红帽 OpenShift 虚拟化提升安全防护的四种方式

使用此检查清单，聚焦您的安全防护工作，并在混合云中的虚拟机（VM）和容器之间应用一致的控制措施。下面介绍了利用红帽® OpenShift® 虚拟化工具来增强安全态势并保护工作负载的四种方式。

1 从底层开始强化平台安全性

OpenShift 虚拟化运行于红帽 OpenShift 之上，后者提供了一个可随时进行强化的基础，并能够同时管理容器和虚拟机。这种架构可确保跨所有工作负载实现一致的安全防护实施。

- **利用红帽的合规性 Operator，在红帽 OpenShift 中强制实施合规基准。**合规性 Operator 可让管理员描述集群所需的合规状态，并为他们提供不合规项概述以及相应的修复方法。
- **将 GPU 和 USB 直通限制为仅适用于经批准的设备**，以降低从连接的硬件进行未经授权的数据访问或代码执行的风险。
- **禁用非必要的功能门控，并使用传输层安全性（TLS）强制实施可信容器镜像仓库**，以降低未经验证的镜像和错误配置带来的风险。

2 在各层级控制工作负载

通过将虚拟机作为 Kubernetes 对象进行管理，OpenShift 虚拟化可让您精细地控制谁可以创建、修改工作负载以及与之交互。一致地应用基于角色的访问权限控制（RBAC）和审计策略，确保对关键虚拟机的更改遵循与容器化应用相同的治理模式。

- **对执行访问、虚拟网络计算（VNC）控制台访问和实时迁移操作进行限制，仅限经批准的管理员进行这些操作**，以降低未经授权的更改或数据泄露的风险。
- 在非必要情况下**禁用客户机内存过量使用和可共享磁盘**，这不仅可以减少租户之间的资源争用，也能在单个工作负载遭到入侵时限制风险扩散。
- 针对关键工作负载**实施一致的错误处理和验证策略**，从而避免跨环境行为不一致，并降低静默故障或数据损坏的风险。

3　将网络流量分段以增强安全态势

OpenShift 虚拟化中的安全防护延伸到了网络配置层面。网络控制同时适用于容器和虚拟机级别，因此您可以在所有工作负载间保持相同的微分段模型。

跨这些环境应用一致的网络策略、可观测性和日志记录，可以更快地检测可疑流量模式，并简化故障排除流程。

- **使用虚拟局域网（VLAN）隔离租户或应用流量**，降低网络分段之间进行横向移动的风险。
- 针对敏感工作负载**应用媒体访问控制（MAC）地址欺骗过滤和多网络策略**，有助于防止网络上的身份欺骗，并确保隔离高价值应用的流量。
- **为单根 I/O 虚拟化（SR-IOV）接口等次级网络定义明确的边界**，并将它们映射到特定的工作负载或租户，以确保绕过虚拟交换机的流量仍可管控且可审计。

4　确保存储中的数据完整性

OpenShift 虚拟化将存储安全防护策略纳入与计算和网络相同的管理平面中。

您可以跨虚拟化和容器化工作负载应用相同的加密、访问控制和复制策略，以简化合规与恢复规划。通过集中管理这些控制措施，也能让存储、安全防护和平台团队更轻松地协作制定一致的策略，并随着时间的推移对策略进行审核。

- **限制跨命名空间的 DataVolume（DV）克隆**，确保敏感数据集仅存在于批准的边界内，并避免受监管或高风险信息的非预期传播。
- **禁用不必要的可共享磁盘**，以减少工作负载之间的非预期数据共享，并降低因并发写入而导致数据损坏的风险。
- **验证关键数据的 errorPolicy 设置和存储权限**，确保以可预测的方式处理失败的存储操作，并且只有获授权的工作负载才能读取或写入敏感卷。

后续步骤

阅读完整的 OpenShift 虚拟化安全强化指南，全面了解如何跨混合云强化企业组织 IT 环境的安全态势。

关于红帽

红帽通过一流的支持、培训和咨询服务，帮助客户跨环境实现标准化、开发云原生应用，并实现复杂环境的集成、自动化、安全防护和管理。

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

红帽官方微博　红帽官方微信

cn.redhat.com

版权所有 © 2025 红帽。红帽、红帽 logo 和 OpenShift 是红帽或其子公司在美国和其他国家/地区的商标或注册商标。