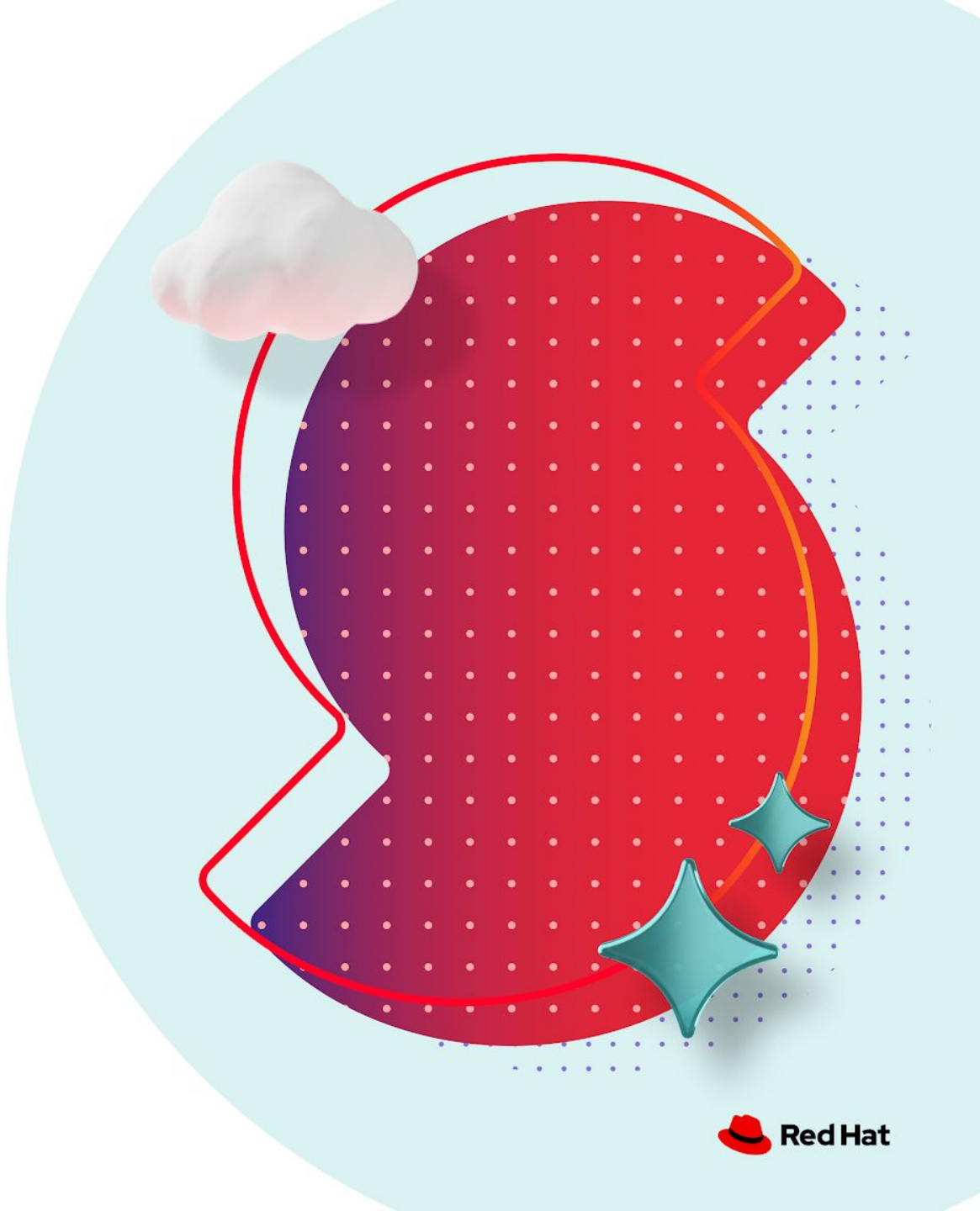

Red Hat
Enterprise Linux

Red Hat Summit

Connect

News from the RHEL Planet

What's new and what's coming next



Red Hat

Add subtitle here or delete



Alessandro Rossi

RHEL Advocate
Red Hat

What we'll discuss today

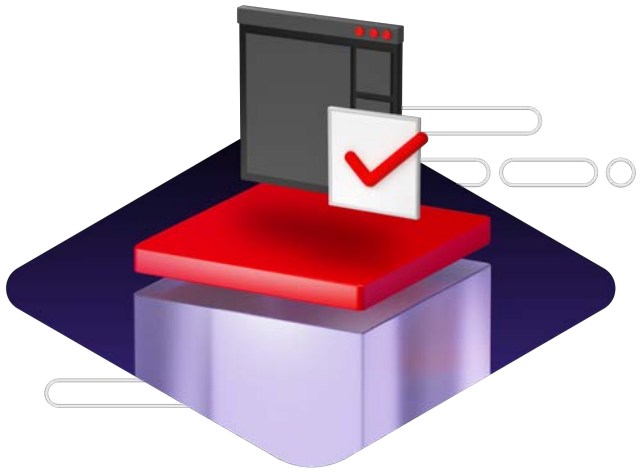
- ⇒ Security starts with a build!
- ⇒ Adding AI to RHEL Management
- ⇒ How can Red Hat help with the CVE sprawl?
- ⇒ What's new in Satellite?



Security starts with a build!







RHEL Image Builder

Red Hat

Build your RHEL custom Image

Image building options for RHEL



RH Lightspeed Image builder

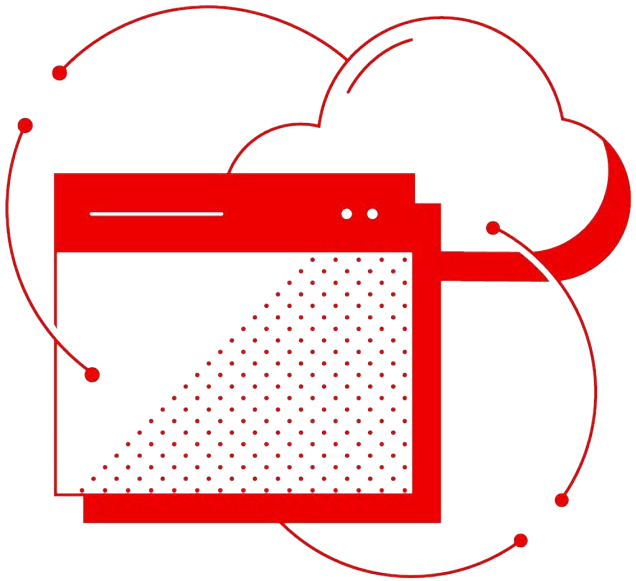
The power of image builder, wrapped up in a UI and hosted by Red Hat.

RHEL Image builder

Image builder on your infrastructure, anywhere you run RHEL.

RHEL Image mode

Building Images using a containerized approach



Multiple ways to use Image Builder

Image Builder | On premise

- Command line tool
- On-premises build node
- Included with Red Hat Enterprise Linux (RHEL) subscription

RHEL Web Console | On premise

- Via interface in RHEL web console
- On-premises build node
- Included with RHEL subscription

Red Hat Lightspeed Image Builder | Hosted

- Cloud-hosted experience
- No infrastructure required
- Included with RHEL subscription
- API for CI/CD automation
- console.redhat.com

Steps for using Image Builder

1. Choose platform

Physical, private cloud, public cloud, or edge

2. Select image builder tool

Red Hat Insights image builder
console.redhat.com

RHEL image builder
On-premises private build

3. Create blueprint

Define and customize the image

4. Build the image

Create a variety of images including Red Hat OpenStack, Amazon Web Services, VMware, and Microsoft Azure, and more

5. Deploy instance

Push image to the cloud provider of your choice or download to your datacenter

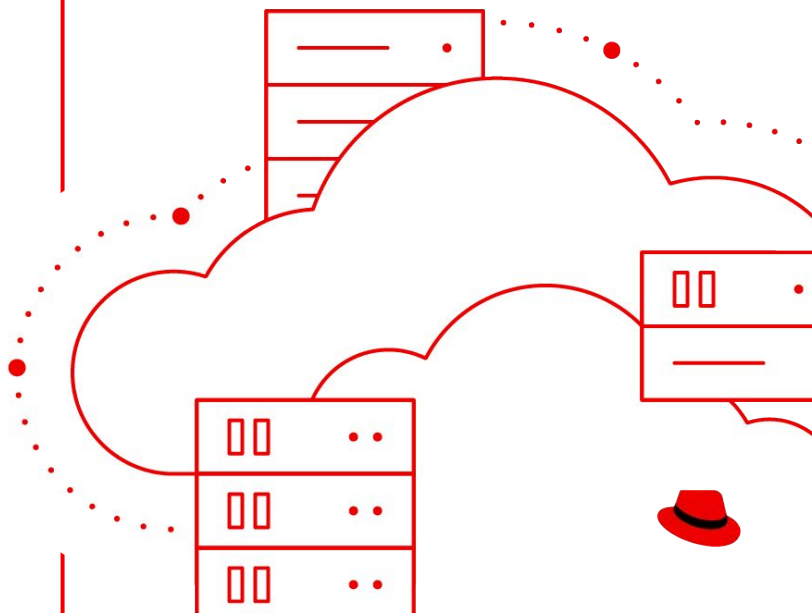
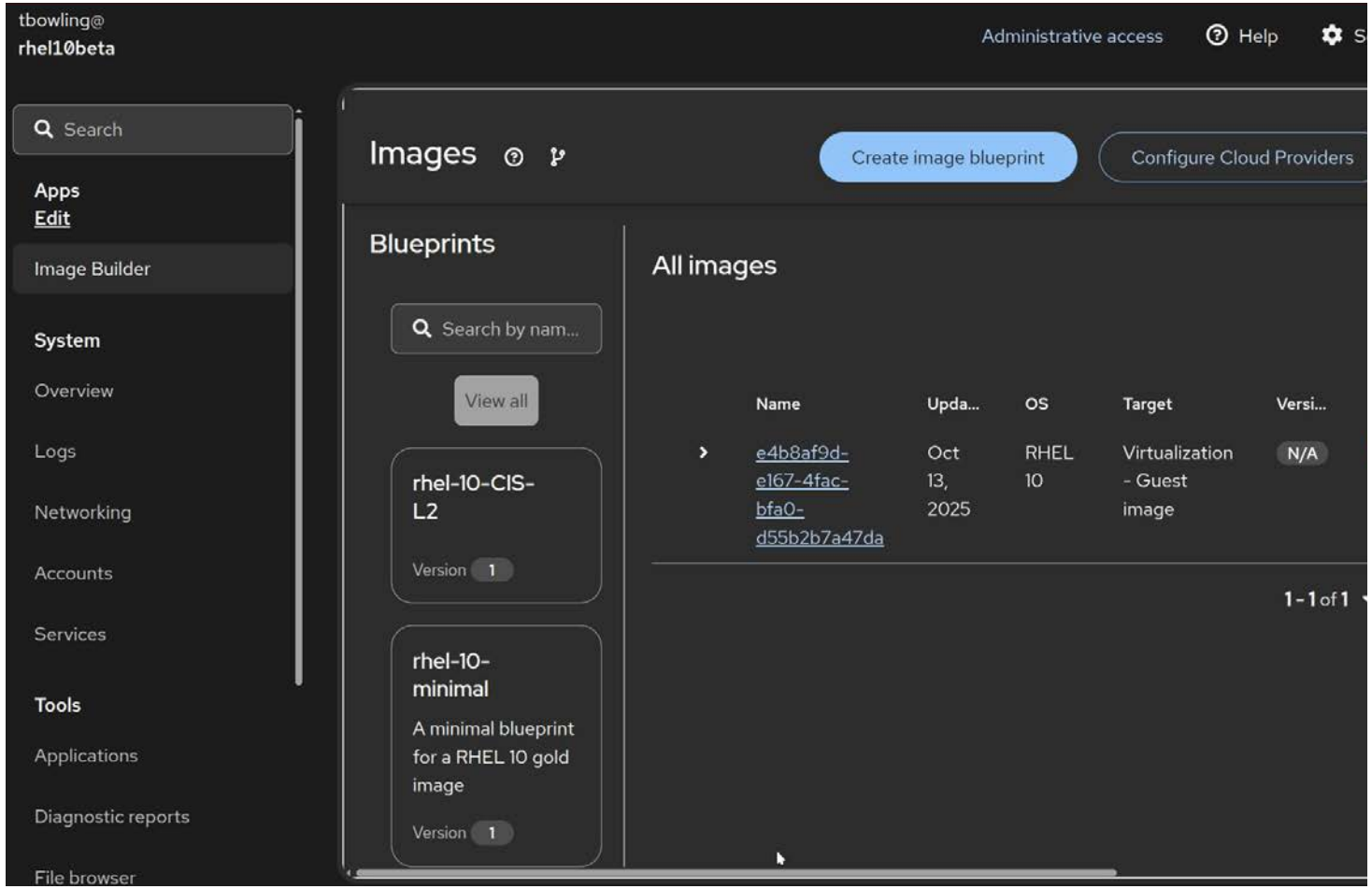


Image Builder design in RHEL 10

Tech Preview in RHEL 10.1 & 9.7

- **osbuild** - pipeline execution engine for operating system artifacts
- **image-builder** - **New** standalone binary providing CLI and self contained builder. Works much better within CI/CD pipelines.
- **cockpit-image-builder** - **New** Graphical frontend within RHEL web console. Inherits the improved UI from Insights image builder.



Red Hat

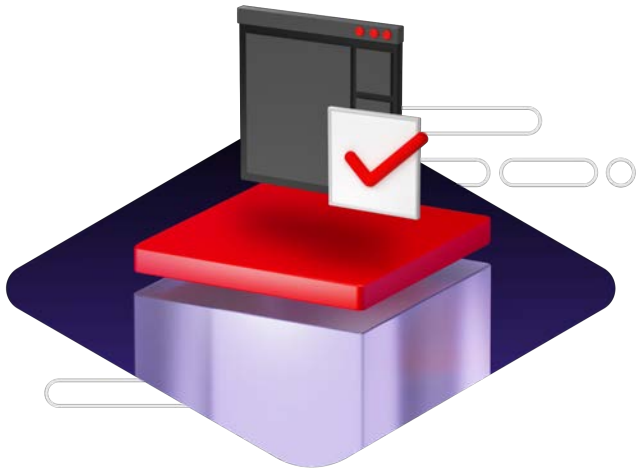


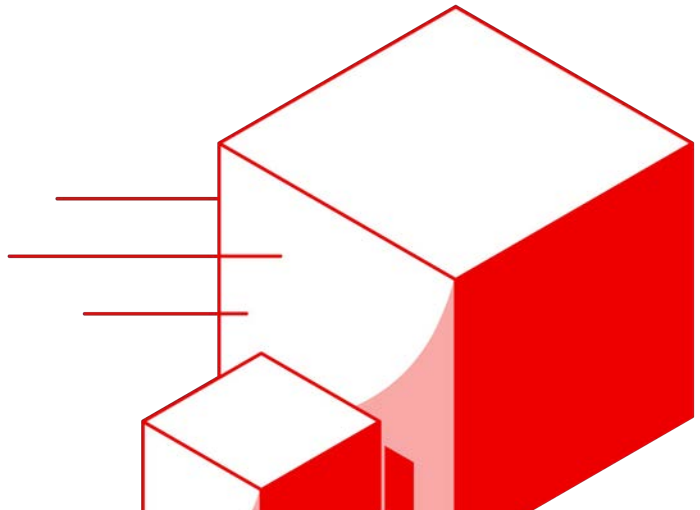
Image mode for RHEL

Red Hat

Image mode for Red Hat Enterprise Linux

A uniform and convenient method for deploying the operating system

Image mode for RHEL is a simple, consistent approach to build, deploy and manage the operating system using container technologies.



Bootc images from scratch

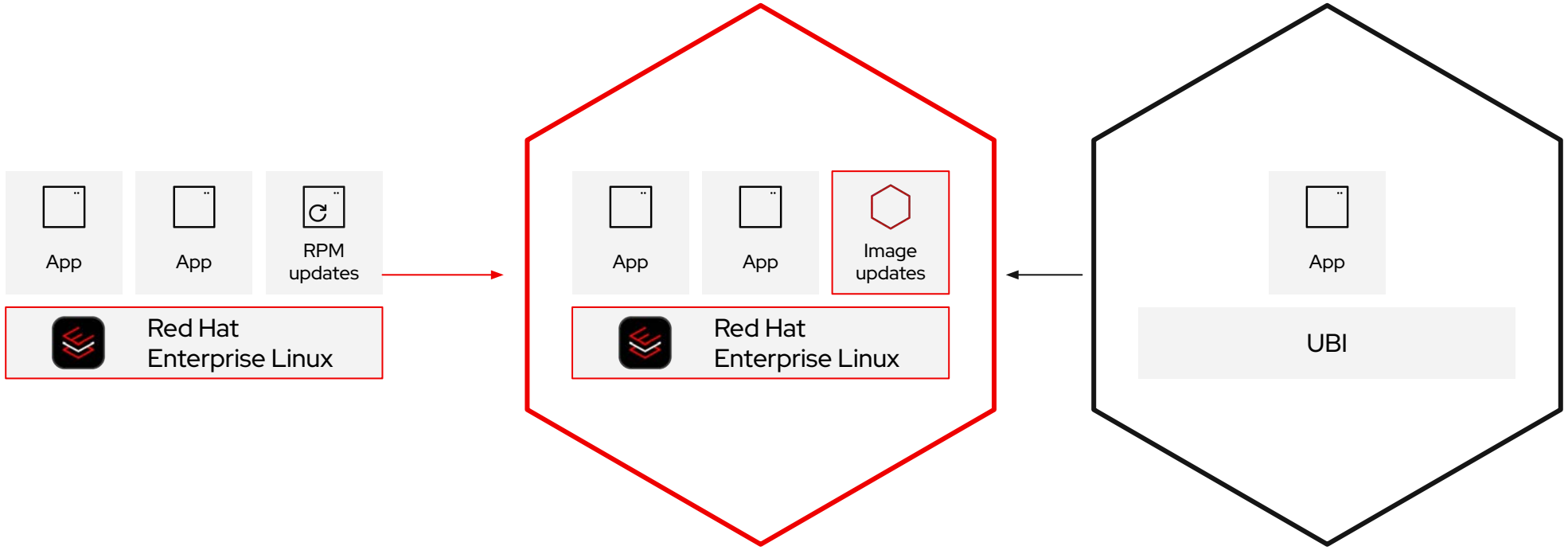
Gain full control over environments, enabling customized solutions for every need and ensuring precise control over included content.

Compliance hardening

Apply the same security hardening profiles across package and image modes for RHEL systems to simplify compliance requirements.

Red Hat

Standardizing and innovating with containers



Package mode

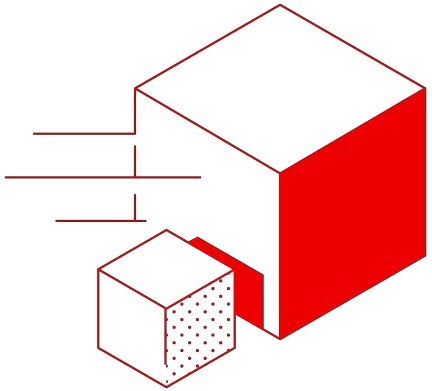
Image mode

Application container

Red Hat

Image mode for RHEL building blocks

- Dedicated bootc base image
- bootc-image-builder
- bootc CLI



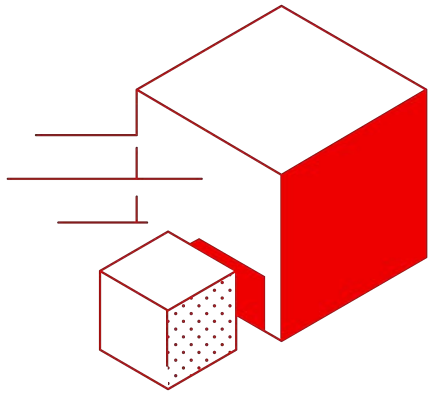




Red Hat

Image mode for RHEL building blocks

- **Dedicated bootc base image**
- bootc-image-builder
- bootc CLI



A base image to rule them all!

Image Specs:

- 439 rpms
- ~785M compressed
- ~2.2G on disk

Primary contents:

- systemd, kernel, bootc
- rpm-ostree
- linux-firmware
- NetworkManager
- podman
- python
- Misc CLI tools: jq, sos

- Available on Quay.io:
  - registry.redhat.io/rhel10/rhel-bootc

Red Hat

Creating a bootc Based Image

It all starts with a standard Containerfile / Dockerfile

```
FROM rhel10/rhel-bootc:latest

RUN dnf install -y [software]
[dependencies] && dnf clean
all

ADD [application]
ADD [configuration files]

RUN [config scripts]
```

Containerfile

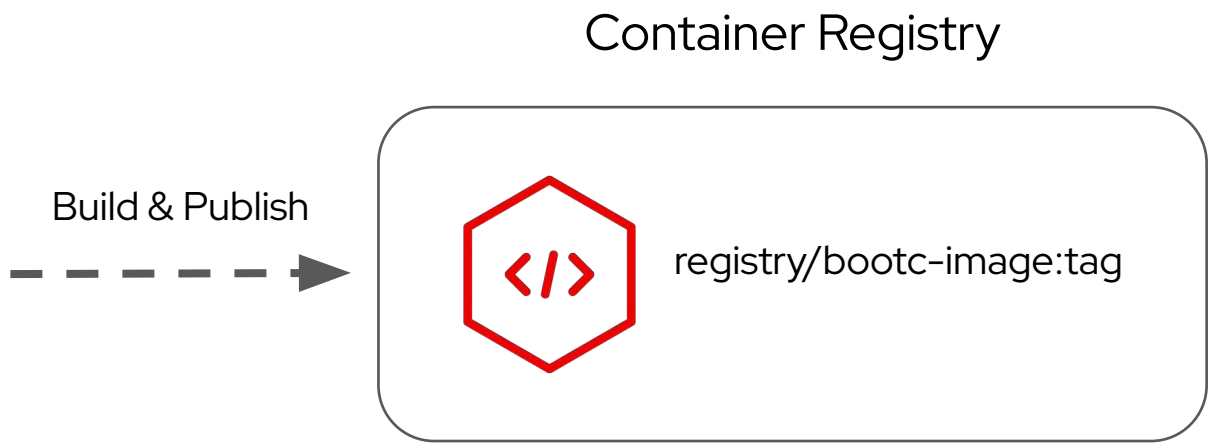


Image mode for RHEL building blocks

- Dedicated bootc base image
- **bootc-image-builder**
- bootc CLI



Convert **bootc images** to consumable formats

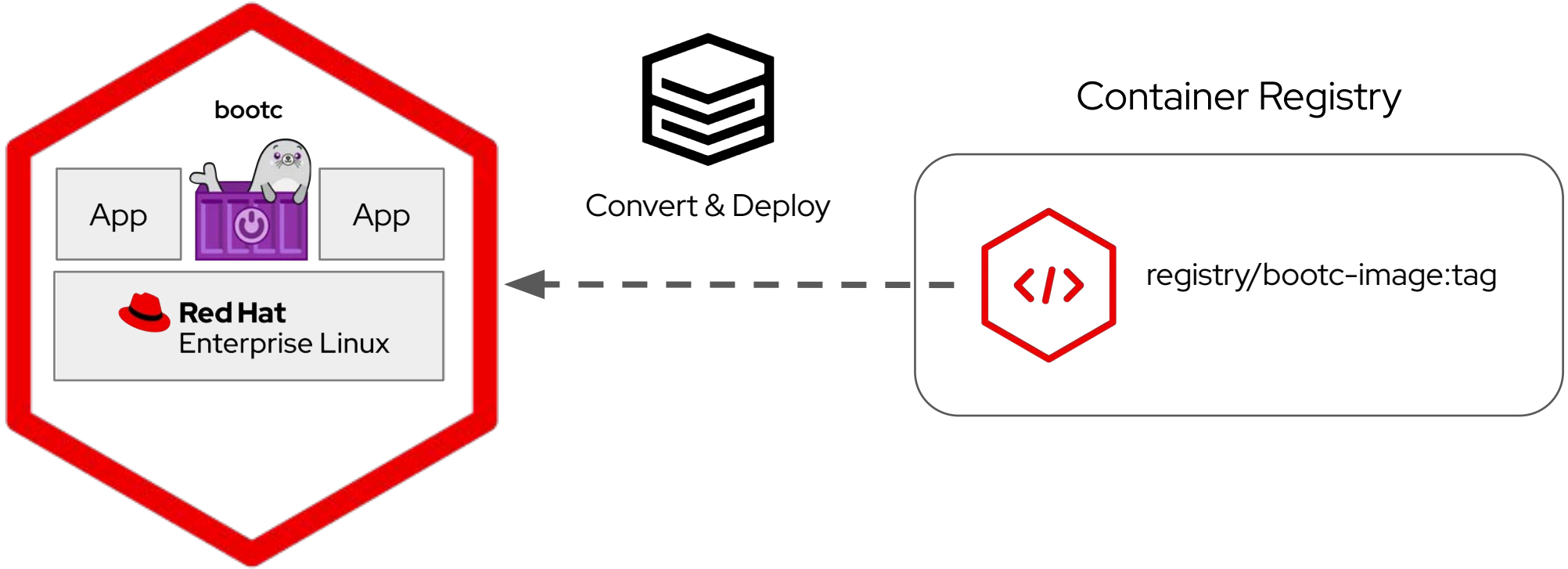
`qcow2`	QEMU Disk Image
`ami`	Amazon Machine Images
`vmdk`	Virtual Machine Disk Image
`vhd`	Azure / Hyper-V disk image
`gce`	Google Compute Engine image
`raw`	MBR/GPT Raw disk image
`iso`	Bare Metal installer

- Available as a container image:
  - registry.redhat.io/rhel10/bootc-image-builder
- Bootable Container Extension for **Podman Desktop**
  - Build for x86 & multi-arch builds

Red Hat

Conversion using bootc-image-builder

Container image to disk image with ease



Red Hat

Image mode for RHEL building blocks

- Dedicated bootc base image
- bootc-image-builder
- **bootc CLI**



Manage the **bootc system** lifecycle

`bootc upgrade`
Download and stage an updated container image based on image reference.

`bootc rollback`
Rollback to the previous state.

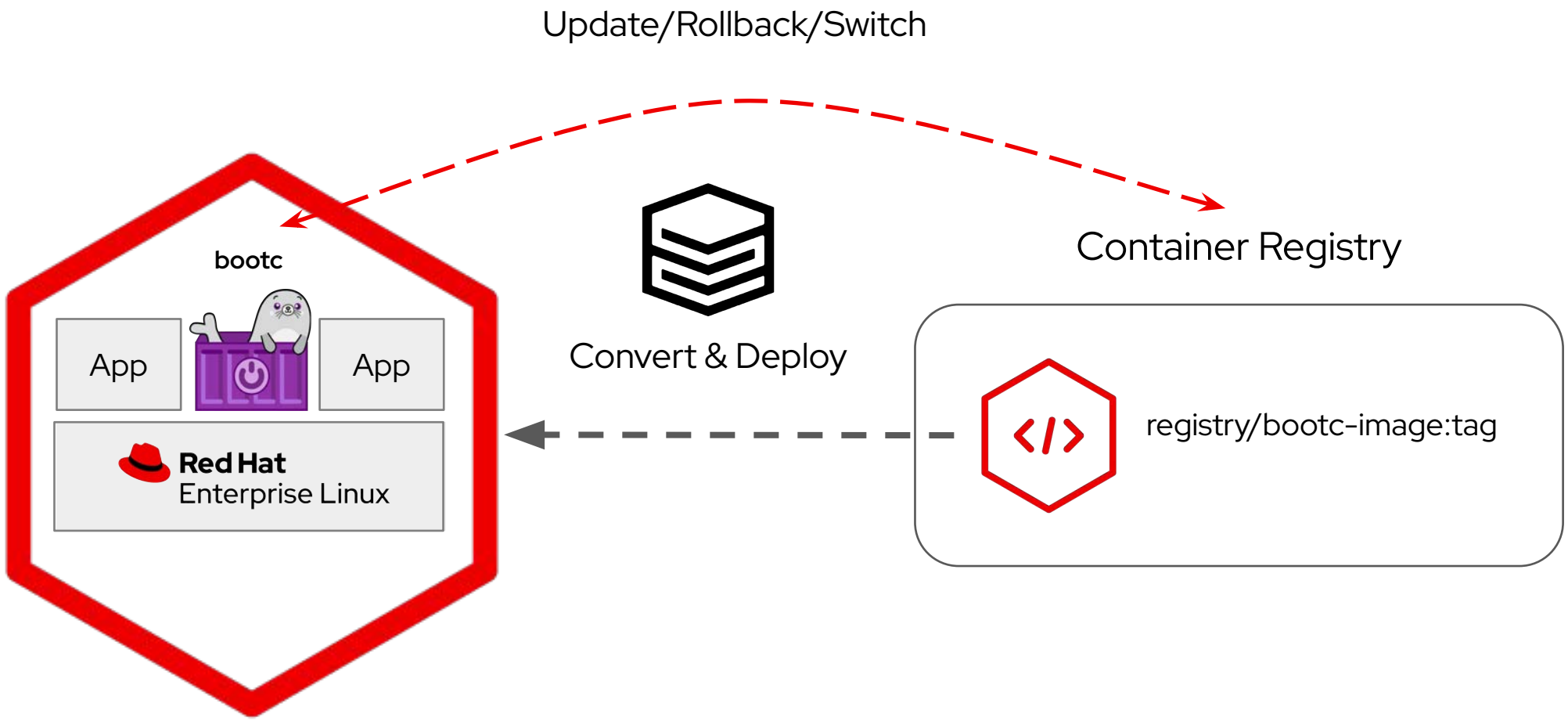
`bootc switch`
Change to a different reference image

`bootc install`
Install container image **`to-disk`** or **`to-filesystem`**

- Upstream docs:
  - https://bootc-dev.github.io/

Red Hat

Manage the Entire Lifecycle

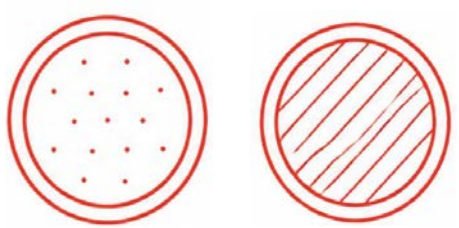


Red Hat

Pizza service

BASE (RHEL Image Mode)

Standardized, consistent foundation

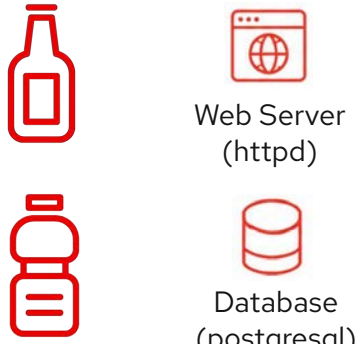


Regular (standard)

Gluten Free (hardened)

Sauce (Base Service)

The core services you offer

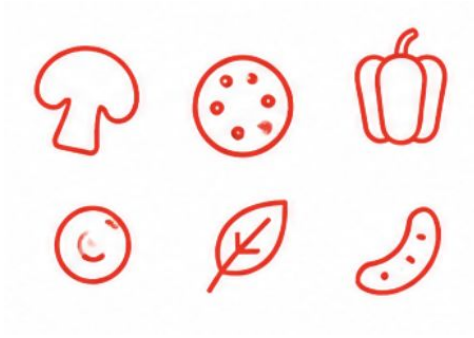


Web Server (httpd)

Database (postgresql)

Toppings (Configuration)

Application and/or config



The Pizza (Running System)

Base + Service + Configuration



The pizza shop provides the dough and the sauce
(IT owns the operating system and base service layer)

The customer decides the toppings
(owned by the application team)

Delivery Service (container registry)



Use Cases

Where does image mode fit today?

Use Cases Blog



AI/ML Stacks

Perfectly version app dependencies from kernel, GPU & accelerator drivers, frameworks, runtimes, etc



1:1 App/Host

Manage the OS AND app as a single unit



Edge appliances

Easily manage a fleet of systems with registries and auto-updates



Standalone container hosts

Use common toolchains and pipelines to build containerized applications and the hosting OS

Red Hat

Available Labs

https://labs.redhat.com

- Image Mode Basics
  Build and deploy an Image Mode system
- Image Mode Day 2 Operations
  Manage a virtual machine running in Image Mode

Try it yourself!

The whole demo shown in this session and other use cases are available in the following Github repository:

https://red.ht/rhel-image-mode-demo

https://gitlab.com/redhat/cop/rhel/rhel-image-mode-cicd

Everybody is welcome to use it, fork and suggest improvements.

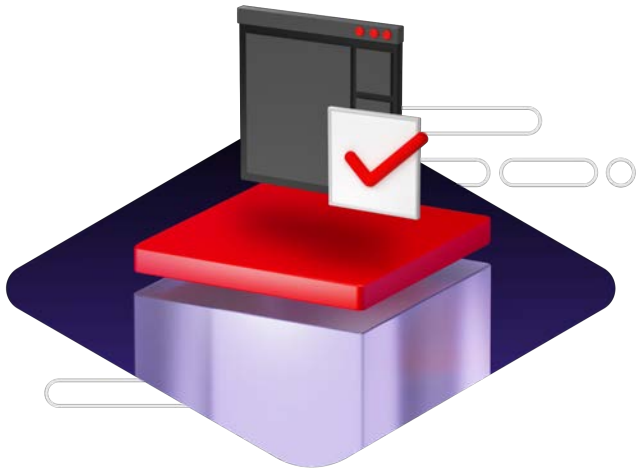


Red Hat

Adding AI to RHEL management







MCP servers

Red Hat

What is MCP?

Model Context Protocol



Open standard

Introduced by Anthropic in November 2024, and later donated to the Agentic AI Foundation



Unlocks new LLM use cases

MCP enables LLMs to interact with outside tools and data sources

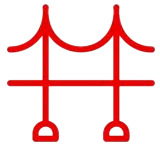
For more info, see:

https://modelcontextprotocol.io/docs/getting-started/intro

Red Hat

We need MCP to bridge the “context” gap

Without MCP, LLMs are powerful, but disconnected from your infrastructure



Bridge between LLM and RHEL infrastructure

Enables LLM to have real-time access to your RHEL system’s actual state (logs, CPU usage, disk space, etc.)



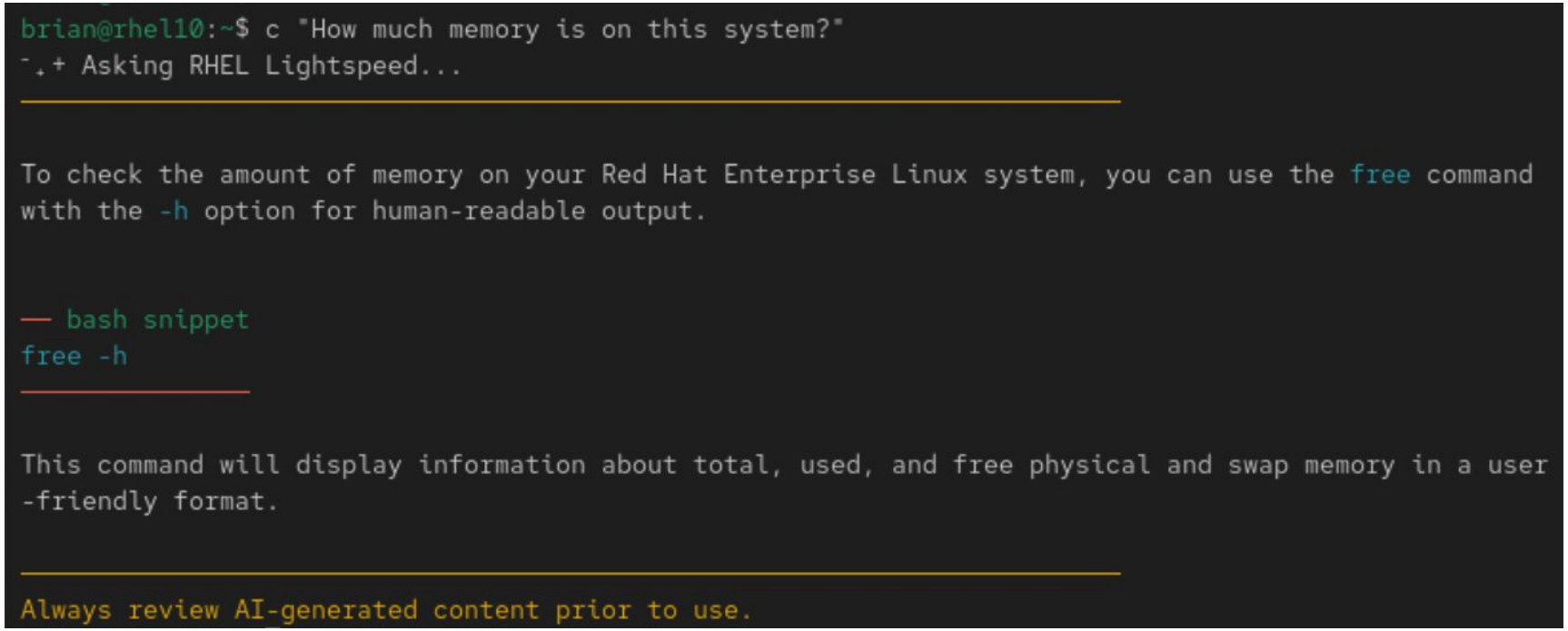
Standardized interoperability

Because MCP is an open standard, it can plug-and-play with a variety of AI clients and tools

Red Hat

Example of life without MCP

Without MCP, the LLM is unable to interact with outside tools and data sources



Example of life with MCP

With MCP, the LLM can use an MCP server to get real-time memory information from the system

```
Context: ○○○○○○○○○○ 0% (0/128000 tokens)
( O)> How much memory is on this system?

── get_memory_information | mcp-server-for-rhel ──────────────────────────

◇  Goose would like to call the above tool, do you allow?
│  Allow
│
The system has 8GB of RAM, with 5.49GB available. There is also 2GB of swap space, all of which is free.


⏱  Elapsed time: 16.02s
Always review AI-generated content prior to use.
```




Prerequisites to get started

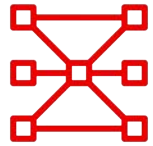
MCP server for RHEL (Developer Preview) is included as part of the value of a RHEL subscription



MCP client

This is the application where you interact with the LLM model.

Use **goose-redhat** or goose from the RHEL Extensions repository, or use the client of your choice which supports the MCP standard.



LLM

Use **goose-redhat** from the RHEL Extensions repository that connects to the Red Hat hosted command line assistant backend infrastructure, or use the LLM of your choice, which can be a hosted model, or a local open source model.

Red Hat

Managing RHEL with MCP

Red Hat Lightspeed

Available as a Developer Preview

Initial use cases:

- Image builder
- Inventory
- Advisor
- Vulnerabilities

Satellite

Launched as a Technology Preview in Satellite 6.18

Documentation

Initial use case:

- Reporting, for example, determine lists of hosts that need to be patched
- Patching hosts
- Promote content views

RHEL

Available as a Developer Preview

Initial use cases include:

- Log analysis
- Performance monitoring
- Troubleshooting

Tools provided by MCP server for RHEL

Pre-vetted read-only tools



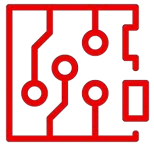
System information

- OS / Kernel
- CPU load
- Memory / RAM
- Disk space
- Hardware



Troubleshooting

- List running processes
- Process details
- List services
- Service status
- System logs
- Service logs
- Specific log file



Network, file, and storage

- Network interface info
- Open ports
- Network connections
- Disk partitions
- List directory info
- List files

For more info, see upstream documentation

https://rhel-lightspeed.github.io/linux-mcp-server/

Red Hat

Example use case: checking health of systems

I have 5 systems named rhel10-server[123].example.com and rhel9-server[12].example.com. Check the health of these systems and generate 2 tables of info: 1 table should have an overview of the systems, and the other table should have a list of high priority potential issues on the systems that should be further investigated.

I'll check the health of all 5 RHEL systems by gathering comprehensive system information. Let me start by collecting data from each system.

- Get System Information host: rhel10-server1.example.com
- Get System Information host: rhel10-server2.example.com
- Get System Information host: rhel10-server3.example.com
- Get System Information host: rhel9-server1.example.com
- Get System Information host: rhel9-server2.example.com
- Get Cpu Information host: rhel10-server1.example.com
- Get Cpu Information host: rhel10-server2.example.com
- Get Cpu Information host: rhel10-server3.example.com



Example use case: checking health of systems

Table 1: System Overview

System	OS	Kernel	Uptime	CPU Cores	RAM (Total/Used/Available)	Root Disk (Total/Used/Use%)	Network IP	Services Running	Failed Services
rhel10-server1	RHEL 10.1 (Coughlan)	6.12.0-124.28.1.el10_1	9h 6m	1 phys / 8 threads	7.5GB / 1GB (13.2%) / 6.5GB	17GB / 17GB / **96%**	192.168.122.34	35	mcelog
rhel10-server2	RHEL 10.1 (Coughlan)	6.12.0-124.28.1.el10_1	1h 33m	1 phys / 1 thread	15.4GB / 989MB (6.3%) / 14.4GB	35GB / 5.1GB / 15%	192.168.122.221	35	mcelog
rhel10-server3	RHEL 10.1 (Coughlan)	6.12.0-124.28.1.el10_1	9h 6m	1 phys / 2 threads	3.6GB / 851MB (23.3%) / 2.7GB	26GB / 4.7GB / 18%	192.168.122.219	35	httpd, mcelog
rhel9-server1	RHEL 9.7 (Plow)	5.14.0-611.24.1.el9_7	6h 50m	1 phys / 10 threads	3.6GB / 748MB (20.5%) / 2.8GB	22GB / 5.2GB / 24%	192.168.122.144	33	mcelog
rhel9-server2	RHEL 9.7 (Plow)	5.14.0-611.24.1.el9_7	6h 50m	1 phys / 2 threads	7.5GB / 812MB (10.6%) / 6.7GB	26GB / 5.5GB / 21%	192.168.122.84	34	mcelog

Table 2: High Priority Potential Issues

Priority	System	Issue	Severity	Description
CRITICAL	rhel10-server1	Root filesystem 96% full	Critical	Only 792MB available on 17GB root filesystem. Immediate action required.
CRITICAL	rhel10-server3	Apache HTTP service failed	Critical	httpd.service is in 'failed' state. May need to restart or diagnose.
HIGH	rhel10-server2	Extremely high CPU usage	High	91.7% user CPU, 8.3% system, 0% idle. System appears overloaded.
HIGH	rhel10-server2	MariaDB environment warnings	High	Unset environment variables: MYSQLD_OPTS, _WSREP_NEW_CLUSTER.
MEDIUM	rhel10-server1	Network packet drops	Medium	16,390 RX packets dropped. May indicate network congestion or interface issues

Next, we'll look into a few of the potential issues identified here



Example use case: report on the security posture

```
I need a report to share with my security operations team to assess the current security posture of our installed servers. Can you provide all the relevant information of my install base (security advisories, vulnerabilities, compliance data, and malware) with the available data from the Lightspeed, Satellite, and RHEL tools?
```

SECURITY METRICS SUMMARY

Metric	Status	Count
Total Systems	✅Managed	76 systems
Critical CVEs	🔴Active	207 vulnerabilities
Security Errata	🔴Pending	1 system with outstanding security updates
Compliance Status	⚠️ Conflicts	Potential policy conflicts detected
Malware Status	✅Clean	No malware detected
Known Exploits	✅None	No active exploit campaigns

RECOMMENDED REMEDIATION STRATEGY

1. **Emergency Patch Window**: Schedule immediate maintenance for OpenSSL vulnerability
2. **Satellite Health Check**: Investigate and resolve error states on 4 hosts
3. **Container Security Audit**: Review container runtime configurations across affected systems
4. **Upgrade Path Validation**: Begin planning for RHEL 9→10 transitions
5. **Continuous Monitoring**: Enhance vulnerability scanning frequency given high CVE density



Example use case: high level overview of CVEs

```
Give me a count of all CVEs that affect my environment AND list the top 5 most important to
fix based on the criticality of the vulnerability.
```

```
## **CVE Summary for Your Environment**

**Total CVEs Affecting Your Infrastructure: 207 unique vulnerabilities**

### **TOP 5 MOST CRITICAL CVEs TO FIX IMMEDIATELY:**

## **🔴CRITICAL PRIORITY**

### **1. CVE-2025-15467**
- **CVSS Score:** 9.8 (Critical)
- **Affected Systems:** 71 systems (100% of your environment)
- **Impact:** OpenSSL stack buffer overflow - potential **remote code execution**
- **Description:** Remote attackers can exploit a stack buffer overflow vulnerability by supplying crafted CMS messa
ges with oversized IV when parsing AuthEnvelopedData structures using AEAD ciphers like AES-GCM
- **Red Hat Advisory:** https://access.redhat.com/security/cve/CVE-2025-15467

### **2. CVE-2026-3497**
- **CVSS Score:** 8.2 (High)
- **Affected Systems:** 69 systems (97% of your environment)
- **Impact:** OpenSSH GSSAPI **information disclosure** and **denial of service**
- **Description:** Remote attackers can exploit unexpected GSSAPI message types during key exchange, leading to unin
itialized connection variables and undefined behavior
- **Red Hat Advisory:** https://access.redhat.com/security/cve/CVE-2026-3497

### **3. CVE-2025-68121**
- **CVSS Score:** 7.4 (Moderate)
- **Affected Systems:** 71 systems (100% of your environment)
- **Impact:** TLS certificate validation **bypass** - **authentication bypass**
- **Description:** Attackers can bypass certificate validation during TLS session resumption when CA settings are mo
```




Example use case: CVE remediation in Satellite

```
Use ONLY the Satellite MCP AND the RHEL MCP servers to help me create a plan to address important
and critical CVEs for rhel-backend host group.
```

```
# **SECURITY VULNERABILITY MANAGEMENT PLAN**

Based on the Satellite MCP and RHEL MCP server data, I've identified critical security issues requiring immediate
attention.

## **EXECUTIVE SUMMARY**

Both systems are **RHEL 10.1** hosts in **ERROR status** with pending security errata. They share identical vulner
ability profiles and require urgent remediation.

## **CRITICAL SECURITY FINDINGS**

### **System Status Summary**
- **Total Systems:** 2 hosts
- **Operating System:** Red Hat Enterprise Linux 10.1
- **Kernel Version:** 6.12.0-124.8.1.el10_1.x86_64
- **Management Platform:** Red Hat Satellite
- **Assessment Date:** April 9, 2026

### **Vulnerability Overview**
Both systems have **7 pending errata** requiring attention:
  - **Security Errata:** 1 critical
  - **Bugfix Errata:** 6 important
- **Applicable Packages:** 24 packages need updates
- **Upgradable Packages:** 24 packages ready for update

## **PRIORITY 1: IMMEDIATE ACTIONS (Next 24 hours)**

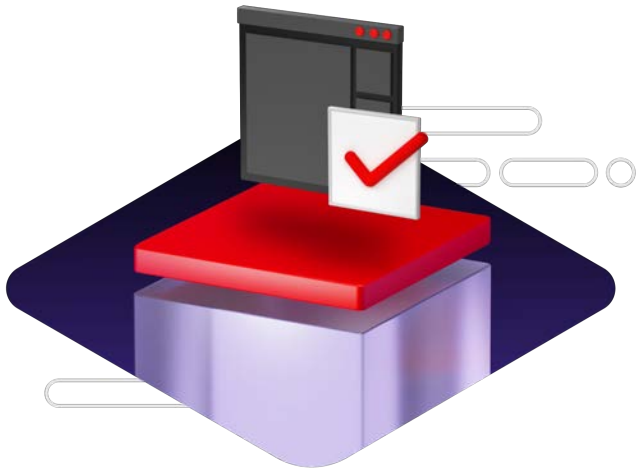
### **Critical Security Updates**
Both systems have **1 critical security errata** that must be applied immediately:
```




How can Red Hat help with the CVE sprawl?







The Challenges

Red Hat

Discovery is exponential. Remediation is linear.



-7 days

Days to exploitation

Attackers exploit before most CVEs are patched [1]



$4.8M

Data breach cost

Cost of a data breach in 2025 [2]



$60B

Attack cost in 2025

Projected $138 billion by 2031 [3]

Source:
1: Anthropic "Project Glasswing" Apr 2026 · NVD Apr 2026 ·
2: IBM Security. "Cost of a Data Breach Report 2025." IBM, 2025,
3: Sonatype 2026 SSSSC

Your attack surface is expanding overnight

AI discovery pours gasoline on the fire with increased volume of CVEs

AI models like Anthropic's Mythos are uncovering vulnerabilities at a scale humans can't match



2,000+

In just 7 weeks, Mythos found over 2,000 **unknown zero-days, and many thousands more since.** The discovery bottleneck has been obliterated.

Source: Mythos Unleashed | Lyrie Research

Red Hat

Self-support security is a significant undertaking

When running a self-supported open source Linux distribution, the following falls to you

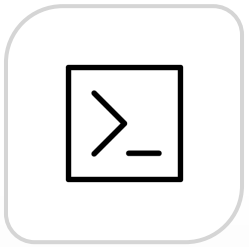
Self-support requires



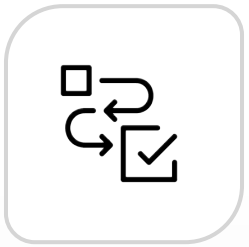
Triage 100s of new CVEs per day



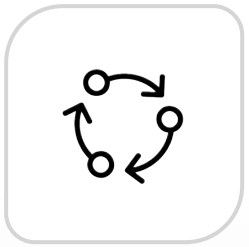
Hunt online for upstream patches



Backport the fix for their version



Quality assurance and testing



Deploy and watch for any issues



In case of fire, ask the community

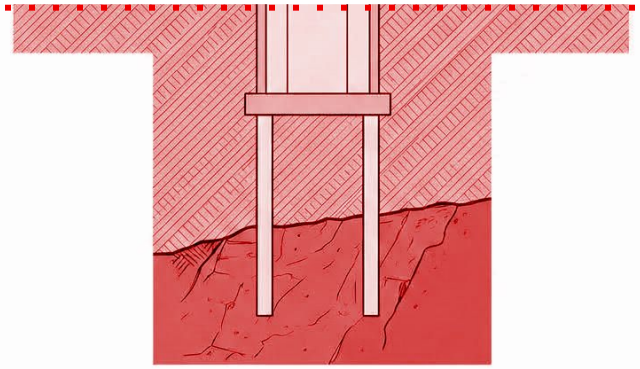
How Red Hat helps with the CVE flood

A hardened platform for applications to **run on**

FOUNDATION LAYER

Red Hat
Enterprise Linux

Red Hat Product Security helps secure the platform applications ***run on.***



FOUNDATION

How Red Hat helps with the CVE flood

Help to secure open source libraries applications are **built with**

APPLICATION LAYER

Lightwell

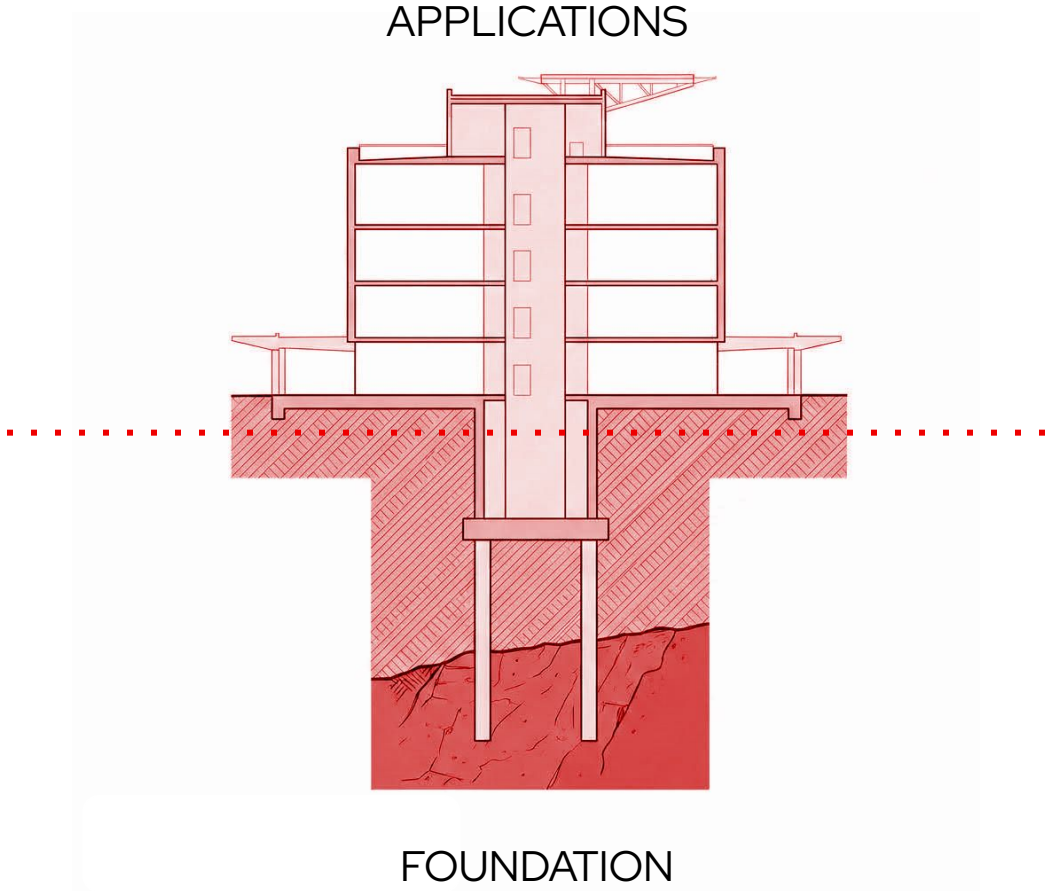
For customer Apps built on maven / PyPI / npm

Helps secure the open source libraries and dependencies that applications are ***built with.***

FOUNDATION LAYER

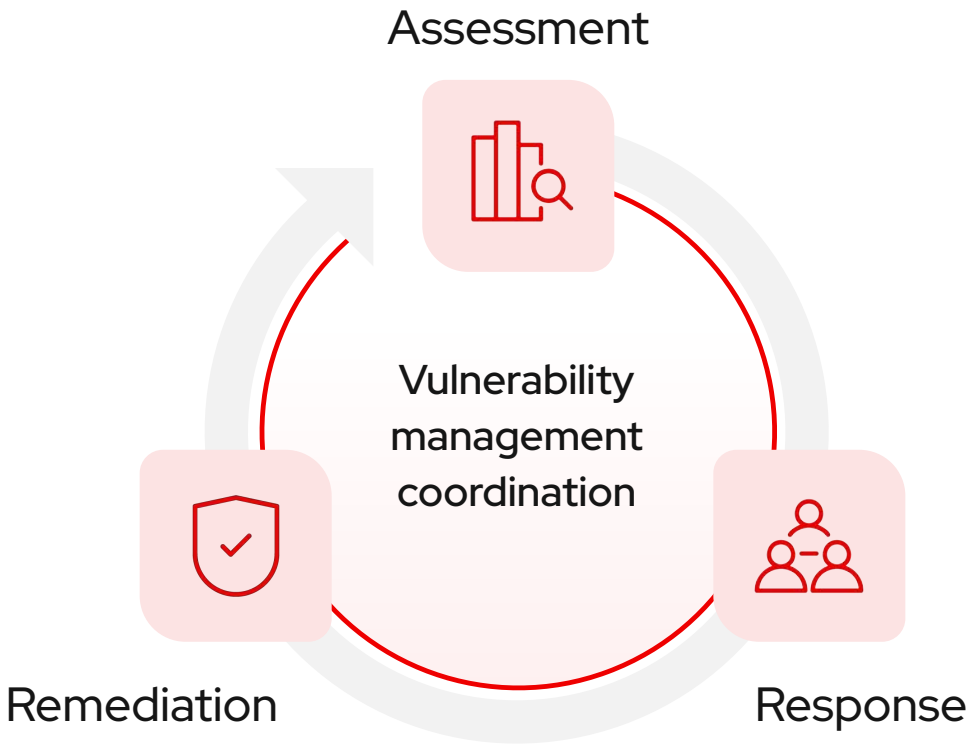
Red Hat
Enterprise Linux

Red Hat Product Security helps secure the platform applications ***run on.***



Red Hat security response at AI scale

Same trusted process, rebuilt for speed and volume



Find earlier

- AI-augmented scanning in CI/CD helps catch issues earlier in production
- Over 455M lines of code scanned (Spring 2026)

Triage smarter

- Expert validation cuts through AI noise
- ~9% signal-to-noise on high-impact findings

Fix and release faster

- Tested, signed advisories at scale
- 2,671 RHEL advisories, only 0.4% were critical (2025)[1]

Source: Red Hat Product Security Risk Report 2025

CI/CD: Continuous Integration and Continuous Delivery/Deployment

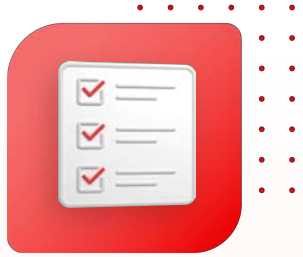
With a Red hat subscription, we take care of these

Offload a massive, non-core technical burden to Red Hat's team of security experts

Red Hat
Enterprise Linux



Monitor for new vulnerabilities



Perform risk assessment



Compliance, standards and testing



Remediation and automation



Red Hat Support in case of fire

Proactive remediation, at any scale



See it

Identifies vulnerabilities in your actual environment, contextualized to your workloads.

Red Hat Lightspeed



Stage it

Loads the patch in content views and promotes it through "dev-test-prod" lifecycle gates.

Red Hat Satellite



Ship it

Applies remediation fleet-wide with a full, policy-driven audit trail.

Red Hat Ansible Automation Platform

Red Hat Enterprise Linux

Start on a hardened foundation with built-in security capabilities

Satellite news



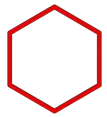


Red Hat Satellite

	6.20 - Nov 2026 *(Limited Availability release)*	May 2027 *(General Availability release)*
Container version	Red Hat Enterprise Linux 10	Red Hat Enterprise Linux 10
Host version	Red Hat Enterprise Linux 10	Red Hat Enterprise Linux 9 + Red Hat Enterprise Linux 10
Who	Product Managers (PMs), approved customers, and internal associates	Everyone
Key features	Post-quantum cryptography (PQC) and sovereign content delivery networks (CDN) support	Event Driven Ansible (EDA), compliance, planning, model context protocol (MCP), and lifecycle flexibility
Constraints	Fresh installs only	None
What	This release is Red Hat's "Security & Sovereignty" release, focused on strengthening Satellite's supply chain via quantum-resistant security and delivering geographically aware updates.	This release is Red Hat's "Agentic & Automation" release focused on delivering integration with the Red Hat Management portfolio (RHEM & AAP), enhanced agentic workflows, and additional on-premise Lightspeed applications.

Upcoming features

November 2026



Deployment flexibility

Containerization provides additional deployment flexibility to allow customers to support larger, more complex, and more resilient topologies



Support Digital Sovereignty efforts

Provide additional Lightspeed applications for customers unwilling or unable to use cloud services. Provide geographically Aware Content Delivery Network (CDN) in the US & EU.



Quantum Resistance

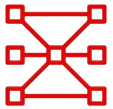
Modernized security stack allows Satellite to operate with quantum resistant encryption algorithms to ensure data integrity.

May 2027



Agentic troubleshooting

Reduce time between failures leveraging local Lightspeed analytics, augmented by the Red Hat Offline Knowledge Portal, even in disconnected environments



Proactive self-healing infrastructure

Drive operational efficiency and remove silos by integrating Satellite's local Lightspeed applications with the Ansible Automation Platform



Lifecycle flexibility

Run Satellite on **your** choice of RHEL version, RHEL 9 or 10, on your schedule

What’s next?





Hands-on Workshop Week • November 30, to December 4, 2026

Red Hat Tech Journey workshop week

One week. Four areas shaping enterprise IT. Hands-on experience.

Discover how to apply open source technologies to build secure platforms, automate operations, and run modern applications across hybrid environments.

Explore the workshops
redhat.com/workshopweek

Red Hat

Q&A





Red Hat Summit

Connect

Thank you

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

x.com/RedHat

Red Hat