

Manage your Linux environment for success

A guide to modern best practices, tools, and techniques for effective system management



See what's inside

Page 1

About this e-book

Page 2

Linux is the foundation for the future

Page 3

System life-cycle management

Page 4

Content and provisioning management

Page 5

Subscription management and drift analysis

Page 6

Configuration management

Page 7

Security vulnerability and compliance management

Page 8

Vulnerability, compliance, and patch management

Page 9

Best practices

Page 10

Tool recommendations

Page 11

Unify and integrate Linux management with expert tools

Page 12

Red Hat management tools for Linux

Page 13

Customer success highlight:
Brinker International

Page 14

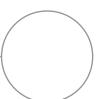
Customer success highlights:
Healthcare and financial services

Page 15

Customer success highlights:
Telecommunications and manufacturing

Page 16

Ready to get started?



About this e-book

This e-book provides expert guidance for Linux® administrators and architects to streamline management of their environments using modern best practices and automated tools. Organizations that applied these recommendations have experienced benefits in IT efficiency, security, reliability, and costs while better supporting their business with innovation and insights.

The suggestions in this e-book can help your organization experience:



Up to
4.5x
greater IT
efficiency
and speed.¹



Up to
20%
lower Linux
environment
operating costs.²



Up to
25%
lower Linux
environment support
costs.¹



Up to
98%
faster storage
provisioning
time.³

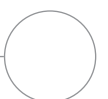


Continue reading to learn more about each of these areas and how your organization can use flexible automation, predictive analytics, and integrated tools to manage your Linux systems more effectively.

¹ Red Hat case study, "Sunrise Communications standardizes on cost-effective Red Hat software," April 2018. redhat.com/en/resources/sunrise-communications-customer-case-study.

² Red Hat case study, "CTOS improves agility for faster business expansion with Red Hat," November 2017. redhat.com/en/resources/ctos-case-study.

³ Red Hat case study, "NXP Semiconductors streamlines product design processes with Red Hat," May 2018. redhat.com/en/resources/nxp-semiconductors-customer-case-study.



Linux is the foundation for the future

Linux® is one of the world's most dominant operating systems, with widespread adoption across industries and emerging technologies.⁴ It is commonly used for highly available, reliable, and critical workloads in datacenters and cloud computing environments and supports a variety of use cases, target systems, and devices. Every major public cloud provider – including Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Alibaba Cloud – offers multiple distributions of Linux in their marketplaces. To sustain modern, digital business initiatives, Linux provides:

- Open source innovation.
- Consistency across infrastructure.
- Container and application portability.
- Massive workload and platform scalability.
- Continuous security capabilities.
- A flexible platform for application development.

Advanced management tools and approaches are critical for large-scale Linux environments. These environments can contain hundreds of systems operated by large teams. The potentially thousands of security patches, bug fixes, and configuration changes are simply too much to track and implement manually.

Adding to this, more organizations are deploying workloads across hybrid environments that encompass bare-metal, virtualized, and private and public cloud resources. This complexity often impedes visibility into your overall environment and compounds management challenges.

A comprehensive management strategy can help you get the most from your Linux environment while protecting your assets and business. A **standardized operating environment (SOE)**, based on consistent operating systems and tools, is at the core of the most effective management strategies. SOEs can simplify your IT infrastructure to improve efficiency, reduce costs, increase uptime, speed deployment and provisioning, boost security, and boost IT productivity.

This e-book discusses the challenges, tools, and best practices associated with managing large-scale Linux environments.

Linux by the numbers

More than

75%

of cloud-enabled enterprises report using Linux as their primary cloud platform.⁴

54%

of all applications running in public cloud infrastructure are running on Linux virtual machines.⁵

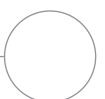
80%

of hiring managers are recruiting Linux talent.⁶

⁴ The Linux Foundation, "Linux is the most successful open source project in history." linuxfoundation.org/projects/linux. Retrieved November 1, 2019.

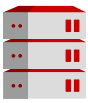
⁵ Management Insight Technologies, sponsored by Red Hat, "State of Linux in the public cloud for enterprises," February 2018. redhat.com/en/resources/state-of-linux-in-public-cloud-for-enterprises.

⁶ The Linux Foundation and Dice, "The 2018 Open Source Jobs Report," 2018.



System life-cycle management

Every system, resource, and workload has a life cycle. A key aspect of effective management strategies, system life-cycle management is the administration of a system from its provisioning, through its operational stage, to its final retirement. An ideal life-cycle management approach will let you:



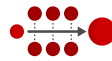
Build

Reliably create systems in an automated and scalable manner.



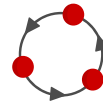
Monitor

Track and account for all systems, assets, and subscriptions.



Maintain

Ensure that systems are consistent across their life cycle.



Retire

Decommission systems and resources when they are no longer needed.

Common life-cycle management challenges

Several circumstances can make it difficult to manage systems effectively.

- **Environment sprawl.** Larger environments contain a greater number of systems, complicating system status and event tracking across your organization.
- **Technical debt.** Legacy systems often require special tools and processes to administer, impeding efforts to bring all systems under a single set of management tools and processes.
- **Limited staff.** IT teams are not growing at the same pace as the infrastructure they manage. This results in more work for the same number of staff, making it hard to get ahead of technological change, innovation, and business demands.
- **Business continuity requirements.** As business increasingly relies on IT, IT infrastructure must become even more reliable and available. Consequently, system management must be accomplished in a manner that does not interfere with critical business operations.

Life-cycle management best practices



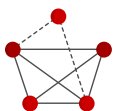
Retire resources at the end of life

Abandoned and unused resources consume staff time and budget, even if no one is using them. Implement a process for retiring unused systems to save management effort and costs.



Deploy automation

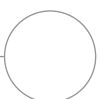
As the size of your infrastructure increases, so does the effort to manage it. Use automation to streamline common tasks, reduce human errors, and free staff to focus on innovation.



Connect your tools

Integrate your tools via available application programming interfaces (APIs). Use your preferred interfaces to perform tasks in other tools, streamlining operations and improving productivity.

The following sections discuss some key areas of system life-cycle management.



Content and provisioning management



Content management

Content management involves the supply chain and administration of the software, packages, and patches you deploy in your environment.

Why is it important?

Using unsigned, unvetted, and outdated software can be risky for your business. It can introduce security vulnerabilities, instabilities, and performance issues. In fact, supply chain attacks, which exploit third-party services and software to compromise a final target, increased by 78% in 2018.⁷

Even so, content management can be time-consuming and error-prone if done manually.

Best practices and recommendations

Effective content management ensures you have a secure supply chain for all of the software you use in production. You should:

- Understand where all content comes from.
- Check whether content has been tampered with in transit and reject any that has.
- Test patches before deploying them into production.
- Place content as close as possible to the target systems in geographically dispersed environments.
- Use tools that let you centralize, collate, curate, and disseminate content easily and automatically.



Provisioning management

Provisioning management is the process of defining and controlling how systems are provisioned and deployed.

Why is it important?

Business relies on IT systems. If the right systems are not available quickly, business can suffer and users may choose to deploy unauthorized resources outside of IT's control to meet their needs.

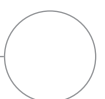
However, many IT teams struggle to standardize provisioning procedures because there are numerous ways to provision systems and many platforms include management tools that are specific to that platform.

Best practices and recommendations

Effective provisioning management requires the ability to provision and scale systems across platforms and geographically dispersed environments.

- Separate system definition from system provisioning using platform-agnostic tools.
- Adopt a comprehensive, cross-platform tool that lets you define systems once and deploy them consistently across a variety of platforms – including bare metal, virtualized, and private and public cloud – without needing to define additional platform-specific implementation details.

⁷ Symantec, "Internet Security Threat Report, Volume 24," February 2019.



Subscription management and drift analysis



Subscription management

Subscription management is a means to identify how many assets you have deployed and their characteristics. It can often be associated with a system of record for your assets.

Why is it important?

If you use software that is sold on a subscription basis, you have a contract that states how many subscriptions of a given product you can use. Breaching your contract terms by deploying too many systems can result in fines, contract termination, and lack of support. At the same time, purchasing more subscriptions than you actually need causes unnecessary costs to your organization.

Best practices and recommendations

Effective subscription management lets you optimize your costs while staying in compliance with vendor contracts. You should:

- Choose a tool that provides visibility into the number of subscriptions your organization uses and how they are used. This will help you ensure efficient subscription use and determine when you need to purchase more subscriptions.
- Select platforms that can connect to your existing and planned inventory management products.
- Implement processes and safeguards to ensure that only authorized users can deploy subscriptions on new systems and that those subscriptions are correctly allocated.
- Adopt procedures to identify and retire old and unused systems so you can avoid paying for subscriptions that you don't need.



Configuration assessment and drift analysis

Configuration assessment is the process of scanning systems to understand current configurations and identify those that require action. Drift analysis uses configuration assessment to compare systems against baseline configurations, past configurations, and other systems to find similarities and differences.

Why is it important?

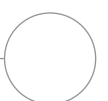
While your base images may be configured properly, systems change over time due to end user adjustments and installations, ad hoc fixes, and new image deployments. Regular monitoring of system configurations is essential. Nevertheless, manually tracking configurations is time-consuming at best, and nearly impossible in large-scale environments. Even with a scanning tool, it can be difficult to sift through massive data files and understand which systems require updates and patches.

Best practices and recommendations

Effective configuration assessment and drift analysis can give you visibility into your system configurations to identify operational and performance issues, detect noncompliant systems, and control drift.

Choose a management tool that lets you track configuration changes on a regular and continuous basis. Daily monitoring is recommended. The ideal tool will let you:

- Collect and record system configurations.
- Detect configuration changes and systems that have drifted from their baseline.
- Validate applied updates.
- Revisit previous configurations.
- Compare system configurations for differences.
- Automate monitoring to streamline operations, schedule regular scans, and ensure consistency.



Configuration management



Configuration management

Configuration management involves defining a desired system state, then building and maintaining systems accordingly. It is closely related to configuration assessment and drift analysis and uses both to identify systems that require updates, reconfiguration, or patching.

Why is it important?

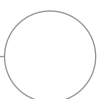
Misconfigurations and outdated settings can lead to poor performance, inconsistencies, and noncompliance with standards and negatively impact business operations and security. Even so, the process of identifying systems that require attention, determining remediation steps, prioritizing actions, and tracking completion and validation is often too complicated to perform manually in large environments.

Best practices and recommendations

Effective configuration management lets you consistently define system configurations and build and maintain systems according to those baselines. An ideal configuration management tool will let you:

- Classify and manage systems by groups and subgroups.
- Modify base configurations in a centralized way and roll new settings out to all applicable systems.
- Automate identifying, patching, and updating of systems with outdated, poorly performing, and noncompliant configurations.
- Easily and simply prioritize findings and actions.
- Access and apply prescriptive remediation actions.

Limit the number of base configurations you manage to only what you really need. Each distinct configuration directly impacts management time and effort. Like systems can be managed with less time, effort, and staff.



Security vulnerability and compliance management

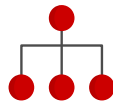
IT security is an ongoing concern for all organizations. In fact, 30% of CEOs consider cyber attacks to be a top threat to their organization's growth prospects.⁸ And threats are growing. The average size of data breaches increased by 3.9% from 2018 and the likelihood of experiencing a breach within two years is 29.6%.⁹ Adding to this, industry and government regulations are also changing.

Security vulnerability and compliance management involves monitoring and assessing systems to ensure they comply with security and regulatory policies. An ideal security vulnerability and compliance management approach will let you:



Assess

Identify systems that are noncompliant, vulnerable, or unpatched.



Organize

Prioritize remediation actions by effort, impact, and issue severity.



Remediate

Quickly and easily patch and reconfigure systems that require action.



Report

Validate that changes were applied and report change results.

Common security and compliance challenges

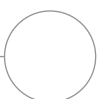
Several factors can make security vulnerability and compliance management challenging:

- **Changing security and compliance landscapes.** Security threats change quickly, requiring rapid response to new threats and evolving regulations.
- **Distributed, multiplatform environments.** Infrastructures are becoming more distributed across on-site and cloud platforms, as well as geographies, preventing you from gaining a complete view into your environment. Hosted providers typically offer their own platform-specific management tools. Views and reports from each of these tools must be pieced together to understand the compliance and vulnerability status of your environment.
- **Large environments and teams.** Large, complex infrastructures and teams can complicate coordination across your environment and organization. In fact, system complexity can increase the cost of a data breach by US\$10.96 per record lost or stolen.⁹

The following sections discuss some key areas of security and compliance management.

⁸ PWC, "22nd Annual Global CEO Survey: CEO's curbed confidence spells caution," 2019.

⁹ IBM Security, "2019 Cost of a Data Breach Report," 2019. [ibm.com/security/data-breach](https://www.ibm.com/security/data-breach).



Vulnerability, compliance, and patch management



Vulnerability identification and remediation

Vulnerability identification and remediation is the process of evaluating infrastructure to find and fix systems that are vulnerable to attack. These vulnerabilities can be caused by emerging threats, outdated patches, or system misconfiguration. Remediation actions often include patching, updating, and reconfiguring systems to resolve the vulnerability.

Why is it important?

Security vulnerabilities can lead to costly breaches that may also result in lost business. The average total cost of a data breach is US\$3.92 million.¹⁰ Lost business accounts for 36.2% of average data breach costs.¹⁰

Mitre releases thousands of Common Vulnerabilities and Exposures (CVEs) each year.¹¹ Most IT teams are unable to keep pace and do not review every CVE to determine whether and where it impacts their infrastructure. As a result, you may miss relevant CVEs and leave yourself open to attack.



Compliance management

Compliance management concerns ensuring systems are compliant with corporate policies, industry standards, and applicable regulations over time. It uses infrastructure assessment to identify systems that are noncompliant due to regulatory, policy, or standards changes, misconfiguration, or other reasons.

Why is it important?

Noncompliance can result in fines, damage to your business, and loss of certification, in addition to security breaches.



Patch management

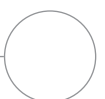
Patch management entails identifying systems that require patches or updates, patching or updating those systems, and testing to validate that they are successfully installed and functional.

Why is it important?

Unpatched and out-of-date systems can be a source of compliance issues and security vulnerabilities.

¹⁰ IBM Security, "2019 Cost of a Data Breach Report," 2019. [ibm.com/security/data-breach](https://www.ibm.com/security/data-breach).

¹¹ For more information about Mitre and CVEs, visit [mitre.org](https://www.mitre.org).



Best practices

Scan systems regularly

Daily monitoring can help you identify compliance issues and security vulnerabilities before they impact business operations or result in a breach. The average time to identify and contain a data breach in 2019 was 279 days. Finding and containing a breach in 200 days or less can reduce the cost of the breach by US\$1.22 million on average.¹²

Deploy automation

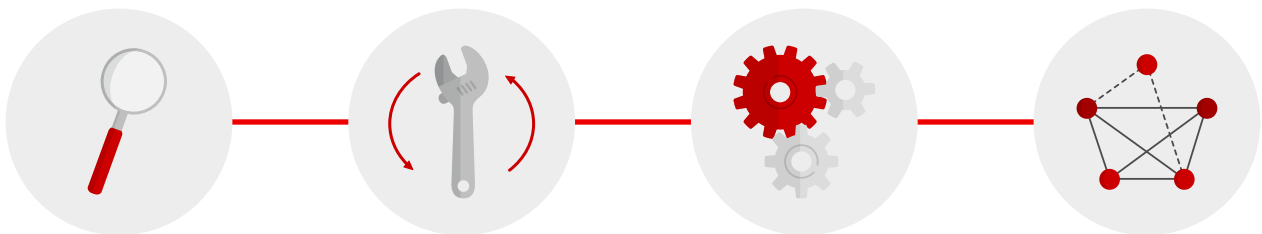
As the size of your infrastructure grows, it becomes harder to manage manually. Use automation to streamline common tasks, improve consistency, and ensure regular monitoring and reporting. Fully deploying security automation can reduce the average cost of a breach by 95%, but only 16% of organizations have done so.¹²

Patch often and test your patches

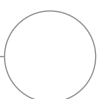
Keeping systems up to date can boost security, reliability, performance, and compliance. Patches should be applied once a month to keep pace with important issues. Patches for critical bugs and defects should be applied as soon as possible. Test patched systems for acceptance before placing them back into production.

Connect your tools

Distributed environments often contain different management tools for each platform. Integrate these tools via APIs. Use your preferred interfaces to perform tasks in other tools. Using a smaller number of interfaces streamlines operations and improves visibility into the security and compliance status of all systems in your environment.



¹² IBM Security, "2019 Cost of a Data Breach Report," 2019. [ibm.com/security/data-breach](https://www.ibm.com/security/data-breach).



Tool recommendations

Ideal security and compliance tools will include several key features and capabilities.



Proactive scanning

Understanding your security and compliance status is the first step to improving it. Tools that provide automated scanning can ensure systems are monitored at regular intervals and alert you to issues without expending much staff time and effort.

Actionable insight

Tools that provide information that is tailored to your environment can help you more quickly identify which compliance issues and security vulnerabilities are present, which systems are affected, and what potential impacts you can expect.

Customizable results

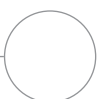
Some compliance checks may not apply to certain systems due to their specific configuration, use, or workload. Tools that let you define business context to reduce false positives, manage business risk and provide a more realistic view of your security and compliance status are ideal.

Prescriptive, prioritized remediation

Tools that provide prescriptive remediation instructions eliminate the need to research actions yourself, saving time and reducing the risk of mistakes. Prioritization of actions based on potential impact and systems affected help you make the most of limited patching windows.

Intuitive reporting

Tools that generate clear, intuitive reports about which systems are patched, which need patching, and which are noncompliant with security and regulatory policies increase auditability and help you gain a better understanding of the status of your environment.



Unify and integrate Linux management with expert tools

Red Hat takes a holistic approach to IT management that improves speed, scalability, and stability across your entire IT environment, from bare-metal and virtualized servers to private, public, and hybrid cloud infrastructure. Red Hat® management tools are based on years of Linux development and support experience. They work seamlessly together to streamline IT administration, saving your team time and effort and making your environment more secure, optimized, and reliable.



Configurable tools and baselines reduce false positives and give you an accurate view of your infrastructure status.



Automation capabilities improve configuration and patching accuracy and reduce human errors.



Customizable views deliver the right information at the right time, fast.



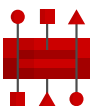
Automated and proactive remediation help you fix issues faster, without needing to contact support.



An extensive library of resources provides detailed, targeted information 24x7.

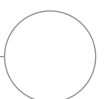


On-site and Software-as-a-Service (SaaS) options let you deploy tools according to your preference.



APIs connect with your preferred tools and interfaces.

Read more about IT management with Red Hat at redhat.com/en/topics/management.



Red Hat management tools for Linux



Systems management for Red Hat infrastructure

Red Hat Satellite simplifies deployment, management, and scaling of Red Hat infrastructure to increase efficiency, reduce operational costs, and allow IT to focus on strategic business needs.

- Works across physical, virtual, and cloud environments
- Provides content, patch, configuration, provisioning, and subscription management
- Supports on-site, cloud, and disconnected environments
- Delivers complete system life-cycle control
- Allows automation of most system maintenance tasks

Cloud Management Services for Red Hat Enterprise Linux

Software-as-a-Service (SaaS) infrastructure management

Cloud Management Services for Red Hat Enterprise Linux streamline security vulnerability, compliance, and configuration drift analysis to optimize your Red Hat environment.

- Provides vulnerability and compliance assessment and monitoring
- Automates issue remediation
- Reduces tools maintenance requirements via a SaaS-based service
- Delivers a single view of all hosts in your environment
- Uses the same central repository for data and inventory as Red Hat Insights



Predictive IT risk analytics

Red Hat Insights helps IT teams proactively identify and remediate threats to security, performance, availability, and stability to avoid issues, outages, and unplanned downtime, and to ensure their Red Hat environment is operating optimally.

- Fast and easy to get started
- Included with all active Red Hat Enterprise Linux subscriptions
- Incorporates years of support expertise
- Provides actionable knowledge and automation
- Accesses minimal system metadata
- Dynamically generates **Red Hat Ansible® Automation Platform** Playbooks to help automate remediation



Brinker International


Deliver digital hospitality experiences with Red Hat solutions

Challenge

Brinker International, Inc., the parent company of Chili's Grill & Bar and Maggiano's Little Italy, focuses on providing exceptional dining with innovative digital guest experiences. Brinker's digital guest offerings evolved to meet guest expectations, but its legacy technology couldn't keep pace. The process to update website code took hours, required downtime, and didn't guarantee a consistent configuration. Brinker needed to unify its digital platforms in a new e-commerce environment to provide a more consistent guest experience and increase adoption of its digital offerings.

Solution

To incorporate the necessary innovation and flexibility, Brinker decided to use open source technology. It chose Red Hat's platform as the foundation of its new e-commerce environment, which also hosts Chili's new digital curbside service. Brinker incorporated Red Hat solutions for storage, management, and data analytics. The new unified e-commerce environment supports faster development and deployment, scales to meet peak traffic demands, and ensures the protection of guest data.



“Red Hat Insights provides risk mitigation and visibility into the state of our systems. It helps us make sure our IT environment and data is secure with automated resolution of any threats.”

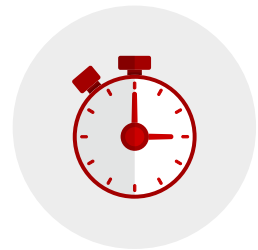
Pankaj Patra
Senior director of IT enterprise solutions,
Brinker International



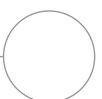
Improved sensitive customer data protection



Built an innovative, scalable e-commerce environment



Sped feature and service development and launch



Healthcare and financial services



HCA Healthcare uses its data resources to find innovative solutions to long-standing industry challenges like detection of sepsis, a potentially life-threatening condition. The healthcare company deployed a real-time predictive analytics product, SPOT (Sepsis Prediction and Optimization of Therapy), based on optimized container and automation technology. With SPOT, the company can more accurately and rapidly detect sepsis, helping to save lives.



Knowledge Creates Confidence

CTOS Data Systems Sdn. Bhd., Malaysia's largest private credit reporting agency (CRA), wanted to increase its national market reach and product portfolio. CTOS migrated from a community version of a Linux platform to a virtualized environment based on Red Hat technologies. The new environment reduced operating costs, streamlined management and security, and provided the scalability to keep pace with business demands and customer traffic shifts.



Sped sepsis detection by up to 20 hours



Gained new insights using machine learning algorithms



Reduced risk and cost of innovation



Reduced downtime and simplified management with expert support



Gained enterprise-grade security to protect data

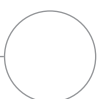


Reduced Linux environment operating costs by around 20%



“The Red Hat solution has given us more confidence in terms of our work and a sense of security. We’re all able to get a good night’s sleep without worrying about our infrastructure.”

Benjamin Lau
IT manager, CTOS Data Systems Sdn. Bhd.



Telecommunications and manufacturing

Sunrise

Sunrise Communications, Switzerland's largest private telecommunications provider, needed stable, secure and flexible IT services with cost-effective operations. The company consolidated all of its IT infrastructure to SAP® HANA® and enterprise software from Red Hat, reducing costs, improving speed and performance, and taking advantage of open source community development to release innovative, cost-effective services.



NXP Semiconductors N.V., one of the world's largest producers of electronic components, required greater compute power to support simulations and testing completed by its 10,000 design engineers. With an efficient, Red Hat-based IT environment, the company has reduced provisioning time, improved quality through standardization, and simplified management to deliver high-quality components to market faster.



Improved IT efficiency by a factor of 4.5



Increases efficiency via simplified and automated management



Reduced SAP environment support costs by 25%



Streamlined global work by standardizing IT configurations



Gained access to open source expertise and support

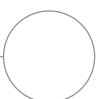


Reduced storage provisioning times from 8 hours to 5 minutes



Because it is centrally managed with Red Hat Ansible and Red Hat Satellite, Red Hat Enterprise Linux is more efficient.

Sebastiaan Laurijsse
Senior director of IT infrastructure services, NXP Semiconductors



Ready to get started?

Linux is a key platform in modern datacenters. A comprehensive management strategy can help you get the most from your Linux environment while protecting your assets and business.

Red Hat provides interoperable management tools that empower you to increase the performance, reliability, and security of large-scale Linux environments.



Learn more about Red Hat management tools:
redhat.com/management