Sysadministrivia

Linux, Lagers, and Late Nights

S2E21: "Barenaked Boxen"

Posted 2017-12-04 04:59
Modified 2017-12-14 19:14
Comments 0

Navigation

Previous Episode	Next Episode
S2E20: "The Shell Game"	S2E22: "Shitshow III: Son of Shitshow"

Log

Recorded (UTC)	Aired (UTC)	Editor
2017-11-28 03:55:51	2017-12-04 02:30:07	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	2a9e03ade91af9c3d5ef26bb0411db0f31e47c560a5388706ad55e079046a0a8	click	click
OGG	1f71c7fa5ed18a9c1364162ffdb804001b3a43f9b6d1999cb419dc412733f2f0	click	click

Quicklisten:

In this episode, we talk about installation preconfiguration (via e.g. Kickstart, etc.) vs. configuration management (Ansible, Puppet, etc.) for baremetal turnups. We also answer an email from a listener!

“May many portable gloryholes descend upon you and surround you and make you feel wildly uncomfortable.” – Jthan

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

- (Not mentioned during news segment; see 1h11m0s) We are still running a contest! **You need to get your answers/submissions in!**
- Speaking of announcing contest winners, we are also having season 2’s shitshow **December 6, 2017 at 2100EST**! You can find more info here!

- There was an Imgur breach
- Some pro-repeal comments on the FCC’s Net Neutrality feedback might have been faked (again)
  - The vote on the proposal occurs on December 14, 2017.
  - You can find the proposal here
  - The notice of event is here (the horribly mis-named “Restoring Internet Freedom” item)
  - It seems that they are still accepting comments on this (untested at time of composing notes)

- Intel had firmware flaws in their ME (which we mention in S2E7, S2E15, and S2E20)
- It seems there’s a new version of Bank Bot making the rounds in Google Play Store
- TP-Link firmware downloads are pretty hard to come by in EU
- The drone company DJI has leaked a ton of information, including their private key
- AWS is **finally** moving to KVM from Xen
- Results from Pentagon’s bug bounty program (“Hack the Pentagon”) are released

Notes

Starts at **27m54s**.

I was drinking a Jack and Coke, but with a Bulleit 95 rye instead of Jack Daniels. Paden was drinking Leffe Blonde, a Stella, and Absolut vodka. Jthan was drinking Lagavulin 16-year.

- Which tasks should you use baremetal provisioning for and which shoukd you use configuration management for?
  - Baremetal provisioning (Kickstart, Preseed, AIF-NG, etc.)
  - Jthan makes good points about “code” (task, etc.) re-use for configuration management
  - He also mentions Kickstart doing the OS install and Puppet agent installation, and have Puppet handle literally everything else past that
  - And he finds baremetal provisioning configurations a little too inflexible
  - Paden follows the same methodology – baremetal prov for only installing the configuration management and using the cfg mgmt for everything else
  - I hold to the same basic idea, but I make the additional suggestions of using baremetal provisioning to also install core packages (since it’s faster,

    - especially if it's a local repository mirror)
  - I also mention using the baremetal configuration to set up the basic security controls as well (firewall rules, pubkey auth for SSH, etc.), as well as NTP (and, I didn't mention this on-air, but a non-root administrative account is a good idea to set up in the baremetal configuration too).
  - I also bemoan the disadvantages – it's harder to get the current status of a build/provision/turnup/etc. when done via a baremetal install (unless you explicitly enable SSH to run for it) as opposed to a configuration management tool.
  - I also speak specifically to role/group/etc.-based functionality. Baremetal provisioning should be reserved for the most **common components** shared across all machines, and should be tasks that should (ideally) only need to be done once.
  - PXE (at least via PXELINUX) or iPXE can use things like host-specific configurations or scripted use of variables, respectively, to let you serve specific baremetal provisioning profiles to specific machines/specific VLANs, etc.
    - However, cfg mgmt is (again) probably *more* ideal for **role-based** or **group-based** configuration.

- Just why **do** we hate the "Cloud"/containerization? **(44m28s)**
  - Thanks to **raindev** in our IRC channel for the question!
  - Jthan's hate train is moving a little slower then Paden and I's in this regard – his userbase (researchers) are getting easier grants …er, granted by targeting these large "cloud" providers (AWS, Google's services, etc.)
  - He also mentions the validated and custom-built container templates he built for specific research tasks.
  - He kind of hints towards the cost-savings too.
  - BUT he also is a **little** on the hate train – e.g. NodeJS developers suddenly think they're able to deploy to production without considering things like resource consumption, security, comprehensive reliability, privacy, data integrity, etc.
  - He also talks about the dangers of putting all your eggs in one basket **that you don't even have direct access to or control over**.
  - Paden mostly hates that it's owned by someone else. The lack of liability for maintenance is nice, but the reliability of a third party does add complication.
  - My hate for containers/the "cloud" is manifold.
    - You can't guarantee that third-parties are going to attempt to protect against cross-customer abuse.
    - Paden mentions the prevalence of overselling, which is atrocious. (They're essentially a perpetual minimum viable product.)
    - One of the things I hate the most is how people will jump onto new/flashy/"hip" tech **just because** it's popular, and try to shoehorn it into cases it doesn't belong (see also: blockchain, the majority of startups that keep re-inventing existing things, etc.)
    - And the security inherent to the technology of these containerization platforms etc. is flawed. ***They do not belong in production.***
    - I **highly** recommend in-house full virtualization over containerization.

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(1h13m30s)**

Uber's done it again! They:

- Dropped 100K USD to breachers who exfiltrated private data to keep them quiet
  - 57 million users' data was breached
  - There is no way to verify that the breachers have indeed removed/deleted their data.
  - They failed to release notice of the breach – we didn't find this out until a long time after.

- This is after being in talks about previous privacy violations…
- AND an FTC case about mishandling customer data.

Errata

- I'm waiting on Jthan for the link to the Scotch Test Dummies video
- The datacenter I refer to on an abandoned oil rig was Sealand HavenCo – but it seems that it is no longer a thing as of 2008.
  - Even Google's plan at imitating this, Google barges, failed as well.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	It feels good to be alive too	Loyalty Freak Music	click	CC0 1.0
Outro	Close Your Eyes	Def Manic	click	CC-BY 4.0

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

Author r00t^2
Categories Season Two

Comments

There are currently no comments on this article.