

Optimizing IT Operations in the DoD

Run containers and VMs on one cluster

“By optimizing the use of innovative products, improving IT user experiences, and *enhancing operational effectiveness*, we can accelerate the Department’s modernization efforts and expand our military’s strategic advantage.”

Kathleen Hicks
Deputy Secretary of Defense¹

Reduce dependence on legacy virtualization platforms

During its multiyear transition to Linux® containers, the Department of Defense (DoD) will continue to host and manage virtual machines (VMs). Today, hundreds of thousands of VMs contribute to DoD IT operations across all agencies, many supporting mission-critical applications and systems.

Dependence on the existing VM hosting platform causes operational risk, limits paths to modernization, and inhibits innovation. To maintain dominance in modern warfare and improve the nation’s cyber posture, the department needs a modern, cloud-native virtualization infrastructure that:

- ▶ Is secure, trusted, and reliable.
- ▶ Allows rapid delivery of capabilities to warfighters in the theater to outmaneuver the adversary. This requires virtualization infrastructure that can run on any hardware, anywhere—at the tactical edge, in datacenters, and in public clouds.
- ▶ Provides cloud-native development and delivery capabilities to accelerate the department’s modernization efforts, such as automation (e.g., self-healing, software defined storage and networking) and a single source of truth for configuration files.
- ▶ Simplifies infrastructure and reduces maintenance requirements by hosting VMs and containers side by side on the same platform.
- ▶ Meets stringent DoD compliance requirements, such as a trusted software supply chain for platform components, zero trust strategies, Federal Information Processing Standards (FIPS), and others.

Unified platform for VMs and containers: Red Hat OpenShift Virtualization

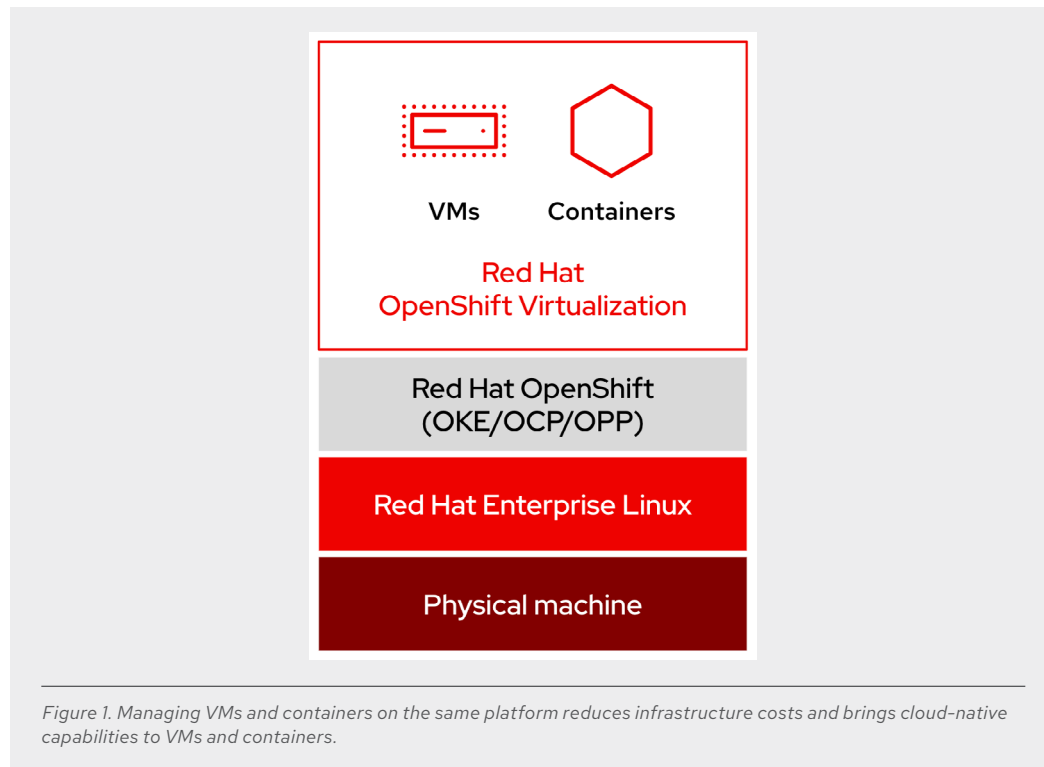
An included feature of all Red Hat® OpenShift® subscriptions, Red Hat OpenShift Virtualization is a modern application platform for running and deploying new and existing VM workloads alongside containers on the same OpenShift nodes. VMs run on the kernel-based VM (KVM) hypervisor included with Linux. They behave as they would on a traditional VM platform while gaining the advantages of modern DevSecOps and [GitOps](#) pipelines. OpenShift is available as a fully managed public cloud service edition or as a self-managed edition that can be deployed across the DoD’s hybrid cloud, including the tactical edge.

Early access to new capabilities for information dominance

With OpenShift Virtualization, VM workloads have access to new capabilities being built around Kubernetes in the Cloud Native Computing Foundation (CNCF) landscape. Among these are [Prometheus](#), [Istio](#), [Knative](#), [Tekton](#), and [Argo CD](#).

Cost-effective AI performance

With OpenShift, the DoD can achieve cloud-like artificial intelligence (AI) application performance in datacenters and the tactical edge—at less cost than in the cloud. OpenShift provides access to on-premise NVIDIA graphics processing units (GPUs) that accelerate AI workloads running either as VMs or containers. Included with Red Hat OpenShift, the NVIDIA GPU Operator provides tools to manage the full lifecycle of NVIDIA software components. Learn more [here](#).



Simplify VM lifecycle by adding cloud-native capabilities

Red Hat OpenShift Virtualization is a Kubernetes Operator built atop the open source [KubeVirt](#) project. It provides additional capabilities that simplify management of VMs at large scale, including push-button automation and cloud-native capabilities built into OpenShift. These capabilities include monitoring and alerting, traffic management and telemetry, serverless environments, continuous integration/continuous delivery (CI/CD) pipelines, GitOps, and more. Using either a graphical user interface (GUI) or command-line interface (CLI), DoD system administrators can:

- ▶ Warm-migrate VMs onto the OpenShift platform at scale using [Migration Toolkit for Virtualization](#), a free tool. The toolkit can import VMs from VMware vSphere, Nutanix, other OpenShift clusters, and image repositories. Source VMs continue running while the data is copied, minimizing downtime. When all data is copied, the administrator stops the running VM and the new instance begins running in the new location.
- ▶ Create and manage new Windows and Linux VMs.
- ▶ Manage network interface controllers and storage disks attached to VMs.
- ▶ Live migrate VMs between nodes in datacenters, cloud, and edge for continuity of operations (COOP).

Red Hat credentials

Red Hat is the [#1 overall contributor to Cloud Native Computing Foundation \(CNCF\)](#) projects. We represent our customers in key communities, encouraging new capabilities and fixing issues. Using our software to build applications gives special operations early access to the latest innovations in security and performance. Our technology complies with standards such as FIPS 140-2, Common Criteria, and others, including an early FIPS 140-3 validation submission that is [pending review](#) at the time of writing.

OpenShift Virtualization Training

Managing Virtual Machines with Red Hat OpenShift Virtualization ([DO316](#))

Red Hat Certified Specialist in OpenShift Virtualization ([EX316](#))

Mission value of OpenShift Virtualization for the DoD

With Red Hat OpenShift Virtualization, DoD software teams can preserve their existing investment in VMs while benefiting from the simplicity and speed of a modern hybrid cloud application platform.

Reduced operational risk. Bringing enterprise-class stability to open source software, Red Hat OpenShift lets the DoD host VMs on any hardware platform, avoiding reliance on any single vendor. In addition, use of open source components supports the DoD's efforts to strengthen the security of end-to-end software supply chains. Open source provides the visibility and traceability that proprietary software lacks, reducing the risk that components will inject malicious software or code into the enterprise.

Technology force multiplier. With a single platform for VMs, container-based, and serverless workloads, DoD IT teams can standardize infrastructure deployment and use a common, consistent set of established tools. DoD software teams can also integrate Red Hat OpenShift with open source development tools they already use for container management, such as GitLab for DevSecOps and JFrog Artifactory for image storage. In addition to reducing Day 2 operational costs, consolidating VMs, Kubernetes containers, and serverless workloads on a single platform lowers infrastructure costs.

A path to infrastructure modernization. OpenShift Virtualization supports DoD infrastructure modernization goals, which call for preserving existing virtualization investments while adopting modern application lifecycle practices such as DevSecOps and automation.

Automation and self healing. The DoD Software Implementation Plan directs agencies to "...leverage automation to replace manual processes and increase the security of DevSecOps processes by reducing human-caused unintentional mistakes or malicious interference with the software integration and delivery process."² Used in conjunction with OpenShift Virtualization, Red Hat Ansible® Automation Platform can automate Day 2 VM operations such as configuration changes, patching, and rebooting. Automation also supports DoD COOP planning. For example, if Ansible Automation Platform detects that a VM has drifted from the desired state, it automatically executes self-healing actions. Similarly, if one node in a cluster stops responding, Ansible Automation Platform can automatically restart services on another node.

Increased flexibility and resilience. Envision a scenario in which VMs for a mission-critical system need to be stood up in a new location within 6 hours. With traditional VM hosting platforms, IT staff need to manually configure the VM for the new environment, a time-consuming and error-prone process that might not be completed by the mission deadline. When Red Hat OpenShift Virtualization is paired with Ansible Automation Platform, VM migration can be executed automatically. Code and files are stored in a centralized Git repository to ensure the configuration is accurate and secure.

Faster time to production for new VMs. By combining OpenShift Virtualization with modern application development processes and tools, such as Red Hat Trusted Software Supply Chain, [Red Hat OpenShift Dev Spaces](#), and [Red Hat Developer Hub](#), the DoD can achieve its objective to deliver resilient software at the speed of relevance.

² *"Department of Defense Software Modernization Implementation Plan Summary."* Department of Defense Chief Information Officer. March 2023.

Security compliance. Both Red Hat OpenShift and Red Hat Ansible Automation Platform have a Security Technical Implementation Guide (STIG) published through Defense Information Systems Agency (DISA). Agency software teams can define different security zones on OpenShift for VMs with similar security profiles. Each security zone is isolated from the others with firewall rules, a technique called microsegmentation. For example, one zone might be reserved for VM workloads containing sensitive information that cannot be shared with workloads outside the zone.

Learn more

For more information, check out [Red Hat's work with the Department of Defense](#).

Learn more about [Red Hat OpenShift Virtualization](#).



About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with [award-winning](#) support, training, and consulting services.

f facebook.com/redhatinc
x @RedHat
in linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

**Europe, Middle East,
and Africa**
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com