Red Hat OpenShift Virtualization 提升資安防護的 4 種方式

使用此檢查清單以將重點擺在您的資安工作，並在混合雲端中的虛擬機器 (VM) 與容器上套用相同的控管措施。本文提供 4 種運用 Red Hat® OpenShift® Virtualization 工具的方式，可讓您強化資安態勢，並保護工作負載。

1 從底層開始強化平台安全性

由於 OpenShift Virtualization 在 Red Hat OpenShift 上執行，因此可直接強化安全性，並能同時管理容器與 VM，可在所有工作負載上執行相同的安全性策略。

- **透過 Red Hat 的 Compliance Operator，在 Red Hat OpenShift 中強制執行合規性基準。**Compliance Operator 可讓系統管理員定義叢集所需的合規狀態，並列出所有不符合項目，以及對應的修復方式。
- **只有核准的裝置可以執行 GPU 與 USB 直通功能**，以降低透過連接硬體，在未獲授權的狀況下存取資料或執行程式碼的風險。
- **停用非必要的功能閘道，並透過傳輸層安全性協定 (TLS) 強制使用受信任的容器登錄檔**，以降低未驗證映像與錯誤設定所帶來的風險。

2 控管各層級的工作負載

OpenShift Virtualization 會以 Kubernetes 物件的形式管理 VM，讓您精細控管可以建立、修改工作負載，以及與工作負載互動的人。套用相同的角色型存取控制 (RBAC) 與稽核原則，確保變更關鍵 VM 時能遵循與容器化應用程式相同的治理模式。

- **限制只有核准的系統管理員可以執行存取、虛擬網路運算 (VNC) 主控台存取，以及即時移轉作業**，以降低未授權變更或資料外洩的風險。
- 在非必要情況下，請**停用訪客記憶體超額配置與可共用磁碟**，以降低租用戶間資源競用的狀況，並在單一工作負載遭到入侵時，減少暴露風險。
- 針對關鍵工作負載**強制套用相同的錯誤處理與驗證原則**，以避免在不同的環境中出現不一致的行為，並降低靜默失敗或資料毀損的風險。

3 區隔網路流量以強化資安態勢

OpenShift Virtualization 的安全性也延伸至網路設定層面。網路控管同時適用於容器與 VM 層級，讓您能在所有工作負載中維持相同的微分段模型。

在這些環境中套用相同的網路原則、可觀測性與記錄機制，更快速偵測可疑的流量模式，並簡化疑難排解流程。

- **使用虛擬區域網路 (VLAN) 來隔離租用戶或應用程式流量**，以降低在不同網路區段之間進行橫向移動的風險。
- **針對敏感工作負載套用媒體存取控制 (MAC) 位址欺騙過濾與多重網路原則**，以協助防止網路上的身分欺騙，並確保隔離高價值應用程式的流量。
- **為 Single Root I/O Virtualization (SR-IOV) 介面等次要網路定義明確的邊界**，並將其對應至特定的工作負載或租用戶，以確保可以控管並稽核繞過虛擬交換器的流量。

4 確保儲存體內資料的完整性

OpenShift Virtualization 將儲存體安全性原則納入與運算與網路相同的管理平面中。

您可以在虛擬化與容器化工作負載之間套用相同的加密、存取控制與複寫原則，以簡化合規性與復原規劃。集中管理這些控管措施，也能讓儲存、資安與平台團隊更容易協同合作，共同制定一致的原則，並隨時間進行稽核。

- **限制在命名空間之間複製 DataVolume (DV)**，以確保敏感資料集僅存在於核准的邊界內，並避免意外散佈受管制或高風險資訊。
- **停用不必要的可共用磁碟**，以降低工作負載之間的非預期資料共享，並減少因同時寫入而導致資料毀損的風險。
- **驗證關鍵資料的 errorPolicy 設定與儲存體權限**，確保能以可預期的方式處理儲存作業失敗的狀況，且只有經授權的工作負載才能讀取或寫入敏感磁碟區。

下一步

閱讀完整的 OpenShift Virtualization 安全強化指南，深入了解如何在混合雲端環境中全面強化您組織的 IT 環境安全性。