Astra
Infrastructure
Cloud

Инструкция для автоматизированной установки -- Baremetal_brest-aldpro-ceph-rubackup

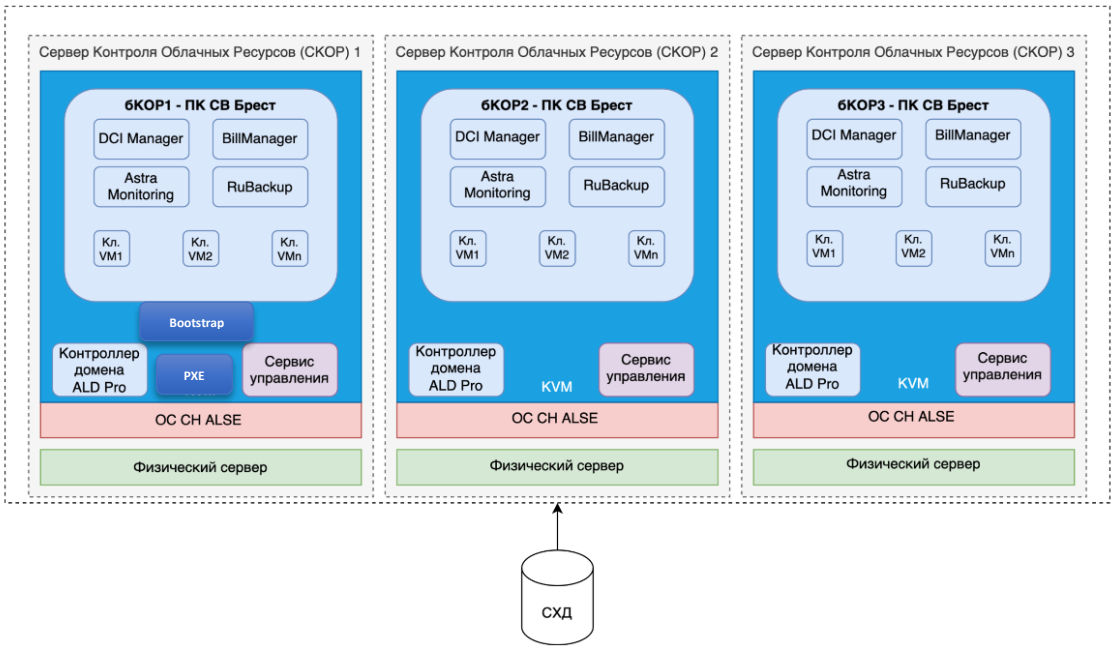
1 Описание сценария разворачивания инфраструктуры

Данный сценарий предполагается к разворачиванию на трёх физических серверах.

Шаги по настройке:

- Установка ОС на первый железный сервер
- Настройка QEMU/KVM в ОС первого железного сервера, в дальнейшем сервер будет выполнять роли **node1-test** и **ceph1-test**
- Установка ВМ **VM-bootstrap** и **VM-PXE** на первом железном сервере из qcow2 образов
- Установка ОС на втором и третьем физическом сервере по PXE для **node2-test/ceph2-test** и **node3-test/ceph3-test** соответственно
- Установка ВМ для **dc1-test**, **dc2-test** и **rubackup-test** из qcow2 образов на первом физическом хосте
- Подготовка bootstrap сервера **VM-bootstrap**
- Инициализация проекта и дальнейшее развертывание ресурсов на **VM-bootstrap**

**VM-Bootstrap и VM-PXE могут находиться на одном из трёх целевых физических серверов либо вне их (например, на арм администратора). В данной инструкции рассматриваем вариант, когда Bootsrtap и PXE находятся на первом физическом хосте.*



Следующие серверы будут развёрнуты для работы инфраструктуры:
dc1-test
dc2-test
node1-test
node2-test
node3-test

ceph1-test
ceph2-test
ceph3-test
rubackup-test

- Версионность продуктов
  - Brest - 3.2
  - ALD Pro - 2.1.0
  - Ceph - 16
  - RuBackup - 2.0
  - Astra Linux SE 1.7.2uu1
  - Astra Linux SE 1.7.4 for ALD Pro

2 Установка ОС на первый железный сервер

Открыть консоль через iDRAC, подмонтировать iso образ, загрузиться с образа.

Выбрать установку, на диск целиком (без LVM), выбрать любой диск нужного размера (~200GB), в выборе программного обеспечения необходимо выбрать только 3 пункта - "Графический интерфейс Fly", "Консольные утилиты" и "Средства удалённого подключения SSH". В меню выбора параметров безопасности нужно убрать выбор со всех средств защиты. Дальнейшая установка проводится в стандартном режиме.

Первоначальная настройка сети

Для использования служб systemd-networkd / systemd-resolved во избежание конфликтов следует отключить, остановить и заблокировать все остальные службы управления сетевыми интерфейсами:

```
# Прописать сетевые настройки в файле
sudo vim /etc/network/interfaces

sudo systemctl --now mask NetworkManager
sudo systemctl --now mask networking
sudo systemctl --now mask resolvconf

# И разблокировать и запустить systemd-networkd / systemd-resolved:
sudo systemctl unmask systemd-networkd
sudo systemctl enable systemd-networkd
sudo systemctl start systemd-networkd
sudo systemctl unmask systemd-resolved
sudo systemctl enable systemd-resolved
sudo systemctl start systemd-resolved

sudo rm /etc/resolv.conf
# sudo mv /etc/resolv.conf /etc/resolv.conf.save
sudo ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf
```

3 Настройка QEMU/KVM в ОС первого железного сервера, в дальнейшем севрер будет выполянять роли node1-test и ceph1-test

Для автоматизированной установки системы виртуализации QEMU/KVM в дистрибутивы Astra Linux включен пакет astra-kvm. Пакет может быть установлен с помощью графического менеджера пакетов (см. Графический менеджер пакетов synaptic) или из командной строки командой:

```
sudo apt install astra-kvm
```

При установке этого пакета будет автоматически установлен графический инструмент управления виртуальными машинами virt-manager и выполнены все действия, необходимые для установки и запуска системы виртуализации.

```
sudo usermod -a -G kvm,libvirt,libvirt-qemu,libvirt-admin root
```

Других пользователей, которые должны работать с виртуализацией, следует добавить в указанные группы вручную

```
sudo usermod -a -G kvm,libvirt,libvirt-qemu,libvirt-admin <имя_пользователя>
exec su - $USER
```

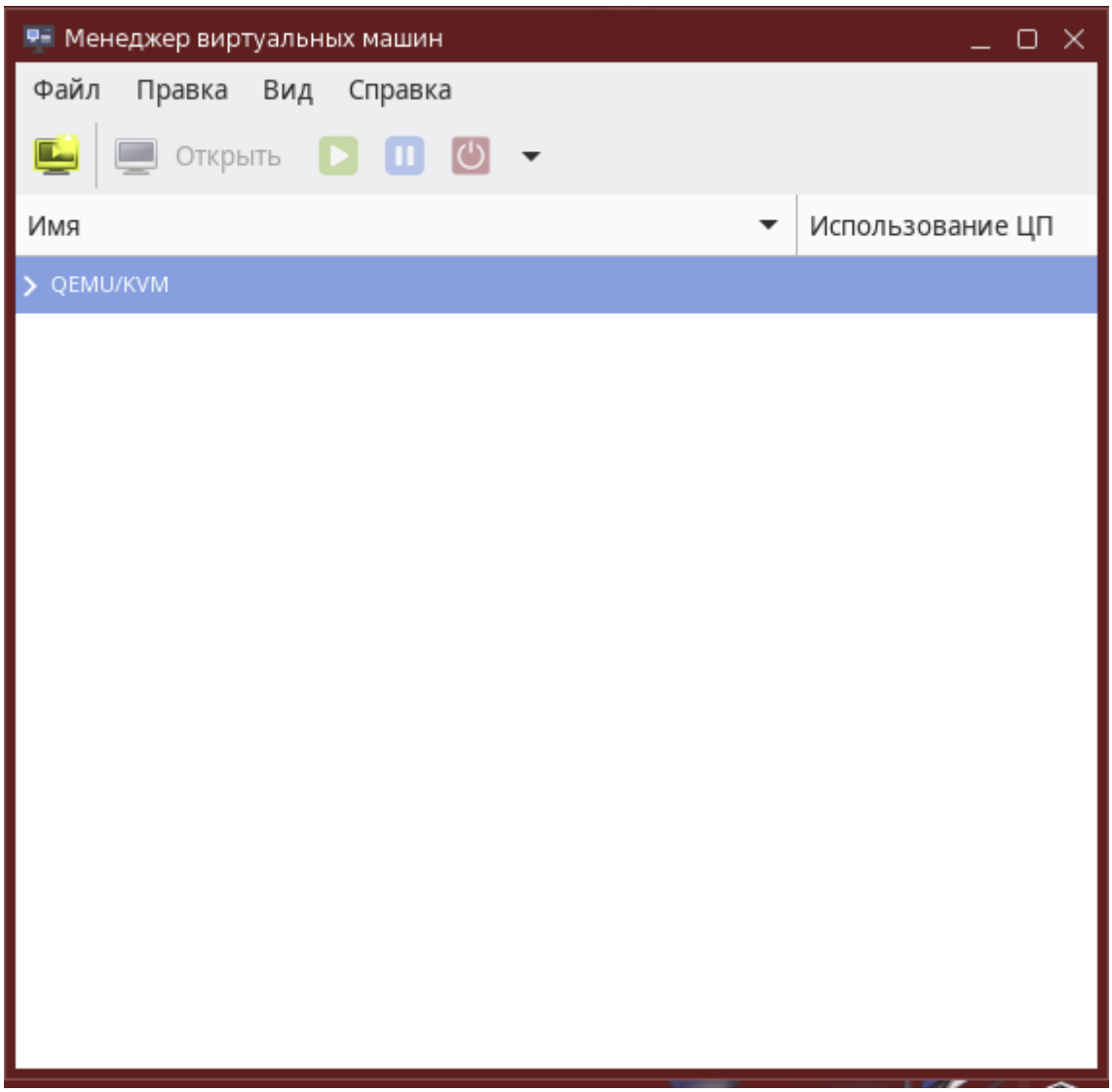
Для того, чтобы добавление в группы вступило в силу, нужно перезапустить пользовательскую сессию. В целях тестирования для того, чтобы добавление в группы вступило в силу, можно выполнить следующую команду (потребуется ввести пароль пользователя): Для хранения образов виртуальных машин при первом запуске графической оболочки управления виртуализацией *virtmanager* автоматически создается пул данных. По умолчанию этот пул данных располагается в каталоге */var/lib/libvirt/images*. Дополнительные пулы данных могут быть созданы по мере необходимости.

4 Установка BM VM-bootstrap и VM-PXE на первом железном сервере из qcow2 образов

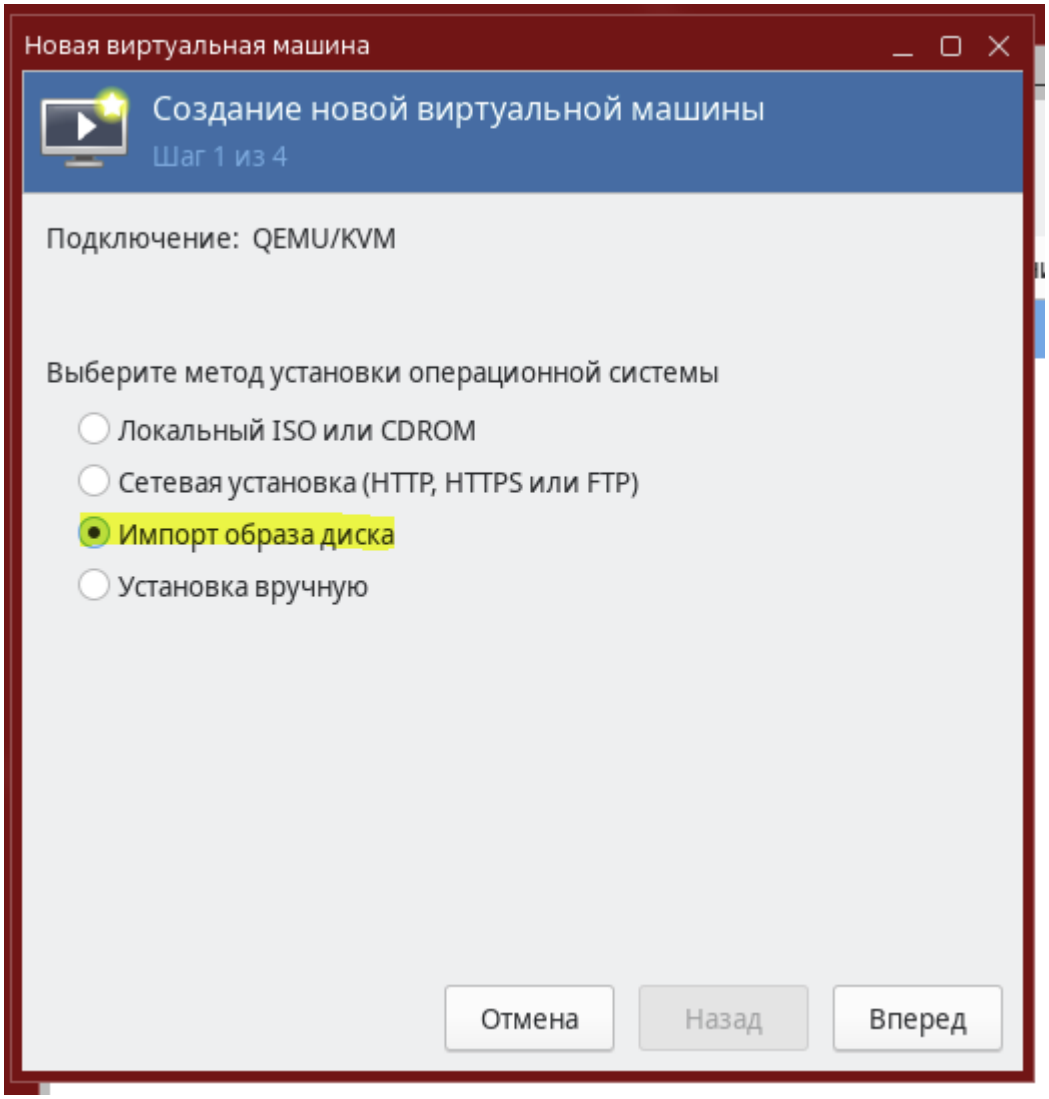
Ниже описано создание виртуальных машин.

Общий репозиторий со всеми образами можно найти перейдя по ссылке:
https://dl.astralinux.ru/ui/native/mg-generic/alse/qemu/
Скачать образ используемый в этом пункте инструкции можно из вышеуказанного репозитория, прямая ссылка на его скачивание: https://dl.astralinux.ru/artifactory/mg-generic/alse/qemu/alse-vanilla-1.7.4-qemu-adv-mg11.3.0.qcow2

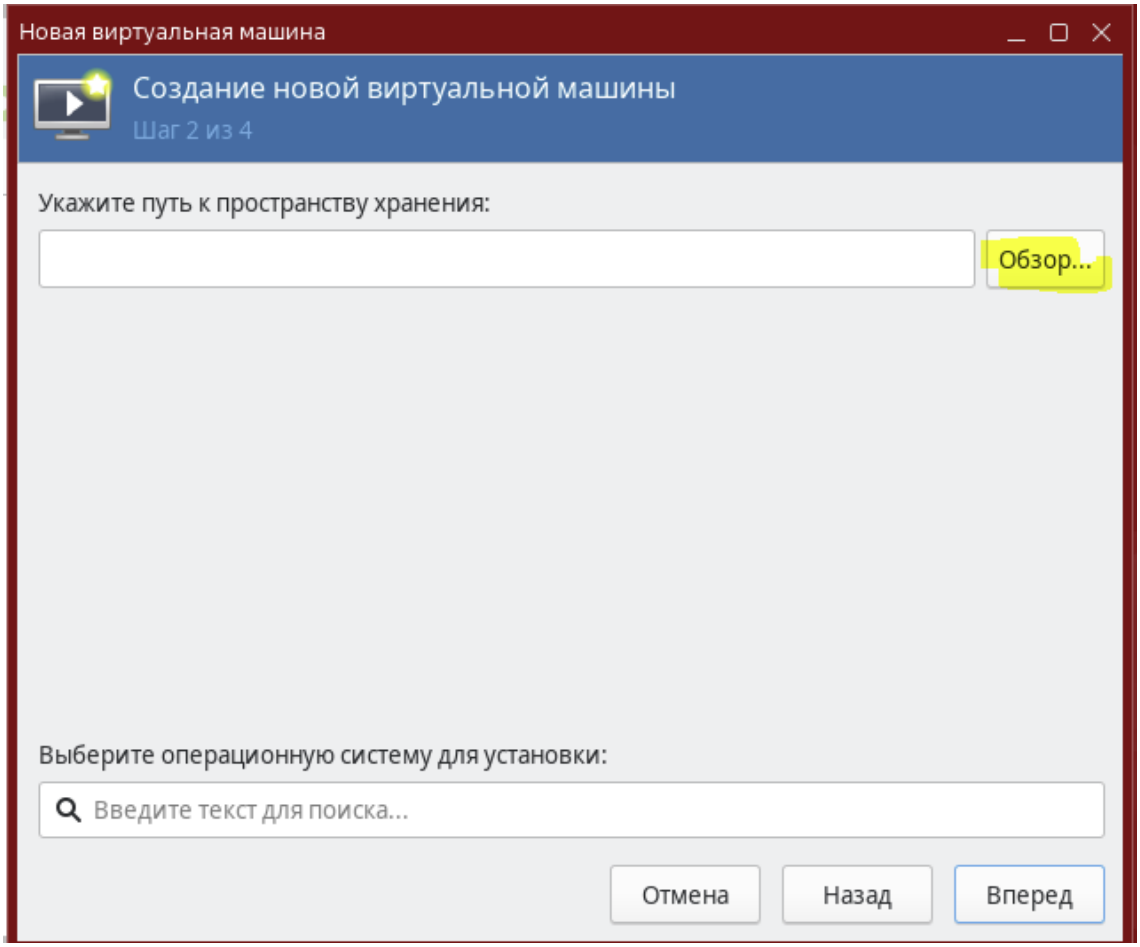
Для начала работы нужно открыть приложение **virtmanager** и нажать кнопку "*Создать*"



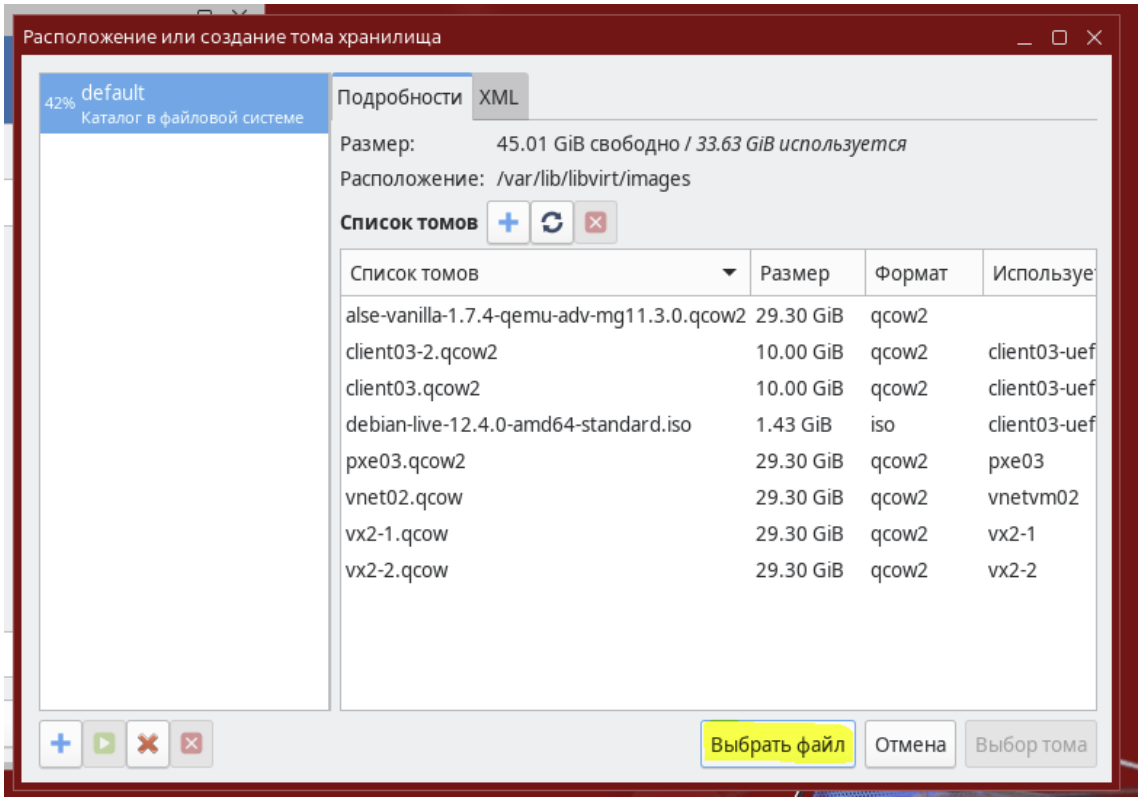
Выбрать "*Импорт образа диска*"



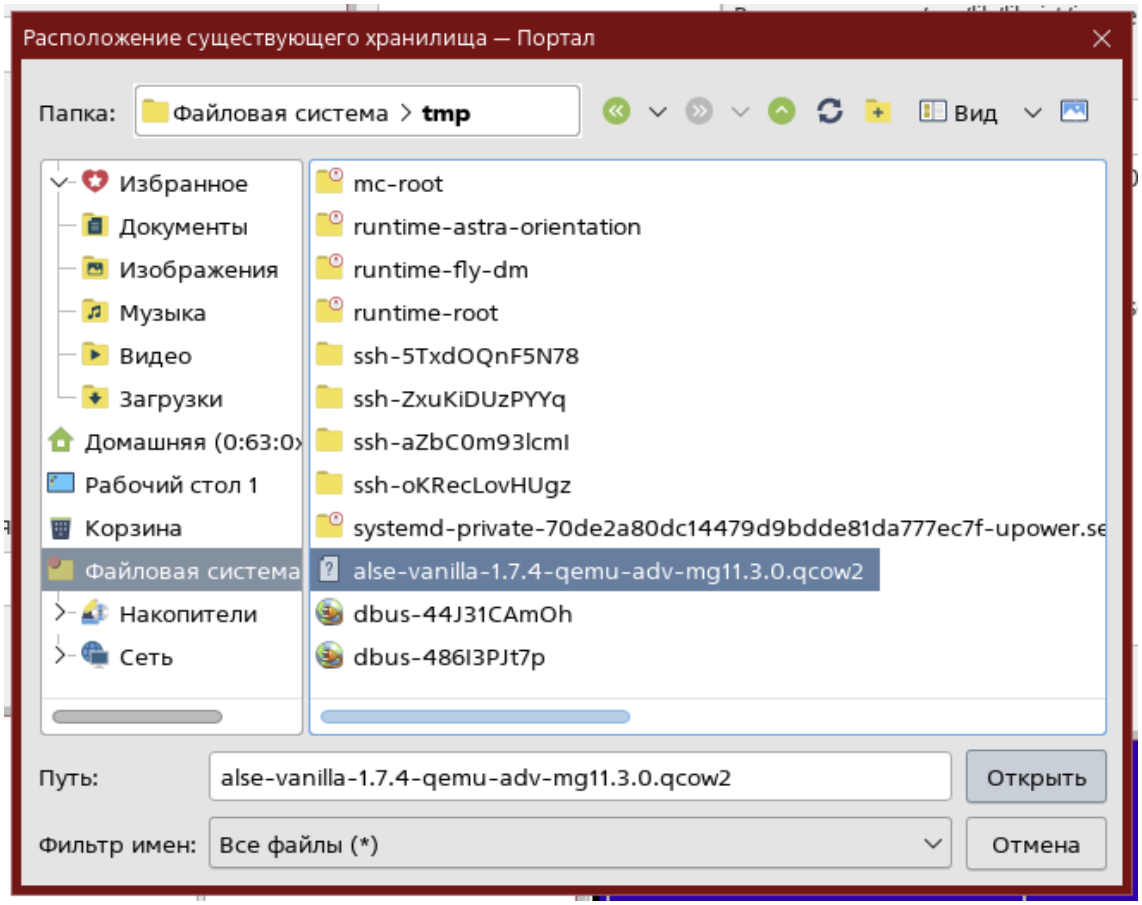
Нажать кнопку "*Обзор...*"для выбора образа будущей виртуальной машины



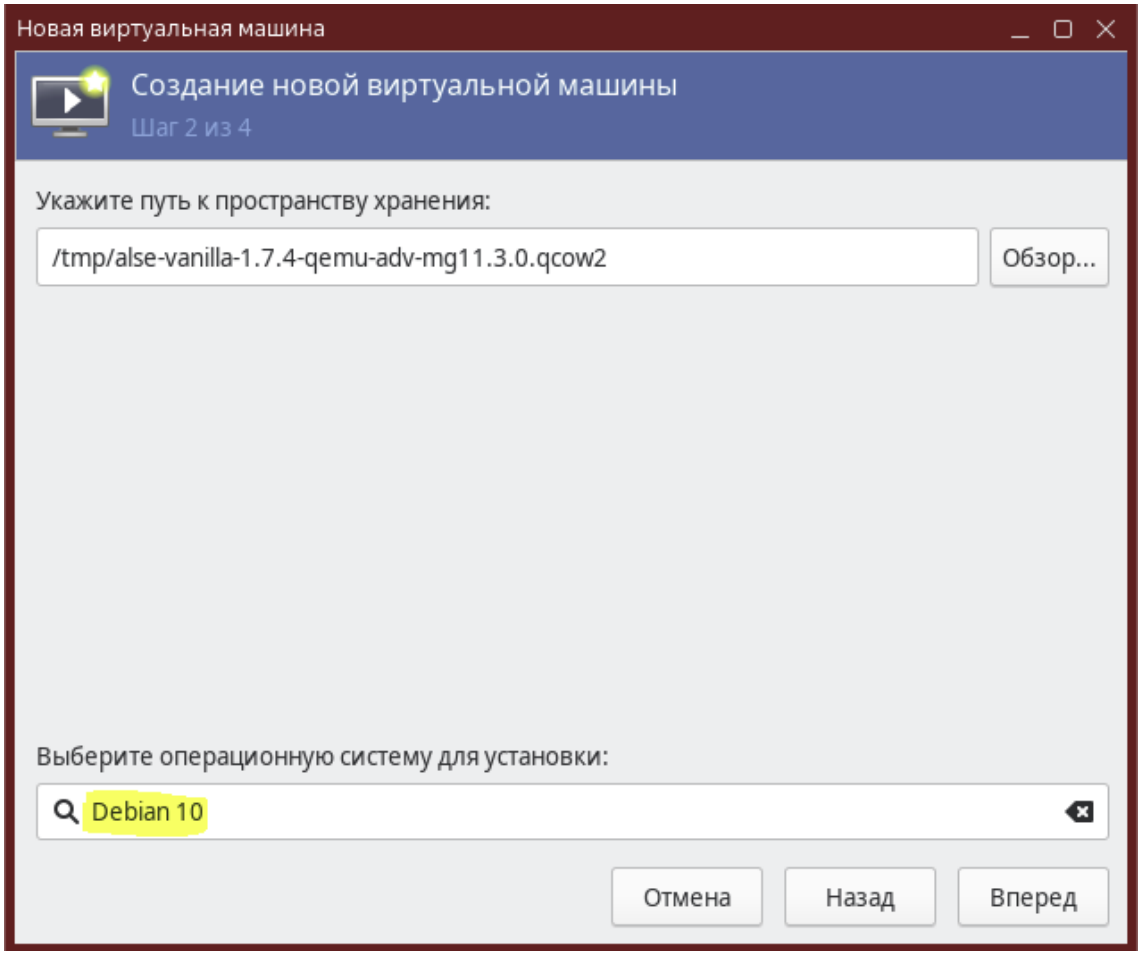
В открывшемся окне нажать кнопку "*Выбрать файл*"



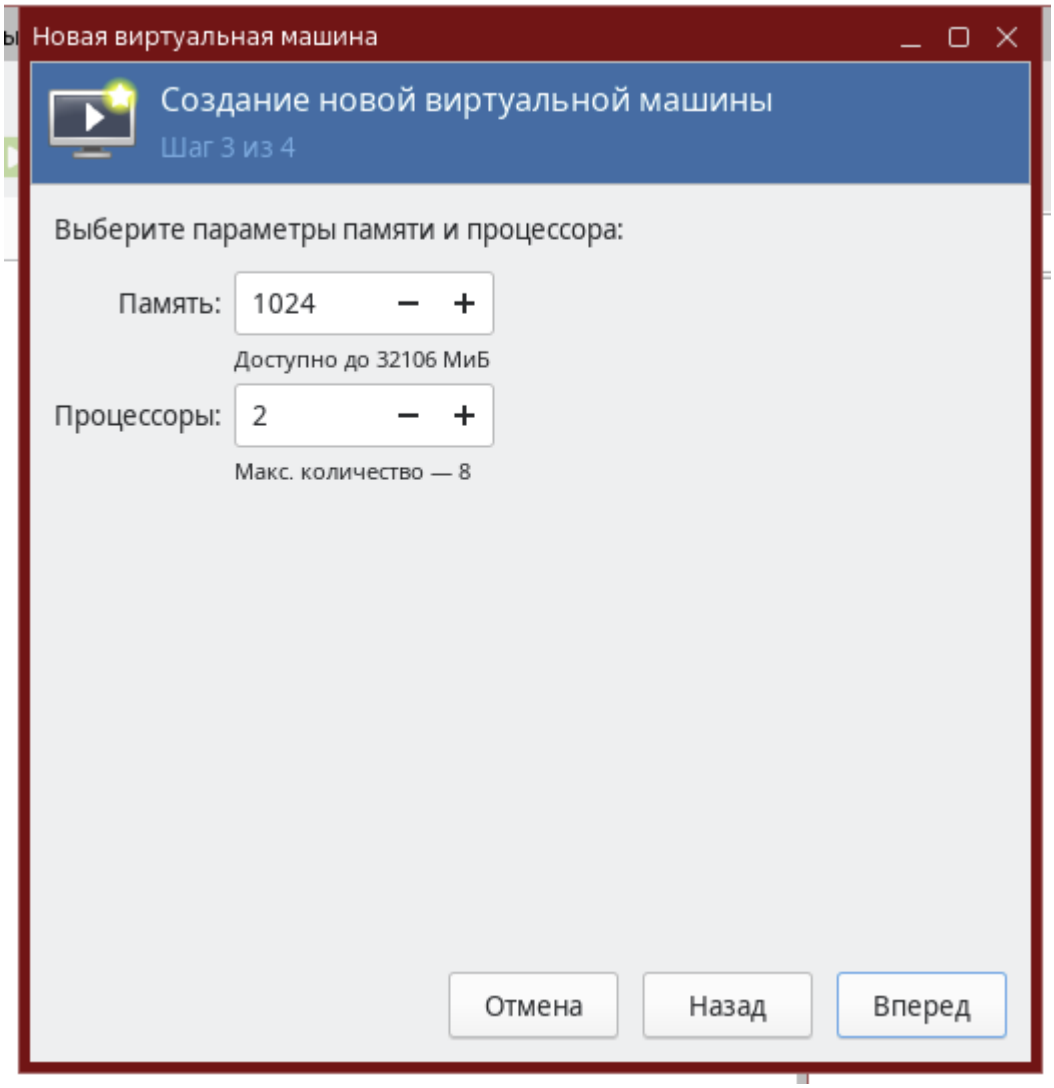
Далее нужно выбрать скаченный ранее файл - образ формата "qcow2" и нажать "**Открыть**"



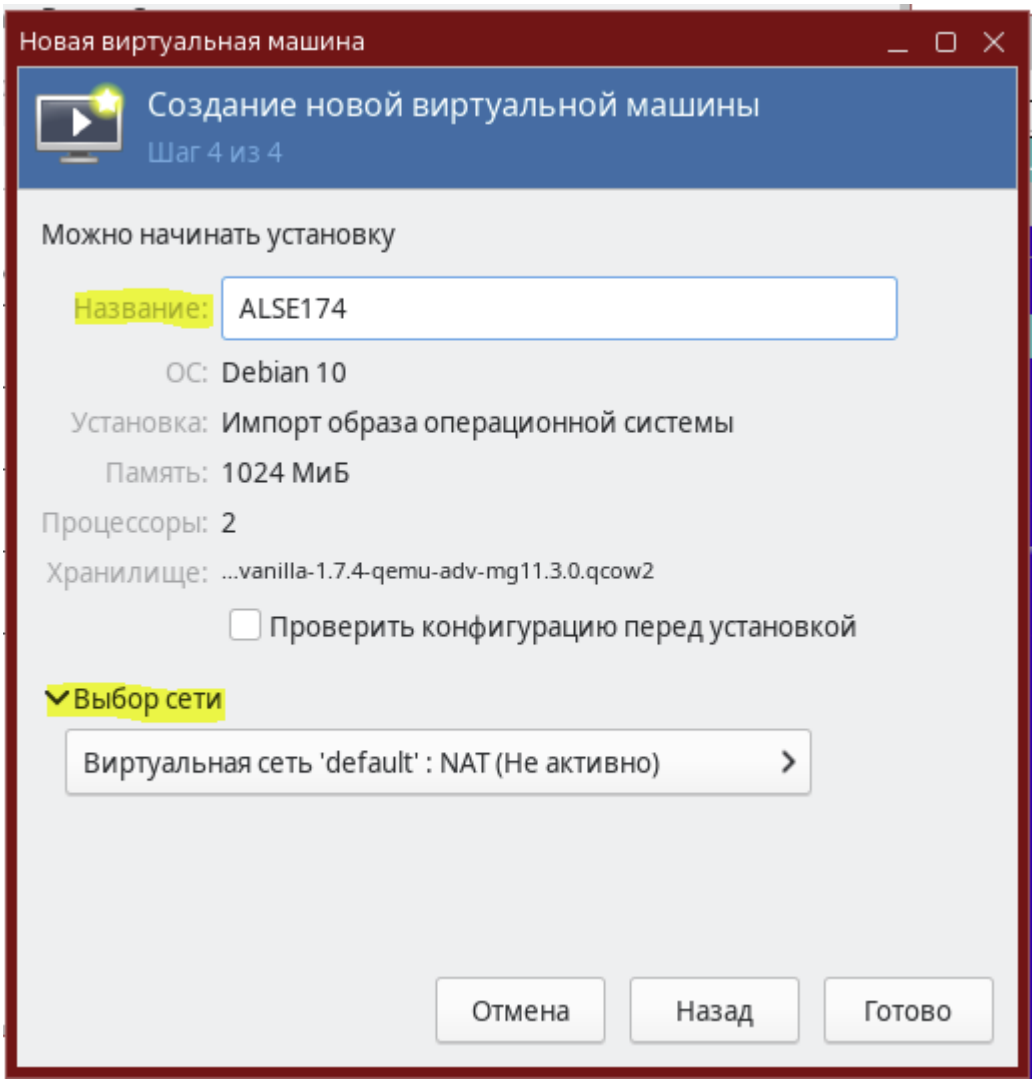
В следующем окне в строке "*Выберите операционную систему для установки"* необходимо указать "**Debian 10"**



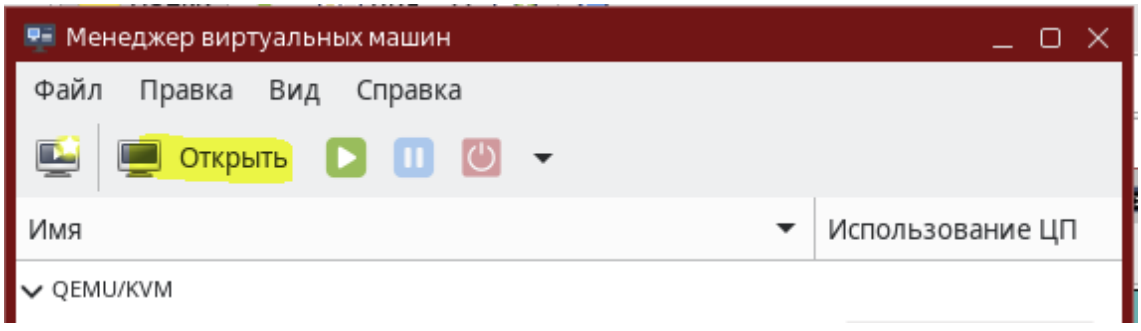
На следующем шаге нужно задать необходимый объём памяти и количество виртуальных ЦПУ



Далее мы задаём имя будущей виртуальной машине, затем выбираем нужную сеть и нажимаем "готово", после чего ВМ будет создана



Далее нажать *"Открыть"*, после чего откроется VNC сессия, где уже можно настроить сеть и далее уже подключиться по SSH



5 Установка ОС на втором и третьем физическом сервере по PXE для node2-test/ceph2-test и node3-test/ceph3-test соответсвенно

Для установки ОС по сети с помочью PXE необходимы будут следующие шаги:

- Подготовка сервера репозиториев
- Настройка DHCP + TFTP
- Настройка PXE
- Структура каталогов и файлов PXE сервера
- Настройка меню GRUB
- Формирование файлов ответов preseed.cfg
- Формирование файлов recipe
- Скрипт postinstall
- Сетевая загрузка

6 Подготовка сервера репозиториев

В качестве репозиториев используются установочные ISO. Используемые версии ALSE:

- 1.7.2
- 1.7.2-update-uu1 - отдельный ISO с оперативным обновлением, содержит только обновление
- 1.7.4
- 1.7.4uu1 - установочный ISO со встроенным оперативным обновлением

Файлы ISO должны быть предварительно скачаны и загружены на BM PXE.

Установка и настройка FTP сервера

```
apt install vsftpd

# /etc/vsftpd.conf
listen=yes
listen_ipv6=no
anonymous_enable=YES
local_enable=no
anon_root=/srv/ftp
no_anon_password=yes
hide_ids=yes
```

Создание директорий и монтирование ISO образов

```
mkdir -p /srv/ftp/scripts
mkdir -p /srv/ftp/iso/1.7.2
mkdir -p /srv/ftp/iso/1.7.2-update-uu1
mkdir -p /srv/ftp/iso/1.7.4
mkdir -p /srv/ftp/iso/1.7.4uu1

mount /iso/alse-1.7.2.iso              /srv/ftp/iso/1.7.2
mount /iso/alse-1.7.2_update_uu1.iso   /srv/ftp/iso/1.7.2-update-uu1
mount /iso/alse-1.7.4                  /srv/ftp/iso/1.7.4
mount /iso/alse-1.7.4uu1.iso           /srv/ftp/iso/1.7.4uu1
```

Создание systemd unit, который будет монтировать ISO образы при каждой загрузке

```
#/etc/systemd/system/mount-iso-offline.service
[Unit]
Description=Mount ISO images for offline repos

[Service]
Type=oneshot
ExecStart=/bin/bash -c " \
     mount /iso/alse-1.7.2.iso              /srv/ftp/iso/1.7.2              ;\
     mount /iso/alse-1.7.2_update_uu1.iso   /srv/ftp/iso/1.7.2-update-uu1   ;\
     mount /iso/alse-1.7.4uu1.iso           /srv/ftp/iso/1.7.4uu1           "
ExecStop=/bin/bash -c " \
    umount /srv/ftp/iso/1.7.2              ;\
    umount /srv/ftp/iso/1.7.2-update-uu1   ;\
    umount /srv/ftp/iso/1.7.4uu1"
RemainAfterExit=true

[Install]
WantedBy=multi-user.target
```

Включить юнит, для проверки можно запустить его, предварительно размонтировав ранее примонтированные ISO.

```
systemctl enable mount-iso-offline.service
```

7 Настройка DHCP + TFTP

В качестве DHCP сервера используется isc-dhcp-server.

```
apt install isc-dhcp-server tftpd-hpa
```

Настройка dhcp сервера

> Указанные в примерах конфигов IP и MAC адреса условны, их нужно заменить актуальными.

Значения опций domain-name и domain-name-servers заменить актуальными.
Опция next-server должна указывать на IP адрес PXE сервера.
Блок host client1, host client2 использовать при необходимости, заменив MAC адреса актуальными.
Блок subnet привести в соответствие с используемыми IPv4 сетями.

```
# vim /etc/dhcp/dhcpd.conf
option domain-name "aic.local";
option domain-name-servers 77.88.8.8;

default-lease-time 300;
max-lease-time 7200;

authoritative;

allow booting;
allow bootp;
option fqdn.no-client-update    on;
option fqdn.rcode2            255;
option pxegrub code 150 = text ;

option architecture code 93 = unsigned integer 16 ;

next-server 10.0.9.11;

if option architecture = 00:07 {
  filename "bootx64.efi";
} elsif option architecture = 00:09 {
  filename "bootx64.efi";
} else {
  filename "pxelinux.0";
}

#host client1  {
#  hardware ethernet bc:97:e1:5e:ca:a6; fixed-address 10.0.9.21;
#}
#host client2  {
#  hardware ethernet bc:97:e1:5e:ca:a7; fixed-address 10.0.9.22;
#}

subnet 10.0.9.0 netmask 255.255.255.0 {
    range 10.0.9.24 10.0.9.28;
    option broadcast-address 10.0.9.255;
    option routers 10.0.9.1;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 10.0.9.1;
    option domain-name "aic.local";
}
```

Задать интерфейс, запросы с которого будут обслуживаться DHCP сервером

```
vim /etc/default/isc-dhcp-server

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="eth1"
```

Настройка tftp сервера

```
# /etc/default/tftpd-hpa
TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/srv/tftp"
TFTP_ADDRESS="10.0.9.11:69"
TFTP_OPTIONS="--secure"
```

[Пере]запуск служб

```
systemctl restart tftpd-hpa.service
systemctl restart isc-dhcp-server.service
systemctl status tftpd-hpa.service isc-dhcp-server.service
```

8 Настройка PXE

В контексте потенциального использования на физических серверах имеет смысл настройка PXE только для UEFI, поэтому действия, необходимые для настройки BIOS сознательно опускаются.

Для начала настройки нужно загрузить на сервер подготовленный образ bootx64.efi и grub. Скачать по ссылке: https://nextcloud.astralinux.ru/s/AfHKawSywceJ2df

Ссылка позаимствована из статьи Подготовка инфраструктуры PXE на Astra Linux

Распаковать netinst.tar.gz

```
mkdir -p /srv/tftp/se
tar xvf ~/Загрузки/netinst.tar.gz -C /srv/tftp
cd /srv/tftp
ln -s debian-installer/amd64/grub grub
```

Из примонтированного ISO (1.7.2 подойдет) скопировать ядро и initrd для сетевой установки

```
cp -p /srv/ftp/iso/1.7.2/netinst/{initrd.gz,linux} /srv/tftp/se
```

Предполагается, что в той же директории будут находиться preseed файлы:

`/srv/tftp/se`

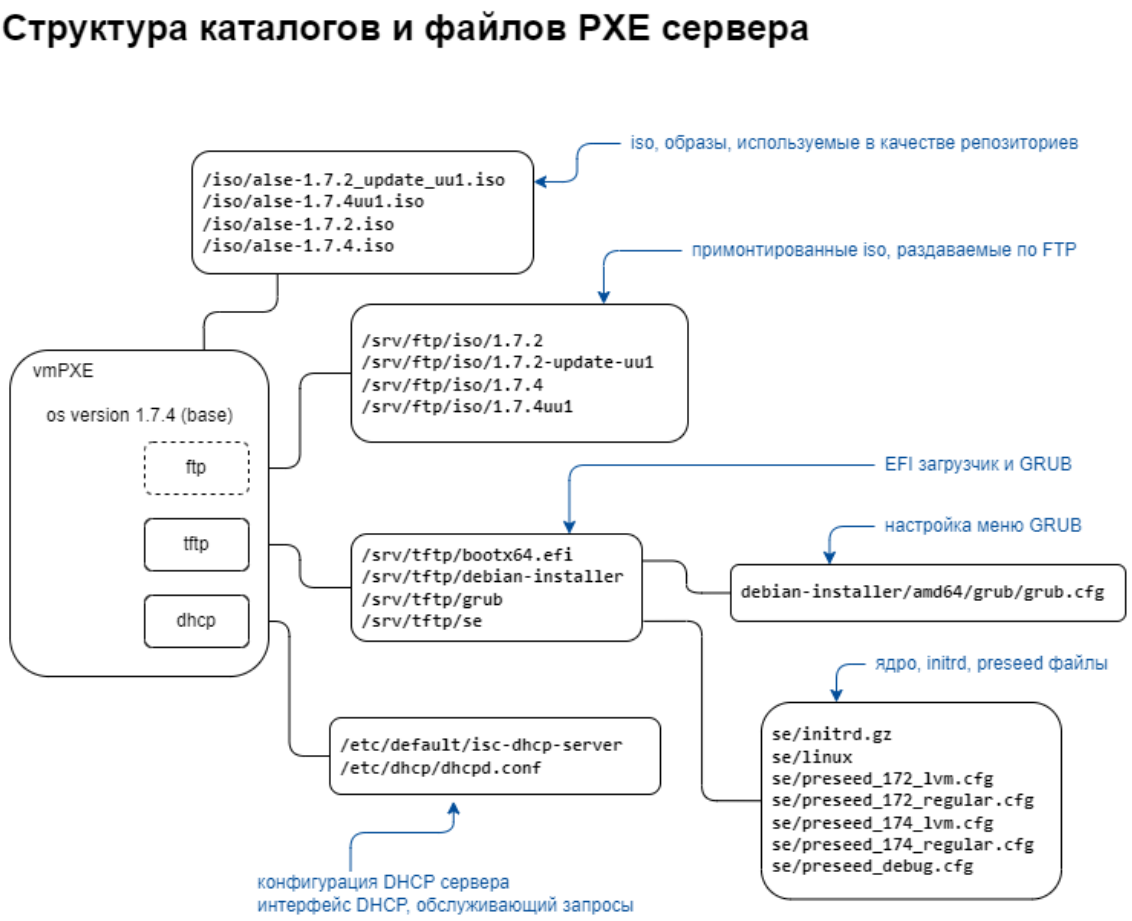
Меню GRUB настраивается в файле

`/srv/tftp/debian-installer/amd64/grub/grub.cfg`

На этом настройка PXE сервера завершается, дальнейшие шаги сводятся к настройке файлов preseed и меню GRUB.

9 Структура каталогов и файлов PXE сервера

Перед продолжением настройки при необходимости свериться с представленной схемой.



10 Настройка меню GRUB

Файл конфигурации располагается на сервере PXE по пути

```
/srv/tftp/debian-installer/amd64/grub/grub.cfg
```

При настройке меню GRUB создается по пункту меню на каждую версию ОС ALSE. В каждом пункте меню в строке url= заменить IP адрес актуальным.

Файл меню GRUB...

```
if loadfont $prefix/font.pf2 ; then
  set gfxmode=800x600
  set gfxpayload=keep
  insmod efi_gop
  insmod efi_uga
  insmod video_bochs
  insmod video_cirrus
  insmod gfxterm
  insmod png
  terminal_output gfxterm
fi

if background_image /isolinux/splash.png; then
  set color_normal=light-gray/black
  set color_highlight=white/black
else
  set menu_color_normal=cyan/blue
  set menu_color_highlight=white/blue
fi

#set timeout=3

menuentry 'Auto install ALSE 1.7.2 LVM' {
    set background_color=black
    linux    /se/linux \
    modprobe.blacklist=evbug \
    debian-installer/allow_unauthenticated=true \
    auto=true \
    priority=critical \
    debian-installer/locale=en_US \
    console-keymaps-at/keymap=ru \
    hostname=netinst \
    domain=aic.local \
    astra-license/license=true \
    netcfg/dhcp_timeout=10 \
    nomodeset \
    interface=auto \
    url=tftp://10.0.9.11/se/preseed_172_lvm.cfg
    initrd   /se/initrd.gz
}

menuentry 'Auto install ALSE 1.7.2 no LVM, partitions' {
    set background_color=black
    linux    /se/linux \
    modprobe.blacklist=evbug \
    debian-installer/allow_unauthenticated=true \
    auto=true \
    priority=critical \
    debian-installer/locale=en_US \
    console-keymaps-at/keymap=ru \
    hostname=netinst \
    domain=aic.local \
    astra-license/license=true \
    netcfg/dhcp_timeout=10 \
    nomodeset \
    interface=auto \
    url=tftp://10.0.9.11/se/preseed_172_regular.cfg
    initrd   /se/initrd.gz
}
```

```
menuentry 'Auto install ALSE 1.7.4 LVM' {
    set background_color=black
    linux    /se/linux \
    modprobe.blacklist=evbug \
    debian-installer/allow_unauthenticated=true \
    auto=true \
    priority=critical \
    debian-installer/locale=en_US \
    console-keymaps-at/keymap=ru \
    hostname=netinst \
    domain=aic.local \
    astra-license/license=true \
    netcfg/dhcp_timeout=10 \
    nomodeset \
    interface=auto \
    url=tftp://10.0.9.11/se/preseed_174_lvm.cfg
    initrd   /se/initrd.gz
}

menuentry 'Auto install ALSE 1.7.4 no LVM, partitions' {
    set background_color=black
    linux    /se/linux \
    modprobe.blacklist=evbug \
    debian-installer/allow_unauthenticated=true \
    auto=true \
    priority=critical \
    debian-installer/locale=en_US \
    console-keymaps-at/keymap=ru \
    hostname=netinst \
    domain=aic.local \
    astra-license/license=true \
    netcfg/dhcp_timeout=10 \
    nomodeset \
    interface=auto \
    url=tftp://10.0.9.11/se/preseed_174_regular.cfg
    initrd   /se/initrd.gz
}
```

11 Формирование файлов ответов preseed.cfg

Актуализировать следующие значения preseed.cfg:

- адрес FTP репозитория:

```
d-i mirror/ftp/hostname string
d-i mirror/ftp/directory string
```

- ссылка на файл recipe с адресом сервера, где располагаются скрипты (совпадает с адресами DHCP/PXE/TFTP/FTP):

```
d-i partman/early_command string wget -O /tmp/recipe_lvm
ftp://<ip>/scripts/recipe_lvm_ph
```

- выбор между наличием или отсутствием графической оболочки:

```
tasksel tasksel/first multiselect Base
tasksel tasksel/first multiselect Base, Fly, Fly-ssh
```

1. установка дополнительных пакетов, представленный список пакетов предлагается дополнить нужными:

```
d-i pkgsel/include string ssh htop ifenslave vlan bridge-utils parted
```

1. (для LVM) выбрать, какой процент от свободного пространства диска отдать под системную volume группу, рекомендуется выставить max:

```
d-i partman-auto-lvm/guided_size string 80%
d-i partman-auto-lvm/guided_size string max
```

1. Целевой диск для установки ОС:

```
d-i partman-auto/disk string /dev/sda
```

Файлы ответов для версий 1.7.4 создаются схожим образом.

Файл preseed.cfg для установки с LVM...

```
#Принять лицензию
astra-license astra-license/license boolean true
#
#Автоматический выбор сетевого интерфейса
d-i netcfg/choose_interface select auto
#
# при обнаружении DHCP требует ввести в каком домене будет АРМ, ввести нужный домен
d-i netcfg/get_domain string aic.local
d-i netcfg/hostname string aichost1
d-i netcfg/dhcp_timeout string 10
d-i netcfg/dhcpv6_timeout string 1
d-i clock-setup/ntp boolean false
#
# Mirrors
d-i mirror/country string manual
d-i mirror/protocol string ftp
d-i mirror/ftp/hostname string 10.0.9.11
d-i mirror/ftp/directory string /iso/1.7.2
#
#Локаль и язык
d-i debian-installer/language string ru
d-i debian-installer/country string RU
d-i debian-installer/keymap string ru
d-i debian-installer/locale string ru_RU
d-i debian-installer/locale select ru_RU.UTF-8
#
# Выбор клавиатуры
d-i console-tools/archs select at
d-i console-keymaps-at/keymap select ru
d-i console-setup/toggle string Alt+Shift
d-i console-setup/layoutcode string ru
d-i keyboard-configuration/toggle select Alt+Shift
d-i keyboard-configuration/layoutcode string ru
d-i keyboard-configuration/xkb-keymap select ru
d-i countrychooser/country-name select Russia
#
# Временная зона
d-i time/zone string Europe/Moscow
d-i partman/early_command string\
      wget -O /tmp/recipe_lvm ftp://10.0.9.11/scripts/recipe_lvm_ph
#
# Автоматическая разметка дисков
d-i partman-auto/disk string /dev/sda
d-i partman-auto/method string lvm
d-i partman-lvm/device_remove_lvm boolean true
d-i partman-lvm/confirm boolean true
d-i partman-lvm/confirm_nooverwrite boolean true
#d-i partman-auto-lvm/guided_size string 80%
d-i partman-auto-lvm/guided_size string max
d-i partman-auto-lvm/no_boot boolean true
d-i partman-auto-lvm/new_vg_name string sysvg
d-i partman-auto-lvm/purge_lvm_from_device boolean true
d-i partman-lvm/confirm boolean true
d-i partman-efi/non_efi_system boolean true
d-i partman-partitioning/confirm_write_new_label boolean true
d-i partman-partitioning/confirm_new_label boolean true
d-i partman-partitioning/choose_label string gpt
d-i partman/choose_partition select finish
d-i partman/confirm boolean true
d-i partman/confirm_nooverwrite boolean true
```

```
d-i partman-auto/expert_recipe_file string /tmp/recipe_lvm
#
#Установка дополнительных модулей ядра
d-i anna/no_kernel_modules boolean true
#
#Выбор ядра
d-i base-installer/kernel/image select linux-5.15-generic
#
# Имя пользователя
d-i passwd/username string astra
#
# Пароль пользователя
d-i passwd/user-password password astra-01
d-i passwd/user-password-again password astra-01
#
# Выбор ПО
#d-i tasksel/first multiselect Base
tasksel tasksel/first multiselect Base
d-i pkgsel/include string ssh htop ifenslave vlan bridge-utils parted
#
# Samba WINS dhcp
d-i samba-common/dhcp string false
#
# Поиск CD
d-i apt-setup/cdrom/set-first boolean false
d-i apt-setup/use_mirror boolean false
#
# Уровень защищённости
d-i astra-additional-setup/os-check select Maximum security level Smolensk
#
# Дополнительные настройки уровня защищённости
d-i astra-additional-setup/additional-settings-smolensk multiselect  Enable Mandatory Integrity
Control, Enable Mandatory Access Control
#
dictionaries-common dictionaries-common/selecting_ispell_wordlist_default note
# Установка загрузчика GRUB
#
# Установка пароля GRUB
d-i grub-installer/password password astra-01
d-i grub-installer/password-again password astra-01
#
# Post install commands
d-i preseed/late_command string \
wget -O /tmp/grubnet.sh ftp://10.0.9.11/scripts/grubnet.sh ;\
sh "/tmp/grubnet.sh"
# Не показывать диалог окончания установки
d-i finish-install/reboot_in_progress note
#d-i finish-install/exit/poweroff boolean false
```

Code Block 1 se/preseed_172_lvm.cfg

Файл preseed.cfg для установки без LVM (regular)...

```
#Принять лицензию
astra-license astra-license/license boolean true
#
#Автоматический выбор сетевого интерфейса
d-i netcfg/choose_interface select auto
#
# при обнаружении DHCP требует ввести в каком домене будет АРМ, ввести нужный домен
d-i netcfg/get_domain string aic.local
d-i netcfg/hostname string aichost1
d-i netcfg/dhcp_timeout string 10
d-i netcfg/dhcpv6_timeout string 1
d-i clock-setup/ntp boolean false
#
# Mirrors
d-i mirror/country string manual
d-i mirror/protocol string ftp
d-i mirror/ftp/hostname string 10.0.9.11
d-i mirror/ftp/directory string /iso/1.7.2
#
#Локаль и язык
d-i debian-installer/language string ru
d-i debian-installer/country string RU
d-i debian-installer/keymap string ru
d-i debian-installer/locale string ru_RU
d-i debian-installer/locale select ru_RU.UTF-8
#
# Выбор клавиатуры
d-i console-tools/archs select at
d-i console-keymaps-at/keymap select ru
d-i console-setup/toggle string Alt+Shift
d-i console-setup/layoutcode string ru
d-i keyboard-configuration/toggle select Alt+Shift
d-i keyboard-configuration/layoutcode string ru
d-i keyboard-configuration/xkb-keymap select ru
d-i countrychooser/country-name select Russia
#
# Временная зона
d-i time/zone string Europe/Moscow
#
# Автоматическая разметка дисков
d-i partman/early_command string\
      wget -O /tmp/recipe_regular ftp://10.0.9.11/scripts/recipe_regular_ph ;\
      wget -O /tmp/fcdiskdetect.sh ftp://10.0.9.11/scripts/fcdiskdetect.sh ;\
      sh /tmp/fcdiskdetect.sh ;\
      debconf-set partman-auto/disk "$(tail -n1 /tmp/disks)"
#d-i partman-auto/disk string /dev/sda
d-i partman-auto/method string regular
d-i partman-efi/non_efi_system boolean true
d-i partman-partitioning/confirm_write_new_label boolean true
d-i partman-partitioning/confirm_new_label boolean true
d-i partman-partitioning/choose_label string gpt
d-i partman/choose_partition select finish
d-i partman/confirm boolean true
d-i partman/confirm_nooverwrite boolean true
d-i partman-auto/expert_recipe_file recipe_regular
#
#Установка дополнительных модулей ядра
d-i anna/no_kernel_modules boolean true
#
#Выбор ядра
```

```
d-i base-installer/kernel/image select linux-5.15-generic
#
# Имя пользователя
d-i passwd/username string astra
#
# Пароль пользователя
d-i passwd/user-password password astra-01
d-i passwd/user-password-again password astra-01
#
# Выбор ПО
#d-i tasksel/first multiselect Base
tasksel tasksel/first multiselect Base
d-i pkgsel/include string ssh htop ifenslave vlan bridge-utils parted
#
# Samba WINS dhcp
d-i samba-common/dhcp string false
#
# Поиск CD
d-i apt-setup/cdrom/set-first boolean false
d-i apt-setup/use_mirror boolean false
#
# Уровень защищённости
d-i astra-additional-setup/os-check select Maximum security level Smolensk
#
# Дополнительные настройки уровня защищённости
d-i astra-additional-setup/additional-settings-smolensk multiselect  Enable Mandatory Integrity
Control, Enable Mandatory Access Control
#
dictionaries-common dictionaries-common/selecting_ispell_wordlist_default note
# Установка загрузчика GRUB
#
# Установка пароля GRUB
d-i grub-installer/password password astra-01
d-i grub-installer/password-again password astra-01
#
# Post install commands
d-i preseed/late_command string \
wget -O /tmp/grubnet.sh ftp://10.0.9.11/scripts/grubnet.sh ;\
sh "/tmp/grubnet.sh"
#
# Не показывать диалог окончания установки
d-i finish-install/reboot_in_progress note
#d-i finish-install/exit/poweroff boolean false
```

12 Формирование файлов recipe

Файлы recipe используются утилитой partman для разбивки целевого диска на партиции перед началом установки. Сами файлы расположить в директории /srv/ftp/scripts (см. приведенную выше структуру каталогов и файлов).

Файлы для методов lvm и regular различаются, но между версиями ОС различий нет, поэтому для множества версий в обем случае достаточно двух файлов recipe.

Выставить лимиты (limits). Три числа означают следующее, слева направо: <minimal size>_<priority>_<maximal size>_<parted fs>.

Рекомендации по выбору значений priority:
1) для небольших партиций (около 1 Гб) выставлять равным или большим максимального значения,
2) для остальных случаев - выбирать между минимальным и максимальным числами.

regular recipe

```
custom ::
512 1025 512 fat32
$primary{ } $bootable{ }
method{ efi } format{ }
mountpoint{ /boot/efi }
.
768 1026 1024 ext2
$primary{ } $bootable{ }
method{ format } format{ }
use_filesystem{ } filesystem{ ext2 }
mountpoint{ /boot }
.
10000 20000 40000 ext4
method{ format } format{ }
use_filesystem{ } filesystem{ ext4 }
mountpoint{ / }
.
1024 8192 8192 linux-swap
method{ swap } format{ }
.
```

LVM recipe

```
custom ::
512 1025 512 fat32
$primary{ } $bootable{ }
method{ efi } format{ }
mountpoint{ /boot/efi }
.
768 1024 1024 ext2
$primary{ } $bootable{ }
method{ format } format{ }
use_filesystem{ } filesystem{ ext2 }
mountpoint{ /boot }
.
7000 8000 9000 ext4
$lvmok{ } lv_name{ rootlv }
method{ format } format{ }
use_filesystem{ } filesystem{ ext4 }
mountpoint{ / }
.
256 256 512 linux-swap
$lvmok{ } lv_name{ swaplv }
method{ swap } format{ }
#.
#1024 1025 -1 ext4
#$lvmok{ } lv_name{ homelv }
#method{ format } format{ }
#use_filesystem{ } filesystem{ ext4 }
#mountpoint{ /home }
.
```

13 Скрипт postinstall

Файл скрипта расположить в каталоге

```
/srv/ftp/scripts
```

Сформированный файл interfaces для настройки сети на установленной системе расположить там же, поправив ссылку в теле скрипта.

Указать в теле скрипта корректный адрес зеркала.

```
#!/bin/sh
MIRROR=10.0.9.11
# remove net.ifnames, update grub
sed -i 's/net.ifnames=0//g' /target/etc/default/grub
in-target update-grub
in-target systemctl enable ssh.service
#
# update interfaces
wget -O /tmp/interfaces ftp://${MIRROR}/scripts/interfaces_ph_v1
cat /tmp/interfaces > /target/etc/network/interfaces
```

14 Сетевая загрузка

В настройках BMC выставить сетевой загрузке высший приоритет и перезагрузить машину. Выбрать необходимый пункт установки.

Операционные системы на всех хостах установлены, перейдём к Bootstrap для разворачивания, собственно, программного комплекса AIC.

15 Подготовка bootstrap сервера VM-bootstrap

Первым этапом происходит обновление кэша пакетов и установка необходимых пакетов - зависимостей для дальнейшей работы.

```
sudo apt update && sudo apt install curl git docker.io -y
```

Далее нужно создантъ пары ключей SSH (приватный и публичный).
Для создания пары ключей выполните в консоли следующую команду. По умолчанию два ключа сохраняются в папке ~/.ssh, которая находится в корне текущего пользователя. (полный путь к папке /home/<имя текущего пользователя>/.ssh/)

```
ssh-keygen -N ""
```

Для корректного запуска taskfile SSH ключ должен быть создан без секретной фразы.
Пустое значение параметра -N команды ssh-keygen -N "" в примере выше подразумевает пустую секретную фразу для SSH ключа

```
astra@alse-vanilla-gui:~/.ssh$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/astra/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/astra/.ssh/id_rsa.
Your public key has been saved in /home/astra/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:5B91hbH3A+Oyrbty6yzCW7XvRLaeO0QRehqlJvNefow astra@alse-vanilla-gui
The key's randomart image is:
+---[RSA 2048]----+
|             ooo.|
|            +.,o |
|         .o =.++ .|
|        o  =.=oo..|
|         S .=.=  ..|
|          .o.X.+ .|
|       .   ..+.E o |
|        o.o..=.o  |
|        .o =B=*o  |
+----[SHA256]-----+
astra@alse-vanilla-gui:~/.ssh$
```

Если Вы ранее добавляли публичный SSH ключ на порталы git.astralinux.ru и hub.astra-automation.ru и хотите продолжать пользоваться существующими ключами, можно их скопировать (приватный и публичный ключи) на "джамп" машину в папку SSH текущего пользователя по умолчанию ~/.ssh/

Приватный ключ должен иметь особые права на чтение, запись и выполнение - только владелец файла может читать и редактировать файл (chmod 0600).
Чтобы проверить и поправить права на использование файлом, можно выполнить всю следующую команду в консоли:

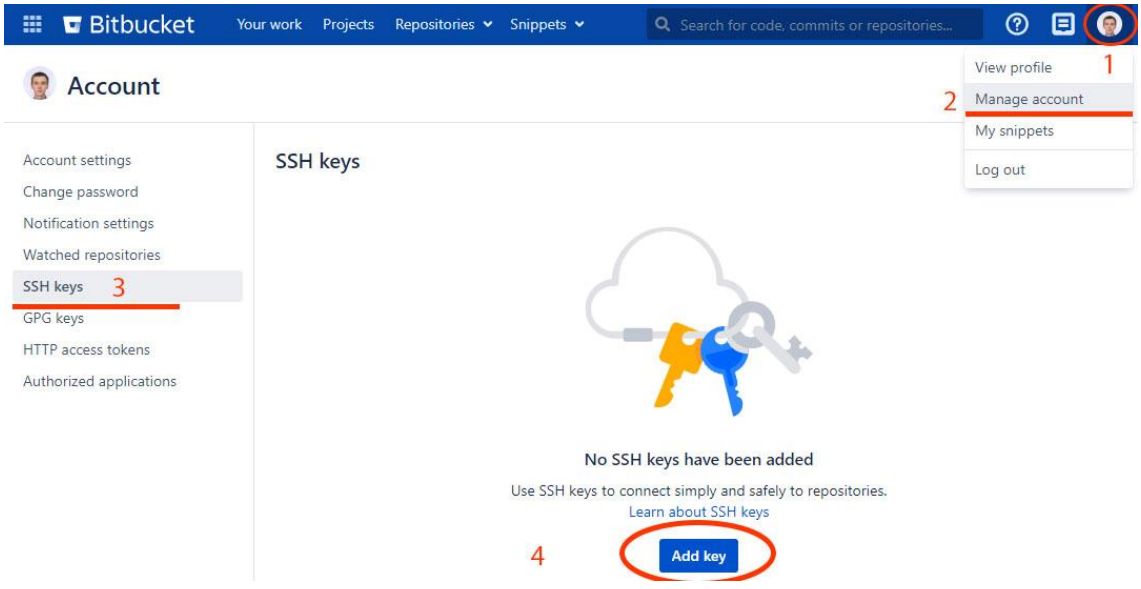
```
### В интерактивном режиме будет запрошен полный путь до приватного SSH ключа. Например, /home/astra/.ssh/id_rsa. Автозаполнение пути по нажатию клавиши TAB в данном случае не работает!


read -p "Provide full path to the private SSH key: " filename; if [ -r "$filename"  ] && [ -w "$filename"  ] && [ ! -g "$filename"  ] && [ ! -x "$filename"  ]; then echo "File " "$filename" " has correct permissions"; else echo "File " "$filename" " has wrong permissions. Setting 0600 permissions." && sudo chmod 0600 "$filename" && if [ -r "$filename"  ] && [ -w "$filename"  ] && [ ! -g "$filename"  ] && [ ! -x "$filename"  ]; then echo "File " "$filename" " now has correct permissions"; fi; fi
```

Добавление публичного ключа на порталы git.astralinux.ru **и** hub.astra-automation.ru

git.astralinux.ru

2. Перейти на портал https://git.astralinux.ru.
3. В настройках профиля в разделе SSH keys добавить содержимое свежесозданного приватного ключа **id_rsa.pub** в список авторизованных ключей для Вашего профиля.

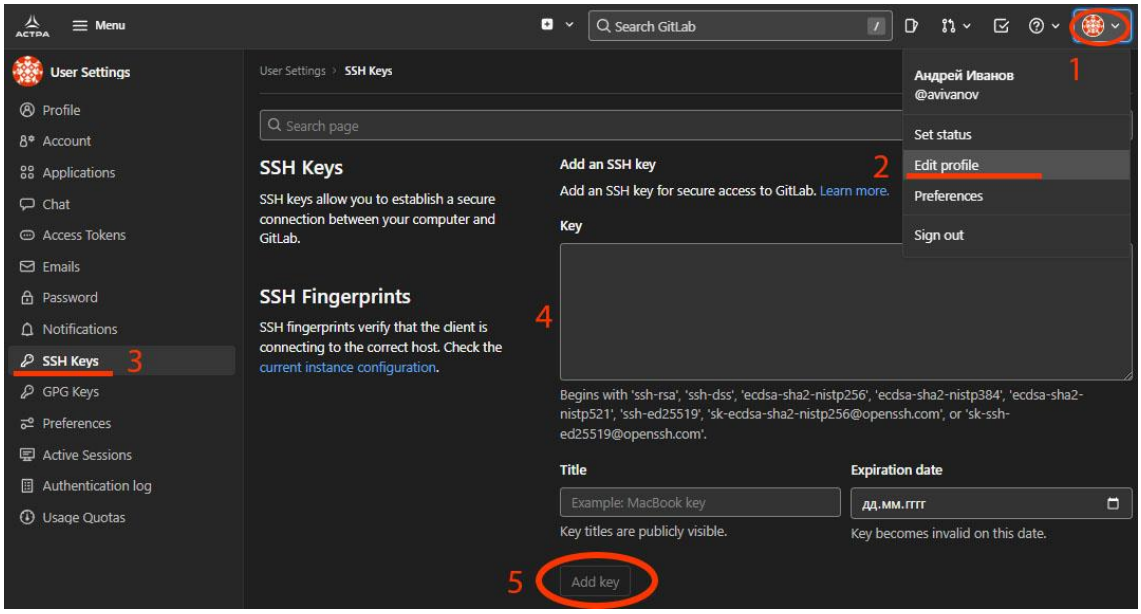
git



hub.astra-automation.ru

2. Перейти на https://hub.astra-automation.ru
3. В настройках профиля в разделе SSH keys добавить содержимое свежесозданного приватного ключа **id_rsa.pub** в список авторизованных ключей для Вашего профиля.

hub


Menu
Search GitLab
User Settings
Profile
Account
Applications
Chat
Access Tokens
Emails
Password
Notifications
SSH Keys
GPG Keys
Preferences
Active Sessions
Authentication log
Usage Quotas
3
User Settings › SSH Keys
Search page
SSH Keys
SSH keys allow you to establish a secure connection between your computer and GitLab.
SSH Fingerprints
SSH fingerprints verify that the client is connecting to the correct host. Check the current instance configuration.
Add an SSH key
Add an SSH key for secure access to GitLab. Learn more.
2
Key
4
Begins with 'ssh-rsa', 'ssh-dss', 'ecdsa-sha2-nistp256', 'ecdsa-sha2-nistp384', 'ecdsa-sha2-nistp521', 'ssh-ed25519', 'sk-ecdsa-sha2-nistp256@openssh.com', or 'sk-ssh-ed25519@openssh.com'.
Title
Example: MacBook key
Key titles are publicly visible.
Expiration date
дд.мм.гггг
Key becomes invalid on this date.
5
Add key
Андрей Иванов
@avivanov
1
Set status
Edit profile
Preferences
Sign out

16 Установка ВМ - контроллеров ALD Pro, серверов управления KVM и CEPH машин из qcow2 образов на физических нодах KVM

2. Перейдите в папку, в которую Вы бы хотели загрузить репозиторий
3. Выполните в консоли команду:

```
git clone ssh://git@git.astralinux.ru:7999/cloud/aic-tasks.git
cd aic-tasks
```

Нам нужно назначить переменные в файл env_variables и далее запустить развертывание ВМ машин:

```
vim env_variables
./rolloutvm.sh
```

Логика работы rolloutvm.sh скрипта заключается в следующих шагах:

- Для каждого KVM хост последовательно подготавливается инфраструктура:
  - Если не сгенирирована SSH пара ключей, то она генерируется
  - Загружаются образы (qemu image) ASTRA - 1.7.4, 1.7.2
  - Публичный ключ и образы копируются на KVM хост
  - Создаются условия на KVM для успешного изменения сети:
    - удаляется пакеты: avahi-daemon network-manager wpasupplicant
    - деактивируются службы: firewalld dnsmasq ModemManager one-context one-context-online one-context-local (последние 3 имеют смысл для вложенной виртуализации, то есть для тестового окружения)
    - проверяется что предустановлены astra-kvm и bridge-utils
- Изменяется сеть в /etc/network/interfaces (далее ENI)
  - добавляется bridge с названием brald
  - Интерфейс сети с ранее назначенным IP адресом добавляется в bridge
  - bridge назначается ранее используемый адрес
  - перегружается KVM хост
- Задается Виртуальная сеть для виртуальной инфраструктуры, привязанная к brald, и названная management.
- Поднимается внутренный DHCP сервер - dnsmasq (может конфликтовать с bootstrap, нужно определить данный момент)
- Создается Виртуальная Машина ald
  - DHCP отдает адрес, мы его перехватываем. И переопределяем статическую конфигурацию как задано в env_variables.
- Создается Виртуальная Машина front
  - DHCP отдает адрес, мы его перехватываем. И переопределяем статическую конфигурацию как задано в env_variables.
- Создается Виртуальная Машина ceph

    - DHCP отдает адрес, мы его перехватываем. И переопределяем статическую конфигурацию как задано в env_variables.
- Удаляем временные файлы на KVM хосте, деактивируем DHCP сервер
- Создается пустой диск и добавляется на ceph vm (только для тестовой среды !)

Результатом выполнения является работающие на каждом KVM ноде 3 виртуальные машины, имеющие IP адреса заранее заданные в файле env_variables.

17 Инициализация проекта и развертывание ресурсов brest-aldpro-ceph

Репозиторий https://git.astralinux.ru/projects/CLOUD/repos/aic-nano-cloud-env-dvis содержит сценарий развертывания brest-aldpro-ceph

17.1 brest-aldpro-ceph

- Environments:
  - Bare-metal
- Component versions:
  - Brest - 3.2
  - ALD Pro - 2.1.0
  - Ceph - 16
  - Astra Linux SE 1.7.2
  - Astra Linux SE 1.7.4uu1 for ALD Pro

17.2 Совместимость

Для запуска сценария необходимо установить

- git curl wget
- Task version: 3.18.0
- Docker version: 20.10.2

17.3 Настройка и запуск сценария, клонирование репозитория

```
git clone ssh://git@git.astralinux.ru:7999/cloud/aic-nano-cloud-env-dvis.git
```

17.4 Настройка параметров сценария

Расположите RSA ssh key-pair в `conf/ssh_keys/` директории для доступа к ВМ во время развертывания:

```
mkdir conf/ssh_keys
ln ~/.ssh/id_rsa conf/ssh_keys/id_rsa
ln ~/.ssh/id_rsa.pub conf/ssh_keys/id_rsa.pub
```

`Установите необходимые значения в файлах конфигурации деплоймента`

conf/group_vars/all.yml файл содержит настройки ALD Pro, Brest, Cheph

conf/inventory.yml в файле указаны IP адреса машин для развертывания ALD Pro, Brest, Cheph

Запустить развертывание:

```
task deploy
```

18 Развертывание RuBackup внутри установленного Бреста

Подразумевается что к этому этапу уже был развёрнут Брест

1. Заходим в подготовленный ранее Брест и создаем в нём сеть:
    a. В интерфейсе Бреста заходим в левой панели в меню **Сеть**, **Вирт.Сети**, нажимаем на заленую кнопку и выбрать **Создать**
    b. Во вкладке **Общие** задаем имя сети, например - Net
    c. Во вкладке **Конфигурации** в поле **Интерфейс сет. моста** указываем имя сетевого интерфейса, по которому будем происходить коммуникация, например, br0 или eth0, в зависимости от сетевой конфигурации серверов, в поле **Режим работы сети** выбираем **Bridged**
    d. Во вкладке **Адреса** в поле **Первый IPv4 адрес** указываем IP адрес, с которого начнется присвоение адресов ВМ, в поле **Размер** указываем количество доступных адресов, например 100 или 254
    e. Во вкладке **Контекст** указываем Адрес сети, Маска подсети, Шлюз, DNS.
2. Следующий шаг – это получение токена для учетной записи администратора. Для этого необходимо перейти в левой панели в меню Система, Пользователи. Выбираем пользователя Badmnin, во вкладке Аутентификация нажать на кнопке Управление токенами входа. В открывшемся окне скопирвать токен.

    Пожалуйста, обратите внимание на дату в поле **Действительно до**
3. На бутстрап сервере склонировать проект из репозитория ssh://git@git.astralinux.ru:7999/cloud/aic-repo2.git
4. По аналогии проделанных шагов по развёртыванию инфраструктуры выше, необходимо выполнить шаги по настройке ssh ключей и внесений измений в файлы **conf/inventory.yml** и **conf/group_vars/all.yml**
    a. В файле conf/inventory.yml указать следующее:
        i. Указать адрес рубекап сервера
        ii. Указать эндпоинт подключения к Бресту
        iii. Указать имя пользователя и токен подключения
        iv. Указать имя сети, созданной на первом шаге
        v. Указать id хранилищ
        vi. В параметер rubackup_client нужно указать IP адреса серверов для добавления их в рубекап, это те сервера, которые были созданы при разворачивании Бреста, их можно скопировать из проекта по его разворачиванию
    b. В файле **conf/group_vars/all.yml** указать следующее:
        i. Прописать репозиторий для RuBackup. За это отвечает переменная rubackup_default_repository. Строка с этой переменной должны выглядеть следующим образом: rubackup_default_repository: deb https://dl.astralinux.ru/rubackup/repository-deb-main/

c. В файле **/core/rubackup-core/ansible/group_vars/rubackup_server.yml** `в параметре rubackup_server_psql_password_rubackup нужно указать` пароль для пользователя rubackup для подключения к консоли управления рубекап

5. На заключительном шаге нужно перейти в корень папки проекта и выполнить команду **task deploy**