Gillware Inc.
Your data recovery experts

10 Terrace Court, Suite 103
Madison, WI 53718
gillware@gillware.com
www.gillware.com

RAID-5 Failure Common Sense Tips

Brian Gill
CEO Gillware Inc. Data Recovery
www.gillware.com

Don't Panic and Start Pushing Buttons

When a RAID array is inaccessible it is common for IT professionals to feel somewhat responsible. Sometimes a client is screaming at the top of their lungs that their whole business is ground to a halt without this array and they are losing thousands of dollars for every hour of downtime. Worst case scenarios about losing a client or facing litigation can creep into the IT professional's psyche. The urge to get it up and running quickly can be overwhelming. It's important to try and relax and don't do anything without full understanding of the ramifications.

Respect the RAID Card

The RAID card, assuming it isn't smoked, likely knows a lot more about the situation than you do. If you try to initiate a process and the card replies that it can cause catastrophic data loss, believe it and don't do it.

Read the Manual

All RAID card manufacturers produce high quality manuals that explain the interworking of the card and give useful tips on configurations and troubleshooting. They typically take 30-60 minutes to read and will give insight into the sometimes archaic and non-descriptive error messages and warnings. If you didn't read the manual when you installed it or didn't install it in the first place, read the thing! If someone threw it in the trash, you can probably find it in ten seconds using your favorite search engine.

Understand RAID-5 Concepts

While outside the scope of this document here's a short tutorial.

http://www.gillware.com/RAID5.php

Never RMA or Re-Use Drives from the Failed Array until the Backup is Verified

While it may seem like common sense to many, I've seen many scenarios where we call a client mid-recovery effort asking them where the other drives are. They inform us that the drive was dead, not even detecting in the controller, so they sent it back to the manufacturer for their warranty replacement. We shouldn't need it, because it's a RAID-5 and we only need N-1 drives. Then we let them know that one of the drives they sent to us actually was taken offline by the array many months ago and the drive they returned had died most recently because their array has been running degraded for months. The process of retrieving a drive that has been returned to a manufacturer is horrible and usually fruitless.

Cont'd >

Gillware Inc.
Your data recovery experts

10 Terrace Court, Suite 103
Madison, WI 53718
gillware@gillware.com
www.gillware.com

Understand What a RAID Rebuild Doesn't Do

A rebuild doesn't repair anything in the file system or make data accessible that previously wasn't. Any data that's missing will not magically appear after a rebuild. It doesn't fix any corrupt files or partitions. It won't make your server boot if it wasn't booting in the first place. If the current state of the union is the array is not mounting, the server isn't bootable, or lots of the recently updated files are appearing corrupted or inaccessible, a rebuild will actually render this failure state permanent. While the array will no longer be degraded, the newly redundant array is full of corrupted garbage.

Understand What a RAID Rebuild Does Do

What a RAID-5 rebuild does is take the current state of affairs on a degraded array and restore redundancy. A good rule of thumb is to never initiate a rebuild unless all your data is currently accessible and 100% functional. A RAID-5 rebuild will perform XOR calculations on the degraded set and writing those calculated values onto the new, healthy drive you just inserted when you replaced a failed one. Unless the array is accessible and all of the important, recently updated data is proven valid, never run any RAID rebuilds.

Test Your Backups on a Different Volume

I can't tell you how many times we've had clients notice two hard drives in a RAID-5 failed and simply replaced both drives (annihilating the previous volume) because they knew they had a solid recent backup. After the annihilation they restore hundreds of GB of data from the backup onto the new array. Then they realize that the backup was corrupted, incomplete, or many months old. This scenario is easily avoided by testing your backup on a storage array that has nothing to do with the hard drives inside the original failed array. Don't make a rush decision to restore to the only available working drives, simply explain to the client your game-plan is to source a new array, test all the backups, and then deal with the dead array.

Don't Assume a Hot-Spare Didn't Engage

We've seen many scenarios where an IT professional has yanked a hot-spare to use in a new storage array, fully confident that it never engaged and is blank. Again, verify your backups are current and consistent on another volume completely unrelated to the failed array before utilizing any of the failed array's drives, including hot-spares.

Never "Guess" the Parity/Rotation/Stripe/Offsets and Force a New Configuration

If you don't know 100% (because it's documented in a log file or the technician setting it up was meticulous) then the odds of you guessing correctly are tiny. Guessing incorrectly can be catastrophic. The operating system may notice array or file system "corruption" and start running "repairs" which will be catastrophic. The file system indeed is corrupted from the operating systems point of view. The problem being it only appears corrupted because you have the wrong configuration. After these "repairs" are complete, even if you guess the correct configuration the second time around, it will be too late to salvage any of these file definitions that were "repaired."

Cont'd >

Gillware Inc.
Your data recovery experts

10 Terrace Court, Suite 103
Madison, WI 53718
gillware@gillware.com
www.gillware.com

Be Extremely Wary of Forcing Drives Online

Until a backup is verified, I'd almost say never force an offline drive online. The array likely took it offline for a reason, it was failing! Unless you know exactly when it was removed, and know for a fact that zero critical files were updated after that fact, it's just a bad idea. If a drive failed many days or months ago and you jam it back into the array, all data of relevant size will be "corrupted" since the "stale epoch". The newly updated data won't actually be "corrupted", a more appropriate term would be "incomplete." Say you have a 3 drive array and the stripe size is 64kb. Now, you force a drive that failed months ago online. Any file bigger than 192kb is virtually guaranteed to have stripes of its binary run list residing across all three drives. Any file bigger than 192kb that has been created or updated subsequent to the initial drive failure is guaranteed to be full of "holes" and essentially useless. There would be a 1/3 chance that the actual file definitions of any file created/updated since the failure would be corrupted or missing. Often in these situations the operating system will notice these inconsistencies in the file system and run a "helpful" check-disk subroutine to "repair" these problems. These were not corruptions to be fixed, these were inconsistencies due to plugging a stale drive into the array. These "repairs" will permanently destroy valuable current data across all member drives, not just the "stale" one.

Never Plug in Independent RAID Drives "Individually"

It is alarming the amount of folks we talk to who have removed all the individual members of an array and plugged them into USB chassis to run data recovery software to try and recover data. Not only is this a waste of time but it could be highly destructive. The operating system has no concept that it is looking at 1/4 of a RAID. It may automatically "fix corruptions" in the partition table / indexes / master file table. There's a high probability the drive will show up as unallocated or available space, and some misinformed IT staff will actually "initialize" the independent drive with a new volume in order to "access its data." These drives weren't corrupted in the first place, so "fixing" the "corruptions" will typically lead to massive data loss. Running off-the-shelf data recovery software on 1/3 of a 3 drive RAID-5 will yield 1/3 of the file definitions, none of the run-list entries will be correct (file definitions only make sense in the context of the full partition), and the only data yielded will be extremely tiny file definitions where the data was "resident" to the file-definition itself (tiny ini files or log files).

Summary

Don't panic. Approach these situations with full knowledge of how RAID-5 works. If the RAID configuration utility warns you that you are about to destroy all the data with a particularly action, don't do it. You should read and understand the RAID manufacturer's manual before doing anything. You should only rebuild to a newly added drive if the volume is currently peachy but running degraded. Don't' re-use any of the drives in the failed volume until verifying your backups on a different set of hardware. If more than one drive is offline and you do not have a good backup, remove the drives from the array and contract a data recovery professional to assist you.

About Brian Gill

CEO Gillware Inc. Data Recovery

Connect with Brian on LinkedIn

After a successful IT consulting career I founded Gillware Inc. in Madison, WI to provide data recovery services from failed electronic media. Gillware is now one of the world's most successful data recovery labs, currently recommended by Dell and Western Digital.

Connect with Gillware on