Mandarins and Guerrillas – The growing waves in the Linux ecosystem, and its squeaky wheels

AUTHOR | DAVID DINGWALL, VP OF PRODUCT MARKETING

In the early 1990s the Open Software Foundation formed a committee to select and standardize a new Management Platform Toolset for and from the UNIX ecosystem. After much soul searching over a few months the OSF Management Platform never arrived. One of the committee, from the team that invented The Newcastle Connection (1980s *NIX history, go Google it) made a compelling presentation explaining why they failed. He spent the next 40 minutes wearing two hats, an exquisite red silk Chinese mandarin hat (with feather), and a green canvas guerrilla cap. Swapping back and forward hats on each topic, he had the audience full of system administrators rolling in the isles with laughter at both perspectives; an OSF selection team executive, and what hand-crafted practices were happening in the real world, and how the admin grunts felt about it.

THE LATEST LINUX WAVE

Since you're reading this article you will have your own perspective on the Linux ecosystem. A lot has changed even in the last year, we're experiencing a massive wave of Linux take-on via virtualization and the cloud as accelerators. New companies are growing from 10 servers to 10 thousand instances in two or three years. For older customers, however, we're also living with a legacy of old infrastructure decisions made (for some) decades ago, some pre-Linux.

In the middle of all this is you, that rare and finite resource the Linux admins. You may now be a manager (who was an admin grunt when decisions were made years ago), or you may be a grunt on the front line right now. In the same tone as that meeting in the early 1990s let's try two viewpoints with the following piece of statistics:

The good news -- Linux is on the up and moving like a freight train. 87% or organizations added Linux servers this year. About the same will add more Linux next year. Windows deployment has fallen from 46% to 26%

A Linux Mandarin might say: The organization took a strategic decision last year to standardize on Open Systems Infrastructure to manage our asset and cost base more efficiently, streamlining technical and operational silos.

A Linux Guerrilla might say: Let's be honest, we're migrating to Linux VMs and Linux in the Cloud to save money. The business may have LIKED Windows server in the past, but Microsoft's licencing mechanisms seem to be purposely designed not to work in virtualized and cloud infrastructures, unless the business has gone Azure. And if that had happened I wouldn't be here. We're already expected to support twice as many server instances as we did before, and to be honest expect to see that will rise again without our team growing at all, so we're going to need more automation.

AND ITS SQUEAKY WHEELS

A worldwide, year-long survey of what people are ACTUALLY doing with their infrastructure is just moving into its second year. FoxT will be presenting their first year results formally over the next few weeks.

Some valid commentary that can be made on some of the initial raw data, both as a Linux mandarin, and a Linux admin guerrilla. Beyond the marketing and positive news of new companies and projects going live in the ecosystem worldwide there is quite a bit of acerbic and wry grumblings over a few (Ed: Few??) beers and margaritas at Linux user group meetings. Your admins are talking, and it's not all good news.

Here are four quick samples of the annoying squeaky wheels we're dealing with as the ecosystem grows.

[1] 70% of organizations worldwide use LDAPS and Kerberos for secure authentication

Linux Mandarin: It is encouraging that industry best-practice is being utilised by the majority of the ecosystem for LDAP based (48%) and Kerberos (21%) authentication, providing centralization and control of user and session access.

Guerrilla: A couple of things here:

What the survey also says is 10% of larger enterprises are still using NIS and NIS+. Mainly larger, global companies (many web-facing) still have not migrated away from NIS, even though it has been End-Of-Lifed a while ago. I follow the news, if those servers are already penetrated, our host, group and user information is zipping around in the clear. Does the Board appreciate that?

If I'm running or migrating into a G-Cloud, which requires complete separation between infrastructure layers then LDAP and Kerberos break the rules because they both have to be pervasive for authentication on all network layers for the support teams to work. We have to start bridging networks and adding strange proxies, breaking the G-Cloud architectural model.

[2] 50% still manage Linux privilege escalation with internally developed solutions

Site Specific Mandarin: We're making effective use of existing toolsets to ensure we can audit privileged escalation, and show evidence to our System Owners and Auditors. Extending some of our existing Configuration Management and Operational reporting tools we have saved the business from investing in a commercial product, or purchasing an additional service from our business partners.

Guerrilla: Internal, as in non-standard, maybe non-best-practice (I can't remember the last time we updated our rules), untrained (in the unlikely event we do get another or have to replace a team member), and badly documented. Most damningly it's unaudited and violating segregation of duties. My team maintains and supports this stuff, and it's my team's activities that are being monitored. Do you see the problem?

[3] Over half of organizations worldwide provision and deprovision their Linux servers manually

Linux Mandarin: This is scary – I was pretty shocked when I saw this result. I see 44% use tools to enable automatic account and group provisioning which is encouraging, we interact with new customers and projects all the time recommending best practice to use automation or IAM tools to enable this. Obviously from these results we still have a long way to go, we need to keep evangelizing, and especially with smaller customers.

Guerrilla: That's a huge number of guys and girls still doing essential operational tasks to make sure critical applications are setup properly. Not the most inspiring part of my day let me tell you, and probably assigned to the most junior team member on shift, who might miss something. Remember that NIS directory we turned off last year because we were told to by the auditors? Now we now have no control of UID/GID consistency.If we do add automation it may take months to fix that system by system before we get any benefits, you're going to see that as a cost, not an efficiency saving.

[4] 71% or organizations worldwide plan to use Red Hat Enterprise, Ubuntu Enterprise or SUSE Enterprise Linux in the next year

Mandarin: The Linux ecosystem is maturing, and the positive trend of customers migrating to Enterprise Linux editions for rollout into their production infrastructures shows this. Even

with an exploding Linux installed base, organizations are seeking business level assurance provided by the maintenance and SLAs provided by Enterprise Editions from the vendors.

Guerrilla: Ok we used (CentOS/Debian/Open SUSE) (Ed: delete where appropriate) as a start-up, and this move makes a lot of sense, change and patch management integrated with automation is v. good.

Boss, I need to take you out for a beer and a chat. Looking at this there is going to be a lot of market competition for trained staff. Let's talking about training and certification. We're going to need to formally train and certify a chunk of the admin team before we do this to meet the vendor's minimum SLA requirements. Off the cuff that will take an ongoing FTE of two out of support for a few months. Do you have the budget to hire some consultants to cover that? And talking about budget, about my next review . . . .

What do you think? Heard something similar? Obviously we've all seen the positive strides Linux has made in market share worldwide, and it is a nice feeling to be part of a growing trade that values our skills. That has its own pressures, especially on staffing and day to day operations. FoxT is an info-security company, so many of their questions are in that area, however I'm sure similar grumbles exist in configuration management, operational monitoring, and deployment.

ABOUT FOXT

Fox Technologies, Inc. helps companies protect corporate information assets with network security and access management software as well as striving to simplify compliance and streamline administration with an award-winning access management and privileged account control solution. Our access management software centrally enforces granular access entitlements in real time across diverse server environments.

To learn more about Fox Technologies, please visit us at: **www.foxt.com**

CONTACT INFO

North America
3300 Eagle Run Drive NE, Suite 202
Grand Rapids, MI 49525
+1 877 818 3698 (Toll Free)

Sweden
FoxT Sweden AB
Kungsängsgatan 18A
SE-753 22, Uppsala
+46 18 16 00 00 (Main)

United Kingdom
400 Thames Valley Park
Reading , Berkshire RG6 1PT
+44 1189 637 681 (Main)

www.foxt.com | info@foxt.com

foxtechnologies.

You may also be interested in: Best Practices for Unix/ Linux Privileged Identity and Access Management