5 Linux backup and restore tips from the trenches

Ken Hess ⋮ 5-6 minutes ⋮ 3/26/2020

It's easy to quote best practices and to tell someone what they should do, but it doesn't always work in actual practice. "Everything works on paper," was my response to an architect who told me that I need to "adhere to the recommended guidelines and best practices rather than being a rogue sysadmin." The fact is that I wasn't a *rogue* sysadmin. The problem was that this "architect" had never even been inside a data center, nor had he ever seen a server enclosure. He was simply reading a manual and telling me how it should be done, although he'd never had the experience of doing it himself.

My experiences (and attitude) aside, you should follow, as closely as possible, the guidelines and the best practices for your systems. But, also follow your own best judgment in whatever you do as long as you have your users' and your system's best interests at heart. Here are my five Linux backup and restore tips from the trenches, in no particular order.

1. The old 3-2-1 rule—I don't think this one is absolutely necessary for every situation, but you'll also never be fired for having too many good copies of your company's data or for protecting corporate data too much. The 3-2-1 rule states that you should keep **three** (or more) copies of your data on **two** different media and **one** in an offsite location. Those who use this method rarely find themselves without a viable backup available from which to restore their files. The downsides to this rule are space requirements and management. Three copies of data require a lot of space, and storing on two different media is expensive. Offsite pickup and storage are also expensive, but you have to weigh the expense of 3-2-1 against not having a good and recoverable backup.

2. A dedicated backup network—Add a network interface card (NIC) to your server systems, place those NICs on their own isolated VLAN (so that heavy backup traffic doesn't affect production traffic), and use a central backup location such as a storage server or network-attached storage. Be sure to bond multiple NICs together on the storage server to handle all that incoming data. High-speed disk arrays also help with simultaneously recording data from multiple locations.

3. Stagger your backups—It seems like everyone wants to set their backups to start at 1:00am. Don't do that. You'll flood the network with backup traffic, even a segregated VLAN, and your backups will end up not finishing because they timeout, or they'll run forever. Calculate how long each backup takes and then stagger accordingly. Also, not every server needs to be backed up during the night. Some servers might become quiet as early as 6:00pm when everyone has logged off the corporate network. You can backup multiple systems at the same time—just not EVERY server.

4. Document your backup procedures—I know that documentation is everyone's least favorite thing to do, but remember that you don't work completely in a vacuum. There are other people who might have to follow your instructions or to pick up where you leave off when you change jobs. Please document your backup strategy, the steps you take to backup data, where the data is backed up, identify and explain automation, and explain how to retrieve backed-up data. Verify your documentation by having someone else perform a backup and a restore. Handoff is critical, and if you leave your current company in a bad situation, you're limiting your future career possibilities. Technology circles are small, and everyone talks. If you get a bad reputation for sabotage or negative separations, you will damage that company temporarily, but you'll permanently hurt yourself.

5. Verify your backups—Although this tip should go without saying, many system administrators run backups, check to see if they ran, but never verify that the backup is actually useful. The way I verify backups is I plant a file named something like **backup_verify.txt** somewhere on the filesystem, usually in **/etc/configs** that I restore on a regular basis. You can automate this restore if you want to; it doesn't have to be a manual restore process to verify that you can grab this file out of a backup and restore it to a known location.

Wrapping up

Backups are a major, common pain-point among system administrators. No one loves to perform backups, and it seems to make us angry when we have to restore from a backup. Backups are simply a universal pain. They are, however, a necessary evil. A good backup can save you a lot of time, while bad backups, or forbid, no backups at all, will do little to enhance your sysadmin career.