Automated Operating System and Environment Certification at LinkedIn
Reducing Toil and Increasing Velocity

Adam Debus has been a Staff Site Reliability Engineer at LinkedIn since 2019. Following over a decade of experience leading systems engineers in the eDiscovery and Compliance fields, he now leads the Fleet Compliance initiative at LinkedIn. Currently hailing from San Jose, California with his husband, he’s frequently found repeatedly removing his cats from his keyboard in the middle of meetings.

https://www.linkedin.com/in/adamdebus/

Good afternoon, I’m Adam Debus, and I am a Staff SRE for LinkedIn. Before joining LinkedIn 3 years ago, I spent more than a decade working at one of the largest ediscovery and Legal Compliance firms, leading the systems engineering team, both in managing their worldwide datacenters and product development.

While at LinkedIn I’ve had the pleasure to work on some truly interesting projects, most notably our Fleet Compliance initiative, where we’re taking a holistic view of our entire Operating System Lifecycle from image creation through deployment, and even post-deployment issue management. Today, I’d like to talk with you about the philosophies behind one specific portion of this lifecycle, OS image certification, and how we’re approaching this very complex problem.
First, I’d like to talk a bit about the motivation why we’re looking at this now, followed by a discussion of some of the ways we’re addressing this very complex problem. Next, a very quick look at some of the results that we’ve achieved, and then we’ll wrap up with some final thoughts about this process.

It’s important to note that I’m not going to dive into specifics of our technical implementations, as many of those are going to be specific to our particular buildout and software, but instead focusing on some of the process and philosophies we’re employing to achieve our goals.
LinkedIn has been doing environmental certification for a long time, so why now? What’s changed?
Firstly, LinkedIn has grown, more than a little bit. We’ve experienced a 1200% increase in our member growth since 2010. But, in the same time, the infrastructure supporting those members has grown by about 6000%, nearly 5 times faster! New features, additional offerings, increasing growth of AI driven features, all add server resources and complexity to the environment.

Environmental Growth

From 2010 to 2022:
Member Growth from 65 million to 800 million (a ~1200% increase)
Infrastructure grew by ~6000%, nearly 5 times faster than members!
In 2019, LinkedIn announced that we’re investing significantly into Azure. As everyone’s aware, moving to any cloud-based platform is a significant shift in the way we approach operating systems and server infrastructure. These shifts require us to think differently about how we handle certification and OS lifecycle.

---

Azure Here We Come!

- In July 2019 LinkedIn announced a multi-year migration to Azure.¹
- Significant paradigm shifts in server and operating system builds.
- More flexibility means more complexity!

¹https://engineering.linkedin.com/blog/2019/building-new-infra
There were a few major issues that were encountered leading us to evaluate how we certify kernels in our environment. Two issues occurred in close proximity to each other that caused us to take a deeper look at some of these processes.

The first was the nature of the way older kernels handled clearing memory pages: by completely dropping the page cache and trying to compact neighboring pages. This caused a long-tail issue where filesystem read-heavy applications would suddenly see their performance drop off to impacting levels until the cache rebuilds, especially with heavy IO applications.

The second involved discovering a bug in the EXT4 filesystem driver. Under certain circumstances and hardware configurations read/write performance would drop off to a fraction of normal speeds until the triggering I/O queue cleared.

In both cases, numerous new kernel builds were required for isolating and testing the issue itself, but then any potential release candidate kernel required validation for the environment at large.
New vulnerabilities are being discovered at an ever increasing rate. Since 2010 the number of CVEs reported has increased over 400%. And this is just CVEs. This doesn’t include every other method of reporting vulns, or the vulns that never get publicly announced.

Coupled with that, to reiterate one of the running themes so far this week: software increasingly touches more aspects of our lives, and covers a broader range of technologies – as represented between 2016 and 2017 when cloud adoption started rapidly expanding and additional categories of software and vulnerabilities were added to the tracking by MITRE.

This means that the rate of response to these vulnerabilities has to get ever faster.

Finally, there’s the human cost. As environments get more complex, additional validations need to be made. More and more of that work ends up with different teams of SMEs, each of which will have varying degrees of automation and standardization.

You still get high quality results, but it takes time and additional effort. And it has to be repeated for every release candidate.
Designing A Solution
In designing a solution, we had to take a step back and look at the whole picture. Can a framework be built that encapsulates everything that the company is today, and flexible enough to grow with what it will be tomorrow? To answer that question, you need to take a holistic look at the environment. We have stateless and stateful applications. Two very broad categories to be sure, and ones that start to have their own complexities as you look at them more closely. Even within, say, the Stateful environment a database has different needs and requirements from, say, a Kafka implementation. Additionally, an application running in our On Premise environment has different underlying infrastructure from an application in the Azure environment.

All of these combinations have different testing requirements! All of this can get overwhelming very quickly!

Environments and Applications
Designing a scalable solution for all of LinkedIn

These two applications have dramatically different testing requirements!
The first priority is taking this very complex problem domain is breaking it down into more manageable chunks. The best way to do that was to look at what some of the logical groupings of tests are. And then see how you can put them all together. What we started developing for is a multi-stage certification process that builds on the layer before it. And thus I present the Layer Cake of Certification. Much like with a layer cake, each stage of the certification forms the foundation of the next stage. If your first layer is underbaked, all of the stages above it become unstable.

We came up with these three stages: Infrastructure, Tooling, and Application. And the frosting on the cake is the automation that we have built to hold it all together.
In the first stage, Infrastructure, we’re focused on building tests that ensure OS compatibility with our hardware. At an OS level, does it perform as well, do all the device drivers work as expected. We also apply hardening, validate it, and scan for known vulnerabilities. This is also where any environmental specific tests will be run.

The second stage really starts to dive into a lot of the specifics of our environment and the tools that support our applications. Deployment pipelines, containerization, language frameworks, and synthetic tests.

Finally, we do application testing. We do a set of functional tests and comparative performance analysis of canary applications. We test the applications side by side on the old and the new OS version, and ensure that applications receive at least the same level of performance on the new version as on the old version.
Partnerships Are Paramount!

- Nobody is a Subject Matter Expert in everything!
- Identify critical teams
- Shared ownership

- Framework features depend heavily on partner needs.

Individual test creation is a very critical piece of the entire project. Without accurate and maintained tests your platform framework doesn’t do anything. Nobody is expected to be a SME in every part of your technology stack, especially at a company as large as LinkedIn. So partnerships and setting clear expectations becomes very important. It becomes a symbiotic relationship. On the one hand, you have the teams creating tests and taking ownership for maintenance and troubleshooting, and the feedback you get from. Your partners helps to guide your framework feature development.
Keeping in mind that we’ve been launched for about 9 months, we’ve seen a significant reduction in turnaround time – over 70%. There’s been a significant reduction in manual testing by some teams, with many more improvements in the pipeline. And, finally, it allowed us to rethink the way we’re doing some of our testing and add new lines of testing that we hadn’t been doing before.
Final Thoughts
Scope is Important!
...but one of the hardest things to zero in on.

You must find the Goldilocks Zone: Not too narrow, but not too wide.

Scope creep is a constant presence.

Define a core purpose, and always ask yourself: “Is this in service to it?”

“Develop a comprehensive, automated, extensible, and defensible OS snapshot testing process.”
There needs to be a constant awareness of how the company is developing. Even in the year that was spent putting together the initial framework, some of the technology in the company had progressed beyond what we had been designing for. You need to be able to adapt, but more importantly, you have to have processes in place that allow you to be plugged into the overall technical development of the company. And this extends to your partner teams, too. They need to be continually creating new tests for new technologies, updating their existing tests, and depreciating old ones that are no longer relevant.

Regular Evaluation of Processes
Fast paced evolution requires frequent reviews

It’s very easy for the pace of innovation to be faster than the growth of support structures.

Introduces the potential for:
• Gaps in certification
• Manual processes (toil)
• No longer relevant tests (tech debt)
Additionally, an important thought, but one that becomes more important year over year: Information Security Compliance, at all levels, forms the foundation of a resilient and reliable environment. It's easy to focus on individual services and applications and just trust that the OS is being taken care of. But when issues like Heartbleed or Spectre occur, having the infrastructure to test fixes and roll out updates quickly with minimal friction will do an enormous amount to reduce friction and keep your engineers from having to work nights and weekends to remediate an issue.
A project like this is _big_. And it takes a huge amount of work to get it over the finish line. This kind of certification process touches nearly every part of your organization in some way, and you have to build awareness of the processes and their importance in at every level.

Culture

It takes a village, city, country

OS Certification and Information Security Compliance is everyone’s concern.

Investment in processes up front reduces ongoing costs.

Shared responsibility with SME teams creates a culture of ownership.

Integration with post-mortem and new project processes ensures consistent evaluation.
Thank you!
The OS Certification Framework Team At LinkedIn:

Justin Anderson
Safia Anjum
Aniket Dhuri
Brandon Hastings
Hengyang Hu
Phil Hollenback
Franck Martin
Shinjo Melosh

Gaurav Pathak
Sean Patrick
Aditya Prakash
Kyle Reid
Asli Sareen
Ramodass Venkadasamy
Nishan Weragama
Rob West