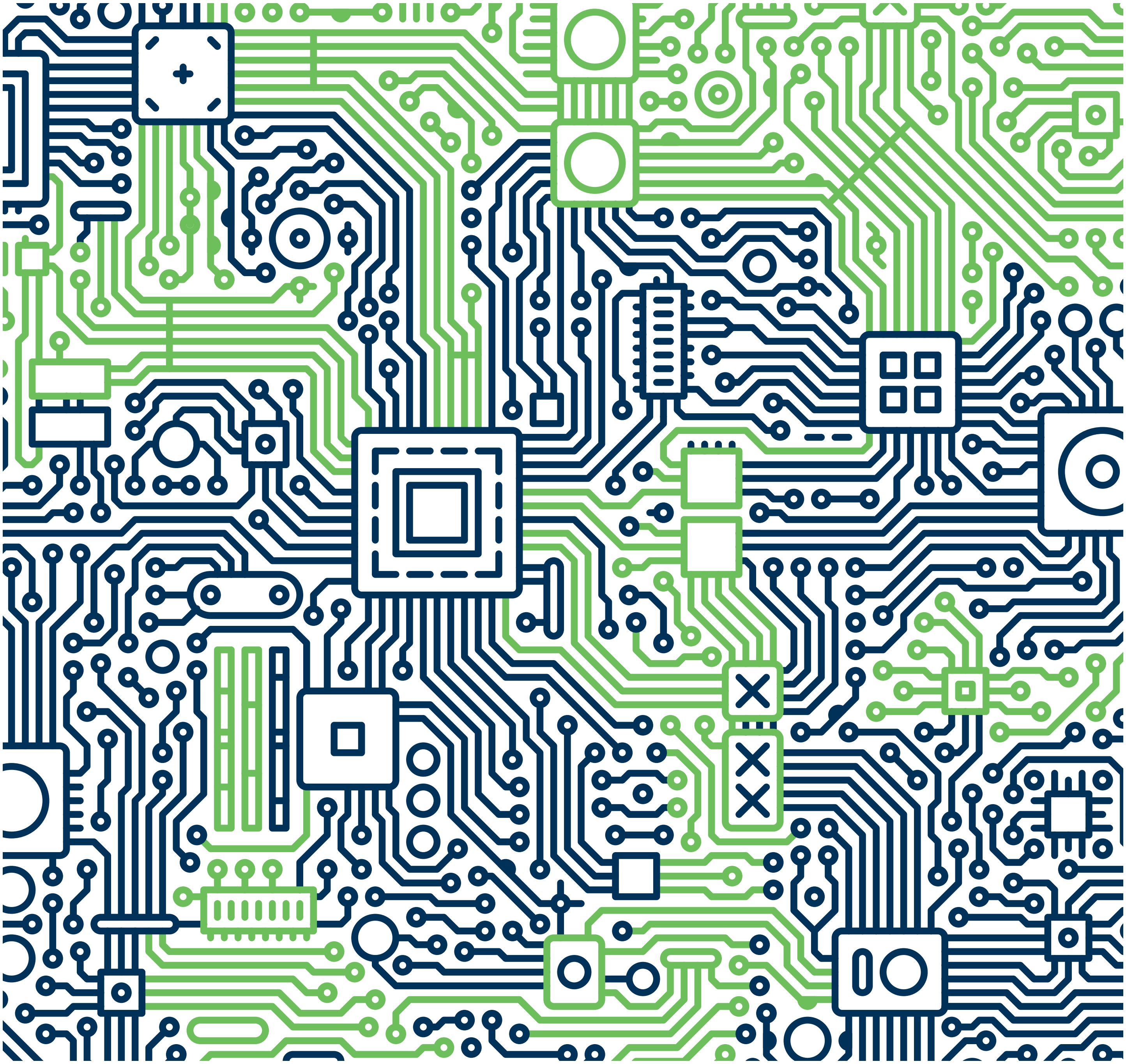
WHITE PAPER



Managing the New IT

A new generation of IT technologies has led to a revolution in IT management. Today's IT infrastructure management systems put the emphasis on automa-tion, remote configuration and rapid deployment.

In the old days, system administrators spent a majority of their time watching file servers, managing user accounts and ensuring network connectivity, but today's infrastructure is a busier and more exotic place.

Applications hide in containers, systems hide in other systems, new configurations appear and disappear with a single mouse click, and every file is a potential threat. It is no wonder that CIOs and IT managers are looking for new tools and a new approach that will bring harmony, safety and economy to precious IT assets in changing times. Welcome to the new world of IT infrastructure management.

How We Got Here

In the early years of computers, an organization owned a single computer and had a staff of several experts watching it (see Figure 1). New software was rarely installed and was often managed directly by the hardware vendor. Viruses and malware that we know today didn't even exist, in fact, neither did computer networks as we know them today.

The development of the personal computer and the rise of networking protocols led to small workgroups, often gathered around a single file and print server. These networks were eventually gathered into enterprise networks (see Figure 2), sometimes with remote sites linked through a WAN connection. Networks grew larger and gained new features, but at a fundamental level, they were still an extension of the original mainframe model. Each computer was managed separately, every hardware system had exactly one operating system running on it, and the number of hardware systems was constrained by the area of available floor space.

This model served the IT industry for many years, but it was eventually overtaken by some innovative new technologies that forever changed the face of the infrastructure. The most revolutionary development to date is the emergence of virtualization and container technologies, which have unglued the software infrastructure from the limitations of the hardware environment. A single hardware system might contain several virtual systems, each deployed for a different role. Hardware resources are gathered into data centers, where the resources might support dozens or even hundreds of virtual machines (VMs) or containers.

The result is that, rather than being tied to a specific hardware system on a one-to-one basis, operating systems inhabit an abstraction layer that floats above the hardware environment (see Figure 3). The resulting model, which is known as software-defined

Figure 1. The first commercial computers were isolated mainframes administered by a team of experts (© Lawrence Livermore National Laboratory).

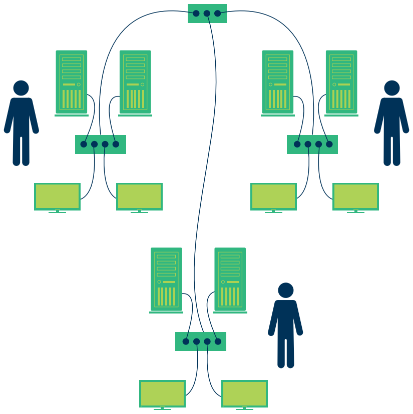


Figure 2. The earliest workgroups morphed into enterprise networks, but the basic principle remained the same as with the early mainframes: Every hardware system ran exactly one operating system.

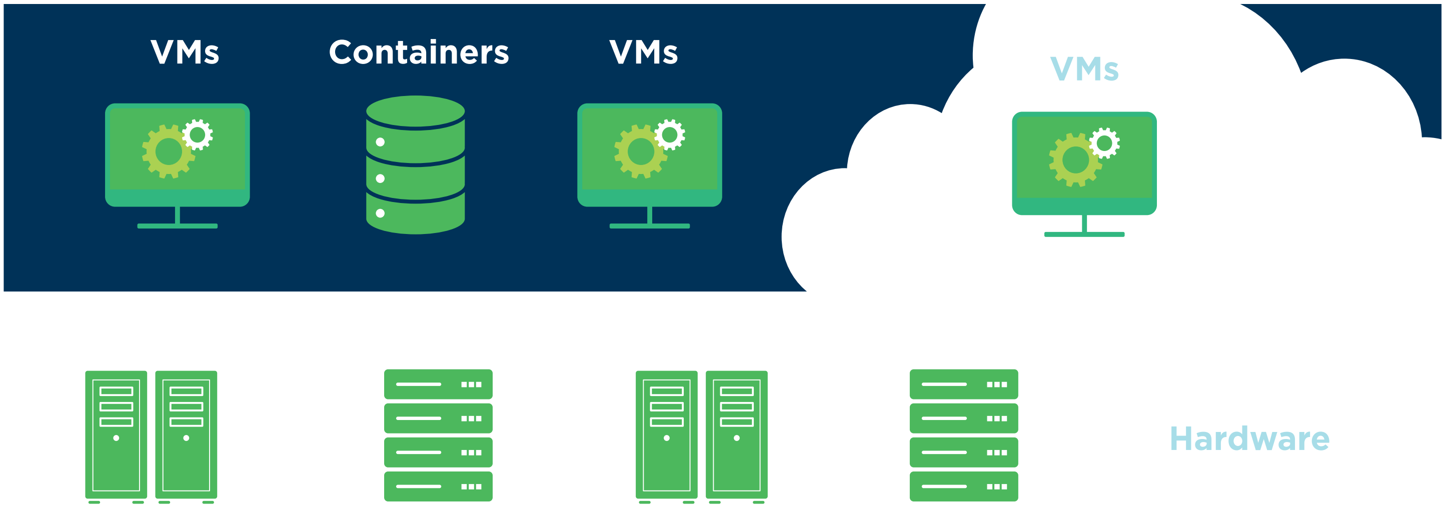


Figure 3. The new IT offers a radically different approach: VMs and isolated container environments operate freely in an abstraction layer that floats above the hardware.

infrastructure, means that the whole network of resources can expand, contract and transform to respond to the changing needs of the environment. VMs spin up to perform specific tasks and spin back down, absorbing workloads as circumstances require. Cloud computing further expands the promise of software-defined infrastructure, offering the possibility of virtual systems that require no hardware footprint at all in the data center. Meanwhile, IoT units and edge devices add still more complexity to the configuration.

As you can imagine, in this dynamic environment, where software floats independently above the hardware and systems deploy on short notice to respond to changing needs, the problem of tracking, managing and securing operating system and application resources expands exponentially. Fortunately, a new generation of automated tools for remote management has emerged to contend with the complexity of managing deployments in a software-defined infrastructure. At the same time, a new generation of malware and intrusion techniques has heightened the need for automated security updates and systematic auditing of system resources.

A new generation of malware and intrusion techniques has heightened the need for automated security updates and systematic auditing of system resources.

The rise of software-defined infrastructure, the growing importance of automation in the field of system administration and a heightened need for defensive measures in response to a new generation of cyber threats are driving innovation in IT infrastructure management.

Modern IT infrastructure management systems focus on features such as:

+ **Virtualization and containers**
+ **Deployment and remote configuration**
+ **Software installation and updates**
+ **Auditing and verification**
+ **Automation**

The goal of modern IT infrastructure management is to address all these issues while simultaneously contending with the expanding complexity of the IT landscape. Management techniques such as DevOps evolved to address the needs of IT infrastructure management in a way that encourages rapid development with minimal downtime (see the box entitled “DevOps”). The following sections take a closer look at the challenges of modern IT infrastructure management.

Virtualization and Containers

Virtualization and container technologies are a driving force in the evolution of software-defined infrastructure. Today’s enterprise must have management tools that can accommodate the power and flexibility of container and virtual environments. Admin tools in the software-defined infrastructure environment must offer strong support for OpenStack, Docker, Kubernetes and other orchestration systems.

The best management systems offer a uniform view of the landscape that allows for oversight of this diverse assortment of systems running on bare metal, VMs and containers located in your data center, at the edge or in the cloud, without burdening the user with details (see Figure 4).

Deployment and Remote Configuration

The flexible software-defined environment, which enables the whole landscape to expand, contract and transform to meet evolving needs, requires a sophisticated approach to deploying, configuring and decommissioning systems. The management environment should provide a means for automated deployment, with tools that enable the admin to preconfigure a complete system in advance, and then launch the installation with a few mouse clicks. A library of ISO images (for container, VM and bare-metal installations) should be close at hand for easy deployment and orchestration.

Software Installation and Updates

Insecurity is frequently embedded within the software environment. In addition to lurking malware and the presence of unauthorized files that could lead to intrusion, insecurity exists in the presence of exploitable bugs in out-of-date software.

IT infrastructure management systems should maintain active control of how and when new software is installed. Updates should occur systematically from reliable sources and no software from unauthorized sources should reach the system. Locking down software installation also promotes uniformity, which improves security and reduces administration costs.

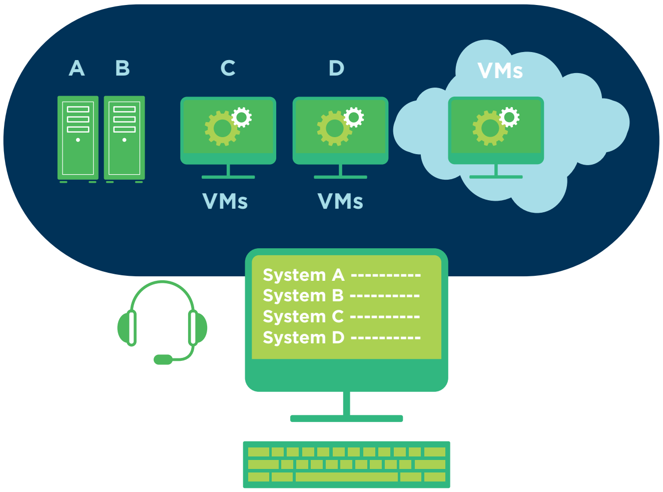


Figure 4. The management environment oversees containterized, virtual and bare-metal systems from a single user interface, offering a unified logical view of the infrastructure that hides platform differences.

Auditing and Verification

In today's IT infrastructure, security is not an abstract objective; it is an active state of mind. Auditing tools ensure that all systems remain in compliance with external security standards and internal policies. You can also use automated auditing to look for unauthorized changes to any managed system.

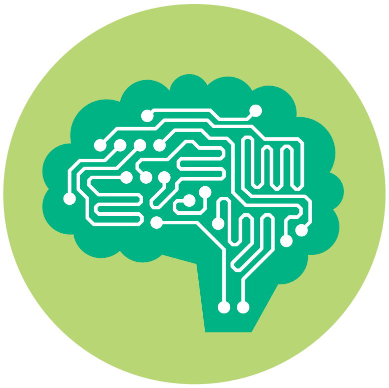
Automation

The ambitious new objectives of today's IT infrastructure management systems are made possible through the power of automation.

DevOps

The term DevOps refers to a collection of management and programming practices that focuses on encouraging closer collaboration between development and operations teams. The DevOps model rejects the paradigm of long development cycles and independent deployment, striving instead for a culture of continuous integration—with coding, testing, deployment and feedback occurring in a tight loop for maximum efficiency and minimal downtime.

With its strong emphasis on orchestration, remote configuration and automation, the modern IT infrastructure as described in this paper is a DevOps friendly environment.



In today's IT infrastructure, security is not an abstract objective; it is an active state of mind.

Automation that is built into the structure of everyday tasks, such as deployment, configuration, auditing and software installation.

A full-featured IT management infrastructure should also provide a means for the admin to expand the power of the system through custom scripts and extensions.

Platform Independence

With the myriad of available tools and the rapid rate of change within the IT industry, many modern solutions put the focus on avoiding vendor lock-in. Tools or services that limit the user's future choices ultimately cost more and constrain flexibility that might one day be needed for efficient growth. To avoid vendor lock-in:

- **Use open source tools with a common codebase to allow for easy migration.**
- **Aim for flexibility: Don't build your infrastructure in a way that will require future expansion to center on a single vendor environment.**

In addition to providing flexibility for future expansion, platform independence also saves money because a locked-in environment is a monopoly that is vulnerable to non-competitive pricing and planned obsolescence.

IT Infrastructure Management: What You Need to Know

IT infrastructure management poses a challenge for the IT team and this challenge requires a new generation of better and more powerful management tools. The proliferation of virtual and container-based systems—combined with the complications of contemporary security, the promise of automated configuration and the need for vendor-independent cloud support—require tools that can respond to the possibilities of the environment, lock down security and manage complexity. Are your management tools ready for the future? Ask yourself:

- **Does the solution let the user administer hardware-based systems, virtual systems and containers?**
- **Can you deploy, manage and decommission systems through a single user interface?**
- **Does the solution lock down updates and installation sources?**
- **Does the solution offer automated auditing?**
- **Does the solution make effective use of automation to extend the power of a single admin and provide a programming interface for integrating custom scripts and programs?**
- **Does the solution offer long-term platform independence or could it lead to vendor lock-in?**

Embracing the latest developments in IT can lead to improved efficiency and significant cost savings, but be aware that you will need IT infrastructure management solutions that can manage the increasing complexity and exploit the benefits of software-defined infrastructure. If you are building your IT management tools for the future, look for a solution that is ready for the challenge of today's IT infrastructure.

For more information, contact your local SUSE Solutions Provider, visit us online or call SUSE at:

1-800-796-3700 (U.S. and Canada)
1-801-861-4500 (Worldwide)

SUSE
Maxfeldstrasse 5
90409 Nuremberg
Germany

www.suse.com