;login:

THE MAGAZINE OF USENIX & SAGE

February 2003 • volume 28 • number 1

inside:

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

Appropriate Responsibilities

by Tina Darmohray

Tina Darmohray, contributing editor of *;login:*, is a computer security and networking consultant. She was a founding member of SAGE. She is currently a Director of USENIX.

<tmd@usenix.org>

You see just about everything in the consulting business. Sometimes you see examples of "doing everything right," and those are invigorating. You leave those sites thinking, "Wow! Now that's the way a bunch of machines should be run." You revisit those sites in your mind; they are so technically correct and clean that it's a pleasure to think about, like looking under the hood of a customized hot rod and proclaiming that the engine compartment is a thing of beauty.

For every lean and mean site you have the pleasure of seeing you also come across those at the other end of the spectrum. The system administrators are disgruntled, the managers are frustrated, the machines and network are laid out in a haphazard way, and the applications are insecure and underperforming. You revisit those sites in your mind too, but to work out what went wrong, rather than to enjoy the image of a technical thing of beauty.

While perhaps unpleasant, revisiting the "wrong" sites in order to determine what brought them to where they are can be tremendously rewarding in a different way. Figuring out what got them to where they are can be instructional and prevent having to learn the lesson firsthand the hard way.

I spent quite a bit of time trying to determine what had gone wrong at one particular site. There was no apparent plan for the way things were laid out, and the symptoms were insecure applications, inefficient use of resources, and a downtrodden staff. Further inspection revealed the root of the problem: professional responsibility was left to the folks in the trenches and they failed to take it on. That's right, the system administrators in the trenches were mostly at fault for this particular SNAFU.

Wow! That's kind of harsh. A public proponent of system administrators placing the blame for a SNAFU on the good guys? When did she join the opposition? Well, I was surfing on the sageweb site the other day and I came across the SAGE Job Descriptions for an Intermediate/Advanced administrator. Under "Required Skills" it says, among other things:

- Strong interpersonal and communication skills; *capable of writing purchase justifications*, training users in complex topics, making presentations to an internal audience, and interacting positively with upper management.
- Independent problem-solving, *self-direction*.

and under "Appropriate *Responsibilities*":

- *Initiates* some new responsibilities and helps to *plan for the future of the site/network.*
- Evaluates and/or *recommends purchases*; *has strong influence* on purchasing process.

These qualities clearly describe a senior professional who is expected to be proactive, persuasive, and has a stake in the systems s/he is managing. That is, we're not talking about a naive novice who doesn't know enough to "know better." We're talking about a technically savvy individual who is capable of, and should be held responsible for, knowing the requirements and planning for the needs of the organization they're supporting. And that's where the system administrators of this particular site had failed.

Several years earlier, as the organization moved off mainframes, they had mimicked their earlier environment by purchasing large UNIX servers and "selling" space on them. As departments and services required computing resources, they came to the central IT group. The group gave out resources on an as-needed basis, filling up the servers which had been purchased based on space and load. While this approach may streamline the purchasing process for servers (just buy another one of what we already have), it fails on almost every other front.

The machines, while mostly identical from a hardware standpoint, are unique in every other way. There are Web servers, applications, databases, and core services on these systems, but they are not distributed in any predictable way. That is, Web servers share database servers, core services are colocated with applications, and any other combination that is possible. As they say on Saturday Night Live, these machines were "a floorwax and a dessert topping." As a result, the system administrators were unable to efficiently scale their operations because they could not take advantage of the cookie cutter approach: with every machine a unique mixture of the endless possibilities, there was no way to create standard builds, for instance. When it came time to secure the most sensitive databases, this hodgepodge of systems tripped them up: with multitiered applications deployed on single systems, isolating the databases behind firewalls and restricting administrative access to core systems was impossible. When it comes to disaster preparedness, this approach fails again: some pivotal machines are so complex that when they fail it will almost certainly take days (and nights) of intense system administration heroics to put Humpty Dumpty back together again.

The system administrators at this site are complaining bitterly that they're understaffed. Their systems are so complicated that they're indeed difficult to manage, but I don't think I could justify additional staff in this case. Rather, these SAGE Level III system administrators should start working up to their capacity and taking responsibility for planning the future computing requirements of their organization. Instead of complacently buying another server and blindly installing the next seven requests for resources on it, the system administrators should take the initiative to understand the needs of the departments and services and size any new servers to the applications. If this includes selling the upper management on these ideas, that's in their job description too. Retroactively, they need to create a migration plan which co-locates similar applications and begins to leverage their time with standard builds and cold-swap spares for disaster readiness. Finally, once they've located Web servers with Web servers, but separately from database servers, they can secure their site from external mischief and place sensitive data behind firewalls and restrict access to such systems or applications to "need to know/administer." In short, they need to understand the requirements and specifically and proactively plan for them.

In any job we do, we all take direction from someone, but the more senior we become, the more self-directing and proactive we're required to be. When you get to that level, you can no longer expect your manager to spell out implicit tasks. Planning for resiliency, scalability, security, and efficiency are givens that are part of doing a "good job" as a more senior system administrator. In fact, they're not only "Appropriate Responsibilities," they're required.