Solution Flyer

SUSE Manager

Managing Compliance for Linux Systems with SUSE® Manager

SUSE® Manager automates Linux configuration, patching and management to provide a unified management infrastructure. SUSE Manager 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.

SUSE Manager at a Glance:

SUSE Manager eliminates the time and expense of compliance tracking by enforcing configuration control, automating auditing and alert notification, locking down package updates and placing all the necessary information at your fingertips.

- **Products:**
  SUSE Manager

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 U.S. 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 which 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 eliminates the time and expense of compliance tracking by enforcing configuration control, automating auditing and alert notification, locking down package updates and placing all the necessary information at your fingertips.

See It All

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

The powerful tools collected within the SUSE Manager 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 ensures compliance through configuration control, auditing, patch management and security monitoring.

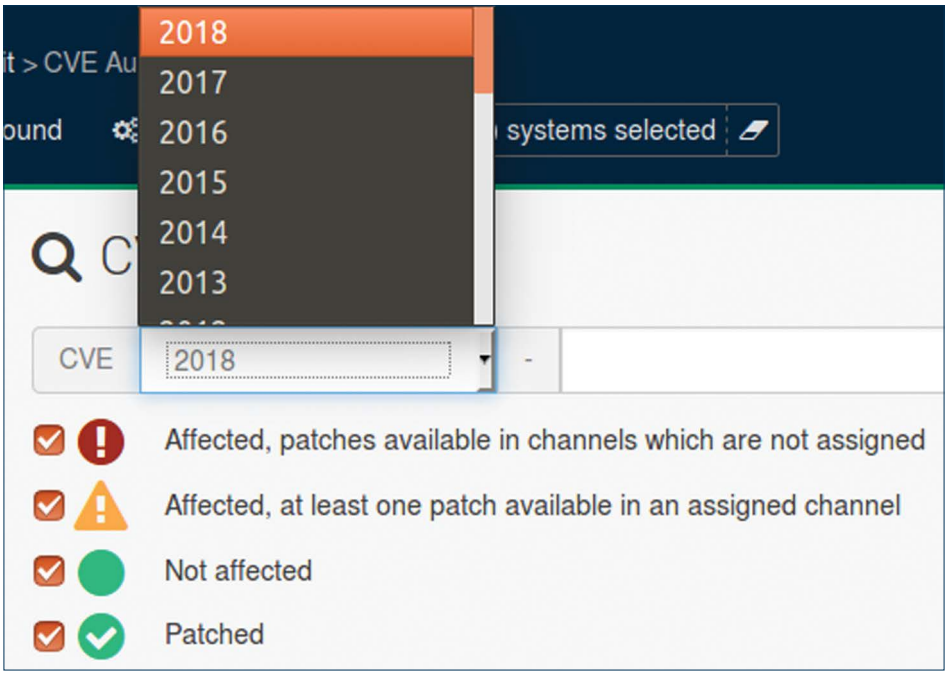


Figure 1. SUSE Manager watches for vulnerabilities and shows the status of each system.

Uniform Configuration with Salt

The Salt configuration management system built into SUSE Manager 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. Figure 2 shows how systems are grouped for easier management.

SUSE Manager comes with several preconfigured Salt formulas and allows you to create custom formulas that can be easily parametrized through ordinary web forms. You can apply formulas to single systems

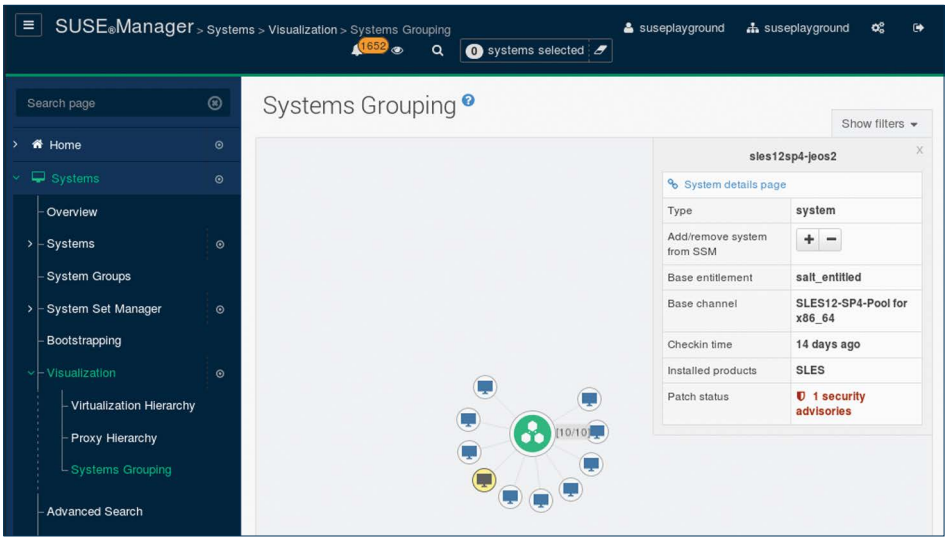


Figure 2. SUSE Manager allows you to group systems for more efficient management.

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 let you 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.

Auditing

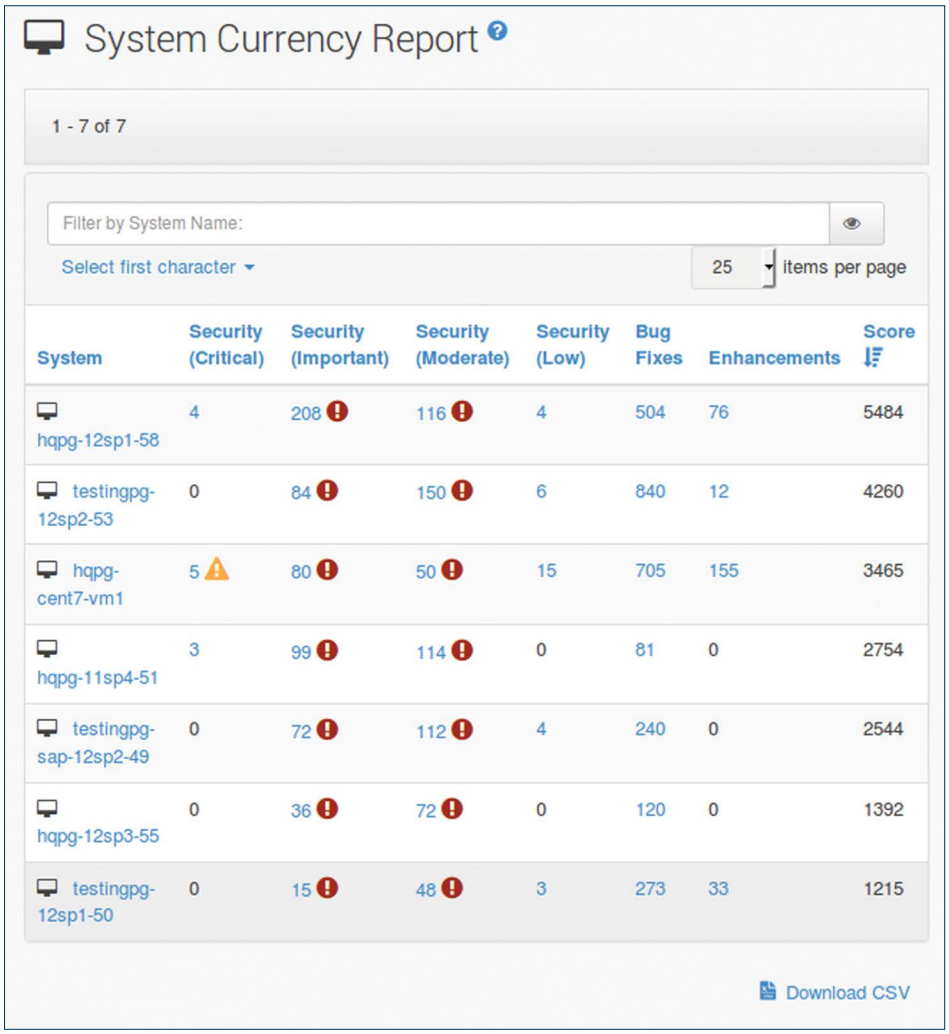
You can create an inventory of the contents of your Linux systems, and SUSE Manager will allow you to easily identify non-compliant software that should not be installed on a system. SUSE Manager also checks whether all software on the system is up to date, manages patch levels automatically and sends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

Patch Management

SUSE Manager 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. SUSE Manager's channel system lets you guarantee the source of any package or patch installed on any managed system, ensuring that all systems are free of non-compliant software.

Flexibility and Interoperability

SUSE Manager 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 also includes programming interfaces that let you control the features of your landscape using custom scripts.



System	Security (Critical)	Security (Important)	Security (Moderate)	Security (Low)	Bug Fixes	Enhancements	Score
hqpg-12sp1-58	4	208	116	4	504	76	5484
testingpg-12sp2-53	0	84	150	6	840	12	4260
hqpg-cent7-vm1	5	80	50	15	705	155	3465
hqpg-11sp4-51	3	99	114	0	81	0	2754
testingpg-sap-12sp2-49	0	72	112	4	240	0	2544
hqpg-12sp3-55	0	36	72	0	120	0	1392
testingpg-12sp1-50	0	15	48	3	273	33	1215

Figure 3. SUSE Manager automatically generates status reports on non-compliant systems.

Lock Down and Keep Watch

SUSE Manager automates Linux configuration, patching and management to provide a unified management infrastructure. The SUSE Manager 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 *(see Figure 4)*. SUSE Manager 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.

You can also use SUSE Manager to watch for vulnerabilities defined in 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.

Contact us at:
www.suse.com

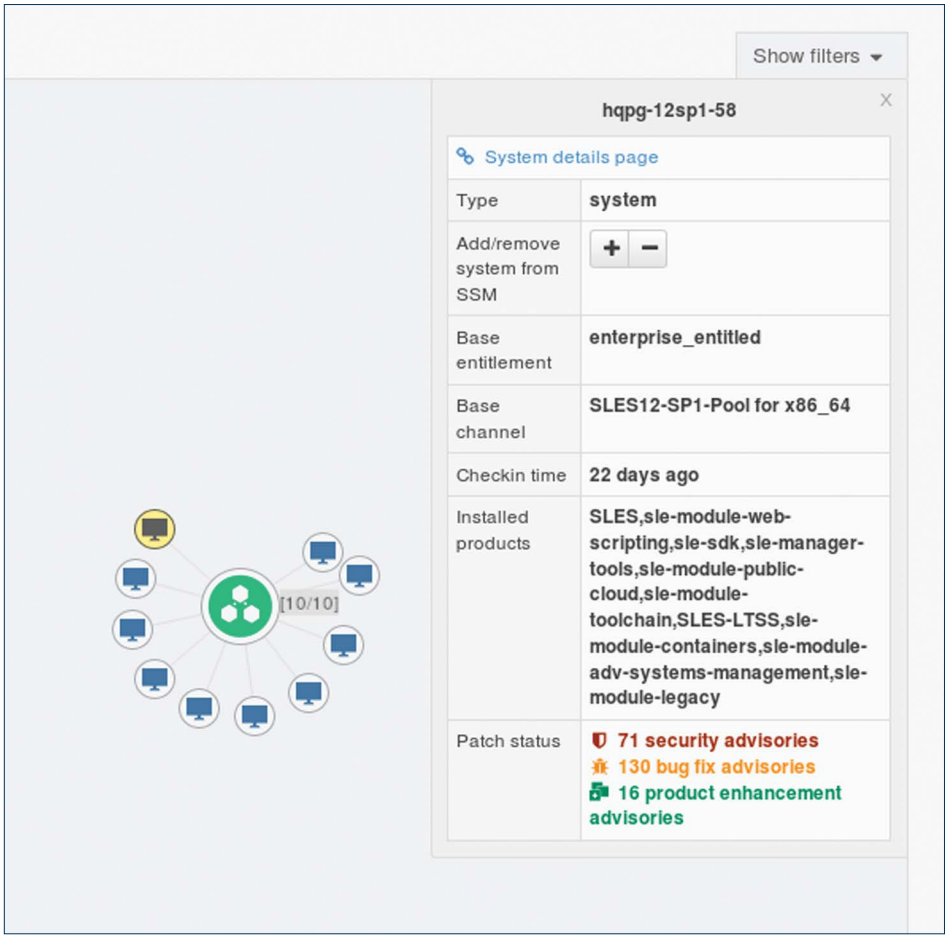


Figure 4. SUSE Manager makes it easy to review the status details of each system.