WeGet letters

by Michael W Lucas

Dear Letters Column,

My employer has dozens of servers, and I don't know how many operating systems. One of them has an uptime longer than *I* do, and nobody dares touch it. But some doofus left a computer magazine in the bathroom, the boss found it, and now his brain has latched onto "configuration management" as the solution to all our problems when what the datacenter really needs is a backpack nuke. How can I make him understand that these tools are not for environments like ours?

—I'm Already Doomed,
Asking You Can't Hurt

Dear Doomed,

"Asking me can't hurt." As if there's a limit to how much pain a sysadmin can experience, or how doomed they can be. Doom is not an integer value that can overflow. Doom is a social construct, and yours is fully built.

We've all seen the propaganda on configuration management. Deploy dedicated-purpose, highly tuned servers with a single command! Adjust computation clouds with a simple playbook! Seamlessly and transparently migrate from server to server! *Containers!* That's fine for people starting from a green field, but most system administrators work in environments best described as "baroque" if not "antediluvian." I find myself with a green field only when I personally raze the earth and wait for clover to grow. Not grass. Lawns are a climate atrocity. Unless you own sheep. Or goats, but if you own any kind of goat, you won't have a lawn for long, which demonstrates that any force for good is also an agent of desertification. Besides, who wants to wait for clover before installing a datacenter? Bulldoze away the rubble of that razed kindergarten and get on with your day.

Configuration management is one of those things where the advertised ideal is the enemy of reduced agony. Yes, the Canadian Hockey League can devops up a whole fleet of web servers to dynamically manage the increased load of their nation's entire citizenry simultaneously watching the last game of the Memorial Cup, and I told they can also devops up additional mental health facilities to handle the crushing depression when the London Knights lose to the Saginaw Spirit — who aren't even Canadian! You? Not so much. Dynamic purchasing is a prerequisite for dynamic provisioning, and you clearly lack both.

But you *can* deploy configuration management, and not in a malicious compliance sense. Skip the magic pixie dust of managing the entire server fleet. Your fleet couldn't be managed with a chair, a whip, and a flamethrower. But the painful parts of your systems can be taken under control.

Configuration management is a sysadmin tool. So, use it to fit your needs. Start with a handful of systems. Configure a management account with access so that your management system can ping those hosts. Congratulations — you've achieved malicious compliance! That serves your need with management, but it doesn't fit your management needs.

Each server is its own special snowflake, albeit a snowflake with rabies. When you start bringing these systems under control, start with something comparatively simple, with known good values, that's mostly consistent across Unix variants. There's a cliché about problems: "it's always DNS." It's always DNS because sysadmins don't understand DNS, and don't consistently update /etc/resolv.conf when nameservers change. That's where I always start. You're not only bringing systems under initial configuration management, you are auditing current DNS configurations as a prerequisite to that project. Your manager will love it. Group your hosts by operating system and bring their resolver under your management. If you're kind, comment the file.

```
# under configuration management
# your changes will be overwritten without a human ever seeing them
search mwl.io tiltedwindmillpress.com
nameserver 203.0.113.53
nameserver 2001:db8::53
```

Congratulations! You have DNS resolution under control. Will it change often? Hopefully not. But you could now change it trivially. If you want people to take you seriously you must always implement your threats, so schedule a monthly configuration management run to update resolv.conf.

You can legitimately claim your hosts are under configuration management, but you haven't used it to make your life easier. Look at another common service that every host has but is often configured inconsistently: SSH. Your organization probably has rules like "no password-based authentication." If it doesn't, wait until you have a security incident then propose it. Never waste a good crisis! The simplest way to lock down SSH and make sure it remains locked down is to bring sshd_config under centralized management. Yes, every operating system has its own sshd_config tweaks, because before integrating software Unix maintainers feel compelled to rub it in their armpits so it smells like them, but management systems use templates to accommodate such unhygienic behavior. You could probably recite the default sshd_config while sleeping through your commute, so make your managed configuration looks nothing like the default.

```
#Configuration Under Management
#Manual Changes Will be Overwritten
Port 9991
PasswordAuthentication no
Subsystem       sftp    /usr/libexec/sftp-server
```

Any sysadmin thinking "I'll just comment out the default option" will feel alarm all the way down their brainstem upon seeing this.

Piece by piece, you can bring broad sections of your environment under your control.

Changes to managed services will become trivial. Coworkers will see that. Discussions of changing unmanaged services will turn into "how can we bring this service under management?" Use those discussions to implement necessary changes in the environment, or to get yourself a better fourth monitor. Doom is a social construct, but with configuration management you can transform it into a protective shell. Or a battering ram. At the very least, you can share that pain.

Deploying configuration management has a rarely discussed but horrid side effect, however: whoever controls the environment, *controls the environment*. Any change must go through you. People can't permanently enable password authentication on that public-facing server, but that doesn't mean they won't whine at you about it. They'll expect you to participate in problem-solving, and nobody can survive becoming known as a problem-solver. That ineradicable reputation stain will serve only to get you the title of Company Scapegoat.

Fortunately, you know what goats are agents of. Start grazing.

Have a question for Michael?
Send it to letters@freebsdjournal.org

MICHAEL W LUCAS is the author of *Networking for System Administrators* and a multitude of other crimes against civilization. A collection of these columns, Dear Abyss, will launch on Kickstarter soon, proving premeditation. See it for yourself at https://mwl.io/ks.