System Administration in Higher Education Workshop at LISA15

JOSH SIMON

Josh Simon is a Senior Systems Administrator for the University of Michigan's College of Literature, Science, and the Arts. In addition to higher education, he's worked for hardware manufacturers, software companies, and multinational financial institutions. He's also a long-time *;login:* contributor. jss@umich.edu

The System Administration in Higher Education Workshop asked what's different and what's the same for system administration in higher education versus industry, including the challenges faced by practitioners. About half of the attendees worked in central IT at their institution as opposed to a distributed IT shop such as college (within a university) or department level. Most of us were at bigger institutions...or ones that felt bigger.

Improving Support

Our first topic of discussion was practical ideas for improving support. One manager reported that he has a team of five engineers and 12 students. Outsourcing work to students works really well except during finals week. They have about 40 to 50 products in their service portfolio, most of which are commercial off-the-shelf products, and half his staff spend most of their time maintaining them. He wants to move towards a service center model so that his engineers can be freed up to work on problems more interesting than provisioning and day-to-day operational tasks. Suggestions included providing self-service access for faculty and students to do certain provisioning tasks themselves, abstracting the work into smaller chunks, generalizing (e.g., "students" as opposed to "art students" and "engineering students"), and retiring obsolete services or combining common services in the portfolio.

Keeping staff engaged by handing off the routine stuff to the help desk helps. What are other ways to keep staff engaged? Automate (or "provide consistent service delivery for") the daily-operations tasks so that people can work on projects instead. Over time, people find their interests and that's okay. Another attendee's organization is stable: employees have been there for 35 years, so there aren't a lot of new people. Some people want to be more engaged, but the institutionalists don't want people to be engaged because that means the old-timers would have to change.

In another case, someone is unwilling to disengage when workload says he should. Someone wants to be the de facto SPOF: he's holding knowledge and won't document or disengage or relinquish tasks. This needs management buy-in and culture change (no one product owner). There may still be specialization, but information needs to be shared (e.g., SMEs are okay).

An attendee suggested switching jobs and not asking each other for help, doing the routine tasks, and just using the documentation. Mentoring was raised as another possibility.

How do we measure success and translate that into the right operational changes? Ticketing systems can provide some metrics. Surveys to faculty ("How're we doing?") can be useful, especially if repeated so that you can measure change over time. Justify new projects or products by (faculty) demand. What if your goals ("faculty: keep this guy here") conflict with the dean's ("move this FTE to Central")? If you do surveys, who gets to see the results (raw data, analysis, future actions or priorities)? Some people wish they got more negative feedback than they do, even if it's "I like this but..."—we're not perfect.

Setting Priorities

Our next discussion was on priorities. Other than incident handling, how do you prioritize what's important? It's not unique to higher education but we put a twist on it: there's no obvious budget bottom line to point to. A lot of institutions of higher learning care about teaching and research; how do you measure that?

In an ideal world, priorities would be obvious, and management would help with guidance. Our priorities should align with those of the college or university, which is usually about teaching and learning, research, and service, depending on your environment. Those areas are inherently messy and can't be planned the way "build a building" would be (which is messy but in a constrained way).

Can you abstract priorities to "my faculty, students and staff"? Not entirely. You still need to plan for end-of-life and capacity changes. Ask faculty if there'll be other changes (e.g., Java to C or whether Eclipse will go away). Remember that priorities may be different for the group (maintain stable network) and for yourself (continually learn, teach, and research in your own field). Regardless of that, you need to make sure things keep working. Build things to stay stable 24/7 in a one-person shop yet move technology ahead.

One team has a goal of stability (changing hardware or software is declined), and they do trouble tickets for issues and weekly meetings with the researchers for possible future planning. Another team is cleaning up after years of non-management.

In a department of 21 (plus students) on a four-person infrastructure team, someone went from taking direction from their boss into creating a feedback loop—providing ideas for improvement, simplifying workflows, presenting new ways of contributing (including beyond their own group).

As an ITIL teacher, the business drives the priorities, and it's based on urgency and impact in the operational work. Trouble-ticketing systems are a good start for incident handling.

For another attendee, it varies at the university (research, teaching, and patient care), college (research and teaching), department (projects based on survey results as defined by the director), and team (e.g., infrastructure) levels. Having regular one-on-one meetings is essential.

Individual priorities are yours regardless. On a professional basis, what you're prioritizing needs to align with the rest of your institution. We need to provide clear advice and recommendations to senior management for them to draw on in making decisions; we shouldn't be making decisions at our levels.

You need to be sensitive to the unwritten rules: what about those with bad histories (e.g., faculty person A has more problems than another faculty person, or there are HR issues behind the scenes)? Can VIPs be flagged in the system? If your manager is not setting your priorities, let them know what you are prioritizing.

We need to set priorities because we don't have enough resources. Kanban is a way to organize and prioritize work and can help with communications (in all directions).

Security

Next we talked about security. Universities aren't really that much like businesses. What are the unique aspects of higher ed? Some can't say "No" (e.g., "no porn" or "no Netflix"), but some rate-limiting may be useful.

Someone thought they had a security problem and hired a CISO. Their only directive is "Security." Issues of privacy are being disregarded in the name of security.

Some of the challenges: research institutions have short-timers—but IT isn't told when and where they went. How do we ensure accounts are closed when they should be? What about when credentials or machines are compromised (and three-letter agencies come for it)? How do you get those with prestigious awards to choose longer passwords without writing both ID and password on a sticky note?

Other challenges include personally owned devices ("BYOD"), application hosting (where the institution provides containers and infrastructure but the customers build their own insecure front-ends with SQL injection possibilities), worldwide collaborators (so the institution can't block countries known as threats—which won't work long-term anyway because the threats move), and senior faculty who don't want to change what they've been doing.

A policy or advisory group that meets regularly can help write the policies and make them sane and applicable *with buy-in from the relevant sources.* Have the CISO keep the chancellor or executives quiet until they're ready to act. Remember that "declare by edict" often doesn't work in academia; there's no boss-employee relationship here. We don't have the ability to tell faculty how to do things; we can make recommendations, but they are responsible for their data.

Some places are trying top-down edicts, and IT is having to dance around the push-to-centralize. "Academic freedom" is a red herring: we're not trying to prevent faculty or researchers from doing their work. In reality, a "grant" is a contract between the granting agency and the university and has requirements that may include security. Some grants have specific security requirements (including FISMO). One is "You might have to monitor logs"—but they could use that requirement to justify it for a Splunk license...to monitor those logs as well as everything else.

What's at risk? Intellectual property of research and the reputation of the researcher and institution. It seems like the lawyers and executives are finally catching up to what we understood 15 years ago about how dangerous technology can be. They seem to be much more interested in a vendor-provided solution or service, shifting the responsibility and blame (and liability) to someone else. Is that good or bad?

Some places use a combination of vendor and internal tools, VLAN segmentation, and SQL injection review. Even with all those, you have to use them correctly. Remember, though, that regardless of whether it's internal or vendor, it's still your institution's name above the fold of *The New York Times* front page.

There are some types of liability you can't get away from. Some have to store SSN, PCI, or PPI somehow. Some business processes need to be fixed (e.g., an SSN is needed in one place but stored in multiple places).

Budget

Our penultimate discussion was about budget. Some places have an adequate budget overall, some adequately budget for equipment but not for people, and some just don't adequately budget.

One place is moving towards cloud-based services like AWS. They also let their Symantec contract expire and moved to Sophos. They could move from hosting their own to AWS, which is PCI-compliant. It shifted the expense from capital expenditure (CapEx) to operational (OpEx) and freed up FTE resources internally. CapEx is almost always easier to justify than OpEx.

Do an honest analysis: Are you *the* service provider or *a* service broker? Can you manage external services? Remember you may be a customer not a provider. Recommending others' stuff instead of your own may be hard. Remember that doing customer support is hard when you're at the mercy of the third-party provider.

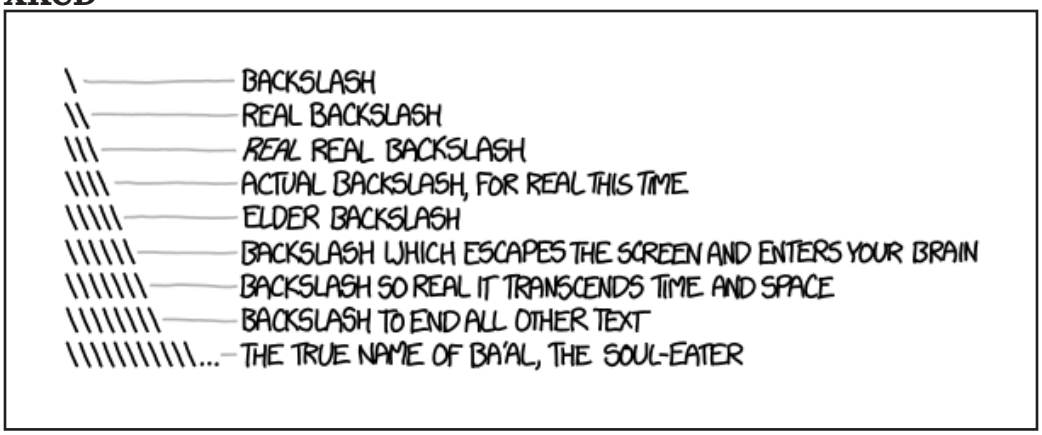
Monitoring and alerting (your internal people) is not necessarily possible when you're not the provider. How do you monitor cloud-based services? (You don't.) You may or may not have lowered your users' service level.

Handing off the "fun" stuff to the cloud and being a service broker can lead to disengagement of the IT staff. It might save time and money (at least CapEx), but it loses the staff engagement. Handing off some stuff to the cloud lets you focus on the stuff that you're keeping.

Campus Participation

Our last topic was participation on campus. We generally advised everyone to get involved on campus-level committees, both technical and nontechnical. Faculty and staff boundaries may be problematic but making the connections is very valuable. There are also off-campus activities like ACM, EduCause, IEEE, LISA, LOPSA, USENIX, and so on. Find those formal and informal networking groups that work for you and participate.

XKCD



xkcd.com

Do you have a USENIX Representative on your university or college campus?

If not, USENIX is interested in having one!

The USENIX Campus Rep Program is a network of representatives at campuses around the world who provide Association information to students, and encourage student involvement in USENIX. This is a volunteer program, for which USENIX is always looking for academics to participate. The program is designed for faculty who directly interact with students. We fund one representative from a campus at a time. In return for service as a campus representative, we offer a complimentary membership and other benefits.

A campus rep's responsibilities include:

- Maintaining a library (online and in print) of USENIX publications at your university for student use
- Distributing calls for papers and upcoming event brochures, and re-distributing informational emails from USENIX
- Encouraging students to apply for travel grants to conferences
- Providing students who wish to join USENIX with information and applications
- Helping students to submit research papers to relevant USENIX conferences
- Providing USENIX with feedback and suggestions on how the organization can better serve students

In return for being our "eyes and ears" on campus, the Campus Representative receives access to the members-only areas of the USENIX Web site, free conference registration once a year (after one full year of service as a Campus Representative), and electronic conference proceedings for downloading onto your campus server so that all students, staff, and faculty have access.

To qualify as a campus representative, you must:

- Be full-time faculty or staff at a four-year accredited university
- Have been a dues-paying member of USENIX for at least one full year in the past

If your campus does not have a representative and you or someone you know would like to represent USENIX on your campus, please contact the Campus Rep Administrator, campusrep@usenix.org.

www.usenix.org/students