Аварийное восстановление Linux

систем



Версия 1.9



Содержание

Введение	3
Подготовка к созданию спасательного образа	5
Создание спасательного образа	7
Восстановление системы с помощью спасательного образа	9
Мастер-ключ	13



Введение

Система RuBackup резервного копирования предоставляет возможность создания спасательных образов (rescue image) для операционных систем Linux, располагающихся на виртуальных машинах и «голом железе» (bare metal) с возможностью их быстрого восстановления в случае возникновения аварийных ситуаций. Так же спасательные образы могут быть использованы для переноса систем из виртуальных машин на «голое железо» и с «голого железа» в виртуальные машины. Спасательные образы хранятся так же как и другие резервные копии в системе резервного копирования RuBackup. От обычной резервной копии они отличаются только тем, что создать и восстановить их можно только при помощи RuBackup key.

При создании спасательного образа используется по-файловый метод резервного копирования. Это означает что резервная копия будет занимать, как правило, меньше места чем общий объем дисков системы, а так же что при помощи RuBackup можно переносить спасательные образы на системы с меньшими или большими дисками с тем условием, что объем данных резервной копии уместится на новой системе.

Создание спасательного образа и восстановление системы осуществляется с помощью **RuBackup key (специализированный** загрузочный образ **RuBackup)**, который обеспечивает взаимодействие с сервером резервного копирования.

При помощи RuBackup можно восстанавливать системы так называемой «стандартной установки». Операционные системы Linux предоставляют пользователю беспрецедентный уровень вариативности при их использовании, в том числе богатые возможности по конфигурированию систем во время инсталляции и последующего использования. Возможности RuBackup по созданию и восстановлению систем из спасательных образов ограничены следующими условиями:

– восстановление системы происходит на один диск (одно устройство: sda, vda и т.п.), даже если резервное копирование делалось для системы, расположенной на нескольких устройствах;

— система имеет один файл подкачки (swap), который располагается либо в отдельном дисковом разделе, либо в файле.

При создании спасательной резервной копии из нее исключаются:

- мастер ключ RuBackup;
- пара ключей электронной подписи RuBackup.

Содержимое следующих каталогов:



lost+found /proc /sys /tmp /boot/efi

/var/log/journal

В том случае, если swap располагается в файле, то он так же исключается из резервной копии, но при восстановлении будет создан заново.

В том случае, если в системе присуствует и включен *SElinux*, то при восстановлении в файле /etc/selinux/config будет установлен параметр SELINUX=disabled.

Если после успешного восстановления системы нужно включить *SElinux,* то этот парамет необходимо установить как

SELINUX=enforced

и перезагрузить систему.



Подготовка к созданию спасательного

образа

Для возможности создания спасательного образа на систему необходимо установить клиента RuBackup и этот клиент должен быть авторизован в системе резервного копирования. При восстановлении потребуется ввести пароль клиента, он должен быть заранее установлен.

Порядок установки, инсталляции, настройки, запуска клиента RuBackup, а также авторизации клиента на сервере резервного копирования изложен в документе «Руководство по установке системы резервного копирования RuBackup для серверов резервного копирования и Linux клиентов».

При установке клиента RuBackup в OC Astra Linux SE 1.6 Смоленск, то может оказаться, что в официальном репозитории нет компрессора pigz. В этом случае можно сделать ссылку:

sudo ln -s /bin/gzip /usr/bin/pigzc

Важно! В ходе создания спасательного образа из него будут принудительно исключены во избежании утечки *master key* и ключи электронной подписи. *Master key* используется для защитного преобразования резервных копий на стороне клиента. Ключи электронной подписи используются для подтверждения подлинности резервных копий клиента. **Рекомендуется сразу после установки клиента скопировать** *master key* и ключи электронной подписи в надежное место. Ключи расположены в каталоге /opt/rubackup/keys.

При создании спасательных образов и восстановлении из них при помощи RuBackup key используется возможность сервера резервного копирования RuBackup предоставлять клиенту сетевую файловую систему NFS для временных операций с резервными копиями. Для этого на сервере резервного копирования RuBackup должен быть выделен соответствующий каталог при помощи RBM с достаточным пространством для временных операций клиентов с резервными копиями (рисунок 1) (подробнее см. «Руководство по установке системы резервного копирования RuBackup для серверов резервного копирования и Linux клиентов» и «Руководство системного администратора RuBackup»).



			Мен	еджер адмі	инистрато	pa RuBac	kup:					a 😣
Конфигура	ция Просмот	р Действия Ан	налитика Ин	формация								
Объекты	Стратегии	Глобальное рас	писание	/даленная рег	пликация	Серверн	ая групп	ировка Ru	Backup			
Имя хоста		Описание	Файл	овые системы	Ленточ	ные библи	отеки	Облака	Блочн	ые устроі	иства	
1 ubuntu	Primary RuBa	ackup server	Обыч Обща Испол Авар Обща Испол Врем Катал	иное хранили я емкость: ийное храни. ия емкость: пьзовано: иенное храни пог для NFS //	іще: .99 .05 лище: .99 .05 лище: rubackup-tm	r6 r6 r6 r6	583 <mark>6</mark>]				
			Пулы									
			File	system 🔺	Total, GB	Availab	le, GB	Used, %	6	0	писание	
			1 /deta	ult_pool 23	.99	9.93	5	8				
			Лицен	зия: Закакзчи	к pcalhost	Емкость:	1	Тб, исп.:	0.00	T6 09	6 Клиентс)в: ∞
Соединение:	rubackup@rub	oackup:ubuntu		тип:	Backend	начало:	2-03-17	конец:	3-03-17	Дог	Нормальны	: ∞ й режим

Рисунок 1



Создание спасательного образа

Для создания спасательного образа необходимо запустить систему с помощью *RuBackup key*. Необходимо, чтобы имя сервера резервного копирования разрешалось с помощью DNS.

Важно! Так как RuBackup key при загрузке необходимо получить временный IP адрес от DHCP сервера, необходимо обеспечить, чтобы в списке клиентов RuBackup не было записей других клиентов, которые ранее использовали этот адрес, в противном случае операция будет завершена с ошибкой или не сможет начаться.

При загрузке системы с помощью RuBackup key будет запущено оконное приложение *rbkey* (рисунок 2):

			RuBac	:ku	ıp key				0	
View										
Select clie	ent interfa	ce ens3 👻								
Backup	Restore									
Select roo	ot target v	da 👻 Crypto	nocrypt 👻							
Name	fstype L	abel UUID			1	Aountpoir	ιt			
~ vda	-									
vda	a2 ext4	c25810e8-4fc	9-11ea-9321-52540	003	380fc					
Found at	this device			fstab						
Hostname	:	clear		Backup		ackup	Filesystem Mount poil		Туре	
OS:		Ubuntu 18.04.4 LTS			1 🗸		UUID=c2581	/ ext4		
Ctart				4					,	
rhkov actio			PuPackup client los							
rokey actio	715		Rubackup client log	,						
Device /de Device /de device	ev/vda2 was ev/vda2 look	s mounted to /mnt cs like a root								
Device /de	ev/vda2 was	unmounted								

Рисунок 2



Необходимо выбрать вкладку «Backup». Здесь необходимо выбрать *root target* (например *vda* или sda), то есть то устройство, на котором располагается / системы, после чего выбрать раздел, на котором располагается /системы.

При выборе раздела rbkey проверит действительно ли выбранный раздел может являться / системы и в случае правильного выбора будет разблокирована кнопка «Start». В таблице fstab можно выбрать какие файловые сиистемы должны войти в резервную копию. Рекомендуется не выбирать пользовательские файловые системы, для которых резервное может выполняться регулярно правилами резервного копирование копирования RuBackup, а выбрать только то, что необходимо для аварийного восстановления. Все пользовательские данные могут быть впоследствии восстановлены из наиболее свежих резервных копий правильным способом (однако необходимо заранее позаботится о том, чтобы резервные копии тех или иные данных периодически создавались с помощью RuBackup).

Для начала создания спасательного образа необходимо нажать кнопку «*Start*» (рисунок 3). После окончания создания спасательного образа систему можно выключить.

bkey actions	RuBackup client log
Copy master key Copy digital signature secret key Copy digital signature public key Load client's config file to modify Config file was modified Start RuBackup client Backup was started. Task ID: 1401 task status: New task status: Transmission Backup was done	 ResourceType 21:snap 2>&1 Sun May 24 17:45:41 2020: Create digital signature for / rubackup_nfs_mountpoint/1401/ clear_TaskID_1401_NORuleOrStrategy_0_D2020_5_24H17_43_09_BackupType_1 _ResourceType_21:snap Sun May 24 17:46:05 2020: Execute OS command: sudo /bin/umount -f / rubackup_nfs_mountpoint/1401 2>&1 Sun May 24 17:46:05 2020: NFS share was unmounted and this mountpoint was deleted: /rubackup_nfs_mountpoint/1401 Sun May 24 17:46:05 2020: Task was done. ID: 1401

Рисунок 3

Важно! В том случае, если для создания спасательного образа вы выбрали защитное преобразование резервной копии с помощью того или иного алгоритма, вы должны заранее сохранить в надежном месте мастер ключ клиента (он формируется при инсталляции клиента RuBackup на систему), в противном случае вы не сможете без этого мастер ключа восстановить систему из спасательного образа.



Восстановление системы с помощью

спасательного образа

Для восстановления системы из спасательного образа необходимо запустить систему с помощью **RuBackup key**. Необходимо, чтобы имя сервера резервного копирования разрешалось с помощью DNS.

Важно! Так как **RuBackup key** при загрузке необходимо получить временный IP адрес от DHCP сервера, надо обеспечить, чтобы в списке клиентов RuBackup не было записей других клиентов, которые ранее использовали этот адрес, в противном случае операция будет завершена с ошибкой.

При загрузке системы с помощью **RuBackup key** будет запущено оконное приложение *rbkey* (рисунок 4):

				RuBack	up key				0
View									
Select clie	ant interfa	e ens3 💌							
Backup	Restore								
RuBackup	server						Por	rts	Connect
Client host	iname								
Resque are	:hives								
Restore ta	get	- (L)							
rbkev actio	ons		RuBackup c	lient log					

Рисунок 4



Необходимо выбрать вкладку «*Restore*». Здесь в поле *RuBackup server* необходимо ввести имя сервера резервного копирования RuBackup и соединиться с ним, нажав кнопку *Connect*. Клиент резервного копирования при восстановлении с помощью RuBackup key обращается к серверу, представляясь клиентом с именем rubackup_rescue. Если это первый случай восстановления системы, то rbkey отобразит сообщение, что системный администратор должен авторизовать клиента *rubackup rescue* (рисунок 5):

rbkey actions	RuBackup client log								
	Sun May 24 18:45:55 2020: Connected to RuBackup server: 192.168.0.5 Sun May 24 18:45:55 2020: Warning: Required autorization at RuBackup server. Please contact system adminitrator. Sun May 24 18:45:55 2020: Warning: Execution restricted Sun May 24 18:46:14 2020: Load core config Sun May 24 18:46:14 2020: RuBackup client runs in rescue mode Sun May 24 18:46:14 2020: RuBackup client will connect to this primary server: 127.0.0.1 Sun May 24 18:46:14 2020: Shutdown RuBackup client process Sun May 24 18:46:14 2020: RuBackup client process is shutted down	•							

Рисунок 5

После авторизации в **rbkey** еще раз необходимо ввести имя сервера резервного копирования RuBackup и соединиться с ним (рисунок 6). Для дальнейших действий требуется ввести пароль *RuBackup key* (задается заранее системным администратором, см. «Руководство системного администратора RuBackup»). Без этого пароля невозможно получить информацию о спасательных образах клиентов RuBackup.

Resque archives	Enter RuBackup	Enter RuBackup key password 🛛 😣					
	Show password	Сапсеl					
Restore target sda * Cry	ypt key						
bkey actions	RuBackup client log						
Start RuBackup client	Sun May 24 18:51:55 2020: M Sun May 24 18:51:55 2020: L	lodule version: 1.4 /M version: 2.02.176(2)	-				

Рисунок 6

Далее потребуется выбрать клиента RuBackup, систему которого планируется восстановить из спасательного образа (рисунок 7):



C-		RuBackup key			
View					
Select client	interfa	ce ens3 💌			
Backup R	estore				
RuBackup serv	verlanta	res		Ports	Disconnect
Client hostnan	ne anta	ires			
	astr	a-ce			
	astr	a-se			
	clea	r -			
	med	lia			
	on-f	ront			
Resque archiv	es pro	:mox1			
nesque arenves	rede	is.rubackup.local			
	reso	ue			
	reso	jue-test			
	rub	ackup_rescue			
	srv.	prest.loc			
	4				•
Restore target	sda	* Crypt key			
Start		(1999)			
rbkey actions		RuBackup client log			
Start RuBackup client		Sun May 24 18:51:55 2020: Module Version: 1.4 Sun May 24 18:51:55 2020: LVM version: 2.02.1 Sun May 24 18:51:55 2020: module LVM logit Sun May 24 18:51:55 2020: Execute OS comma rb_module_rescue_image t 2>&1 Sun May 24 18:51:55 2020: OS: RuBackup key Sun May 24 18:51:55 2020: Module version: 1.4 Sun May 24 18:51:55 2020: module Rescue in	776(2) cal volume was check e: Rescue image ind: /opt/rubackup/mo f mage was checked su	ed successful dules/ ccessfully	ly

Рисунок 7

Потребуется выбрать резервную копию для восстановления и устройство (restore target), на которое планируется восстановить систему (например, *sda*) (рисунок 8):

				R	uBackup key					000
View										
Select client in	nterface	ens3 -								
Backup Re	store									
RuBackup serve	rantares	5						Ports,		Disconnect
Client hostname	clear							-		*
	Id	Resource	Backup type	Pool	Archive size	Snapshot size	Crypt algo	ythm	Digit	tally signed
	1 203	/dev/vda	full	Default	4905656320		nocrypt	у	/es	
Resque archive	5									
Restore target	∢ sda	Crypt ke	y							Þ
Start										
rbkey actions			RuBack	up client l	og					
Start RuBackup	client		Sun Ma Sun Ma Sun Ma	y 24 18:5 y 24 18:5 y 24 18:5	51:55 2020: Modu 51:55 2020: LVM v 51:55 2020: mo	le version: 1.4 rersion: 2.02.176(2) dule LVM logical vol	ume was check	ed succes	sfully	-

Рисунок 8



Для начала восстановления требуется нажать кнопку "Start". В том случае, если на этом устройстве располагаются какие либо логические тома или группы LVM, потребуется подтвердить продолжение процедуры восстановления. Для начала процедуры восстановления требуется ввести пароль клиента (рисунок 9):

Resque archives		Get your password 🛛 ⊗	
Restore target Start	Sha Crypt key	ow password	Þ
bkey actions		RuBackup client log	
Start RuBackup LVM logical volu LVM volume gro LVM physical vo	client imes was deleted: ubuntu-vg vup was deleted: ubuntu-vg ilume was removed: /dev/sda3	Sun May 24 18:51:55 2020: Module version: 1.4 Sun May 24 18:51:55 2020: LVM version: 2.02.176(2) Sun May 24 18:51:55 2020: module LVM logical volume was checked successfully Sun May 24 18:51:55 2020: Try to check module: Rescue image Sun May 24 18:51:55 2020: Execute OS command: /opt/rubackup/modules/	-

Рисунок 9

Необходимо убедиться в том, что задача восстановления была выполнена успешно (рисунок 10):

	4		P.
Restore target	sda 🔹 Crypt key		
Start			
rbkey actions		RuBackup client log	
Start RuBackup Restore was sta task status: Neu task status: At_ task status: Sta Backup was don task status: Don	o client arted. Task ID: 1409 w Client art_Transfer ne ne	Sun May 24 19:40:05 2020: /mnt/run unmounted Sun May 24 19:40:05 2020: /mnt/run unmount UUD=c25810e8-4fc9-11ea-9321-5254000380fc Sun May 24 19:40:05 2020: Congratulation!!! Now you can shutdown, remove RuBackup key and boot from /dev/sda Sun May 24 19:40:05 2020: Execute OS command: sudo /bin/umount -f / rubackup_nfs_mountpoint/1409 2>&1 Sun May 24 19:40:05 2020: NFS share was unmounted and this mountpoint was deleted: / rubackup_nfs_mountpoint/1409 Sun May 24 19:40:05 2020: Task was done. ID: 1409	4

Рисунок 10

После успешного окончания восстановления системы из спасательного образа можно выключить систему, убрать RuBackup key из загрузки, загрузить ее со штатного диска и продолжить восстановление пользовательских данных.

После первого запуска восстановленной системы в нее необходимо загрузить ранее сохраненные в надежном месте, либо создать заново *master key* и ключи электронной подписи. Создать заново ключи можно с помощью *RBC* или *rb init*.



Мастер-ключ

В ходе инсталляции будет создан мастер-ключ для защитного преобразования резервных копий и ключи для электронной подписи, если предполагается использовать электронную подпись.

Внимание! При утере ключа вы не сможете восстановить данные из резервной копии, если последняя была преобразована с помощью защитных алгоритмов.

Важно! Ключи рекомендуется после создания скопировать на внешний носитель, а также распечатать бумажную копию и убрать эти копии в надежное место.

Мастер-ключ рекомендуется распечатать при помощи утилиты hexdump, так как он может содержать неотображаемые на экране символы:

