White Paper

IT Infrastructure Management

Managing Compliance for Linux Systems with SUSE Manager 4

SUSE

Managing Compliance for Linux Systems with SUSE Manager 4

SUSE Manager 4 is a best-in-class open source infrastructure management solution that lowers costs, enhances availability, and reduces complexity for lifecycle management of Linux systems in large, complex, and dynamic IT landscapes. You can use SUSE Manager 4 to configure, deploy, and administer thousands of Linux systems running on hypervisors, as containers, on bare metal systems, on IoT devices, and on third-party cloud platforms. SUSE Manager 4 also enables you to manage virtual machines and enforce key best practices to ensure compliance through the whole lifecycle of all your Linux systems—from bare metal to containers, for both internal company policies and external regulations.

Many industries and governments require compliance with security standards to ensure security, identity, confidentiality, and data integrity. These standards specify a minimum-security level and also mandate measures such as logging and auditing to reveal any hints of unauthorized use.

Some of the most widely adopted standards are:

- *Sarbanes-Oxley (SOX)—a US standard intended to improve confidence in financial reporting and accountability of publicly traded companies*
- *HIPAA—a set of US regulations primarily associated with maintenance and privacy of medical records*
- *PCI DSS—an independent set of worldwide standards governing credit card transactions*
- *PIPEDA—Canada's Personal Information Protection and Electronic Documents Act*
- *Several European Union directives on data protection and company law*

This complicated landscape became even more so in May 2018 with the arrival of the European Union General Data Protection Regulation (GDPR). GDPR, which applies to any organization serving individuals based in the European Union, introduces new compliance requirements for data control, security, due diligence, risk mitigation, and breach notifications.

In addition to external regulations, system administrators also have to contend with company policies designed to ensure a minimum level of security, reporting, and accountability. Policies might specify an update schedule or declare which versions of applications are authorized to run on which systems.

The need to scale these external and internal compliance requirements across a whole company can become a massive undertaking that requires significant staff time. SUSE Manager 4 eliminates the time and expense of compliance tracking by enforcing configuration control, automating auditing and alert notification, locking down package updates, working with Kernel Live Patching, and placing all the necessary information at your fingertips.

See It All

SUSE Manager 4 offers a single user interface for managing the complete lifecycle of all your Linux systems, including virtual machines, containers, and bare metal systems running in the cloud or on site. You only need to learn one tool to keep watch over deployments, configurations, upgrades, and other significant events in the life of your Linux systems.

The configuration, auditing, and automation features of SUSE Manager 4 make it easy to keep your systems in compliance. You can predefine a complete system configuration and watch for unauthorized changes automatically. SUSE Manager 4 also checks for vulnerabilities defined through the Common Vulnerabilities and Exposures (CVE) list or OpenSCAP (Figure 1).

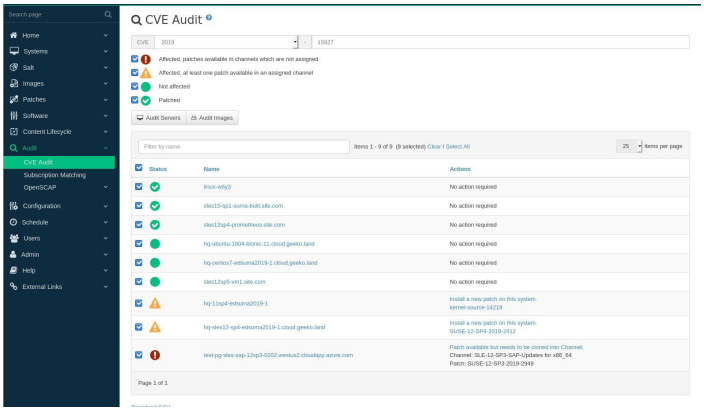

Figure 1. *SUSE Manager 4 can quickly check to see if any deployed servers include CVE vulnerabilities.*

The powerful tools collected within the SUSE Manager 4 user interface help you secure your Linux systems and keep them in continuous compliance with external standards and internal requirements. Read on for a closer look at how SUSE Manager 4 ensures compliance through configuration control, auditing, patch management, and security monitoring.

Uniform Configuration with Salt

The Salt configuration management system built into SUSE Manager 4 enables you to predefine a complete system configuration through centrally managed state files. Whenever a Salt client (called a Salt minion) running inside a managed system receives a state file, it reconfigures the host to make it match the description. Collections of state files that describe complete configurations of systems or services are often bundled as Salt formulas.

SUSE Manager 4 comes with several preconfigured Salt formulas (Figure 2) and enables you to create custom formulas that can be easily parametrized through ordinary web forms. You can apply formulas to single systems or whole groups. Salt also enables you to execute Action Chains—sequences of actions that implement a complex configuration task but are executed as a single command. Salt formulas and Action Chains enable you to create a compliant prototype system in a controlled setting and replicate it to other systems automatically, ensuring uniformity and full compliance across the Linux landscape.

Figure 2. *The image-synchronize Salt formula from the SUSE Manager 4 Formula Catalog.*

Auditing

You can create an inventory of the contents of your Linux systems and then use SUSE Manager 4 to easily identify noncompliant software that should not be installed on a system. SUSE Manager 4 also checks whether all software on the system is up to date, manages patch levels automatically, and sends daily notifications listing any noncompliant systems (Figure 3).

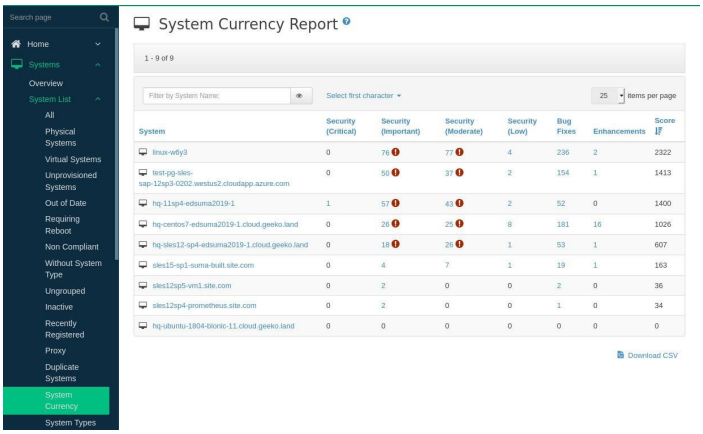

Figure 3. *SUSE Manager automatically generates status reports on noncompliant systems.*

Patch Management

SUSE Manager 4 controls and automates software installations and updates. You can define software channels that group packages by application or use case. A managed system can only receive updates and patches through a secure channel. The channel system in SUSE Manager 4 enables you to guarantee the source of any package or patch installed on any managed system, ensuring that all systems are free of noncompliant software.

Flexibility and Interoperability

SUSE Manager 4 offers efficient automation to reduce errors and delivery times. Detailed reports are available at every step to verify the state of compliance with external standards and internal corporate policies. You can manage all your Linux assets from a single interface, with automated reporting and improved visualization—regardless of whether those systems are IoT edge devices, containerized workloads, Kubernetes clusters, traditional on-metal servers, or virtual machines. SUSE Manager 4 also includes programming interfaces that enable you to control the features of your landscape using custom scripts.

Lock Down and Keep Watch

SUSE Manager 4 automates Linux configuration, patching, and management to provide a unified management infrastructure. The SUSE Manager 4 solution enforces key best practices to ensure compliance through the whole lifecycle of all your Linux systems—from bare metal to containers, for both internal company policies and external regulations. You can specify a predefined configuration and customize it as needed for a uniform and fully compliant Linux landscape. SUSE Manager 4 also watches for changes that could signal unauthorized access and locks down the package installation process to ensure that only compliant software reaches your network (Figure 4).

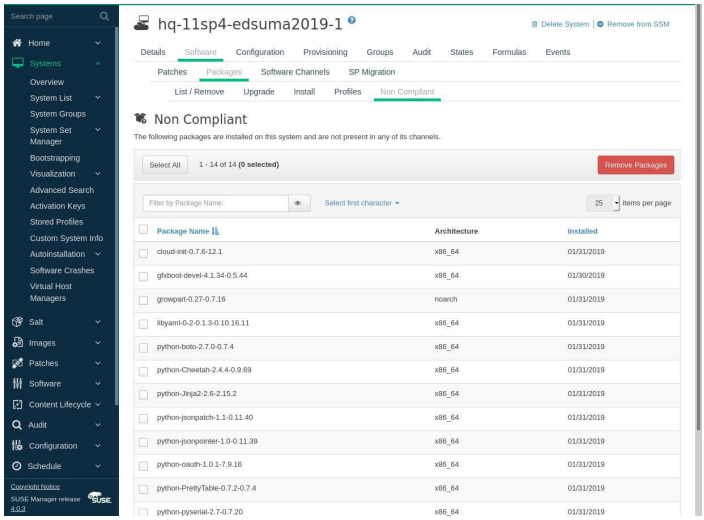

Figure 4. *SUSE Manager 4 makes it easy to remove noncompliant software packages.*

You can also use SUSE Manager 4 to watch for vulnerabilities defined through the CVE list or the OpenSCAP protocol. If you are looking for a way to organize and automate the compliance process to save money and workforce time, take a closer look at the compliance features of SUSE Manager 4.

Live Kernel Patching

With SUSE Manager 4, you gain even more control over compliance via projects and systems that include live patching. Through this, you can validate that all of your patches work before they are promoted (Figure 5), which enables you to move content independent of system registrations.

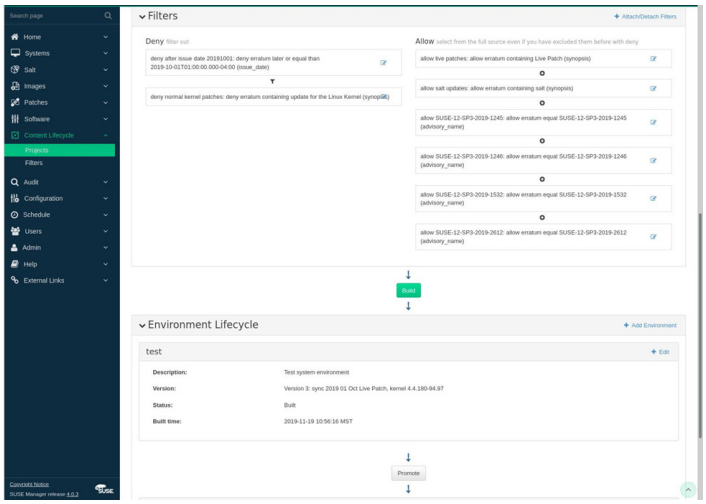

Figure 5. *Using filters to validate patches for live patching a kernel.*

Filters are used to make this happen. For example, you could deny any kernel patch that does not meet a specific timeframe or filter out any patch that would require a reboot. This enables you to make sure a build won't fail because of a problematic patch. In the case of live patching, you can define the time period for a specific kernel lifecycle with live patching and control when you want to reboot.

Additional contact information and office locations:
www.suse.com

www.suse.com