Save administrator time with the automated remediation capabilities of Red Hat Insights

Across a range of common use cases, Red Hat Insights let us identify and remediate issues in a Red Hat Enterprise Linux environment more quickly than an approach using manually scripted workflows

For maintaining wide-ranging Red Hat® Enterprise Linux® deployments, administrators often use workflows they have scripted manually to determine the health of the environment. While this approach works, it can require investing considerable time and resources into maintaining these scripts. Using the built-in Red Hat Insights monitoring tool to automate routine maintenance activities can eliminate or reduce this maintenance effort and simplify the process of identifying issues and remediating them.

Principled Technologies (PT) compared these differing approaches to detecting and remediating configuration issues in a 90-host environment comprising a mix of on-premises VMs and cloud VMs. We performed use cases in three common areas: common vulnerabilities and exposures (CVEs) and patching, known issues, and compliance. We executed each use case twice—once using a representative workflow we manually scripted (though every admin's scripted approach will differ) and once using Red Hat Insights. For each of the three use cases, we found that the Red Hat Insights approach took less time. This could translate to a considerable benefit for companies using Insights: By spending less time on routine remediation tasks, administrators can devote more of their resources to innovation and supporting business goals.

79% less hands-on time to detect and remediate CVEs

86% less hands-on time to detect and remediate known issues

28% less hands-on time to detect and remediate compliance issues

Our test approach

To quantify the effort involved in the manual scripted workflow approach, we recorded the time our administrator needed to write scripts to detect issues, review results, and remediate issues on 90 hosts. For Red Hat Insights, we tracked the time it took our administrator to set up Insights for detection on 90 hosts, review the results, and remediate the issue. We excluded time for tasks that ran automatically without user intervention, but included the time for the actual remediations, even when they used scripts. To see the complete methodologies for both approaches, go to the science behind the report.

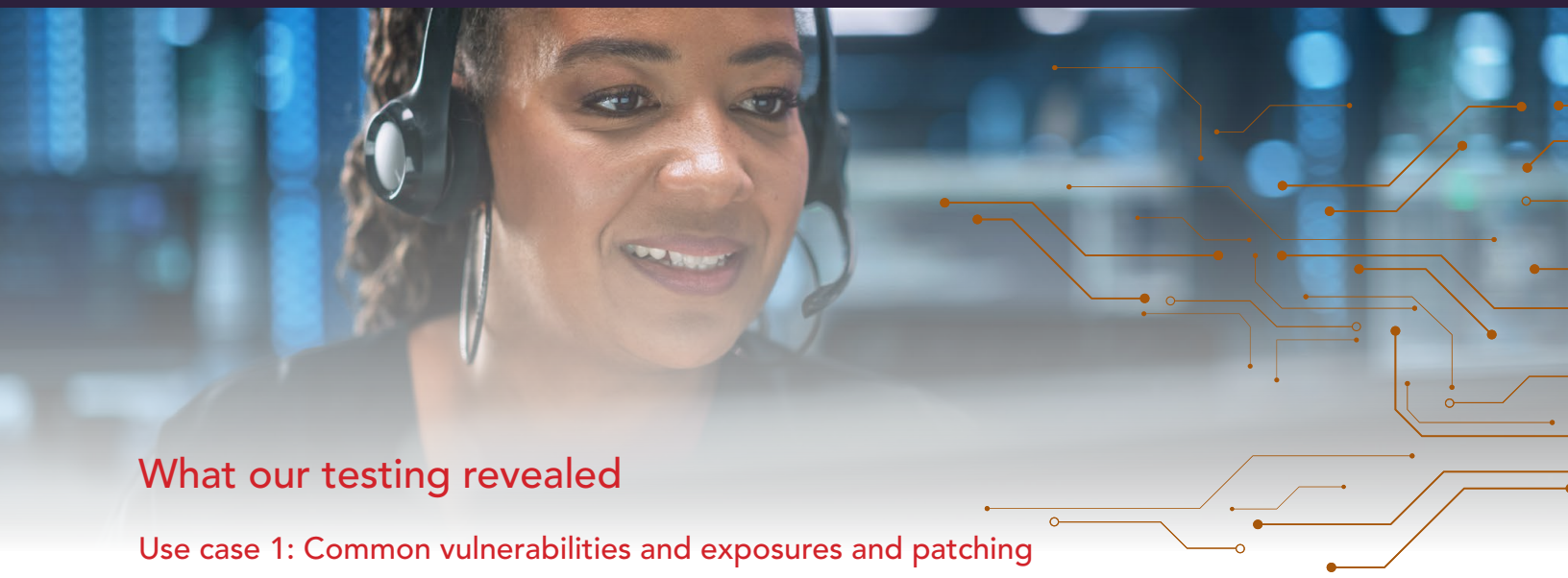
The engineer executing these tests had knowledge of Linux and strong skills in scripting and automation. Prior to testing, they had some exposure to Red Hat Insights. For both the scripted workflow approach and the Red Hat Insights approach, the effort required will vary depending on the level of experience your team members have with Linux and automation.

Our testbed consisted of 90 virtual hosts: 80 on-site in the PT data center, and 10 in the cloud (five on Microsoft Azure and five on Amazon Web Services [AWS]).

Red Hat Insights can modernize system management

Red Hat Insights is included with Red Hat Enterprise Linux at no extra cost,[1] so the process of procuring the infrastructure management solution is straightforward. Delivered as a service, Red Hat Insights uses predictive analytics and comprehensive domain expertise to assess IT environments and proactively identify and prioritize operational and security risks. It can remediate those risks and streamline other system management tasks, such as creating and launching system images to the public cloud. Red Hat states, "Insights uses predictive analytics and deep domain expertise to reduce complex operational tasks from hours to minutes, including identifying security and performance risks, tracking licenses, and managing costs."[2]

Note: The graphs in this report use different scales. Please be mindful of each graph's data range as you compare.



What our testing revealed

Use case 1: Common vulnerabilities and exposures and patching

By monitoring common vulnerabilities and exposures and remediating any that you detect in the environment, you can improve data security and prevent unnecessary interruptions in service. Red Hat Insights helps simplify monitoring environments for CVEs and enables admins to address them quickly.

Insights can provide up-to-date lists of all CVEs and how many servers they affect. The Insights approach to this scenario involved looking at this list to see which all CVEs affected our testbed, determining whether a Red Hat Bug Advisory (RHBA) applied to specific Red Hat Enterprise Linux (RHEL) systems, and applying the appropriate patches. The manual approach required a more hands-on process that begins with the administrator looking at a list of CVEs—either by subscribing to an RSS feed for CVEs or scrolling through the CVE Twitter feed. Once they determined which CVEs were important to patch, they used scripts and Red Hat repositories to patch the CVE on the systems that required it.

As Figure 1 shows, Red Hat Insights reduced the hands-on time to detect and remediate a vulnerability on 90 hosts by 4 minutes and 9 seconds, 79 percent less time than the manual, scripted workflow required. This time savings can not only reduce the burden on administrators, but could even translate to keeping data more secure. As Figure 2 shows, the difference in the total amount of time the process required is even more dramatic: 2 minutes vs. 1 hour and 50 minutes — a 98 percent savings.

Figure 1: Hands-on time in h:mm:ss to detect and remediate CVEs for 90 hosts using Red Hat Insights versus a manual scripted approach. Lower numbers are better. Source: Principled Technologies.

Figure 2: Total time in h:mm:ss to detect and remediate CVEs for 90 hosts using Red Hat Insights versus a manual scripted approach. Lower numbers are better. Source: Principled Technologies.

Use case 2: Identifying and remediating known issues

By monitoring common issues in Linux operating systems, you can improve performance and security, minimizing disruptions to the workplace. Red Hat Insights can automatically discover these issues and recommend fixes for them, including executing scripts to perform the recommended actions. This scenario involved evaluating systems for known security issues, common misconfigurations, and best practices, then fixing these issues. The specific scenario we tested involved using the Insights user interface (UI) to determine that the systems were not configured with appropriate tuned profiles, then initiating a remediation. (Note that Insights checks for other known issues; we chose to use this issue because it was the most reproducible misconfiguration we discovered in our testing.) For the manual approach, we verified the tuned profile we wanted to use for our servers, then used scripts to check the servers against their preferred profile, created a quick report of which servers needed their tunings changed, and applied fixes as needed.

As Figure 3 shows, Red Hat Insights reduced the hands-on time to identify and remediate known issues on 90 hosts by 3 minutes and 52 seconds, a savings of 86 percent over the manual, scripted workflow. As Figure 4 shows, using Red Hat Insights reduced the total time to perform the task by more than half, a savings of 57 percent over the manual approach.

Figure 3: Hands-on time in h:mm:ss to identify and remediate known issues for 90 hosts using Red Hat Insights versus a manual scripted approach. Lower numbers are better. Source: Principled Technologies.

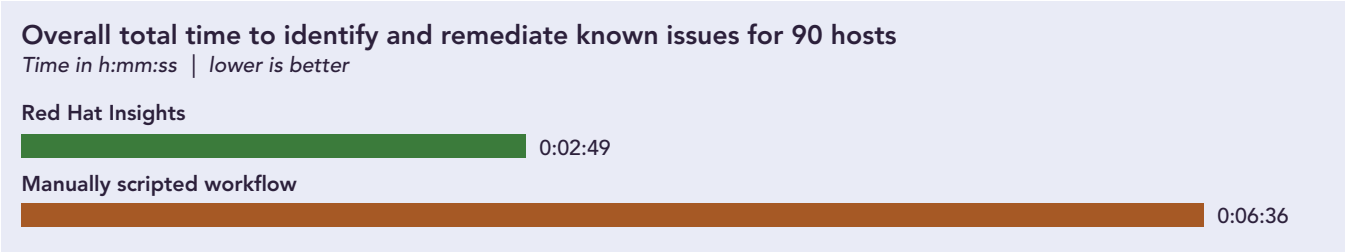


Figure 4: Total time in h:mm:ss to identify and remediate known issues for 90 hosts using Red Hat Insights versus a manual scripted approach. Lower numbers are better. Source: Principled Technologies.

In addition to lightening the load on administrators, these time savings can have other benefits. One large advantage that Insights has over a manual method is that it automatically compares issues against a constantly updating database, notifying the administrator when it determines that issues need remediation. In contrast, a manual approach may involve discovering a potential issue, researching the issue, determining how to fix it, and deploying the fix to the affected systems. This could add up to critical time lost to remediate the issue and minimize the impact to your architecture.

Use case 3: Compliance with regulatory policies

Infrastructure management tools that enable administrators to set uniform policies from a single console and monitor configurations can make it easier to keep all hosts in compliance with organizational and regulatory guidelines. In this use case, we detected and remediated Center for Internet Security (CIS) Linux rule violations in the environment using both Red Hat Insights and the manual scripted approach. (CIS is an organization that specializes in hardening systems against cyberattacks.) This task helps keep the Linux environment healthy and secure while also enforcing regulatory requirements. Because of the complexity of the CIS benchmark and the limited control AWS offers over the operating system we were installing, we encountered compatibility issues; as a result, we removed the five AWS instances from the test.

As Figure 5 shows, detecting and remediating compliance issues with Red Hat Insights reduced hands-on admin time by 28 percent. As Figure 6 shows, the total time to remediate compliance issues using Red Hat Insights took 11 minutes and 24 seconds, a 93 percent savings in total time compared to the manual approach.

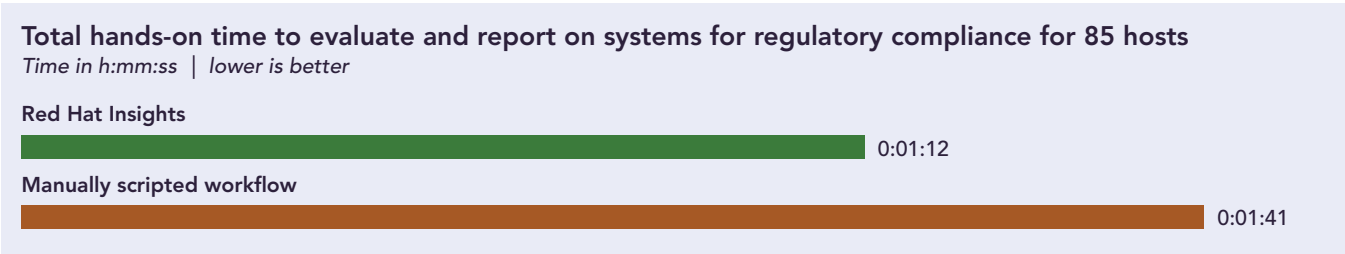


Figure 5: Hands-on time in h:mm:ss to remediate compliance issues using Red Hat Insights versus a manual scripted approach. Lower numbers are better. Source: Principled Technologies.

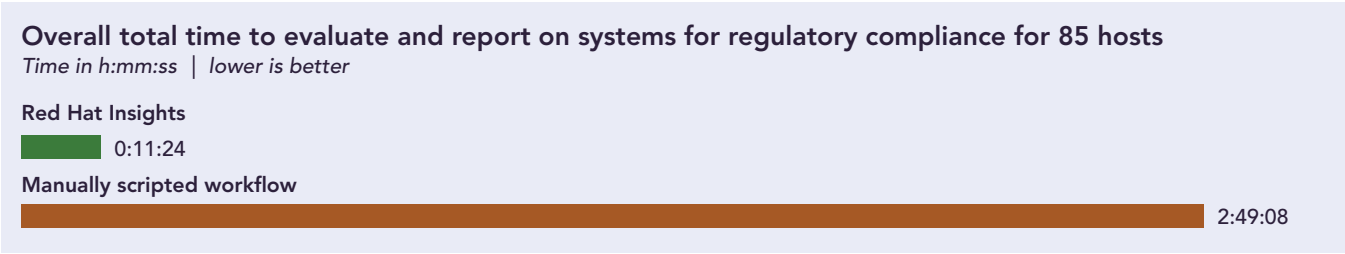


Figure 6: Total time in h:mm:ss to remediate compliance issues using Red Hat Insights versus a manual scripted approach. Lower numbers are better. Source: Principled Technologies.

Monitoring subscription usage

Tracking active software subscriptions is critical to knowing whether your organization holds enough to meet current and future requirements. For example, if you have recently downsized an environment, you don't want to accidentally pay for more subscriptions than you need. Tracking subscriptions can be a time-consuming task. According to Red Hat, IT admins devote an average of 10 hours a week to tracking subscriptions across multiple tools, such as spreadsheets.[3] Many traditional tracking solutions require users to self-report and check subscriptions back in when they no longer need them. These approaches are vulnerable to inaccuracy, so administrations must perform periodic audits.

To help with this vital task, Red Hat includes a service that tracks Red Hat subscriptions directly in the Red Hat Hybrid Cloud Console and lets users export this data to other tracking databases already in use.[4] The service lets administrators easily see how many subscriptions they have altogether and how many are in use, and it breaks them down by type—physical, virtual, public cloud, and hypervisor. Without any additional tracking efforts, IT admins can use this service to quickly gauge whether they must add or release subscriptions, which can help save time and money.

We tested this service and found that it worked smoothly, letting us see the number of RHEL subscriptions in use in less than a minute. To learn more about this service, visit https://docs.redhat.com/en/documentation/subscription_central/1-latest/html/getting_started_with_the_subscriptions_service/index.

Conclusion: Reduce the administrative burden in remediation scenarios with Red Hat Insights

Keeping a Red Hat Enterprise Linux environment current and compliant requires a certain amount of routine monitoring and maintenance. Scripted workflows can deliver some efficiencies, but administrators must spend time maintaining those scripts. An alternative approach is using Red Hat Insights, included with Red Hat Enterprise Linux at no extra cost, to monitor, assess, and recommend actions to strengthen the performance and reliability of your environment, whether on premises or in the cloud. In our tests, using Red Hat Insights to execute three monitoring and maintenance scenarios on 90 VMs took up to 86 percent less hands-on time than using a manual, scripted approach. By employing Red Hat Insights, your administrators could spend less time on these kinds of routine activities and devote more time to new projects and achieving business goals.

---

1. Red Hat, "Red Hat Insights," accessed June 10, 2024, https://www.redhat.com/en/technologies/management/insights.
2. Red Hat, "Red Hat OpenShift Service on AWS GovCloud and Red Hat Insights Achieve FedRAMP® High Authorization," accessed July 18, 2024, https://www.redhat.com/en/about/press-releases/red-hat-openshift-service-aws-govcloud-and-red-hat-insights-achieve-fedrampr-high-authorization.
3. Red Hat, "Introduction to Subscription Watch," accessed July 17, 2024, https://www.youtube.com/watch?v=pHBh5D8Zp_s.
4. According to Red Hat, it tracks a subset of Red Hat subscriptions. The licenses it does not track should, according to Red Hat, "not be considered in the subscription threshold that Subscription Usage counts. For example, Developer subscriptions, Trial subscriptions, etc., do not contribute to what a customer needs to pay for, and including them would inappropriately inflate the subscription threshold and reduce transparency." Source: Red Hat, "What subscriptions (SKUs) are included in Subscription Usage (Subscriptions)?" accessed July 16, 2024, https://access.redhat.com/articles/7015380.

This project was commissioned by Red Hat.

Read the science behind this report at https://facts.pt/SlpYPh4 ▶

Facts matter.®