

/dev/random

ROBERT G. FERRELL



Robert G. Ferrell is an award winning author of humor, fantasy, and science fiction, most recently *The Tol Chronicles* (www.thetolchronicles.com).

rgferrell@gmail.com

By the time you read this the shock of Election 2016 will hopefully have worn off to some extent. I don't customarily engage in political commentary, even in my life outside *login.*, as people plummet into ad hominem-laden irrationality at blinding speed in such "discussions." Irrational arguments make my toes itch, and nothing interferes with developing a devastatingly clever comeback like having to take your shoes off to claw at your metatarsal digits.

I only broach the subject because of a single arresting quote, "the information trumps all," made in the course of a discussion of whether or not to publicize alleged state-sponsored hacking in connection with the US election. (Yes, I noticed the apropos transitive verb. I don't know whether or not it was intentional.) This ends-justifies-the-means paradigm is, of course, hardly a new concept. WikiLeaks is founded on it. Since we are in the information technology business here, it has particular relevance to our pursuits.

At first glance revealing the bare-bones truth about everything might seem a noble undertaking. I mean, who can make sound decisions in a factual vacuum, right? But I would argue that from a social, and at times even a technical, perspective having too much truth is as damaging as having none at all. We each build up comfortable mythologies surrounding the validity of our cherished institutions and the moral underpinning of our vaunted heroes. When the blunt truth is laid before us—that our institutions have inherent flaws and our heroes are subject to human foibles—those mythological foundations crumble and we are left with nothing much to admire or trust. Is this bald veracity an improvement? Not for me.

I am getting to the "relevant" part. Trust me. I just saw *Rogue One* and my brain hasn't yet made the long journey back from a galaxy far, far away.

We, and by that I mostly mean "some of you," have spent a great deal of time, effort, and coffee creating a wide variety of software and hardware tools designed to reveal to us what's really going on in our systems and networks. We as systems managers have an insatiable desire for the real scoop; the bottom line; the raw data; the dank underbelly; the misapplied metaphor. We tell ourselves we need to know precisely how our systems are performing, and why that's the case. But is this really true? Moreover, is conveying that information intact really the best course of action?

In some cases, I suppose a brutal reckoning is necessary, but I would argue that most of the time an approximation erring on the side of optimism might be better suited to the workplace. Submitted for your consideration: you're running low on disk space. You have two utilities for analyzing this. One shows the average disk usage per node, the other a more granular absolute user-by-user value. The first tool indicates that the average storage is approaching quota across the board and that (presuming no extraneous data is being kept) it's probably time to spring for more disks, or at least up the quota and have less reserve available. The other tool demonstrates quite clearly that the only users abusing the quotas are the boss and his two top assistants. Everyone else is way below the max, but those three users are blowing out the average egregiously.

You as the sysadmin need to deal with this problem. Which tool's results are you going to present to your documentation-crazy boss in support of your solution? Too much information might lead to hard feelings at best and unemployment at worst. Sustaining your rosy outlook concerning the practices and motivations of your coworkers has clear advantages here. There are myriad other instances where this is true.

Once upon a time there was a systems manager named Joan who was well-loved by all of her users. She had been with the company for many years and knew everyone's birthdays, their children and spouses, and each of their birthdays, too. She went to all of their parties and social functions. She had them over for cake, tea, and Canasta. She almost never missed a day of work. She kept the computers running most of the time.

One day, while this beloved sysadmin was out of the office for a week attending training, the IT staff member who'd been assigned to cover her duties was running routine network monitoring operations, looking for choke points. She pulled up the system log aggregator and noticed that the status panel indicating critical patch installations was showing red. She decided to investigate further.

The patch management system log showed that all recommended operating system patches had been faithfully installed enterprise-wide until three months ago, when they'd abruptly ceased. The weekly reports to senior management, however, failed to reflect that. This particular company had zero tolerance

for risk. When executive management read the report filed by the IT team member, they summarily dismissed Joan for professional negligence that seemingly placed the entire IT landscape in danger by not installing recommended patches.

Her replacement was ordered to install all the missed patches immediately. The older switches and firewalls were incompatible with those patches, as Joan had tried in vain to explain before her dismissal, and this left the network wide open to a variety of malware as a result. Inept attempts to combat a massive distributed denial-of-service attack launched by an unscrupulous business rival further eroded the once-solid information security barriers surrounding the network, and repeated ransomware demands stemming from spearphishing operations eventually bankrupted the firm entirely.

Notice the consistent negative correlation between full disclosure and longevity of employment in the preceding examples? The truth really will set you free.

Okay, do I really expect to draw a direct, meaningful comparison between journalists who sit on a scoop for fear they might unwittingly be doing some foreign potentate's bidding and a sysadmin hiding the fact that software patches haven't been installed in a timely fashion in order to protect her network from compatibility issues? You bet I do. In this post-rational world linear arguments based on logic and deductive reasoning are, like, *so passé*.

I desperately need to scratch my toes now.