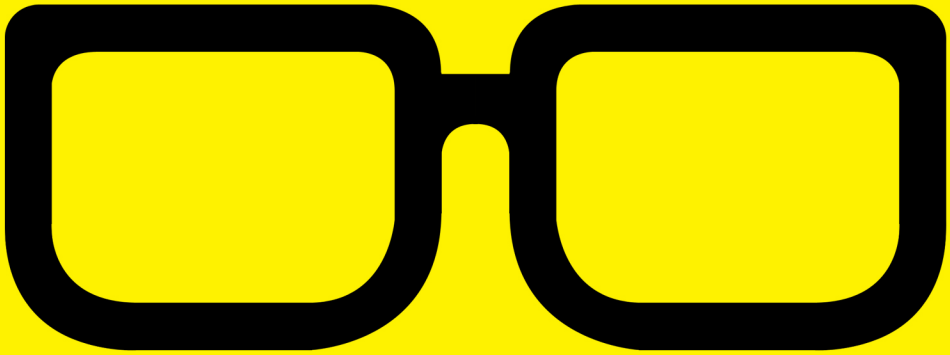
SPONSORED BY

GEEK GUIDE



An Architect's Guide: Linux for Enterprise IT

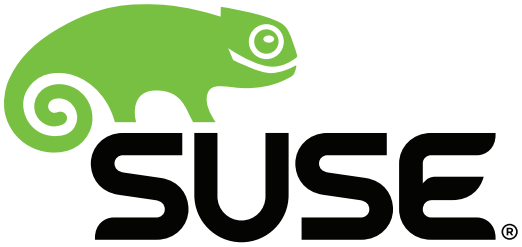
LINUX JOURNAL

Table of Contents

SOL LEDERMAN is a technical people-oriented professional with more than thirty years of broad experience in system administration, software design and development, technical support, training, documentation, troubleshooting and customer management. Sol currently divides his time between running IT for a software firm and providing a variety of tech services to the federal government.

GEEK GUIDES:
Mission-critical information for the most technical people on the planet.

About the Sponsor



SUSE, a Micro Focus company, provides and supports enterprise-grade Linux and open-source solutions with exceptional service, value and flexibility. With partners and communities, we innovate, adapt and deliver secure Linux, cloud infrastructure and storage software to create solutions for mixed enterprise IT environments. We help customers harness the benefits and power of an open enterprise that can empower their possibilities.

An Architect's Guide: Linux for Enterprise IT

SOL LEDERMAN

Introduction

Enterprises engaged in mission-critical computing, either on commodity or proprietary hardware, are choosing open-source Linux in increasing numbers. In this guide, I look at a number of factors driving adoption of Linux in the enterprise, including uptime, performance, high availability, administration and other drivers. In the context of what matters most in the enterprise, I discuss why Linux is the best choice in the enterprise and consider how SUSE has positioned its SUSE Linux Enterprise Server to serve the needs of the most demanding IT organizations.

I make the case here that, although there are a number of operating system choices for running web, application and database servers in small environments, Linux is the natural choice when business priorities include stability, scalability and high availability in a large and distributed computing environment.

In this guide, I consider the major requirements for traditional data-center infrastructure. In a second guide, I'll examine requirements for massive scaling and for deploying and managing cloud-native applications. These advanced DevOps requirements include:

- Cloud support.
- Virtualization beyond hypervisors (that is, containers).
- Agility (modules, packaging and cross-platform support via a common code base).

This guide discusses the requirements to create the necessary foundation that enables building out complex infrastructure, which I'll cover in the second guide.

What Matters in the Enterprise

Stability/Uptime/Resilience Stability, resilience and uptime are inter-related factors that imply high availability of a service. Specifically here, I'm considering high availability of a single physical or virtual server.

Stability implies that the operating system and its running processes crash rarely if ever. Stability is enhanced through

Live patching to fix kernel bugs that affect security, stability and data integrity is key to minimizing downtime.

comprehensive testing of operating system, software and hardware components (such as drivers) in the combinations in which they are to be used in production. Proactive and reactive application of system patches, especially kernel- and security-related patches, is also key to maintaining system stability. System hardening to protect the server from attacks is also important to maximizing stability.

Although stability is concerned with protecting the server from an unplanned outage, uptime also considers planned downtime. Live patching to fix kernel bugs that affect security, stability and data integrity is key to minimizing downtime. Live patching should not only allow for the application of a kernel patch without requiring a reboot, but the process also needs to have no impact on runtime performance, and the process must not interrupt any applications. Another factor in minimizing downtime is to extend operating system and service pack (patch) support to allow enterprises to upgrade servers on their schedules and not on their vendors' timeline.

Resilience is about getting a server back in operation and in a known good state quickly following an outage. Being able to take live snapshots of the running operating system and having the capability to restore the system

from a recent snapshot quickly ensures resilience in the face of operator error or other software problems. Another technology that can help greatly minimize downtime is persistent memory (NVDIMM) to make sensitive data available quickly after a reboot.

Performance Performance of a particular application or service depends on the running environment (for example, platform, operating system, software, network, hardware and other factors). An operating system that maximizes cross-platform support, especially with Windows environments, maximizes the likelihood that performance can be optimized by allowing system architects to choose the hardware and software environments that best support an application. Tight coupling of Windows and Linux operating systems on different hardware platforms improves performance and uptime of the aggregate workload. (I discuss Windows and Linux integration later in this ebook.) A common code base facilitates support for new platforms, further increasing choices for application deployment. Additionally, cross-platform support protects against vendor lock-in.

Performance also is improved by scalability and high availability (clustering).

Scalability Scalability through clustering ensures stability, uptime, resilience and performance in the face of increasing demands on computing resources. Viewed another way, scalability (if architected correctly) ensures high availability and failover capabilities while providing a steady supply of computational, memory, network, storage and other resources to meet ever-changing demands.

A key consideration in pursuing scalability is avoiding vendor lock-in. Although an enterprise may plan carefully for future scalability, undoubtedly technologies, hardware and platforms will change. An enterprise that is locked in to one vendor's operating system or hardware will face serious obstacles to scaling. Scalability ideally will allow for a heterogeneous computing environment, one that can be built from commodity hardware, and a scalability plan should provide a way to upgrade servers incrementally as they become obsolete. And, a scalable operating system will allow for large numbers of CPUs and a large amount of memory.

Also important in achieving scalability is a software-defined storage management solution to create enterprise storage using inexpensive servers and disk drives. Such storage must be distributed and flexible in providing access at the file, object and block levels. And, as scalability increases from terabytes to petabytes of clustered storage, continuous self-monitoring and management becomes critical to maintaining optimal storage performance.

Finally, as technologies move quickly toward more virtualization and geographic distribution of physical resources, it becomes increasingly important to architect infrastructure built on open operating systems with solid support for private and public cloud computing, containers and geo-clustering. Private cloud technologies, particularly OpenStack, are key to scalability and to high availability.

High Availability High availability builds on a foundation of scalability created through clustering and adds mechanisms to maintain uptime in the face of system and component failures. It's important to consider that

Private clouds are an integral part of an IT strategy to survive outages of different magnitudes.

failures can affect more than one or two systems; failures can be site-wide, as in the case of floods, fires, power outages, earthquakes and other disasters. Thus, mission-critical infrastructure must be clustered geographically to survive the loss of an entire site.

Private clouds are an integral part of an IT strategy to survive outages of different magnitudes. In particular, clouds built with the OpenStack free and open-source software platform (https://en.wikipedia.org/wiki/OpenStack) can provide availability in various failure scenarios. These include single or multiple failures of either stateful or stateless services. Availability is also maintained in either active/passive or active/active configurations. See http://docs.openstack.org/ha-guide/intro-ha.html for more information.

It is worth noting that the software-defined storage I mentioned previously serves as a foundation for highly available storage. When you create a redundant architecture, especially one with duplicated knowledge of the storage topology and decentralized access to objects, you eliminate single points of failure and, as a bonus, improve scalability. Ceph is a leading free and open-source technology for reliable

distributed storage, which is particularly well suited to high availability (http://docs.ceph.com/docs/master/architecture/#scalability-and-high-availability).

Security Important security features include:

- Running operating systems and software that have been audited, tested and certified against known attacks.
- Availability of security features: authentication methods, encryption, intrusion prevention (access control) and detection, backups, snapshotting/rollback capability, file integrity, checking tools, network analysis utilities and monitoring/logging utilities.
- Ongoing proactive and quick reactive response to security incidents.
- Prompt delivery of security updates.
- Access to tools to harden systems.
- Ability to lock down system networks via a packet-filtering firewall.
- Ability to encrypt confidential data.
- Extra protection against memory exploitation techniques via process hardening.
- Kernel-level access control (SELinux).

As technology advances exponentially, you no longer can think in terms of architecting computing environments that you expect to remain constant for years.

Beyond operating system and infrastructure security features, security certifications are central to developing a trusted computing environment. Leading certification includes FIPS 140-2 for cryptographic software (https://en.wikipedia.org/wiki/FIPS_140-2), common criteria security certifications (https://en.wikipedia.org/wiki/Common_Criteria) and FSTEC (http://www.globalsecurity.org/military/world/russia/fstec.htm).

Windows Integration As technology advances exponentially, you no longer can think in terms of architecting computing environments that you expect to remain constant for years. You must expect your infrastructure to grow and change. Consistent with this new way of thinking, you would be wise to create computing environments that support interoperability between software running on different platforms. And, given the strong presence of Windows, you should aim to create bridges between Windows and non-Windows platforms.

With mixed environments being the new normal and with the growth of virtualization, via virtual machines and through containers, you should consider

cross-platform virtualization as a strategy for supporting heterogeneous environments. Note that you can combine Linux and Windows in virtualized servers in two ways: a Linux server can host a Windows guest, and a Windows server can host a Linux guest. Note also the matrix of host and guest operating systems and CPUs according to Wikipedia (https://en.wikipedia.org/wiki/Comparison_of_platform_virtualization_software).

Some of the virtualization platforms that stand out for cross-platform support are Microsoft's Hyper-V hypervisor that can run Linux guests on x86 Windows platforms (https://en.wikipedia.org/wiki/Hyper-V) and Xen and KVM as Linux platforms that can host Windows guests.

Beyond just the ability to run a mixed Windows/Linux environment, you need to consider how to facilitate secure cross-platform monitoring and management. SSSD (https://en.wikipedia.org/wiki/System_Security_Services_Daemon) is a Linux package that manages access to remote directories and to authentication mechanisms. SSSD reconciles Active Directory users with Linux users. Samba is another technology in the authentication mix; it allows for secure Linux interoperability with the Windows environment, in particular for file and print services (https://www.samba.org).

In a mixed Windows/Linux environment, managing and monitoring both types of servers from a single console is highly desirable. Being able to deploy Windows and Linux patches from a Windows server is a huge time-saver for system administrators as is managing scheduled maintenance from one console.

Ease of Deployment, Management and Upgrades

Computing environments are increasing in complexity at an accelerating rate. I've discussed a number of leading-edge technologies that are crucial to deploy in mission-critical computer environments: live patching, snapshots, rollbacks, local- and geo-clusters, cloud computing, a variety of security tools, and cross-platform management and monitoring tools to name a few. Having tools that manage (that is, abstract away) the complexities of the ever-increasing list of sophisticated features is no longer merely nice but absolutely necessary.

Tools that manage installed software and patches, plus system, network (including firewall), printer, security and configurations are invaluable. Creating and managing virtual machines is another important function. These tools also should provide monitoring services as well as system provisioning services. And, they need to manage resources across physical, virtual, clustered and cloud environments. Finally, comprehensive reporting of hardware and software inventories is a big advantage.

An often-overlooked aspect with regard to easing deployment efforts is to adopt an operating system that has an extended support life. The longer the support period, the lower the likelihood that issues will surface that can't be resolved. Thus, extended support leads to greater peace of mind. Critical patches, of course, need to be applied to ensure stability and security of the computing environment. But, even in the patching process, if IT staff can apply the current set without needing to install multiple previous sets, that is a huge win.

Support Support is very important in the complex and evolving technology arena, especially for mission-critical services where high availability is not negotiable. There are too many technologies for any team of IT professionals to master, and even if an organization could afford to hire a diverse staff to handle the difficult and obscure problems, it may be more cost effective to pay for support for those difficult issues or for issues that might otherwise require a major effort to resolve independently. And, being able to consult with a trained engineer within an hour to help resolve a high-priority issue that disrupts service and has no workaround warrants paying for support.

Note that paying for support may make as much sense for open-source operating systems as for proprietary ones. TechTarget looks at a number of variables in the "pay for support or not?" equation in its article "Should you pay for support on all Linux servers in your data center?" (http://searchdatacenter.techtarget.com/tip/Should-you-pay-for-support-on-all-Linux-servers-in-your-data-center). The article makes the case both for paid subscription support and for self support.

Why Is Linux the Best Choice in the Enterprise?

The Linux Foundation's "2014 Enterprise End User Report" identifies Linux user trends for the world's largest enterprises (https://www.linux.com/publications/2014-enterprise-end-user-report). The report's executive summary notes that "Cloud computing and security drive increasing

adoption of Linux by the world's largest enterprises." The report summarizes the findings of "responses from 774 individuals, 262 of whom represent organizations with sales of $500 million plus or 500+ employees".

The top enterprises have adopted Linux for their mission-critical applications, and we should consider why they have done so.

Enterprises focused on high performance and high availability should take note of this finding:

> One of the strongest trend lines in our surveys has been the growth in the use of Linux for mission-critical workloads relative to other operating systems. There has been a big uptick in this number, from a healthy 60 percent in our 2011 survey to 72 percent [in 2014].

Features, security and lower TCO were found to be the top three drivers for Linux adoption, according to the survey:

- Feature set: 74%
- Security: 69%
- Lower TCO: 69%

No vendor lock-in and internal experience with Linux also were listed as top drivers, although figures were not provided for those.

Enterprises were upbeat about Linux; 87% were planning to add Linux servers in 2014 and 82% the

following year.

Most of the largest Linux users believed Linux to be the most secure platform:

- More secure: 75%
- About the same: 17%
- Less secure: 2%
- Don't know: 3%

Given the high marks for Linux in performance, security, features, TCO and no vendor lock-in, it's no surprise Linux dominated the cloud platform space:

- Linux: 75%
- Windows: 23%
- UNIX: 2%

Finally, it's no surprise that Linux has grown at the expense of Windows deployments (note that some enterprises deploy both Linux and Windows environments, so the numbers don't add up to 100%):

- Linux: 65% (2011); 79% (2014)
- Windows: 45% (2011); 36% (2014)

How SUSE Linux Enterprise Server Focuses on What Matters Most

More than two-thirds of the Fortune Global 100 use SUSE Linux Enterprise (https://www.suse.com/newsroom/post/2016/new-suse-linux-enterprise-12-service-pack-2-speeds-innovation-with-reliability).

"SUSE Linux Enterprise 12 in 90 seconds" is an introductory video (https://www.youtube.com/watch?v=hEV2Y_P2dLM) that succinctly highlights SUSE's focus on the technologies that enterprise Linux users most need. Transcribed from the video:

> SUSE Linux Enterprise is a highly-reliable, scalable and secure server platform designed to run enterprise-class IT services in physical, virtual or cloud infrastructure. Also, it provides full system rollback, high availability and live kernel patching to increase uptime. You can even fail over across any distance in the world. And, its flexible virtualization choices like container support and easy-to-use tools help improve operational efficiency. SUSE Linux Enterprise 12 further raises the bar in helping organizations accelerate innovation, enhance system reliability, meet tough security requirements, adapt to new technologies and offer public cloud services.

SUSE Linux Enterprise delivers a large set of critical features (https://www.suse.com/products/server/features). Next, I highlight those features for which SUSE provides services that particularly excel in the Linux and UNIX spaces.

SUSE's Enterprise Storage 4 is designed to reduce a number of storage frustrations, including overall cost, performance concerns, complexity/fragmentation, lack of scalability, legacy vendor lock-in and others.

Highly reliable: SUSE Linux Enterprise Real Time Extension provides a number of features to improve the performance and reliability of time-sensitive mission-critical applications (https://www.suse.com/products/realtime). Features include the ability to reduce system latency and ensure predictability, shielding key hardware resources from extraneous threads and processes and assigning critical processes to run on them.

Scalable: two key components of scalability are high availability via clustering (discussed later) and software-defined storage (https://www.suse.com/solutions/software-defined-storage). SUSE's solution is built on open-source Ceph technology that provides self-management and self-healing. SUSE's Enterprise Storage 4 is designed to reduce a number of storage frustrations, including overall cost, performance concerns, complexity/fragmentation, lack of scalability, legacy vendor lock-in and others.

Secure: SUSE provides a number of security-related resources (https://www.suse.com/support/security). These include security advisories and updates, SUSE Linux Enterprise security certificates and features, SUSE Linux

Enterprise Server download verification, flaw remediation process and more.

Physical infrastructure: SUSE offers high kernel limits for maximizing the power of mission-critical servers. SUSE Linux Enterprise 12 is certified to support 64TB of RAM on x86_64 hardware and 8,192 logical CPUs. See SUSE's technical information page to see other kernel limits as well as features supported in Btrfs (for system snapshots and rollback) and in other filesystems: https://www.suse.com/products/server/technical-information.

Virtual infrastructure: SUSE supports both KVM and Xen as hypervisors. SUSE Linux Enterprise guests are optimized in KVM, Xen, Hyper-V and ESX environments. Leading container technologies LXC and the open-source container engine Docker are fully supported. These virtualization choices avoid vendor lock-in (https://www.suse.com/solutions/server-and-application-virtualization).

Cloud infrastructure: SUSE's OpenStack Cloud framework automates the provisioning and removal of services to scale resources efficiently via rules-based scheduling (https://www.suse.com/products/suse-openstack-cloud/features/cloud-infrastructure-management). Template-driven orchestration of multiple composite cloud applications manages servers, floating IPs, volumes and other components allowing for software-driven cloud management.

Full system rollback: Open Horizons Magazine reports on System Rollback in SLES12 (http://ohmag.net/?p=509). A default OS installation and the use of the new default Btrfs filesystem for root enables rollback by default. There's no

configuration work needed even to boot from a snapshot. The article includes a good introduction to Btrfs and shows how to work with snapshots. SUSE also has an excellent white paper on rollback and its impact on data-center uptimes: https://www.suse.com/docrep/documents/kluoursc2k/mitigating_the_risk_of_downtime_with_rollback_wp.pdf.

High availability: SUSE's Linux Enterprise High Availability Extension is a mature (fifth-generation) industry-leading open-source HA solution (https://www.suse.com/products/highavailability). The offering is an integrated suite of open-source clustering technologies for creating physical and virtual Linux clusters. The suite allows administration of Linux clusters from the command line, from a GUI or from a browser.

Live kernel patching: SUSE Linux Enterprise Live Patching applies kernel patches to the system without interrupting or slowing the kernel or any application (https://www.suse.com/products/live-patching). Live Patching provides the benefit of making it easy to install critical security updates without needing to schedule a downtime. Richard Fichera recently blogged about live patching now being supported in production in "Linux vs. Unix Hot Patching—Have We Reached The Tipping Point?" (http://blogs.forrester.com/richard_fichera/16-05-20-linux_vs_unix_hot_patching_have_we_reached_the_tipping_point):

> Early versions of Linux hot patching have been around for several years, most notably in a company called Ksplice, acquired a few years ago by Oracle. But the real change happened earlier this year when SUSE declared that its

hot-patch capability, kGraft, previously in limited availability, was now in GA, suitable for all production workloads.

Fail over across any distance in the world: geo-clustering for SUSE Linux Enterprise High Availability Extension protects workloads from unplanned downtime caused by site or regional failures (https://www.suse.com/products/highavailability/geo-clustering). Rules-based failover allows for automatic and manual transfer of workloads. Physical and virtual clusters can be deployed across data centers.

Container support: virtualization drastically reduced the time to bring up a server, and containers reduced deployment time even further. SUSE customers can build private on-premises registries to host their own container images (which SUSE provides from a verified and trusted source). SUSE also provides easy-to-use tools to simplify deployment and management of containers (https://geekguide.linuxjournal.com/content/tame-docker-life-cycle-suse).

Easy-to-use tools: three SUSE Linux Enterprise Server features that greatly simplify system deployment and management are AutoYaST (https://www.suse.com/documentation/sles-12/singlehtml/book_autoyast/book_autoyast.html), Unattended Upgrade (https://www.suse.com/docrep/documents/e62v58s1ge/unattended_upgrade_feature_in_sles_guide.pdf) and SUSE Manager Management Pack for Microsoft System Center Operations Manager (https://www.suse.com/products/suse-manager/management-pack). AutoYaST installs SUSE Linux Enterprise Server systems automatically and

SUSE Manager Management Pack for Microsoft System Center Operations Manager allows Windows system administrators to monitor and patch both Windows and Linux servers from one console.

unattended. At European Space Operations Centre, "YaST and AutoYaST are being used to create, maintain, and automatically deploy different configurations of SUSE Linux Enterprise Server for different requirements" (http://news.softpedia.com/news/European-Space-Operations-Centre-Now-Runs-on-SUSE-Linux-Enterprise-Servers-45572.shtml). Unattended Upgrade complements AutoYaST's install function by performing unassisted OS upgrades. SUSE Manager Management Pack for Microsoft System Center Operations Manager allows Windows system administrators to monitor and patch both Windows and Linux servers from one console.

Meet tough security requirements: SUSE has achieved FIPS 140-2 certification for OpenSSL for SUSE Linux Enterprise Server 11 SP2, various Common Criteria security certifications and FSTEC certification for protection of Russian technology on SUSE Linux Enterprise Server 11 SP3. Additionally, SUSE provides comprehensive system-hardening configurations and a number of leading-edge security features. More information is available at the SUSE security page: https://www.suse.com/support.security/certifications.html.

Adapt to new technologies: SUSE lists ten enhancements to SUSE Linux Enterprise 12 SP2 in a recent article that support the use of new technologies (https://www.suse.com/newsroom/post/2016/new-suse-linux-enterprise-12-service-pack-2-speeds-innovation-with-reliability). These enhancements include ten-fold increase in packet processing via improvements in software-defined networking, more agile support for SAP applications, reduced downtime and improved performance via persistent NVDIMM memory, support for new hardware and more.

Offer public cloud services: SUSE Enterprise Server is available in more than 50 public clouds, including Amazon AWS, Google GCE and Microsoft Azure (https://www.suse.com/partners/cloud-service-providers/alliance-partners.html). These partnerships certify joint solutions and help customers extend their private cloud infrastructure. Global partners serve North America, EMEA (Europe, Middle East and Africa), Asia Pacific and Latin America.

Conclusion

I hope this guide serves you well as a reference to the important considerations in developing or growing a mission-critical IT infrastructure. I further hope this guide leads you to Linux as the best operating system for building out your computing environment and to SUSE Linux Enterprise Server as a fully featured and mature, yet leading-edge, partner in your computing endeavors.■