

红帽 OpenShift 虚拟化在国防 IT 运维中的应用

减少对传统虚拟化平台的依赖

国防机构仍会继续承担托管和管理虚拟机（VM）的工作。目前，已有数十万台虚拟机为各机构的国防行动提供支持，其中有许多虚拟机还承载着任务关键型应用和系统。这使得其 IT 团队面临着日益增长的压力，亟需优化成本、提高效率并减少网络漏洞。

若继续依赖于现有的虚拟机托管平台，将会引发运维风险，限制现代化路径，并阻碍创新。为在现代战争中保持主导地位并提升网络安全态势，各机构需要一种现代化、云原生的虚拟化基础架构，而且该架构需具备以下特性：

- ▶ 安全、可信且可靠。
- ▶ 能够快速交付功能，以支持和增强国防覆盖范围与实力。这就要求虚拟化基础架构能够在任何硬件、任何地点运行，包括战术边缘、数据中心和公共云。
- ▶ 提供云原生开发和交付能力，以加速机构的现代化进程，例如自动化（如自我修复、软件定义存储和网络）、人工智能，以及配置文件的单一事实来源。
- ▶ 通过在同一平台上并行托管虚拟机和容器，简化基础架构并降低维护需求。
- ▶ 满足严格的合规要求，如平台组件的可信软件供应链、零信任策略、ISO/IEC 标准等。

支持虚拟机和容器的统一平台：红帽 OpenShift 虚拟化

现代应用平台

红帽 OpenShift 虚拟化是所有红帽® OpenShift® 订阅中均包含的一项功能，它作为一款现代应用平台，支持在同一 OpenShift 节点上并行运行和部署全新的及现有的虚拟机工作负载与容器。这些工作负载的运行方式与在传统虚拟机平台上无异，同时还能获得现代 DevSecOps 和 GitOps 管道所带来的优势。OpenShift 既提供完全托管的公共云服务版本，也提供可在各机构的混合云（包括战术边缘）中部署的自助管理版本。



红帽官方微博



红帽官方微信



融入云原生功能，简化虚拟机生命周期管理

红帽 OpenShift 虚拟化是一个基于开源 [KubeVirt](#) 项目构建的 Kubernetes Operator。它提供了一系列增强功能来简化大规模虚拟机管理，包括 OpenShift 内置的一键式自动化与云原生功能。这些功能包括监控与警报、流量管理与遥测、无服务器环境、持续集成/持续交付（CI/CD）管道、GitOps 等。借助图形用户界面（GUI）或命令行界面（CLI），国防机构可以：

- ▶ 使用免费的虚拟化迁移工具包，将虚拟机大规模热迁移至 OpenShift 平台。该工具包可从 VMware vSphere、Nutanix 及其他 OpenShift 集群和镜像存储库中导入虚拟机。在复制数据的过程中，源虚拟机可继续运行，从而最大限度地减少停机时间。所有数据复制完成后，管理员停止源虚拟机，新实例即可在新位置开始运行。
- ▶ 创建和管理新的 Windows 和 Linux® 虚拟机。
- ▶ 管理连接到虚拟机的网络接口控制器和存储磁盘。
- ▶ 在数据中心、云和边缘中的节点之间实时迁移虚拟机，确保运维连续性。

OpenShift 虚拟化在国防领域的使命价值

借助红帽 OpenShift 虚拟化，国防机构软件团队能够在保留对虚拟机现有投资的同时，享受现代混合云应用平台带来的简便性与高效性。

降低运维风险。红帽 OpenShift 为开源软件赋予企业级稳定性，使各机构能够在任意硬件平台上托管虚拟机，避免对单一供应商的依赖。此外，使用开源组件有助于国防机构加强端到端软件供应链的安全防护。开源软件具备专有软件所缺乏的可见性和可追溯性，能够降低组件将恶意软件或代码植入企业系统的风险。

强大技术助力。借助这一可承载承载虚拟机、基于容器的工作负载和无服务器工作负载的统一平台，国防 IT 团队能够实现基础架构部署的标准化，并采用一套通用且一致的成熟工具。国防 IT 软件团队还可以将红帽 OpenShift 与已用于容器管理的开源开发工具相集成，例如用于 DevSecOps 的 GitLab 和用于镜像存储的 JFrog Artifactory。该平台不仅能降低 Day 2 运维成本，更通过将虚拟机、Kubernetes 容器和无服务器工作负载整合到单一平台上，显著减少基础架构成本。

基础架构现代化之路。OpenShift 虚拟化助力国防机构达成基础架构现代化目标，在延续现有虚拟化投资价值的同时，成功引入 DevSecOps 与自动化等现代应用生命周期实践。

自动执行与自我修复。红帽 Ansible® 自动化平台与 OpenShift 虚拟化结合，可实现 Day 2 虚拟机运维的自动化，如配置变更、补丁应用和系统重启。此外，实现自动化还有助于在本地突发紧急事件的情况下，确保系统持续无中断运行。

提升灵活性与弹性。设想这样一种场景：某个任务关键型系统的虚拟机需在 6 小时内于新地点完成部署。在传统虚拟机托管平台中，IT 人员需手动为新环境配置虚拟机，这一过程耗时费力且极易出错，很可能无法在任务截止时间前完成。而若结合使用红帽 OpenShift 虚拟化与 Ansible 自动化平台，便可自动执行虚拟机迁移。代码和文件均存储于 Git 中央存储库中，可确保配置精准无误且安全可靠。

加快新虚拟机的生产就绪速度。通过结合运用 OpenShift 虚拟化与现代应用开发流程及工具，如红帽可信软件供应链、[红帽 OpenShift Dev Spaces](#) 和 [红帽开发人员中心](#)，国防机构能够实现以契合需求的速度交付高弹性软件的目标。

电子安全合规性。红帽会派遣专家团队，协助客户保障 OpenShift 容器环境的安全性并进行合规验证。具体措施包括实施区域隔离和微隔离等安全策略，确保环境满足所有必要要求，以及助力通过 DISA、STIG、BSI 及 E8 等标准的严格验证。

如需了解更多信息，请查看[红帽 OpenShift 虚拟化](#)。



关于红帽

红帽致力于帮助客户跨环境实现标准化，助力开发云原生应用，并利用红帽[一流](#)的支持、培训和咨询服务，实现复杂环境的集成、自动化、安全防护和管理。



红帽官方微博



红帽官方微信

销售及技术支持

800 810 2100
400 890 2100

红帽北京办公地址

北京市朝阳区东大桥路 9 号侨福芳草地大厦 A 座 8 层 邮编: 100020
8610 6533 9300