

Overview

Note: This procedure, though relatively straight-forward, is complex and contains many steps.

• These instructions are available as a printable PDF file here:

Limited support for virtualization of systems containing 4K drives is available in Replibit 10.1.0 and newer.

- The underlying KVM hypervisor requires the use of VirtIO drivers and disks to create virtual 4K volumes. Because Windows does not natively support VirtIO, drivers must be injected into the virtual machine image before Windows is able to boot.
- Virtualization of protected systems in test mode, bootvm checks, and AutoVerify are not currently supported.
- Virtualization in live mode is supported with manual injection of the required drivers.

Before you begin: Mark the recovery point you intend to work with by adding a note.

This will make identification of the persistent snapshot easier later.

Click the **Note** icon and enter some text, then save it.



Manual Driver Installation

To perform virtualization of a protected system with 4K drives, perform the following steps:

Start iSCSI and attach volumes to a Windows machine

1. From the Protected System Details page identify the Recovery Point you wish to virtualize and add a Note as shown above.



2. Click Start iSCSI.

3. Select Live Mode when prompted.

4. Once iSCSI has been started for the recovery point, attach the volumes to a Windows system using iSCSI Initiator, found at **Control Panel > Administrative Tools> iSCSI Initiator**

5. Enter the **IP address** of the appliance in the *Target* field.

6. Click Quick Connect.

argets	Discovery	Favorite Targets	Volumes and Devices	RADIUS	Configuration
Quick C	Connect	a on to a target usin	a a basic connection to	upe the TD	addrass or
DNS na	ame of the ta	arget and then click	Quick Connect.	ype ule tr	
Target	. 192	. 168.90.221			iick Connect
Turger					act connectin
JISCOVE	ered targets			-	Defreeh
7949				5. A.	Kellesh
Name				Status	

7. The available volume targets should be displayed in the *Quick Connect* popup.

Connect each disk device by clicking **Connect.**



rovided are listed below. If multiple targets o each target individually.	are available, you need to connect
onnections made here will be added to the	list of Favorite Targets and an attem
o restore them will be made every time this	computer restarts.
)iscovered targets	
Name	Status
ign.2020-04.com.iscsiexport:9ac2f420-5f6	0-11ea-8 Inactive
ign.2020-04.com.iscsiexport:b10c1abc-f90	05- <mark>4</mark> 8dc-8 Inactive
iqn.2020-04.com.iscsiexport:b10c1abc-f90	05- <mark>4</mark> 8dc-8 Inactive
rogress report	05- <mark>4</mark> 8dc-8 Inactive
rogress report There are multiple Targets discovered.Plea using Quick Connect.	15-48dc-8 Inactive use select a single Target for Login

8. Open *Computer Management* from **Control Panel > Administrative Tools**.

9. Select Disk Management.

10. Locate the attached iSCSI volume(s).

11. Make sure that the volume containing the Windows folder of your protected system is online and has a drive letter assigned.

(You can do this by right-clicking the disk volume and selecting **Online** to mount the device. Then, right-click the volume and select **Change Drive Letter and Path** to assign a drive letter, if necessary.)

Management (Local	Volume	Layout	Type	File System	Status		Actions	
 System Tools Task Scheduler 	Oisk 0 partition 1 Oisk 0 partition 4	4) Simple	Basic Basic		Healthy (EFI System Par Healthy (Recovery Parti	artition) tition)	Disk Management	
	 Bulk Data (E) SSD-Data (D:) VirtlO (F:) Windows (C:) 	More Actions						
Services and Applications	<							
	Disk 0 Basic 978.07 GB Online	260 MB Healthy (El	97 F1	Findows (C:) 77.03 GB NTFS (BitLocker Encry ealthy (Boot, Page File, Crash	ypte 805 MB Dun Healthy (Recove			
	- Disk 1 Basic 238.35 GB Online	SSD-Data 238.35 GB I Healthy (P	(D:) NTFS (E rimary	BitLocker Encrypted) Partition)				
	- Disk 2 Basic 1862-89 GB Online	Bulk Data 1862.89 GB Healthy (P	(E:) NTFS rimary	(BitLocker Encrypted) Partition)		•		
	*O Disk 3 Basic 60.00 GB Offline	350 MB		59.66 GB				
	*O Disk 4 Unknown 59.98 GB Offline	59.98 G8 Unallocate	d	U.				

12. Retrieve the Virtio driver ISO (viostor.iso) by copying it from the root folder of the Replibit appliance or download it here.

13. Extract the required drivers from the Virtio driver ISO.

To do this:

- Open viostor.iso with Windows Explorer and browse to /virtio/<OS
 version>/<architecture>. (Select the drivers that match your Protected System)
- Copy the driver files to a convenient temp folder on your windows machine.

Axcient

A	X	ci	e	n	E
			and the second second		

I I I I I File Home	md64 Share	View								
Pin to Quick Copy access	Paste	从 Cut ‱ Copy path ₽ Paste shortcut	Move to -	Copy to *	Delete Renam	e New folder New	Prope	Tties Open •	Sele	ect all ect none ert selection select
← → * ↑	> Thi	is PC > DVD Drive	(l:) VirtlO	> vios	tor > 2k12R2	> amd64	~ Õ	Search amd64		م
ISOs	* ^	Name	^			Date modified		Туре	Siz	e
Jeff Crystal	*	viostor.cat				7/19/2017 6:46 PN	4	Security Cataloo	1	9 KB
👌 Music	*	viostor.inf				7/19/2017 6:28 PN	1	Setup Informati	on	3 KB
📕 Agent Relea	se 2.	viostor.sys				7/19/2017 6:46 PN	1	System file		40 KB
D2C 3 items	*									

Inject drivers into the protected system image

Next, we will inject the drivers into your protected system image.

43. Open a Windows CMD shell in administrative mode.

To do this:

- Click Start
- Type **cmd**
- Right-click on **Command Prompt**
- Select Run as administrator

15. Using the command window, inject the drivers into the offline system image using Microsoft DISM.

DISM /Image:<Drive Letter containing image>: /Add-Driver /Driver:<Path to Driver Files>

Axcient



For example, if the volume containing the Windows folder of your protected system is mounted at H:, and you copied the driver files to E:\Temp\viostor, then run:

DISM /Image:H:\ /Add-Driver /Driver:E:\Temp\viostor

16. Once you've injected the drivers, dismount the drives from the Windows system and stop iSCSI on the appliance.

17. Go to *Computer Management* from **Control Panel > Administrative Tools** and select **Disk Management.** Right click each mounted iSCSI volume and select **Offline** to dismount the volume.

18. From *iSCSI Initiator*, select each connected volume and click **Disconnect**.

- 19. Remove all entries from the Discovery and Favorite Targets tabs.
- 20. From the appliance, click Stop iSCSI

Axcient

Boot the target recovery point as a virtual machine

From this point forward, the target recovery point should be able to boot as a virtual machine.

21. Click on Start VM.

22. Select the desired amounts of **RAM** and **CPU** to provide the virtual machine.

23. Select Live Mode.

24. Click Start.

Note: Do NOT select 'Setup Virtio' again when launching the VM. If 4K drives are present within your Protected System the BDR will automatically detect this and create the virtual machine using VirtIO devices.

Virtualization settings						
RAM (GB): Free: 13.5						
2						
CPU (cores): Free: 16						
2						
Mode:						
Test mode						
Live mode						
Boot Key:						
None	T					
Boot Device:						
Hard drive	•					
CD-ROM Image:						
None	•					
Network interfaces:						
MAC fc:3f:db:90:2a:bd	eth0 •					
MAC e0:94:67:bb:62:ef	eth0 •					
Setup virtio						
Cancel	Start					