

Подготовка образов

РУСТЭК.VDI 4.0.4

2023



Содержание

1 1.1 1.2 1.3	Подготовка образа Red OS 7.3 Рекомендации перед установкой Действия после установки ОС Опциональные шаги	3 4 8
2	Подготовка образа Alt Workstation 10.1	10
2.1	Рекомендации перед установкой	10
2.2	Действия после установки ОС	11
2.3	Опциональные шаги	14
3	Подготовка образа Windows 10	15
3.1	Рекомендации перед установкой	15
3.2	Установка Cloudbase-init	23
3.3	Настройка групповой политики для использования графического процессора	25
4	Подготовка образа Astra Linux	28
4.1	Рекомендации перед установкой	28
4.2	Действия после установки ОС	28
4.3	Опциональные шаги	34
5	Термины и сокращения	37



1 Подготовка образа Red OS 7.3

Инструкция предназначена для настройки образа персонального рабочего места на базе операционной системы Red OS "Муром".

В процессе настройки потребуется установить операционную систему, агенты и выполнить ряд дополнительных настроек для обеспечения правильного функционирования.

Для удобства настройки рекомендуется иметь доступ в интернет с виртуальной машины и настраивать её через SSH.

1.1 Рекомендации перед установкой

- 1. Перед установкой операционной системы из ISO-образа, рекомендуется ознакомиться с актуальной инструкцией для Linux систем по ссылке: <u>Подготовка</u> <u>образа ОС семейства Linux.</u>
- 2. В образе используются дополнительные средства автоматизации и инициализации для виртуальных машин сервис cloud-init.

Для полноценной работы этого сервиса рекомендуется:

- избегать использование разметки LVM (указана по умолчанию);
- не выносить swap на отдельный раздел;
- вместо этого, рекомендуется использовать тип файловой системы XFS без отдельного раздела под swap.

Пример рекомендуемой разметки:

АЗМЕТКА ВРУЧНУЮ Готово		УСТАНОВКА RED OS MUROM-7.3. Ш ги
▼ Новая установка RED OS MUROM-7.3.2	sda2	
СИСТЕМА /boot 1024 МиБ sda1	Точка монтирования: /	Устройства: QEMU QEMU HARDDISK (sda)
/ 19 ГиБ > sda2	Требуемый объем: 19 ГиБ	Изменить
	Тип устройства: Стандартный раздел ▼ □ Зашифровать	
	Файловая система:	
	Метка:	Имя:
		sda2
		Применить
+ - C	Примеча вступят в ,	ние: сделанные в этом окне изменения действие только после нажатия кнопки «Начать установку» в главном меню.

3. С учетом наличия сервиса cloud-init и возможности автоматического расширения корневого раздела, предлагается использовать минимальный размер образа при подготовке. В текущей версии рекомендуемый размер составляет 20 Гб.



4. При установке базовой операционной системы важно добавить дополнительные пакеты, связанные с средствами облачной настройки:

ЫБОР ПРОГРАММ Готово	УСТАНОВКА RED OS MUROM-7 ги
базовое окружение	Дополнительное программное обеспечение для выбранной среды
 Рабочая станция с графическим окружением Рабочая станция с графическим окружением (МАТЕ) Сервер минимальный Сервер минимальный. Сервер с графическим интерфейсом Сервер с графическим интерфейсом. 	 Клиенты удалённого рабочего стола Поддержка смарт-карт Поддержка аутентификации с помощью смарт-карт. Клиенты виртуальных частных сетей Клиенты виртуальных частных сетей и соответствующие аплеты для NetworkManager
	 Средства облачной настройки. Средства облачной настройки. Библиотеки совместимости Библиотеки совместимости для приложений, созданных в предыдущи версиях Ред ОС. Консольные средства Интернета Консольные средства Интернета Консольные средства доступа к Интернету, обычно используемые администраторами. Средства разработки Стандартная среда разработки. Графические средства диминистрирования Графические программы управления системными компонентами. Совместимость с устаревшими функциями UNIX Программы совместимости для миграции или работы с устаревшими окружениями UNIX. Инженерные инструменты Средства для математических и научных вычислений и преобразований, а также параллельных вычислений. Средства безопасности Средства задиты для обеспечения целостности и проверки подличности.

5. Для обеспечения эффективной и автоматизированной сети на виртуальной машине, рекомендуется обязательно использовать DHCP.

1.2 Действия после установки ОС

1. После установки операционной системы рекомендуется выполнить обновление пакетов:

 sudo dnf update

 После обновления рекомендуется перезагрузить виртуальную машину

 2. После успешной перезагрузки войдите на виртуальную машину и переключитесь в режим суперпользователя root:

 sudo -i

 3. Затем перейдите в директорию /opt:

 cd /opt

4. Скачайте архив с агентом VDI для Red OS "Муром" 7.3, используя curl и соответствующий URL-адрес агента:

Рустэн

curl -O <URL-адрес файла агента Linux>

5. Создайте необходимые для работы директории:

```
mkdir /opt/vdi-agent-astra
mkdir -p /var/log/rustack agent/
```

 Разархивируйте архив с агентом, используя tar, и поместите файлы в созданную директорию:

tar -xvf /opt/<ФАЙЛ_АГЕНТА> --directory /opt/vdi-agent-astra

7. Выполните установку необходимых пакетов с помощью dnf. Можете дополнить список утилитами в соответствии с требованиями вашего образа:

dnf install -y x2goserver-xsession x2goserver-fmbindings x2goserver-common x2goserver x2goagent x2goserver-printing cups-x2go libxcrypt-compat cloud-init cloud-utils

8. Для удобства управления службой rustack_agent создадим символическую ссылку на соответствующий файл службы:

ln -s /opt/vdi-agent-astra/rustack_agent.service
/etc/systemd/system/rustack_agent.service

9. Перезагрузите конфигурацию диспетчера systemd и добавьте сервис rustack_agent в автозапуск:

systemctl daemon-reload && systemctl enable rustack_agent.service

10. Выполните настройки для доменной авторизации:

• Измените конфигурацию для доменной авторизации:

sed -i -e "s/%U@%D/%U/g" /usr/lib/realmd/realmd-defaults.conf

 Добавьте настройку для создания домашних директорий при подключении через SSH:

echo -e "session required pam_mkhomedir.so skel=/etc/skel/ umask=0022" >>
/etc/pam.d/sshd

Измените настройки systemd для обработки пользовательских процессов:

sed -i -e "s/#KillUserProcesses=yes/KillUserProcesses=no/g"
/etc/systemd/logind.conf





• Добавьте строки с настройками клавиатуры в файл /etc/x2go/Xkbmap:



11. Настройка cloud-init.

Чтобы настроить cloud-init, отредактируйте файл /etc/cloud/cloud.cfg и добавьте следующую конфигурацию:



Пожалуйста, убедитесь, что параметр disable_root имеет значение false, если вы хотите разрешить вход пользователя root.

Пример полного конфигурационного файла:



```
# The top level settings are used as module
# and system configuration.
\ensuremath{\texttt{\#}} A set of users which may be applied and/or used by various modules
# when a 'default' entry is found it will reference the 'default_user'
# from the distro configuration specified below
   - default
disable vmware customization: false
# If this is set, 'root' will not be able to ssh in and they
# will get a message to login instead as the default $user
disable root: false
# This will cause the set+update hostname module to not operate (if true)
preserve hostname: false
# If you use datasource_list array, keep array items in a single line.
# Example datasource config
# datasource:
#
       metadata_urls: [ 'blah.com' ]
#
       timeout: 5 # (defaults to 50 seconds)
max_wait: 10 # (defaults to 120 seconds)
#
#
datasource:
  Ec2:
    strict_id: false
    timeout: 10
    max wait: 1
    metadata urls:
      - http://169.254.169.254:80
# The modules that run in the 'init' stage
 - migrator
 - seed random
 - bootcmd
 - growpart
 - disk setup
 - set hostname
 - update_hostname
 - update etc hosts
 - rsyslog
 - users-groups
cloud config modules:
 - ssh-import-id
 - set-passwords
 - disable-ec2-metadata
 - runcmd
# The modules that run in the 'final' stage
```





12. Для автоматического запуска сервиса cloud-init, выполните команду:

systemctl enable cloud-init

13. Для обеспечения уникальности идентификаторов виртуальных машин, необходимо удалить machine-id:

echo -n > /etc/machine-id

Это приведет к очистке файла machine-id, и в будущем будут сгенерированы новые уникальные идентификаторы для каждой виртуальной машины.

После выполнения этих шагов завершается подготовка образа.

Рекомендуется ознакомиться с <u>опциональными шагами</u> . Если они не требуются,
выполните:
cat /dev/null > ~/ bash history && history -c && noweroff

Эта команда очищает историю команд пользователя и выключает систему

1.3 Опциональные шаги

1. Создание файла swap (если отказались от отдельного раздела для swap)

Если решено создавать swap в виде файла (в данном примере 1Гб), выполните следующие команды:



```
dd if=/dev/zero of=/swapfile bs=1024 count=1048576
chmod 0600 /swapfile
mkswap /swapfile
swapon /swapfile
echo 'vm.swappiness=10' > /etc/sysctl.d/swap.conf
sysctl --system
echo "/swapfile none swap sw 0 0" >> /etc/fstab
```

2. Если созданный локальный пользователь на этапе установки не должен присутствовать в будущих виртуальных машинах, выполните следующую команду (в данном примере удаляем пользователя "centos"):

userdel centos -r -f

3. Если был разрешен доступ по SSH для пользователя root, но на виртуальной машине данный доступ не планируется, то его необходимо закрыть.



2 Подготовка образа Alt Workstation 10.1

Инструкция предназначена для настройки образа персонального рабочего места на базе операционной системы Alt Workstation 10.1.

В процессе настройки потребуется установить операционную систему, агенты и выполнить ряд дополнительных настроек для обеспечения правильного функционирования.

Для удобства настройки рекомендуется иметь доступ в интернет с виртуальной машины и настраивать ее через SSH.

2.1 Рекомендации перед установкой

- 1. Перед установкой операционной системы из ISO-образа, рекомендуется ознакомиться с актуальной инструкцией для Linux систем по ссылке: Подготовка образа ОС семейства Linux.
- 2. В образе используются дополнительные средства автоматизации и инициализации для виртуальных машин сервис cloud-init.

Для полноценной работы этого сервиса рекомендуется:

- Избегать использование разметки LVM (указана по умолчанию).
- Не выносить swap на отдельный раздел.

Пример рекомендуемой разметки:

		1 9		4/12: Подго	отовка диска			
Имя BtrFS • Disks • So	p ja 2	азмер [свободно] 10 GB	Файловая система	Точка монтирования	Опции монтирования			
LVM RAID	sdal 3 sda2 1	928 MB (9929 MB) 6 GB (16 GB)	SWAPES Ext2/3	1	relatime			
			Удалузь		Удалить фа	йловую систему		

 С учетом наличия сервиса cloud-init и возможности автоматического расширения корневого раздела, предлагается использовать минимальный размер образа при подготовке. В текущей версии рекомендуемый размер составляет 20 Гб.



4. Для обеспечения эффективной и автоматизированной сети на виртуальной машине, рекомендуется обязательно использовать DHCP.

2.2 Действия после установки ОС

1. Необходимо разблокировать возможность использовать sudo:

control sudowheel enabled

2. После установки операционной системы рекомендуется зайти на виртуальную машину и выполнить обновление пакетов:

apt-get update && apt-get dist-upgrade && update-kernel

После обновления рекомендуется перезагрузить виртуальную машину

 После успешной перезагрузки войдите на виртуальную машину и переключитесь в режим суперпользователя root:

sudo su

4. Затем перейдите в директорию /opt:

cd /opt

5. Скачайте архив с агентом VDI для Alt Workstation 10.1, используя curl и соответствующий URL-адрес агента:

curl -O <URL-адрес файла агента Linux>

6. Создайте необходимые для работы директории:

```
mkdir /opt/vdi-agent-astra
mkdir -p /var/log/rustack_agent/
```

7. Разархивируйте архив с агентом, используя tar, и поместите файлы в созданную директорию:

tar -xvf /opt/<ФАЙЛ_АГЕНТА> --directory /opt/vdi-agent-astra

8. Выполните установку необходимых пакетов. Можете дополнить список утилитами в соответствии с требованиями вашего образа:



apt-get install x2goserver x2goserver-printing cups-x2go cloud-init cloudutils 9. Для удобства управления службой rustack_agent создадим символическую ссылку на соответствующий файл службы: ln -s /opt/vdi-agent-astra/rustack_agent.service /etc/systemd/system/rustack_agent.service

10. Перезагрузите конфигурацию диспетчера systemd и добавьте сервис rustack_agent в автозапуск:

systemctl daemon-reload && systemctl enable rustack_agent.service

11. Выполните настройки для доменной авторизации и X2GO:



12. Настройка cloud-init.

Чтобы настроить cloud-init, отредактируйте файл /etc/cloud/cloud.cfg и добавьте следующую конфигурацию:



```
- default
disable root: false
resize_rootfs_tmp: /dev
ssh_pwauth:
ssh_deletekeys:
ssh_genkeytypes: ~
ssh_svcname: sshd
syslog_fix_perms: ~
datasource:
  Ec2:
   strict id: false
   metadata urls:
manage_etc_hosts: true
 - migrator
 - growpart
 - resizefs
 - disk_setup
 - update_hostname
 - update etc hosts
 - ca-certs
 - rsyslog
 - users-groups
cloud_config_modules:
 - ssh-import-id
 - set-passwords
 - spacewalk
 - runcmd
cloud final modules:
 - package-update-upgrade-install
 - puppet
 - salt-minion
 - rightscale userdata
 - scripts-vendor
 - scripts-per-once
 - scripts-per-boot
 - scripts-per-instance
 - scripts-user
 - ssh-authkey-fingerprints
```



```
- keys-to-console

- phone-home

- final-message

- power-state-change

system_info:

# This will affect which distro class gets used

distro: altlinux

paths:

    cloud_dir: /var/lib/cloud/

    templates_dir: /etc/cloud/templates/

network:

    renderers: ['netplan', 'networkd', 'etcnet']

    ssh_svcname: sshd
```

13. Для автоматического запуска сервиса cloud-init, выполните команду:

systemctl enable cloud-init

После выполнения этих шагов завершается подготовка образа.

Рекомендуется ознакомиться с <u>опциональными шагами</u>. Если они не требуются, выполните:

cat /dev/null > ~/.bash_history && history -c && poweroff

Эта команда очищает историю команд пользователя и выключает систему

2.3 Опциональные шаги

 Если созданный локальный пользователь на этапе установки не должен присутствовать в будущих виртуальных машинах, выполните следующую команду (в данном примере удаляем пользователя "user"):

```
su -
userdel user -r -f
```

 Если был разрешен доступ по SSH для пользователя root, но на виртуальной машине данный доступ не планируется, то его необходимо закрыть.



3 Подготовка образа Windows 10

Инструкция предназначена для настройки образа персонального рабочего места на базе операционной системы Windows 10.

В процессе настройки потребуется установить операционную систему, агенты и выполнить ряд дополнительных настроек для обеспечения правильного функционирования.

Для удобства настройки рекомендуется иметь доступ в интернет с виртуальной машины и настраивать ее через RDP клиента.

3.1 Рекомендации перед установкой

- 1. Перед установкой операционной системы из ISO-образа, рекомендуется ознакомиться с актуальной инструкцией для Windows систем по ссылке: Подготовка образа OC Windows 10. Пройдите все обязательные шаги, пропустите все опциональные.
- 2. После входа на машину скачайте VMWare Horizon OS Optimization tool. Установите и запустите инструмент.
- 3. Нажмите кнопку Analyze.

Optimize	Generali	• ize	Finalize	Update	History	Ten	nplates	References	2107
System Info	rmation			la a			,		
🛄 os					🗍 System Nan	10			
Version					🐣 User Name				
Processor				2683 v4 @ 2.10GHz	🖂 Windows Di	rectory			
 System Typ 	be .	64-bit			🖭 Physical Me	mory			
💷 Windows L	ocale				🗔 Display Con	troller			
🖭 Display Ad	apter RAM				👰 Network Ad	apter		thernet Adapt	
								2	
emplate VMv	ware\Windov	ws 10 and	d Sr 🗸 🛛 💿 co	mmon Options			-	Analysis Result	It PE Import Selections E Export Selections Search Q
			c	lick Ana	ilyze bu	tto	n to	review	optimization items
									@ Analyze

4. Нажмите Optimize и дождитесь завершения.



Optimize General	+ O Horalize	Update	History	Templates	References				2107
System Information					Ana	alysis Summary			
🗖 os			📱 System Nam	e VPN-WORK	: 6	600			
Version			🛆 User Name	Administrat	or 4	100			
Processor			🖂 Windows Di	rectory C:\Windows		385			
(i) System Type			🖭 Physical Me	mory 8,00 GB	2	123	122		
Windows Locale			🖃 Display Cont	troller VMware SV	GA 3D	0 Total		Optional	
🖭 Display Adapter RAM			🗟 Network Ad	apter vmxnet3 Etl	hernet Adapt		Recommended		
						Optimization Not Applie	d Optimization A	pplied	
emplate VMware\Window	ws 10 and Sr 🗸 🛛 🛞 Co	mmon Options		🗗 Export	Analysis Result	⇐ Import Selections	≔ Export Selectio	ns Search <u>Q</u>	
	Opt	imizations				ExpectedValue		Actual Value	
🗸 🗹 Modifications t	o Standard Image (50	B items)							Select "Di
V 🗹 Security (10	8 items)								
> Defender	Antivirus (16 items)								
> Firewall (1 items)								
	itoms)								
	nterns)								
> Security	Center (6 items)								
SmartScr	een (5 items)								
> 🗹 Telemetr	y and Privacy (37 item	s)							
> 🗹 🛛 Windows	Update (36 items)								
🗸 🔽 User Experie	ence (150 items)								
									\rightarrow
								O Anal	yze 🗸 Optimize

- 5. Откройте PowerShell от имени администратора.
- 6. Введите команду для установки политики выполнения PowerShell:

Set-ExecutionPolicy RemoteSigned
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned
Изменение политики выполнения Политика выполнения защищает компьютер от ненадежных сценариев. Изменение политики выполнения может поставить под угрозу безопасность системы, как описано в разделе справки, вызываемом командой about_Execution_Policies и расположенном по адресу https:/go.microsoft.com/fwlink/?LinkID=135170 . Вы хотите изменить политику выполнения? [Y] Да - Y [A] Да для всех - A [N] Нет - N [L] Нет для всех - L [S] Приостановить - S [?] Справка (значением по умолчанию является "N"):А
7. Выберите 'А' - Да для всех.

8. Введите команду для загрузки модуля, обеспечивающего управление обновлениями Windows:

Install-Module -Name PSWindowsUpdate

- 9. Выберите 'Ү' Да.
- 10. Введите команду для подключения модуля PSWindowsUpdate к текущей сессии:

Import-Module PSWindowsUpdate

11. Введите команду для просмотра доступных обновлений:

Get -Wi ı	ndowsUp	date		
DESKTOP-8		<b5005463< th=""><th>4MB</th><th>Обновление для Windows 10 Version 21Н1 для систем на базе процессоров x64 (</th></b5005463<>	4MB	Обновление для Windows 10 Version 21Н1 для систем на базе процессоров x64 (
DESKTOP-8		(B5021087	68MB	2022-12 Накопительный пакет обновления .NET Framework 3.5, 4.8 и 4.8.1 для
DESKTOP-8		(B890830	57MB	Средство удаления вредоносных программ для платформы x64: v5.116 (КВ890830)
DESKTOP-8		(B4023057	3MB	Обновление для Windows 10 Version 21Н1 для систем на базе процессоров x64 (
DESKTOP-8		KB5030211	107GB	Обновление функций до Windows 10, версия 21Н2

12. Введите команду для установки обновлений:



Install-WindowsUpdate PS C:\Windows\system32> Install-WindowsUpdate Подтверждение Вы действительно хотите выполнить это действие? Выполнение операции "(28.09.2023 15:49:43) Обновление для Windows 10 Version 21H1 для систем на базе процессоров x64 (KB5005463), 2022-04[4MB]" над целевым объектом "DESKTOP-8MIHTH3". [Y] Да - Y [A] Да для всех - A [N] Нет - N [L] Нет для всех - L [S] Приостановить - S [?] Справка (значением по умолчанию является "Y"):A 13. Выберите 'A' - Да для всех.

14. Ожидайте завершение установки, это может занять от 5 до 25 минут. Если в консоли долгое время нет движения, нажмите Enter.

```
3 DESKTOP-8... Installed KB4023057 3MB Обновление для Windows 10 Version 21H1 для систем
3 DESKTOP-8... Installed KB5030211 107GB Обновление функций до Windows 10, версия 21H2
Reboot is required. Do it now? [Y / N] (default is 'N')
```

- 15. Подтвердите выбор, нажав 'У', и перезапустите машину.
- 16. После перезапуска машины загрузите установщик агента.
- 17. Запустите его и завершите установку агента.
- 18. Зайдите в настройки.



19. Перейдите в раздел Система.



20. Найдите пункт Удаленный рабочий стол.

Windows не активирован. А



Сис	тема
₽	Дисплей
(1))	Звук
	Уведомления и действия
I	Фокусировка внимания
Ċ	Питание и спящий режим
	Память
귝	Планшет
Ħ	Многозадачность
Ð	Проецирование на этот компьютер
ж	Общие возможности
ĥ	Буфер обмена
><	Удаленный рабочий стол
î	О программе

21. Далее нажмите на выделенный текст в разделе Учетные записи пользователей.



Удаленный рабочий стол

Функция "Удаленный рабочий стол" позволяет подключаться к этому компьютеру и управлять им с удаленного устройства, используя клиент удаленного рабочего стола (доступен для Windows, Android, iOS и macOS). Вы сможете работать с другого устройства так же, как на этом компьютере.

Включить удаленный рабочий стол



Оставлять мой компьютер в режиме бодрствования для соединения, когда он подключен к электросети Показать параметры

Сделать мой компьютер обнаруживаемым в частных сетях для активации автоматического подключения с удаленного устройства Показать параметры

Дополнительные параметры

Как подключиться к этому ПК

Используйте имя ПК, чтобы подключиться к нему с удаленного устройства: DESKTOP-8MIHTH3

На вашем удаленном устройстве нет клиента удаленного рабочего стола?

Учетные записи пользователей

Выберите пользователей, которые могут получить удаленный доступ к этом компьютеру

22. Нажмите Добавить следом Дополнительно.

пьютер в р	режиме	
і соединені	ия, когда он Показать параметры	
росети	Пользователи удаленного рабочего стола 🛛 🗙	
иотер в частных с ического п и́ства	сетях подкл	
летры		
ся к это	User ужимеет доступ. МУГ Добавить Удалить Чтобы создать новую учетную запись или добавить пользователей в	
гобы подкл	ЛЮЧИТ другие группы, откройте панель управления <u>Учетные записи</u>	
Γ	Выбор: "Попьзователи"	×
	Выберите тип объекта:	
стройстве	"Пользователи" или "Встроенные субъекты безопасности" Типы объектов	
	В следующем месте:	
	DESKTOP-8МІНТНЗ Размещение	
пользо	Введите <u>и</u> мина выбираемых объектов (<u>примеры</u>):	
∍й, которь	Проверить имена	
	Дополнительно ОК Отмена	

Рустэн

23. Затем нажмите Поиск и выбираем группу Прошедшие проверку.

Пользователи" или "Ватроенные субъекты безопасности" Пользователи" или "Ватроенные субъекты безопасности" В следующем месте: DESKTOP-8MIHTH3 Pазмещение Oбщие запросы Имя: начинается (Выберите тип объекта:	
В следующем месте: DESKTOP-8MIHTH3 Размещение Общие запросы Имя: начинается ("Пользователи" или "Встроенные субъекты безопасности"	Типы объектов
DESKTOP-8MIHTH3 Размещение Общие запросы	В следующем месте:	
Общие запросы Имя: начинается () Столбшы Описания: начинается () Поиск Описания: начинается () Поиск Описания: начинается () Поиск Описания: начинается () Стол Пароли с неограниченным сроком действия Стол ОК Число дней со времени последнего входа в систему: ОК Отмена Pesyльтаты поиска: Мя В папке С ОК Отмена Proprinta CO3ДАТЕЛЬ ИНТЕРАКТИВНЫЕ КОНСОЛЬНЫЙ ВХОД Локальная учетная запись Подтвержденное службой удостоверение Сертимикат этой организации ССЕТЬ ССИСТЕМА Сертимикат этой организации ССТБИА	DESKTOP-8MIHTH3	Размещение
Имя: начинается () Описание: начинается () Описание: начинается () Поиск Стопонс Пароли с неограниченным сроком действия Число дней со времени последнего входа в систему: Учисло дней со времени последнего входа в систему: ОК Отмена Мя В папке ГРУППА-СОЗДАТЕЛЬ ИНТЕРАКТИВНЫЕ КОНСОЛЬНЫЙ ВХОД Локальная учетная запись Локальная учетная запись Сриженное службой удостоверение Лодтвержденное службой удостоверение Лодтвержденное цлужбой удостоверение Лодтвержденое цлужбой удостоверение Подтвержденое цлужбой удостоверение Лодтвержденое цлужбой удостоверение Лодтвержденое цлужбой удостоверение Лодтвержденое цлужбой удостоверение Подтвержденое цлужбой удостоверение Лодтвержденое цлужбой удостоверение Подтвержденое цлужбой удостовержденое цлужбой удостовержденое цлужбой удостовержденое цлужбой удостовержденое цлужбой удостовержденое	Общие запросы	
Описание: начинается с Поиск Отключенные учетные записи Пароли с неограниченным сроком действия Число дней со времени последнего входа в систему: Соти Результаты поиска: ОК Отмена Результаты поиска: ОК Отмена ОК Отмена ОК Отмена ОК Отмена ОК Отмена ОК Отмена ОК Отмена ОК Отмена ОК Отмена ОК Отмена СОСПЬНЫЙ ВХОД Локальная учетная запись Локальная учетная запись Локальная учетная запись Локальная учетная запись Подтвержденное службой удостоверение Подтвержденное центром проверки подликисти ПОЛЬЗОВАТЕЛЬ СЕРВЕРА ТЕРМИНАТОВ ПРАВА ВПАЛЕЛЫИ Прошедшие проверку Серть ССТЕМА	Имя: начинается (>	Столбцы
Стоп Пароли с неограниченным сроком действия Число дней со времени последнего входа в систему:	Описание: начинается (<>	Поиск
Пароли с неограниченным сроком действия Число дней со времени последнего входа в систему:	Отключенные учетные записи	Стоп
Число дней со времени последнего входа в систему:	Пароли с неограниченным сроком действия	
Сезультаты поиска: Мя В папке ГРУППА-СОЗДАТЕЛЬ ИНТЕРАКТИВНЫЕ КОНСОЛЬНЫЙ ВХОД Локальная учетная запись Локальная учетная запись и член группы "Админ ПАКЕТНЫЕ ФАЙЛЫ Подтвержденное службой удостоверение Подтвержденное службой удостоверение Подтвержденное центром проверки подлиниости ПОЛЬЗОВАТЕЛЬ СЕРВЕРА ТЕРМИНАТОВ ПРАВА ВПАЛЕЛЬЦА Прошедшие проверку Ссертификат этой организации ССТЬ СИСТЕМА	Число дней со времени последнего входа в системи;	<i>Ş</i> 7
ГРУППА-СОЗДАТЕЛЬ ИНТЕРАКТИВНЫЕ КОНСОЛЬНЫЙ ВХОД Локальная учетная запись Локальная учетная запись и член группы "Админ ПАКЕТНЫЕ ФАЙЛЫ Подтвержденное центром проверки подливности ПОЛЬЗОВАТЕЛЬ СЕРВЕРА ТЕРМИНАЛОВ ПРАВА ВПАЛЕЛЫЦ Прошедшие проверку Сертификат этой организации ССТБ	езультаты полока.	
ИНТЕРАКТИВНЫЕ КОНСОЛЬНЫЙ ВХОД Локальная учетная запись Локальная учетная запись и член группы "Админ ПАКЕТНЫЕ ФАЙЛЫ Подтвержденное центром проверки подлизиости ПОЛЬЗОВАТЕЛЬ СЕРВЕРА ТЕРМИНАЛОВ ПРАВА ВПАЛЕЛЬЦА Прошедшие проверку Сертификат этой организации СЕТЬ СИСТЕМА		
КОНСОЛЬНЫИ ВХОД Локальная учетная запись Локальная учетная запись и член группы "Админ ПАКЕТНЫЕ ФАЙЛЫ Подтвержденное центром проверки подлициости ПОЛЬЗОВАТЕЛЬ СЕРВЕРА ТЕРМИНАЛОВ ПРАВА ВПАЛЕПЫЦА Прошедшие проверку Сертификат этой организации ССЕТЬ СИСТЕМА	ГРУППА-СОЗДАТЕЛЬ	
Локальная учетная запись и член группы "Админ ПАКЕТНЫЕ ФАЙЛЫ Подтвержденное службой удостоверение Подтвержденное центром проверки подливности ПОЛЬЗОВАТЕЛЬ СЕРВЕРА ТЕРМИНАЛОВ ПРАВА ВПАЛЕПЬЦА Прошедшие проверку Сертификат этой организации СЕТЬ СИСТЕМА	СГРУППА-СОЗДАТЕЛЬ ИНТЕРАКТИВНЫЕ	
ПАКЕТНЫЕ ФАЙЛЫ Подтвержденное службой удостоверение Подтвержденное центром проверки подлизиости ПОЛЬЗОВАТЕЛЬ СЕРВЕРА ТЕРМИНАТОВ ПРАВА ВПАЛЕЛЬЦА Прошедшие проверку Сертификат этой организации СЕТЬ СИСТЕМА	СРУППА-СОЗДАТЕЛЬ ИНТЕРАКТИВНЫЕ КОНСОЛЬНЫЙ ВХОД	
Подтвержденное служоой удостоверение Подтвержденное центром проверки подливности ПОЛЬЗОВАТЕЛЬ СЕРВЕРА ТЕРМИНАЛОВ ПРАВА ВПАЛЕЛЬЦА Прошедшие проверку Сертификат этой организации СЕТЬ СИСТЕМА	ГРУППА-СОЗДАТЕЛЬ ИНТЕРАКТИВНЫЕ КОНСОЛЬНЫЙ ВХОД Локальная учетная запись Локальная учетная запись и член группы "Админ	
ПОЛЬЗОВАТЕЛЬ СЕРВЕРА ТЕРМИНАЛОВ ПРАВА ВПАЛЕПЬЦА Прошедшие проверку Сертификат этой организации СЕТЬ СИСТЕМА	ГРУППА-СОЗДАТЕЛЬ ИНТЕРАКТИВНЫЕ КОНСОЛЬНЫЙ ВХОД Локальная учетная запись Локальная учетная запись и член группы "Админ ПАКЕТНЫЕ ФАЙЛЫ	
СПРАВА ВПАЛЕПЫЦА Прошедшие проверку Ссертификат этой организации ССЕТЬ ССИСТЕМА	ИНТЕРАКТИВНЫЕ ИНТЕРАКТИВНЫЕ КОНСОЛЬНЫЙ ВХОД Локальная учетная запись Локальная учетная запись и член группы "Админ ПАКЕТНЫЕ ФАЙЛЫ Подтвержденное службой удостоверение Подтвержденное центром проверки подливности	
строшедшие проверку Сертификат этой организации СЕТЬ СИСТЕМА	ГРУППА-СОЗДАТЕЛЬ ИНТЕРАКТИВНЫЕ КОНСОЛЬНЫЙ ВХОД Локальная учетная запись Локальная учетная запись и член группы "Админ ПАКЕТНЫЕ ФАЙЛЫ Подтвержденное службой удостоверение Подтвержденное центром проверки подливности ПОЛЬЗОВАТЕЛЬ СЕРВЕРА ТЕРМИНАЛОВ	
СЕТЬ СИСТЕМА	ГРУППА-СОЗДАТЕЛЬ ИНТЕРАКТИВНЫЕ КОНСОЛЬНЫЙ ВХОД Локальная учетная запись Локальная учетная запись и член группы "Админ ПАКЕТНЫЕ ФАЙЛЫ Подтвержденное центром проверки подливности Подтвержденное центром проверки подливности ПОЛЬЗОВАТЕЛЬ СЕРВЕРА ТЕРМИНАЛОВ ПРАВА ВПАЛЕЛЬЦА	
SCHCTEMA	ГРУППА-СОЗДАТЕЛЬ ИНТЕРАКТИВНЫЕ КОНСОЛЬНЫЙ ВХОД Локальная учетная запись Локальная учетная запись и член группы "Админ Локальная учетная запись и член группы "Админ ПакЕТНЫЕ ФАЙЛЫ Подтвержденное службой удостоверение Подтвержденное службой удостоверение Сортерии и службой удостоверение Подтвержденное службой удостоверение Подтверждение и службой удостоверение Подтверждение и службой удостоверение Подтверждение и службой удостоверение Подтверждение и службой удостоверение и службой удостоверение и службой удостоверение и службой удостоверение и службой и службой удостоверение и службой удост	
K CIIV X 6A	ГРУППА-СОЗДАТЕЛЬ ИНТЕРАКТИВНЫЕ КОНСОЛЬНЫЙ ВХОД Локальная учетная запись Локальная учетная запись и член группы "Админ ПАКЕТНЫЕ ФАЙЛЫ Подтвержденное селужбой удостоверение Подтвержденное селужбой удостоверение Подтвержденное центром проверки подливности ПОЛЬЗОВАТЕЛЬ СЕРВЕРА ТЕРМИНАЛОВ ПРАВА ВПАЛЕПЫ IA Прошедшие проверку Сертификат этой организации СЕТЬ	
СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ	ГРУППА-СОЗДАТЕЛЬ ИНТЕРАКТИВНЫЕ КОНСОЛЬНЫЙ ВХОД Локальная учетная запись Локальная учетная запись и член группы "Админ ПАКЕТНЫЕ ФАЙЛЫ Подтвержденное службой удостоверение Подтвержденное службой удостоверение Подтвержденное центром проверки подливности ПОЛЬЗОВАТЕЛЬ СЕРВЕРА ТЕРМИНАЛОВ ПРАВА ВПАЛЕПЫ IA Прошедшие проверку Сертификат этой организации ССЕТЬ СИСТЕМА	

24. Далее нажмите Ок.

Рустэн

подк	ЛЮЧИТ другие группы, откройте панель управления <u>Учетные запис</u> пользователей.	м
	Выбор: "Пользователи"	×
	Выберите тип объекта:	
істве	"Пользователи" или "Встроенные субъекты безопасности"	Типы объектов
	В следующем месте:	
	DESKTOP-8MIHTH3	Размещение
іьзо	Введите <u>и</u> мена выбираемых объектов (<u>примеры</u>):	
	Прошедшие проверку	Проверить имена
торь		
	Дополнительно ОК	Отмена



3.2 Установка Cloudbase-init

- 1. Скачайте установщик Cloudbase-init.
- 2. Запустите установщик.



3. Следуйте стандартным настройкам и нажмите Next до появления кнопки Install.



🖁 Cloudbase-Init 1.1.4 Setup	- 🗆 🗙
Ready to install Cloudbase-Init 1.1.4	cloudbase 🥂
Click Install to begin the installation. Click Back to re- settings. Click Cancel to exit the wizard.	view or change any of your installation

4. После установки выберите оба пункта. Нажмите Finish.



5. Дождитесь завершения процесса sysprep и выключения машины.

3.3 Настройка групповой политики для использования графического процессора

При использовании графически интенсивного программного обеспечения через удаленный рабочий стол может возникнуть низкая производительность и ошибки, вызванные тем, что Microsoft Windows Remote Desktop по умолчанию не использует графический процессор для рендеринга. Чтобы улучшить работу и избежать проблем с драйверами отображения, выполните следующие действия:

- 1. Откройте редактор групповой политики:
 - Нажмите Win + R, далее введите gpedit.msc и нажмите Enter.
- 2. Перейдите к настройкам RemoteFX:

В левой части окна редактора групповой политики, разверните следующие разделы:

- Административные шаблоны
- Компоненты Windows
- Службы удаленных рабочих столов
- Узел сеансов удаленных рабочих столов
- Среда удалённых сеансов
- Выберите папку RemoteFX для Windows Server 2008 R2.



3. Включите необходимые параметры:

В правой части окна найдите следующие параметры и дважды кликните по каждому из них для открытия настроек:

- "Настройка RemoteFX."
- "Оптимизация визуальных эффектов при использовании RemoteFX."
- "Оптимизировать визуальные эффекты для сеансов служб удаленных рабочих столов."

айл Действие Вид Справка	ки		
• 🔿 🚈 📊 🔒 🛛 🖬 🛛 🍸			
 Регистрация устройс: Рукописный ввод Сборки для сбора даа Сбинхронизация пара 	RemoteFX для Windows Serve Чтобы просмотреть описание элемента, выделите его.	r 2008 R2 Состояние Е Настройка RemoteFX	Состояние Включена Рказонена
 Служба уугановки Ас Службы IIS Службы IIS Службы Ідаленных р Клиент подключе Лицензирование у Узел сеансов удал Безопасность Временные па Лицензирован Ограничение (Перенаправле Подключения Посредник по, Порофили Срах удаленн 		🖹 Оптимизировать визуальные эффекты для сеансов служ	Включена
📔 RemoteFX # 🗸		<	
>	Расширенный Стандартный/		

4. Настройка RemoteFX для Windows Server 2008 R2:

• Для каждого из параметров, в открывшемся окне, выберите Включено.



•

• Нажмите "ОК", чтобы применить изменения.

5. Настройка дополнительных параметров в разделе Среда удаленных сеансов:

- Перейдите в раздел Среда удалённых сеансов
- Найдите параметры:
 - "Использовать аппаратные видеоадаптеры для всех сеансов служб удаленных рабочих столов".
 - "Настройка сжатия данных RemoteFX".
 - Дважды кликните по каждому параметру для открытия окна настройки.
- В каждом окне выберите Включено.
- Нажмите "ОК", чтобы сохранить изменения.

 Лицензирование удаленных рабочих столов Лицензирование удаленных рабочих столов Узел сеансов удаленных рабочих столов Безопасность Временные папки Лицензирование Ограничение сеансов по времени Перенаправление принтеров Перенаправление устройств и ресурсов Подслючения Посредних подключений к удаленному рабочему столу Профили Среда удаленных сеансов RemoteFX для Windows Server 2008 R2 Совместимость драйверов и устройств 	 Среда удаленных сеансов Использовать аппаратные видеоздаптеры для всех сеансов Изменить параметр политики Требования: Не ниже Windows Server 2012, Windows 8 или Windows RT Описание: Этот параметр политики позволяет системным администраторам изменять графическую отрисовку всех сеансов служб удаленных Состояние Состояние RemoteFX для Windows Server 2008 R2 Наибольшая глубина цвета Принудительная отмена фонового рисунка удаленного Использовать аппаратные видеоздалтеры для всех сеанс Ограничить количество мониторов Удалить элемент «Безопасность Windows» из меню «Пус Удалить элемент «Отключение сеанса» из диалога завер Удалить элемент «Отключение сеанса» из диалога завер Удалить элемент «Сотключение сеанса» из диалога завер Удалить элемент «Соключение сеанса» из диалога завер Удалить элемент «Безопасность Windows» из меню «Пус Настройка кодировки оборудования H.264/AVC для подк Настройка скатия данных RemoteFX 	Состоян Не зада Не зада Не зада Не зада Не зада Не зада Включе Включе Включе
 Совместимость драйверов и устройств Совместимость приложений Содержимое облака Среда выполнения приложения Удаленная оболочка Windows Удаленная ифоровыми правами Windows Media Установка нажатием Установ нажатием Установ на катием Установ нажатием Установ на катием Установ дополнительной проверки подлинности Microsoft Центр обелечения безопасности Центр обелечения безопасности Центр обелечения безопасности Цифровой яцик Шифрование диска BitLocker Менов «Пуск» и панель задач Принтеры 	рабочих столов. Если этот параметр политики включен, для всех сеансов служб удаленных рабочих столов используется в качестве адаптера по умолчанию аппаратный обработчик графики вместо базового драйвера отрисовки (Майкрософт). Если этот параметр политики отключен, для всех сеансов служб удаленных рабочих столов используется в качестве адаптера по умолчанию базовый драйвер отрисовки (Майкрософт).	не задан Включен Не задан Не задан Не задан

6. Перезагрузите Компьютер:

• После внесения изменений, рекомендуется перезагрузить компьютер, чтобы изменения вступили в силу.



4 Подготовка образа Astra Linux

Инструкция предназначена для настройки образа персонального рабочего места на базе операционной системы Astra Linux.

В процессе настройки потребуется установить операционную систему, агенты и выполнить ряд дополнительных настроек для обеспечения правильного функционирования.

Для удобства настройки рекомендуется иметь доступ в интернет с виртуальной машины и настраивать её через SSH.

4.1 Рекомендации перед установкой

- 1. Перед установкой операционной системы из ISO-образа, рекомендуется ознакомиться с актуальной инструкцией для Linux систем по ссылке: Подготовка образа ОС семейства Linux
- 2. В образе используются дополнительные средства автоматизации и инициализации для виртуальных машин сервис cloud-init.

Для полноценной работы этого сервиса рекомендуется:

- Избегать использование разметки LVM (указана по умолчанию).
- Не выносить swap на отдельный раздел.

АSTRA LINUX [®] операционная система
Разметка дисков
Перед вами список настроенных разделов и их точек монтирования.Выберите раздел,чтобы изменить его настройки (тип файловой системы,точку монтирования и так далее),свободное место,чтобы создать новый раздел,или устройство,чтобы создать на нём новую таблицу разделов.
Автоматическая разметка
Настройка программного RAID
Настройка менеджера логических томов (LVM)
Настроить защитное преобразование для томов
Настроить тома iSCSI
> #1 первичн. 21.5 GB f ext4 /
Отменить изменения разделов
Закончить разметку и записать изменения на диск

- С учетом наличия сервиса cloud-init и возможности автоматического расширения корневого раздела, предлагается использовать минимальный размер образа при подготовке. В текущей версии рекомендуемый размер составляет 20 Гб.
- 4. Для обеспечения эффективной и автоматизированной сети на виртуальной машине, рекомендуется обязательно использовать DHCP.

4.2 Действия после установки ОС

Если уровень защиты выбран как "Воронеж" или выше, выполните следующие действия:

1. Запустите сеанс входа на главном экране, используя учетные данные административного пользователя.



2. Откройте терминал:

Firefox		Терми	нал Ем
		Моцол	
		менед.	
Корзина		Моцол	
		менед	
		Запуск	приложения
- - -		Инфор	мация о системе
Ф. Офис	<u> </u>	Контро	оль целостности файлов
		Конфи	гурация аудита
(Сеть	>	Менед	жер устройств
😳 Графика	>	Монит	ор батарей QBat
Мультимелиа	,	Мульти	терминальный режим
		Очере,	ць печати
(🔇 Научные		Поиск	файлов
🎘 Утилиты	>	Принте	еры
💮 Системные	>	Провер	ока целостности системы
		Просм	отр системных журналов KSystemLog
💮 Последние	>	Редакт	ор разделов Gparted
荘 Панель управления		Сервис	удаленных USB-накопителей
തി Менелжер файлов		Сессик	восстановить
С менеджер файлов		Сессик	сохранить
Q Начните поиск		Синхро	онизация времени
П+ Завершение работы		Систем	ный монитор
		Управл	ение параметрами звука
ة 📇		Центр	системных отчетов

3. В терминале выполните следующую команду:

sudo fly-admin-scm



Это приведет к появлению следующего окна:



4. В этом окне выберите "Пользователи". Примените фильтр для отображения только системных пользователей, а затем выберите "root".

Ма 🤝 Управление политикой безопаснос a t a t ↓ Файл Правка Настройки Пог t - 🛛 🔇 🌑 🔿 🛇 🗍 🕂 —	ти - Пользователь: 10щь С	root Системны	e v		_ 0 >
ск ck ↓- ↓ vdi-image-voronezh-base ↓- ₩ Аудит	Пользователи)		
>- 🖾 Группы	Имя 🗸	UID	GECOS	Группа	Системный
>- 🚰 Замкнутая программ	🙎 sync	4	sync	nogroup	да
>- 🕡 Мандатные атрибуты	🙎 sssd	115	SSSD syste	sssd	да
>- 🔘 Мандатный контроль	🙎 sshd	106		nogroup	да
— 🕒 Монитор безопасности	ᢞ root	0	root	root	да
>- 🚹 Настройки безопасно	🙎 pulse	109	PulseAudio	pulse	да
>- 🚑 Политики учетной зап	🙎 proxy	13	proxy	proxy	да
🗸 🏛 Пользователи	🙎 ntp	107		ntp	да
- 🖉 Debian-exim	🙎 nobody	65534	nobody	nogroup	да
- 🧟 _apt	🙎 nm-ope	111	NetworkMa	nm-openvpn	да
- 🧟 astra-orientation	Le news	9	news	news	да
— 🖉 avahi	©	405			
— 🧟 backup			(dual me		
- 🧟 bin	Подстановка	×	Филыр		



5. Открываем вкладку МРД и ставим высокий уровень (обычно 63).

🤯 Управление политикой безопасности – МРД атрибуты пользователя: root 🗆 🗙								
Файл Правка Настройки Помощь								
◎ ◎ ◎ ◎ + -		G Ø Bce ~						
- 🏖 gnats		атель: root						
— 🏖 hplip		ие 👶 Блокировка 🗒 Аудит 🦉 Привидерии 🚺 МРД 📑 Сроки						
— 🏖 irc								
— 🧟 list		Уровни						
— 🧟 logcheck		Целостность						
— 🧟 lp		альный: 🖳 О:Низкий 🗸 🗸						
— 🧟 mail		альный: 🖵 63:Высокий 🗸						
— 🏖 man								
— 🙅 messagebus								
— 🧟 news								
— 🏖 nm-openvpn								
– 🖉 nobody		N.						
– 🖉 ntp								
— 🖉 ргоху								
– 🧟 pulse								
- 🧟 root								
·		<u>.</u>						

Далее следуем инструкции:

1. После установки операционной системы рекомендуется выполнить обновление пакетов:

apt update && apt upgrade -y

Если планируете обновлять систему через интернет, проверьте настройки репозиториев в файле /etc/apt/source.list и раскомментируйте нужные строки.

После обновления рекомендуется перезагрузить виртуальную машину.

2. После успешной перезагрузки войдите на виртуальную машину и переключитесь в режим суперпользователя root. Затем перейдите в диреторию /opt:

cd /opt

 Скачайте архив с агентом VDI для Astra Linux используя wget и соответствующий URL-адрес агента:

wget <URL-адрес файла агента Linux>

4. Создайте необходимые для работы директории:





5. Разархивируйте архив с агентом, используя tar, и поместите файлы в созданную директорию:

tar -xvf /opt/<ΦAЙЛ_AFEHTA> --directory /opt/vdi-agent-astra

6. Выполните установку необходимых пакетов. Можете дополнить список утилитами в соответствии с требованиями вашего образа:

apt -y install realmd sysstat vino x2goserver x2goserver-xsession sssdtools sssd libnss-sss libpam-sss adcli krb5-user zenity realmd packagekit cloud-init cloud-utils resolvconf nfs-common

 Для удобства управления службой rustack_agent создадим символическую ссылку на соответствующий файл службы:

ln -s /opt/vdi-agent-astra/rustack_agent.service
/etc/systemd/system/rustack_agent.service

8. Перезагрузите конфигурацию диспетчера systemd и добавьте сервис rustack_agent в автозапуск:

systemctl daemon-reload && systemctl enable rustack agent.service

9. Выполните настройки для доменной авторизации и X2GO:

sed -i -e "s/%U@%D/%U/g" /usr/lib/realmd/realmd-defaults.conf echo -e "session required pam_mkhomedir.so skel=/etc/skel/ umask=0022" >> /etc/pam.d/sshd sed -i -e "s/ScreenSaverDelay=600/ScreenSaverDelay=0/g" /usr/share/fly-wm/theme/default.themerc sed -i -e "s/LockerDpmsOffTimeout=600/LockerDpmsOffTimeout=0/g" /usr/share/fly-wm/theme/default.themerc sed -i -e "s/#KillUserProcesses=yes/KillUserProcesses=no/g" /etc/systemd/logind.conf sed -i -e "s/ServerArgsLocal=/ServerArgsLocal=-dpi 96/g" /etc/X11/flydm/fly-dmrc echo '96' >> /etc/X11/fly-dm/dpi echo '-model pc105 -layout "ru(winkeys),us" -option grab:break_actions,grp:alt_shift_toggle' | tee /etc/X11/Xkbmap >> /etc/x2go/Xkbmap

10. Настройка cloud-init.

Чтобы настроить cloud-init, отредактируйте файл /etc/cloud/cloud.cfg и добавьте следующую конфигурацию:



```
disable root: false
preserve_hostname: false
manage_etc_hosts: true datasource:
  Ec2:
   strict id: false
   timeout: 1
   metadata_urls:
      - http://169.254.169.254:80
cloud init modules:
 - migrator
 - seed_random
 - growpart
 - set hostname
 - update hostname
 - update_etc_hosts
 - users-groups
cloud config modules:
 - ssh-import-id
 - set-passwords
 - timezone
 - scripts-vendor
 - scripts-per-once
 - scripts-per-boot
 - scripts-per-instance
 - scripts-user
apt:
   preserve_sources_list: false
sources_list: |
     deb https://download.astralinux.ru/astra/stable/orel/repository/ orel
locale: ru RU.UTF-8
# System and/or distro specific settings
system_info:
   distro: astra
   paths:
      cloud dir: /var/lib/cloud/
      templates dir: /etc/cloud/templates/
      upstart_dir: /etc/init/
  package_mirrors:
        - arches: [default]
       failsafe:
         primary: https://download.astralinux.ru/astra
         security: https://download.astralinux.ru/astra
```

11. Скопируйте шаблон для автозаполнения /etc/hosts



cat /etc/cloud/templates/hosts.debian.tmpl >
/etc/cloud/templates/hosts.tmpl

12. Для автоматического запуска сервиса cloud-init, выполните команду:

systemctl enable cloud-init

13. Отключите настройку сети через cloud-init:

echo "network: {config: disabled}" >> /etc/cloud/cloud.cfg.d/customnetwork-rule.cfg

14. Отключите NetworkManager:

systemctl disable NetworkManager && systemctl --now mask NetworkManager && apt remove network-manager-gnome

15. Создайте файл для сетевого интерфейса eth0:

echo "auto eth0
iface eth0 inet dhcp" >> /etc/network/interfaces.d/eth0

16. Удалите machine-id для генерации уникальных id у будущих ВМ:

echo -n > /etc/machine-id

После выполнения этих шагов завершается подготовка образа.

Рекомендуется ознакомиться с опциональными шагами. Если они не требуются, выполните:

cat /dev/null > ~/.bash history && history -c && init 0

Эта команда очищает историю команд пользователя и выключает систему

4.3 Опциональные шаги

- Для автоматического увеличения корневого раздела при старте виртуальной машины предлагается использовать сервис cloud-init. Этот сервис обеспечивает инициализацию и настройку виртуальных машин. По умолчанию, с помощью cloud-init задается hostname, аналогичный заданному в портале РУСТЭК, а также происходит расширение корневого раздела. В будущем возможна настройка и других возможностей, таких как редактирование конфигурационных файлов без изменения образа, установка дополнительного ПО и т.д.
- Проверьте наличие и использование swap раздела:



swapon -show

• Отключите swap, если он используется отдельным разделом:

swapoff /dev/vdX(раздел из предыдущего пункта)

• Удалите swap раздел через fdisk:

```
fdisk /dev/vda
d
5
d
2
W
```

• Синхронизируйте изменения:

partprobe

• Создайте файл подкачки (например 1 GB):

```
dd if=/dev/zero of=/swapfile bs=1024 count=1048576
chmod 0600 /swapfile
mkswap /swapfile
swapon /swapfile
```

• Проверить, что swap успешно создан:

swapon -show

• Обновите fstab, указав вместо старого UUID для swap: /swapfile

/swapfile none swap sw 0 0

• Ограничьте использование swap:

echo 'vm.swappiness=10' > /etc/sysctl.d/swap.conf

sysctl -system

• Проверить значение:

cat /proc/sys/vm/swappiness

2. На этапе установки ОС создается локальный пользователь и, если вы, не хотите, чтобы он был во всех ВМ развернутых из образа, то удалите его (в данном примере пользователь user):





3. Если был разрешен доступ по SSH для пользователя root, но на виртуальной машине данный доступ не планируется, то его необходимо закрыть.



5 Термины и сокращения

Термин / сокращение	Определение
OC	Операционная система.
Cloud-init	ПО с открытым кодом, представляющее собой набор скриптов, которые настраивают сервер на основании информации из сервиса метаданных и обеспечивают автоматическую настройку сервера при первом его запуске в среде виртуализации
DHCP	Dynamic Host Configuration Protocol - сетевой протокол, автоматически назначающий IP-адреса и другие параметры сети устройствам.
ISO-образ	Файл, содержащий полную копию данных с оптического диска. Используется для создания установочных дисков или виртуальных машин.
LVM	Технология управления дисками и разделами.
SSH	Secure Shell - защищенный сетевой протокол, предназначенный для обеспечения безопасного удаленного управления устройствами.
Swap	Раздел на жестком диске, используемый операционной системой для временного хранения данных, когда оперативная память заполнена.
VDI	Virtual Desktop Infrastructure – виртуализация рабочих мест сотрудников. Технология создания рабочего стола пользователя на одной из виртуальных машин, запущенных на сервере в центре обработки данных (ЦОДе, дата-центре).
XFS	Файловая система, обеспечивающая хранение, управление и доступ к данным на дисках.
X2GO	Система удаленного доступа, предоставляющая возможность управления удаленным рабочим столом.