Global Knowledge®

Expert Reference Series of White Papers

KVM Security in The Cloud: A Choice That Matters

KVM Security in The Cloud: A Choice That Matters

Kerry Doyle, MA, MSr, CPL

Introduction

Organizations of all sizes have identified the benefits of cloud-based computing, whether it's implementing a private or hybrid cloud on their own or accessing a public cloud through a service provider. Virtualization, a key component for building secure cloud environments, offers many advantages, including higher machine efficiency due to increased utilization, energy savings, and the flexibility to build or destroy virtual machines (VMs) on demand to meet changing organizational needs.

Choosing open-source virtualization over proprietary alternatives can significantly increase savings. However, an open-source Linux Kernel-based virtual machine (KVM) offers several benefits to organizations beyond just cost savings. These benefits include security, reliability, availability, performance, and scalability. In this white paper, we'll look at the relationship between open-source virtualization and the cloud, and explore the security aspects of KVM hypervisor technology, especially in relation to how it leverages SELinux and related capabilities for secure public, private, and hybrid cloud performance.

Introduction to Virtual Machines, and Hypervisors

Virtualization offers the ability to emulate hardware to run multiple operating systems (OSs) on a single computer. It offers a level of efficiency and scalability that makes the complex processing of the cloud possible. One of the reasons why virtualization has proven to be so cost-effective is that it can be implemented on industry-standard x86 system hardware using on-demand, high-capacity networks.

In a virtualized environment, the hypervisor, or virtual machine monitor (VMM), is the software that virtualizes the hardware and provides isolation between the OS processes, or "guests." Without the strict controls put in place by the hypervisor, guests could violate and bypass host security policy, intercept unauthorized client data, and initiate or become the target of security attacks.

In addition, virtual machiones (VMs) require the same kinds of precautions as physical machines, such as applying patches, installing anti-viral protocols, performing security fixes, and providing firewall protection. Hypervisors are designed to manage contention between processes that compete for resources, and they provide the maximum performance possible for each guest VM.

In terms of hypervisor categories, "bare-metal" refers to a hypervisor running directly on the hardware, as opposed to a "hosted" hypervisor that runs within the OS. Further classification groups hypervisors according to types. For example, a Type 1 hypervisor translates physical resources to virtual only once, and a Type 2 hypervisor makes that translation twice.

The capabilities and differences between hypervisor types are often debated. In general, a Type 1 hypervisor controls the hardware and, therefore, manages how resources are allocated to VMs. A Type 2 hypervisor runs on top of another OS (e.g., Windows) and depends on the resource scheduling of that OS. Thus the hypervisor's control is somewhat limited by the OS.

Having efficient CPU control and resource allocation enables the kinds of processing levels that make cloud computing possible. Companies employ virtualization to achieve these higher levels of resource functioning, and cloud providers use virtualization for the same reasons.

One example is web content management provider eZ Systems. The company employs Red Hat Enterprise Linux (RHEL) with KVM along with the open-source elastic cloud, Ixonos, to deliver its management platform and Software-as-a-Service (Saas) features.

eZ Systems found that with the open, hybrid approach of Red Hat and Ixonos, it could provide its customers with the full functionality found in on-premise solutions and the same level of security offered by proprietary alternatives.

Virtualization, the Cloud, and Multi-Tenant Environments

For organizations, the cloud's per-use approach provides tangible relief from hardware or software investments by offering a pay-for-service model. The benefits include greater resource access, dynamic scaling, and improved costs, along with the ease of automated management for resources and performance.

Companies adopt cloud computing to reduce infrastructure overhead, adjust service levels to meet changing needs, and to quickly deliver applications. However, with these advantages come certain limitations, especially in relation to security.

Multi-tenant infrastructures typically offer scaled performance and services based on shared resources, including databases, other applications, and OSs. For some organizations, this leaves them open to a variety of threats both from inside the firewall, as in the case of a private cloud, and from outside.

One example of a company that employs a comprehensive open-source solution is cloud provider Colosseum Online. The company uses both Red Hat Enterprise Virtualization (RHEV) and RHEL KVM not only for its core infrastructure, but also for its cloud platform, which offers IaaS and other services.

RHEV enables the Colosseum IT team to migrate all workloads and specific hypervisors offline for software or hardware updates. Such control extends to security patches, bug fixes, and related updates. It represents a degree of security management and granularity unique to KVM.

The high performance critical to cloud environments and achieved by open-source is due to the fact that KVM leverages Linux to handle high I/O rates. Since it's built into Linux, KVM utilizes many of the OS performance and security capabilities.

When it comes to virtualized environments, such as clouds that contain multiple tenants, the KVM hypervisor provides a level of protection comparable to proprietary technologies. Security takes place at three different levels: the Linux kernel (SELinux), the network filtering level, and hardware isolation.

In the past, open-source solutions lacked a compelling management model with efficient enterprise-level security. However, along with innovations, such as multi-core CPU technology, open-source development via online communities, and support from Open Virtual Alliance (OVA), KVM now offers distinct benefits.

For example, the oVirt project provides advanced capabilities for open-source virtualization management, including high availability, live migration, storage management, and system scheduling. These features, along with high performance and security, make open-source KVM a technology of choice as more datacenters are increasingly mixed open/proprietary environments.

Open-Source KVM vs. Proprietary Approach to Virtualization

Implementing virtualization in the datacenter represents the first step toward leveraging cloud-based computing and reducing costs. For example, in the case of Colosseum Online, the company needed to increase capacity to meet intense provisioning requirements, an expanding customer base, and ongoing management needs.

Instead of operating as a conventional ISP with a standard server-based datacenter, the company wanted to offer co-location, scalable cloud capabilities, and network services.

Colosseum found that moving to an open-source architecture based on RHEL KVM offered the best solution. That's because combining a tightly-integrated, kernel-based hypervisor with an open-source management technology offers a range of advantages, including the following.

Licensing. One reason open-source offers a compelling alternative to proprietary solutions is due to lower software licensing costs. That's because technologies such as RHEV KVM are a fraction of the cost of purchasing a proprietary alternative.

Scalability. KVM's ability to efficiently include more VMs on each physical server increases density and boosts the processing power, reducing the total cost of cloud deployment. For cloud providers, that means improved return on investment (ROI). Since KVM inherits the scalability of Linux, it supports more processors and larger memory, leading to better resource sharing and, by extension, lower costs.

Performance. KVM leverages Linux to handle high I/O rates and features fast VM provisioning. Current advances in management solutions enable KVM to be controlled alongside proprietary VMs in heterogeneous virtualization environments.

Security. KVM expands built-in Linux safeguards by incorporating the managed access control (MAC) of SELinux. KVM security includes a multi-layer set of protections, from the kernel layer through to hypervisor, VM security, hardware isolation, and networking safeguards.

Support. The open-source ecosystem provides critical innovation, primarily through developer communities and the efforts of OVA and its members, such as HP, IBM, Intel, Red Hat, and others. The OVA fosters adoption, encourages interoperability, and promotes best practices, helping to build an ecosystem of third-party solutions for KVM.

KVM Security in Multi-Tenant, Cloud Environments

It's useful to note that security in an open-source KVM environment occurs on three levels: the kernel layer within the Linux OS, network layer, and at the hardware level.

Since its kernel-based protection mechanisms were created early on in Linux development, KVM incorporates key SELinux controls to provide isolation and confinement for processes. This means data and applications are fully protected, even in multi-tenant environments where multiple clients are served by one software instance.

At the kernel level, RHEV KVM maintains the security-hardened virtual host Dom0, which acts as a privileged VM and carries messages to and from the hypervisor. Dom0 represents a minimal Linux implementation and requires its own patches, security scans, and monitoring.

The kernel-level administrative feature, mandatory access control (MAC) and the sVirt API Directory Access Control (DAC) both manage VM resource access. Each supports strong guest isolation and make sure that resource allocation is carefully distributed.

Network filtering represents a second layer of virtualization security. Since virtualization depends on a constant flow of information, filtering ensures separation as network packets travel between machines and hypervisors. KVM manages traffic at this network layer, ensuring effective guest/host communications, bridge filtering, and firewall-related safeguards.

For example, Colosseum Online used RHEL KVM to set up its multiple virtual local area networks (vLANs). These provide customers with a virtual infrastructure to take the place of an array of physical datacenter devices, from physical machines to switches, firewalls, and load balancers.

Built-in processor commands, such as Intel's VM Extensions (VMX) and AMD Secure Virtual Machine (SVM) instructions, constitute the third level of KVM protection and ensure further guest isolation. Such access controls offer hardware isolation protection to prevent any guest from completely controlling the host PC.

Finally, Common Criteria Certification at Evaluation Assurance Level +4 (EAL4+) represents industry-level validation of KVM's virtualization security for the enterprise. The certification ensures that the KVM hypervisor on RHEL and industry-standard x86 servers meets governmental security requirements. Common criteria certification guarantees enterprises, financial institutions, and federal agencies that SELinux and KVM offer stable, high-performance protection for multi-tenant environments based on open source.

Conclusion

KVM virtualization and open-source Linux build on the concept of integrated virtualization, where the hypervisor is a natural extension of the OS. This offers critical advantages in the areas of scalability, performance, and especially security.

Since cloud environments share a common attribute, that is, the allocation of resources, applications, and even OSs, adequate safeguards are essential. And as a core part of the Linux kernel, KVM inherits security features critical to protecting the integrity of cloud environments. KVM has a number of advantages compared to other hypervisors. In addition to performance, it leverages SELinux to provide a very high level of security between VMs. Moreover, allocation features ensure that high priority VMs get the resources they need.

As more organizations evaluate and deploy cloud technology, the risks of unsecured multi-tenancy will become increasingly clear. While lowered costs will remain a key driver, KVM offers greater flexibility, a high degree of security, and processing power unequaled by proprietary technologies.

Learn More

To learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge, Global Knowledge suggests the following courses:

- Red Hat Enterprise Virtualization (RH318)
- Red Hat Enterprise Deployment, Virtualization, and Systems Management (RH401)
- SELinux Policy Administration (RHS429)
- Red Hat Enterprise Security: Network Services (RHS333)

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

Kerry Doyle (MA, MSr, CPL) writes for a diverse group of companies based in technology, business, and higher education. As an educator, former editor at *PC Computing*, reporter for *PC Week Magazine*, and editor at ZDNet/CNet.com, he specializes in computing trends vital to IT professionals, from virtualization and open source to disaster recovery and network storage.