MIRAPOINT®

Replacing a RazorSafe Hard Drive

Replacement Part # XRS-750, S-RSHD-01, S-RSHD-02, S-RSHD-03, S-RSHD-04, S-RSHD-05
October 2010
Part Number: 010-00490g

This document supports RazorSafe RS150, RS200, RS370, RS400, RS6000 and RS6000-B2 until replaced by a newer version.

The Mirapoint Software and Mirapoint documentation are Copyright © 1998-2010 Mirapoint Software, Inc. All Rights Reserved. You may not print, copy, reproduce, modify, distribute or display this work in hard copy, electronic, or any other form, in whole or in part, by any electronic, mechanical, or other means, without the prior written consent of Mirapoint Software, Inc., except that you are permitted to make one copy for archival purposes only in connection with the lawful use and operation of this software.

Mirapoint, RazorGate, and the Mirapoint logo are registered trademarks of Mirapoint Software, Inc. Mirapoint Message Server, Mirapoint Directory Server, Mirapoint Operations Console, RazorSafe, DirectPath, WebMail Direct, WebCal Direct, and GroupCal Direct are trademarks of Mirapoint Software, Inc.

Mirapoint integrates third party software programs within the Mirapoint Software, which are subject to their own license terms. If the user does not agree to abide by the applicable license terms for the integrated third party software programs as defined by the Mirapoint Software License Agreement, then you may not install or operate the Mirapoint Software. These software license agreements, including the Mirapoint Software License Agreement, can be viewed at http://www.mirapoint.com/licenses/thirdparty/eula.php.

Portions of this product are Copyright © 1982, 1986, 1989, 1991, 1993 the Regents of the University of California. All Rights Reserved.

Portions of this product are Copyright © Dell Inc. Used with permission.

Portions of this product are Copyright © 2010 Red Hat, Inc. All Rights Reserved. The “Red Hat” trademark and the “Shadowman” logo are registered trademarks of Red Hat, Inc. in the U.S. and other countries.

Portions of this product are Copyright © 1997, 1998 FreeBSD, Inc. All Rights Reserved.
Portions of this product are Copyright © 1996-1998 Carnegie Mellon University. All Rights Reserved.

Portions of this product are Copyright © 1997-1998 the Apache Group. All Rights Reserved.
Portions of this product are Copyright © 1987-2006 Larry Wall. All Rights Reserved. See http://www.perl.org.
Portions of this product are Copyright © 1990, 1993-1997 Sleepycat Software. All Rights Reserved.

This software is derived in part from the SSLava™ Toolkit, which is Copyright © 1996-1998 by Phaos Technology Corporation. All Rights Reserved.

Portions of this product are Copyright © 1998, 1999, 2000 Bruce Verderaime. All Rights Reserved.
Portions of this product are Copyright © 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved.
Portions of this product are Copyright © 2005-2010, The Dojo Foundation. All Rights Reserved.
Portions of this product are Copyright © 2010, Yahoo! Inc. All Rights Reserved.
Portions of this product are Copyright © 2010 VMware, Inc. All Rights Reserved.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Macintosh is a trademark of Apple Computer, Inc.

Windows, Outlook, Exchange, and Active Directory are trademarks of Microsoft Corporation.

Java and Solaris are trademarks of Sun Microsystems, Inc.

Linux is a registered trademark of Linus Torvalds.

Zimbra and the Zimbra logo are trademarks of VMware, Inc.

All other trademarks are the property of their respective owners.

OTHER THAN ANY EXPRESS LIMITED WARRANTIES THAT MIRAPOINT PROVIDES TO YOU IN WRITING, MIRAPOINT AND MIRAPOINT'S LICENSORS PROVIDE THE SOFTWARE TO YOU “AS IS” AND EXPRESSLY DISCLAIM ALL WARRANTIES AND/OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL MIRAPOINT'S LICENSORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY (INCLUDING NEGLIGENCE OR OTHER TORT), ARISING IN ANY WAY OUT OF YOUR USE OF THE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF DAMAGES. MIRAPOINT’S LIABILITY SHALL BE AS LIMITED IN THE LICENSE AGREEMENT.

Replacing a RazorSafe Hard Drive

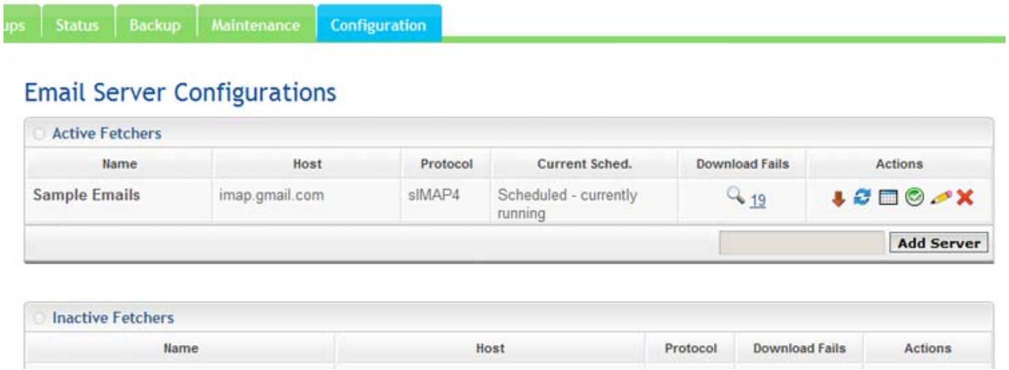
Replacing or adding a RazorSafe hard drive involves the following tasks:

- Turning off Email Fetchers
- Checking RAID Status
- Backing Up the RazorSafe
- Powering Off
- Locating the Failed Hard Drive
- Removing a Failed Hard Drive on page 7
- Adding a New Hard Drive on page 8
- Powering On on page 12
- Check RAID Rebuild Status on page 12
- Turn on Email Fetchers on page 12
- Returning the Failed Hard Drive on page 13

Turning off Email Fetchers

Before removing a failed hard drive, turn off the email fetchers. Use the RazorSafe administration interface **Configuration** tab.

Figure 1 Sample RazorSafe Administration Interface for Email Server Configuration



Email Server Configurations

Active Fetchers

Name	Host	Protocol	Current Sched.	Download Fails	Actions
Sample Emails	imap.gmail.com	sIMAP4	Scheduled - currently running	19	

Inactive Fetchers

Name	Host	Protocol	Download Fails	Actions

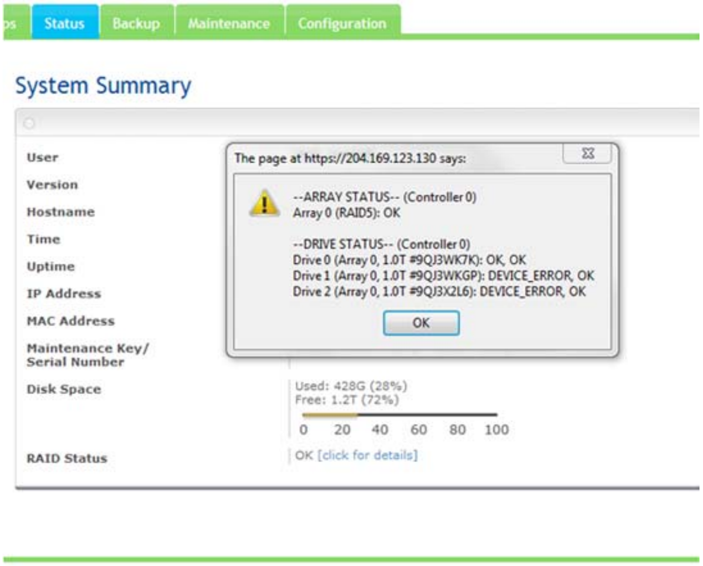
To turn off email fetchers:

1. From the RazorSafe administration interface, click the **Configuration** tab (Figure 1).
2. On the left-side navigation menu under **Email Servers**, click the **POP or IMAP Fetchers** link.
3. In the **Active Fetchers** table, in the **Actions** column, for each server needing to be inactive, click the **red arrow** (Figure 1 on page 3).

Checking RAID Status

Once the email fetchers are turned off, check the RAID status from the RazorSafe Administration Interface. The **RAID Staus** window provides the individual hard drive information including serial number.

Figure 2 Sample RazorSafe Administration Interface for System RAID Status


ps
Status
Backup
Maintenance
Configuration
System Summary
User
Version
Hostname
Time
Uptime
IP Address
MAC Address
Maintenance Key/ Serial Number
Disk Space
RAID Status
0 20 40 60 80 100
OK

The page at https://204.169.123.130 says:

```
--ARRAY STATUS-- (Controller 0)
Array 0 (RAID5): OK

--DRIVE STATUS-- (Controller 0)
Drive 0 (Array 0, 1.0T #9QJ3WK7K): OK, OK
Drive 1 (Array 0, 1.0T #9QJ3WKGP): DEVICE_ERROR, OK
Drive 2 (Array 0, 1.0T #9QJ3X2L6): DEVICE_ERROR, OK
```

Disk Space: Used: 428G (28%) Free: 1.2T (72%)

RAID Status: OK [click for details]

To check the RAID status:

1. From the RazorSafe administration interface, click the **Status** tab (Figure 3).
2. At the bottom of the **System Summary** screen, at the RAID Status line, click the **click for details** link (Figure 3).

   A message window containing the hard drive information displays.
3. Write down the drive number and serial number of the failed drive(s).

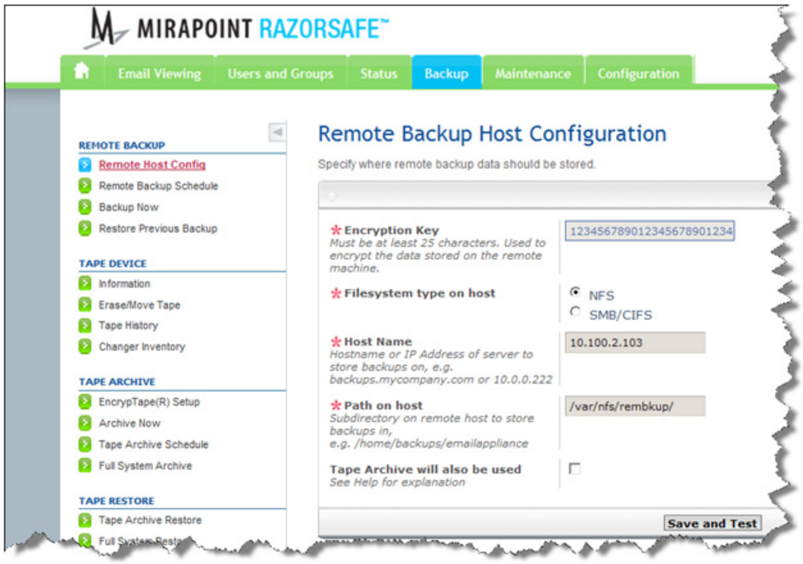
   The drive number represents the bay location in the appliance chassis.

Writing down the failed drive(s) serial number(s) helps you later to verify that the hard drive you pull out of the appliance is the correct hard drive.

Backing Up the RazorSafe

Once the RAID status has been checked and the failed hard drive identified, perform a backup of your RazorSafe data.

Figure 3 Sample RazorSafe Administration Interface for Backup


MIRAPOINT RAZORSAFE™
Email Viewing
Users and Groups
Status
Backup
Maintenance
Configuration
REMOTE BACKUP
Remote Host Config
Remote Backup Schedule
Backup Now
Restore Previous Backup
TAPE DEVICE
Information
Erase/Move Tape
Tape History
Changer Inventory
TAPE ARCHIVE
EncrypTape(R) Setup
Archive Now
Tape Archive Schedule
Full System Archive
TAPE RESTORE
Tape Archive Restore
Full System Resto
Save and Test

Remote Backup Host Configuration

Specify where remote backup data should be stored.

* Encryption Key: 123456789012345678901234
Must be at least 25 characters. Used to encrypt the data stored on the remote machine.

* Filesystem type on host: ● NFS ○ SMB/CIFS

* Host Name: 10.100.2.103
Hostname or IP Address of server to store backups on, e.g. backups.mycompany.com or 10.0.0.222

* Path on host: /var/nfs/rembkup/
Subdirectory on remote host to store backups in, e.g. /home/backups/emailappliance

Tape Archive will also be used: ☐
See Help for explanation

To backup the RazorSafe data:

1. From the RazorSafe administration interface, click the **Backup** tab (Figure 3).
2. On the left-side navigation menu, click the **Backup Now** link.
3. Click the **Remote Backup Host Configuration** link, and for potential use later, save (write or copy and paste into a text file) all of the displayed configuration information, especially the `Encryption Key` (Figure 3).

Locating the Failed Hard Drive

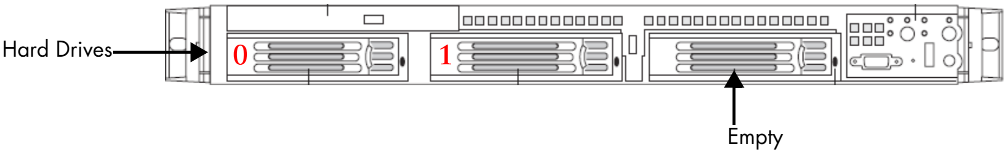
The hard drive bay number locations vary by chassis model.

In addition to identifying the failed disk drive through the RazorSafe administration interface, Mirapoint recommends physically looking at the RazorSafe appliance to identify which disk drive has failed. The failed disk drive will be the one with the amber colored LED illuminated on the disk drive sled, while the functioning disk drives will have green colored LEDs illuminated on the disk drive sleds.

The **Drive #** identified as failed in the RazorSafe administration interface (Checking RAID Status on page 4) should correspond with the amber colored LED and the following drive ID illustrations.

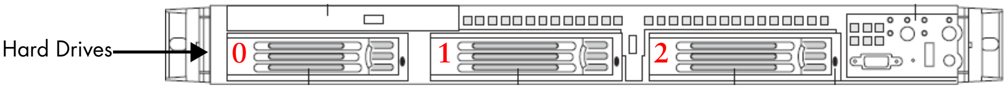
RS150

The RS150 server has 2 hard drives.


Hard Drives
0
1
Empty

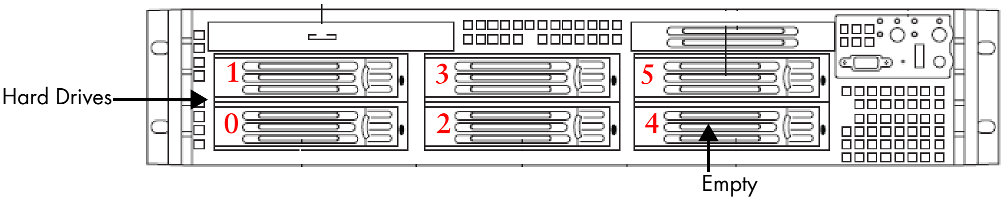
RS200

The RS200 server has 3 hard drives.


Hard Drives
0
1
2

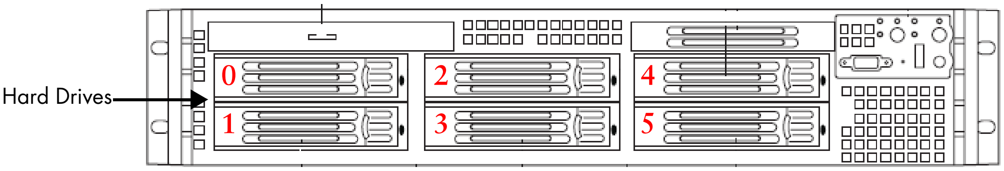
RS400

The RS400 server has 5 hard drives and one empty drive bay.


Hard Drives
1
3
5
0
2
4
Empty

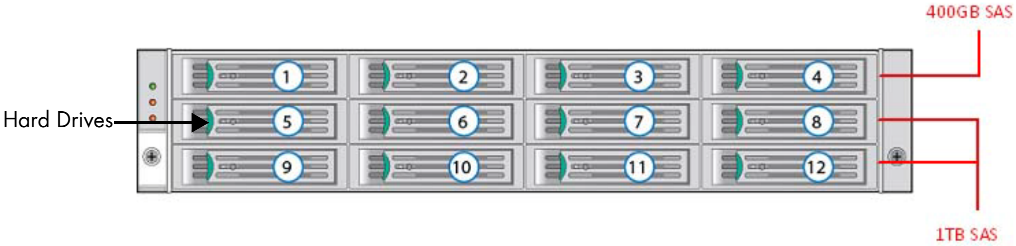
RS370

The RS370 server has 6 hard drives. The corresponding **Drive #** location can vary from the illustrated order. You should always verify that the disk drive serial number on the disk matches the serial number displayed in the **Drive Status** diagnostic window. For assistance, contact a Mirapoint Support representative.


Hard Drives
0
2
4
1
3
5

RS6000

The RS6000 server has 12 hard drives configured with both 400GB and 1TB drives. The four drives on the top row (slots 1–4) are 400GB drives, and the remaining drives in the second and third rows (slots 5–12) are 1TB drives.



RS6000-B2

The RS6000-B2 server, unlike the RS6000, is configured with both 450GB and 1TB drives. The four drives on the top row (slots 1–4) are 450GB drives, and the remaining drives in the second and third rows (slots 5–12) are 1TB drives.

Do not combine 400GB and 450GB drives in the same chassis. Mixing is not supported and will cause failures.

Powering Off

Once you have clearly determined which hard drive needs replacing, and you can reference the serial number, power off the RazorSafe appliance.

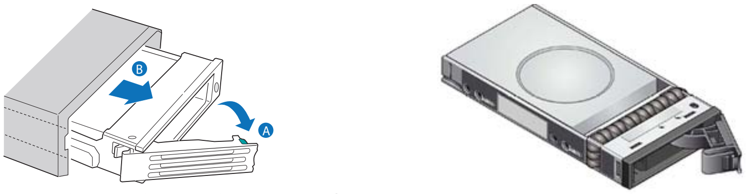
To power off the appliance:

1. From the RazorSafe administration interface, click the **Maintenance** tab.
2. On the left-side navigation menu under **Power Control**, click the **Reboot/Shutdown** link.
3. Click **Shutown**.

   Once the RazorSafe appliance has powered off, disconnect all of the external power cords.

Removing a Failed Hard Drive

Figure 4 Sample Hard Drive Removal



RS150/RS200/RS370/RS400 Hard Drive

RS6000/RS6000-B2 Hard Drive

To remove a failed hard drive:

1. **RS150/RS200/RS370/RS400—**Press the green tab on the right side of the hard drive chassis door until the locking arm releases, then swing the locking arm to the fully unlocked position (approximately 45 degree angle to the left).

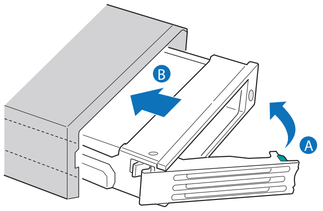
   RS6000 hard drive trays have unique dual purpose latching mechanisms and safety locking arm mechanisms to aid in the prevention of accidental hard drive removals.

   RS6000/RS6000-B2—Unlock the locking mechanism on the locking arm using the Torx* tool provided with your server, or using a “star” bit tool.

   Once unlocked, turn the locking mechanism until the tab can be depressed and swing the locking arm to the fully open position (approximately 45 degree angle to the right).
2. Gently pull the hard drive tray out of the server chassis.
3. Verify that the serial number on the removed hard drive is the same number you wrote down during your drive status diagnostic (Checking RAID Status on page 4).

Do not degauss the failed hard drive until after your RazorGate appliance is verifiably, fully functional again.

Adding a New Hard Drive



RS150/RS200/RS370/RS400 Hard Drive

RS6000/RS6000-B2 Hard Drive

Drive trays are designed to be easily installed with little to no force required.

If there is resistance during installation, do not force a hard drive into the chassis.

RS6000/RS6000-B2—Do not combine 400GB and 450GB drives in the same chassis. Mixing is not supported and causes failures.

To add a new hard drive:

1. Hold the hard drive label side up with the locking arm facing towards you.
2. With the drive tray in an open unlocked position, using as little force as possible, slide the hard drive tray into the corresponding drive number position in the server chassis.

3. Continue to slide the drive tray into the server chassis until the locking arm makes contact with the chassis frame and forces the locking arm to swing closed.

   At this point drive tray should be about ¼” inch from full installation.

4. Gently press the locking arm closed until the hard drive tray fully installs and the locking arm clicks into place.

   RS6000/RS6000-B2—Lock the locking mechanism on the locking arm using the Torx* tool provided with your server, or using a “star” bit tool.

RS150 RAID1 Restoration

The RS150 uses a software-based RAID1 configuration. After replacing your hard drive, complete the process by restoring the RAID1 software configuration.

To restore the RS150 RAID1 configuration:

1. From the console or a putty session, log in and open a shell window.

   To login and open a shell window:

   a. Enter the login and password (case sensitive) assigned during the first-time-setup. For example:

      Login: `miradmin`

      Password: `ChangeMe` (factory default password)

   b. Type `advanced` on the menu.
   c. Stop the supervisor process by typing the `s-` command.
   d. Type “`.`” `<enter>` to get to the shell.

2. See which partitions are missing.

   If a RAID1 array is degraded by something like a temporary drive failure, it can be restored by simply adding the partition back into the array.

   To see which partitions are missing, run the command:

   ```
   % cat /proc/mdstat
   ```

   Normally, part of the output will look like this:

   ```
   |md1 : active raid1 sdb1[1] sda1[0]
   |      9767424 blocks [2/2] [UU]
   |md2 : active raid1 sdb2[1] sda2[0]
   |      3903680 blocks [2/2] [UU]
   ```

   ”mdX” is the RAID array composed of partitions on two physical drives, sdaX and sdbX.

   a. If sdaX or sdbX are missing from the array add them back in with this command:

      ```
      % mdadm --add /dev/mdX /dev/sdYX
      ```

      (substitute `X` with *1*,*2*, or *3*. Substitute `Y` with *a* or *b*)

b. Check the progress of the re-sync with this command:

```
 % cat /proc/mdstat
    |md1 : active raid1 sdb1[2] sda1[0]
    |      9767424 blocks [2/1] [U_]
    |      [>...................]  recovery =  1.0% (100800/
    9767424) finish=3.1min speed=50400K/sec
```

c. Repeat for any other missing partitions.

3. Test the drive speed, which is sometimes unexpectedly low in a drive that is going bad.

```
 % hdparm -tT /dev/sdY
```

a. If the drive is mechanically bad and cannot be added back into the array, it will need replacing.

b. Request a replacement drive and replace the bad drive.

Drive bay 0 is usually drive “sdaX” and drive bay 1 is usually “sdbX”.

4. View the original partition setup.

To see the partition setup of the good/original drive, use the command `fdisk -l`.

The original partition setup on the failed hard drive needs to be replicated on to the new replacement hard drive.

```
% fdisk -l
    |Disk /dev/sda: 500.1 GB, 500107862016 bytes
    |255 heads, 63 sectors/track, 60801 cylinders
    |Units = cylinders of 16065 * 512 = 8225280 bytes
    |
    |   Device Boot      Start         End      Blocks   Id  System
    |/dev/sda1               1        1216     9767488+  fd  Linux
    raid autodetect
    |/dev/sda2            1217        1702     3903795   fd  Linux
    raid autodetect
    |/dev/sda3            1703       60801   474712717+  fd  Linux
    raid autodetect
```

5. Replicate the partition information.

To replicate the partition info from the good/original hard drive on to the new replacement hard drive:

```
 % fdisk /dev/sdX
     Command (m for help): n
    |Command action
    |   e   extended
    |   p   primary partition (1-4)
 p
 Partition number (1-4): 1
 First cylinder (1-60801, default 1):
|Using default value 1
 Last cylinder or +size or +sizeM or +sizeK (1-1216, default
1216): 1216
|
 Command (m for help): t
 Partition number (1-4): 1
 Hex code (type L to list codes): fd
|Changed system type of partition 1 to fd (Linux raid
autodetect)
```

6. Repeat the information replication for the other partitions.
7. Print the partition table.

   To print the partition table and ensure that it exactly matches the other (good) drive, use the `p` command.

```
Command (m for help): p
   |
   |Disk /dev/sdb: 500.1 GB, 500107862016 bytes
   |255 heads, 63 sectors/track, 60801 cylinders
   |Units = cylinders of 16065 * 512 = 8225280 bytes
   |
   |   Device Boot      Start         End      Blocks   Id  System
   |/dev/sdb1               1        1216     9767488+  fd  Linux
   raid autodetect
   |/dev/sdb2            1217        1702     3903795   fd  Linux
   raid autodetect
   |/dev/sdb3            1703       60801   474712717+  fd  Linux
   raid autodetect
```

8. Save the partition table.

   To save the partition table and preserve your changes, use the `w` command.

```
Command (m for help): w
   |The partition table has been altered!
   |
   |Calling ioctl() to re-read partition table.
   |
   |WARNING: Re-reading the partition table failed with error 16:
   Device or resource busy.
   |The kernel still uses the old table.
   |The new table will be used at the next reboot.
```

```
|Syncing disks.
```

9. Re-add the missing partitions identified in Step 2.

   To re-add the missing partitions to each array:

   ```
   % mdadm --add /dev/md1 /dev/sdY1
    % mdadm --add /dev/md2 /dev/sdY2
    % mdadm --add /dev/md3 /dev/sdY3
   ```

   (Substitute *Y* with `a` or *b*)
10. Exit shell by typing `exit`.
11. Restart supervisor by typing `s+`.

Powering On

Once you complete the hard drive replacement, power on your RazorSafe appliance.

To power on your RazorSafe appliance:

1. Re-connect all external power cords (Powering Off on page 7).
2. If you are using an external backup tape device, power it on.
3. Power on your RazorSafe appliance.

Check RAID Rebuild Status

Once the RazorSafe appliance is powered on the RAID array should automatically begin rebuilding. Verify the rebuild status.

To check RAID rebuild status:

1. From the RazorSafe administration interface, click the **Status** tab (Figure 3 on page 5).
2. At the bottom of the **System Summary** screen, at the RAID Status line, click the **click for details** link (Figure 3 on page 5).

   A message window containing the hard drive information displays. The **ARRAY STATUS** should read: `rebuilding`.

Turn on Email Fetchers

Once the disk array rebuild is complete, turn on the email fetchers.

To turn on email fetchers:

1. From the RazorSafe administration interface, click the **Configuration** tab.
2. On the left-side navigation menu under **Email Servers**, click the **POP or IMAP Fetchers** link.
3. In the **Inactive Fetchers** table, in the **Actions** column, for each server needing to be active, click the **green arrow**.

Returning the Failed Hard Drive

For failed hard drive return procedures, refer to the return materials authorization (RMA) documentation provided with the replacement hard drive or contact your Mirapoint Certified Service Provider.