Sysadministrivia

Linux, Lagers, and Late Nights

S0E6: "Backups and Beatdowns"

Posted 2015-05-04 05:10
Modified 2018-12-07 19:18
Comments 0

Navigation

Previous Episode	Next Episode
S0E5: "Textual Attraction"	S0E7: "The Isolation Chamber (pt. 1)"

Log

Recorded (UTC)	Aired (UTC)	Editor
2015-04-15 02:01:52	2015-05-04 05:10:47	brent s.

Verification

Format	SHA256	GPG	Audio File
MP3	`befae5dfdb101a4b3ec6869287b1761d8650244439d99c5b4f47beca712d5553`	click	click
OGG	`74cb89188a3ea8a6da386ec264a0d5bbccf79cfb3294caf97a0b707d2b7689f2`	click	click

Quicklisten:

This episode includes a “CMS Showdown” (mostly we just slam a bunch of blogging/CMS software), managing updates for your fleet of boxen, backups, self-auditing your security, and rsync.

- Notes
- Errata
- Music

Notes

- I found the souce of ‘Your _____ is bad and you should feel bad!’. (Futurama Season 5 Episode 16. “The Devil’s Hands Are Idle Playthings,” originally aired August 10th, 2003)
- We mention a ton of blogs/CMSes:
  - Ghost
  - Joomla
  - Drupal
  - Plone
  - TextPattern
  - And Wordpress
  - For clarification, TextPattern (“TXP”) doesn’t **quite** fit into the blog OR the CMS category because while out of the box it’s a blog, it’s designed to be flexible enough to be made into a CMS, per their FAQ.
  - I gripe about Wordpress security. Joomla’s had a pretty poor security history too, and both are commonly used as malware distribution points. Drupal’s had some bad ones, but they’re not as frequent as Wordpress (or even Joomla).
- MSFT may be cozying up to opensource at the VERY least existing alongside it-but never forget the early aughts. Stay frosty, hackers.
- I should note that Jthan’s blog domain **still** returns the stock nginx welcome page. Get your shit together, son.
- We talk about Audacity to segue into our updates topic. 2.1.1’s been a tiny bit crashy for me but seems to recover unsaved work fine.
- Canonical Landscape is good for Ubuntu shops…
- Whereas RHEL’s Satellite or its open-source counterpart, Spacewalk, is good for RHEL-ish systems (i.e. RHEL, CentOS, Scientific Linux, Fedora Core, etc.)
- Other distro-agnostic GNU/Linux tools similar to these systems are Puppet (Jthan’s arch-nemesis), Chef, Salt, and Ansible.
- Jthan’s cluster software he mentions is TORQUE and Maui. (NOT to be confused with Maui Linux).
- I mention Wayland and XWayland (which is different from Weyland, of Weyland-Yutani, from the Alien franchise though I’m a big fan).
- Some backup options for GNU/Linux are:
  - BackupPC (Uses SMB, SSH, etc. to remotely backup. No client installation necessary.)
  - Bacula (One of the grandpas- Bacula’s been around for a long while and it shows. Not very featureful, but pretty dependable. Difficult configuration.)
  - BoxBackup (Uses encryption for both data in-transit AND at-rest. Simple and clean, low overhead, but takes some severe finagling to play with non-GNU/Linux OSes.)
  - BURP (No, InfoSec nerds- not this Burp). BURP has some nice ACLs, but otherwise it serves as perhaps a slightly more user-friendly alternative to BoxBackup.)
  - DAR (Tarball-builder, but uses a non-tar format- it’s not proprietary, but offhand the only thing I know of that can work with DAR archive files is DAR itself. However, lets you then split this backup archive files into smaller pieces.)
  - Duplicity (Supports GPG encryption/signing and gzip, but basically just builds full or incremental tarball backups.)
  - Obnam (Simple, elegant, uses SSH for transit and allows for encryption of backups via GnuPG. Incremental backups, and allows for its archive files to be mounted via FUSE.)
  - rSnapshot (Doesn’t really delta or version or anything, it just copies over a file to backup if it’s been changed. It uses rsync and is pretty popular as

a “Poor-Man’s Backup”, but it’s not very featureful or good for corporate settings. Similar to Jthan’s custom-brewed solution. ...“Solution.”)
    - R1Soft (A commercial backup system for GNU/Linux and other OSes. It has some nice delta algorithms, but it sometimes eats data and requires a custom kernel module on clients.)
    - Unison (Unique in that it can “merge” snapshots from two different systems into one backup profile. Highly recommended for distributed environments, or git-like operations on the filesystem level/for binary data.)

- ...But we only mentioned **BoxBackup** on the show. :)
- We’d be remiss if we didn’t mention some offline/imaging/baremetal backup systems as well:
    - CloneZilla (Filesystem-aware, supports a multitude of different filesystems too. Can be used for BMR (Bare-Metal Restore) or cloning a single image across many machines. Has a LiveCD for small operations or a server implementation for larger ones.)
    - FSArchiver (PartImage reborn, essentially, except file-based instead of block-based. Much more flexible. Worthy to note that it doesn’t QUITE do the same job as PartImage; see their comparison.)
    - Mondo Rescue (This one’s pretty cool- it lets you take a BMR image from a ‘‘live, running system’‘ and lets you split to smaller archive files. It also can built a restoration LiveCD for you for BMR recovery.)
    - Partclone (Block-based imaging but not very network-friendly. Useful for storing “profiled” installs.)
    - PartImage (Mostly legacy, but offers a somewhat simpler alternative to CloneZilla- block-based. Limited filesystem support- no ext4 or btrfs, for instance.)

- Rsync does some REALLY cool stuff, like…
    - Checksum comparison (can take a LOOOONG time)
    - Resume broken SCP/SFTP transfers

- When doing audits/pentesting of your own company, you’ll want to check out:
    - Metasploit Unleashed
    - This BSides Nashville 2015 talk on using Kali
    - Handy “intentionally vulnerable” GNU/Linux installs such as Metasploitable and others
        - Also some public websites invite security penetration testing, such as HackThis and Smash the Stack (which is basically like an InfoSec version of Warhammer 40k).
    - R.E.M.nux is good for reverse-engineering malware.
    - A good place to start with a nice collection of introductory material can be found here.

Errata

- Plone actually runs on top of **Zope**, a Python framework. Hooray, even more layers for complexity and overhead!
- I ask Jthan how long it takes to Google. I actually edited out a chunk of silence while he searched. It was seriously like, 2 minutes of nothingness.Gorram it, Jthan.
- We mention Node.js’s pronunciation- per the Google group, it’s indeed pronounced “Node J-S”
- Wordpress security is actually pretty horrible, and leads to many great lolz… Textpattern, on the other hand, is a stark comparison.
- When I say “low regard for users”, I don’t mean as people. I mean in the nebulous sense of ID10T/PEBKAC issues, such as (I)users that tell you that you “just need to reboot the server” because that’s how they fix their Windows desktop, or ones that write their passwords down on Post-It™ notes under the keyboard- SURPRISE, EVERYONE AND THEIR MOTHER KNOWS THAT “TRICK”. STOP DOING IT. They continue to do things they are warned against doing multiple times or act as if they know your job better than you do without actual experience to back it up. Those are the (I)users I speak of.
- In Audacity, “meter” is indeed the word I was looking for.
- Jthan, it’s pronounced “Nazz” or “Nasz” or “Nass”, not “N-A-S”.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Pop Dance	Bensound	click	CC-BY-ND 3.0
Outro	Slow Motion	Bensound	click	CC-BY-ND 3.0

(All music is royalty-free, properly licensed for use, used under fair use, or public domain.)

Author r00t^2
Categories (Pilot Season)

Comments

There are currently no comments on this article.