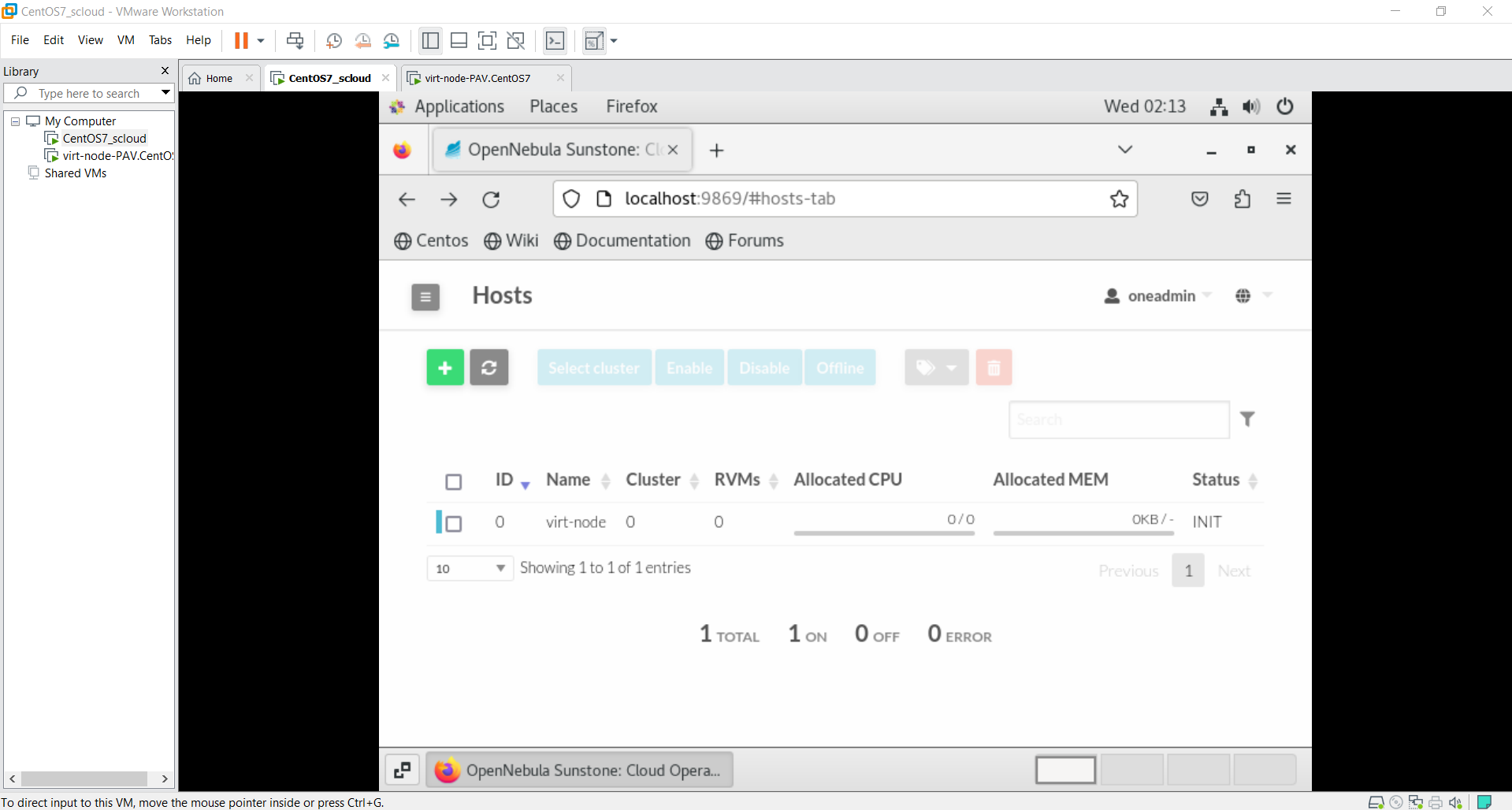
Для добавления УВ в инфраструктуру облака нажимаем значек добавить 

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.

Если хост переходит в состояние err вместо состояния INIT, то для выяснения причины, следует просмотреть записи в журнале работы демона oned/var/log/one/oned.log. Возможно, эта проблема связана с SSH!

**5.2 Добавление хоста с помощью CLI**

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

а) Подключение узла виртуализвации.

**Предупреждение.** Если УВ был подключен с помощью GUI, то **не надо выполнять** команду onehost create <node01>

**Внимание:** Угловые скобки набирать не надо, они будут трактоваться bash как команда которую надо исполнить. В качестве имени хоста надо указать virt-node (или, то имя которое прописано для него в файле /etc/hosts).

$ onehost create <node01> -i kvm -v kvm

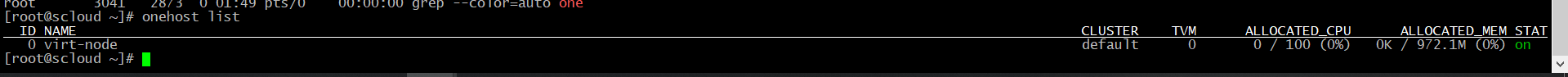
$ onehost list

ID NAME CLUSTER RVM ALLOCATED\_CPU ALLOCATED\_MEM STAT

1 localhost default 0 - - init

# After some time (20s - 1m) (Выполнить по истечении 20сек – 1 минута)

б) Проверка подключения узла виртуализации



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.**