

The Role of the Operating System in Cloud Environments

Judith Hurwitz, President
Marcia Kaufman, COO



**HURWITZ
& ASSOCIATES**
Insight to Action

Sponsored by Red Hat



The Role of the Operating System in Cloud Environments

Cloud computing is a technology deployment approach that has the potential to help organizations better use IT resources to increase flexibility and performance. The underlying automation of cloud-based technology helps organizations access the right computing resource at the right time for an economical price. In addition, cloud-based services can be packaged so that specific workloads can be more easily provisioned through the use of sophisticated automation software. Users of these cloud services are experiencing dramatic improvements in productivity as a result of having consistent access to the right mix of technology to solve business problems. While these productivity improvements result from cloud computing's ability to lift complexity away from the individual user, the cost and productivity benefits of the cloud depend on a highly sophisticated underlying infrastructure.

One of the most important ways to support the underlying complexity of well-managed cloud computing resources is through the operating system. Operating systems such as Linux are designed to support these requirements so that cloud services and application services do not have to recreate underlying technologies tailored for each specific deployment. Users gain control, predictability, scalability, and security by having critical shared infrastructure at the operating system level. In addition, an operating system such as Linux supports important standards that enhance portability and interoperability across cloud environments. Operating system platforms are designed to hide much of the complexity required to support applications running in complex and federated environments. Much of the functionality required for the efficient operation of many applications is built in to the operating system. It needs to work competently in the background to ensure that all the right resources (such as processing power, required memory and storage) are available when needed. In addition, the operating system implements the level of security and quality of service to ensure that applications are able to access the resources needed to deliver an acceptable level of performance.

In an era when the focus is on cloud computing why is the operating system more important than ever? The answer is that in order for end users to benefit from a cloud platform that supports balanced workloads that can scale in a secure manner, the operating system has to be designed to enhance that cloud platform.

One of the most significant requirements for companies adopting cloud computing is the need to adopt a hybrid approach to computing. To do so, most organizations will continue to maintain their traditional data center to support complex mixed workloads. For example, an organization may choose a public cloud environment for development and test workloads, a private cloud for customer-facing web environments that deal with personal information, and a traditional data center for legacy billing and financial workloads. It is no surprise that hybrid computing environments will be the norm. Therefore, it is more important than ever for the operating system to support and federate the

One of the most important ways to support the underlying complexity of well-managed cloud computing resources is through the operating system.



various computing deployment models so they appear to be a single system from a customer experience and a systems and service management perspective.

Operating systems have evolved over the past decade to keep pace with the innovation of distributed computing. In the past it was normal to have each application exist as a closed environment—a world unto itself. However, in order to maintain a competitive advantage in business environments that demand superior customer service and efficient operations, organizations require interoperability across platforms that manage their important applications.

The elements required to create an operationally sophisticated hybrid cloud computing environment include the following four:

- Well defined interfaces that hide implementation details
- Core security services
- The ability to manage virtualization
- Management of workloads to provide quality of service and performance.

In this next section we will detail the issues involved in achieving each of these elements.

Well-defined and abstracted interfaces

It is not a simple task to make applications work effectively in a distributed, heterogeneous environment. To benefit an organization's needs for interoperability and predictability, developers are updating applications so that they consist of well-defined services with well-defined interfaces. Data itself is treated as a separate set of services so that the information can be shared across applications and across customers, suppliers, and partners. In order to manage the interaction between these services either each application has to be designed with its own integration and management services or the applications must be part of a third party infrastructure.

Since the goal of interoperability is to provide flexibility across platforms, it makes sense to leverage third party infrastructure management services. These services have to be mature and well designed in order to support a variety of situations. Linux has the maturity and community support to provide application programming interfaces (APIs) that enable data and services interoperability across distributed environments, including cloud environments. Mature operating systems provide a rich set of services to the applications so that each application doesn't have to invent important functions such as virtual machine monitoring, scheduling, security, power management, and memory management. In addition, if APIs are built on open standards it will help organizations avoid lock in and create a more flexible environment.

Linux has the maturity and community support to provide application programming interfaces (APIs) that enable data and services interoperability across distributed environments, including cloud environments.



For example, linkages will be required to bridge traditional data centers and public or private cloud environments. The fluidity of movement across these systems demands the operating system provide a secure and consistent foundation that makes all the advantages of cloud computing a reality.

Flexibility is one of the hallmarks of cloud computing. However, if customers lack the ability to move data and workloads from one cloud to another, their flexibility is dramatically damaged. Therefore, workloads are best managed if the data or logic is not hard coded into a single cloud platform. In order to gain the true benefits of cloud computing, organizations need to support reusability through well-defined interfaces between software components.

Developers build well-defined interfaces between software components in order to achieve the desired level of reusability. Hard coding applications to fit specific business and cloud technology requirements would tend to slow down the process and make it hard for developers to achieve the level of reusability needed. Not only would this create an enormous amount of work but it would undermine the value and benefit of the cloud as an on demand platform. The operating system must be counted on to make sure the right connections are made between IT resources and the applications. This requirement holds true in all IT environments, but is even more critical in hybrid cloud environments. Therefore, any well-designed cloud environment must have well - defined APIs that allows an application or a service to be plugged into the cloud easily. These interfaces need to be based on open standards to protect customers from being locked into one vendor's cloud environment.

Support for security at the core

Whether your organization is considering a public, private, or hybrid cloud environment, security is the most important foundation to ensure protection for your assets. It is a complicated problem because security issues are exacerbated in a cloud environment that is highly distributed and may involve dynamically connecting and disconnecting from a huge variety of internal and external systems and assets. Therefore, the cloud environment has to protect the identity of users and information from external threats. Even more importantly, security has to be managed across a diverse set of resources, each with its own way of managing security. To support the needs of most organizations, cloud security requires an integrated management capability within the operating system that can track all IT assets in the context of how they are being used. This capability needs to be able to override weak links in the overall system so that the security meets an organization's compliance and governance requirements.

While the cloud itself provides incredible economies of scale that allow customers to share resources, the environment has to be designed in a manner that protects the individual customer's workloads. The prerequisite for effective cloud computing is the ability to isolate workloads from each other.

The operating system must be counted on to make sure the right connections are made between IT resources and the applications. This requirement holds true in all IT environments, but is even more critical in hybrid cloud environments.



Virtualization requires some level of workload isolation since virtualized applications are stored on the same physical server. However, cloud computing adds the concept of multi-tenancy. Multi-tenancy—the sharing of resources by multiple organizations—requires that each customer's data and applications be stored and managed separately from other customers' data and applications.

Both virtualization and multi-tenancy support have to be implemented in a secure manner. As virtualization and multi-tenancy become the norm in cloud environments, it is critical that security be built in at the core. When servers are virtualized it makes it very easy for a new image to be created with little effort. This expansion of virtual images raises the risk of attack because it increases the possibility that a security flaw in the hypervisor can be exploited by a guest instance. It can expose both existing systems and partners that interact with those systems. When security is implemented as a framework within the operating system it improves the overall security of both virtualized and non-virtualized environments. In fact, the same operating system services can apply whether you implementing an on-premises, cloud, private, or public cloud environment.

Managing virtualized workloads

Virtualization is fundamental to cloud computing because it breaks the traditional links between the physical server and the application. Many organizations do not understand how fundamental virtualization will become to their cloud strategy because they are initially focused on improving utilization of underutilized servers.

However, in cloud computing, virtualization impacts more than the physical server. Virtualization is used to abstract various hardware assets so that one piece of hardware can be used in many different situations. In cloud computing it is common for virtualization to be applied to other IT resources as well such as memory, networks, storage, and software. These virtualized environments are controlled and managed by a hypervisor. In essence, the hypervisor is an operating system on the physical hardware and presents the core hardware abstraction and Input/Output instructions needed by the guests in its environment.

The hypervisor plays the role of the traffic cop by bringing order to a complex environment comprised of multiple images of various IT resources. It enables a specific application to exist on many different systems without actually being physically copied onto each system. The Hypervisor relies on important capabilities within the underlying operating system to manage the interaction between applications and their interfaces so that they are well managed and protected.

Virtualization is fundamental to cloud computing because it breaks the traditional links between the physical server and the application.

Workload optimization and Quality of Service

As organizations begin to look at hybrid cloud environments as the foundation for their future IT systems, they are looking for methods of ensuring that this environment will protect the integrity of the customer experience. What does this mean? Looking at individual services in isolation would have been acceptable when each application was operated for a specific group of users. However, in a hybrid cloud environment all the various workloads need to be managed based on the quality of service required by all constituents. This means that complex workloads such as enterprise analytics have to be supported as predictably as simple email workloads.

Customers on the receiving end of these cloud services do not distinguish between workloads. They are only concerned with a predictable quality of service. To achieve the benefits of the cloud, organizations need to understand the different requirements for each of its workload types and create a plan to balance and optimize these workloads. Therefore, there have to be abstracted service management environments that look across workloads so that they can be managed as though they are a single system.

Conclusion: the role of the operating system in hybrid cloud computing management

Cloud computing will inevitably change the way IT services are delivered across an organization's ecosystem of partners, customers, and suppliers. However, relying on this approach to computing across the data center, private and public clouds requires a set of mature, standardized, and well defined abstractions. The Linux operating system because of its maturity, scalability, manageability, and open source community support is an important partner in creating a predictable and manageable hybrid computing future.

... in a hybrid cloud environment all the various workloads need to be managed based on the quality of service required by all constituents. ... [and] enterprise analytics have to be supported as predictably as simple email workloads.



About Hurwitz & Associates

Hurwitz & Associates is a consulting, market research and analyst firm that focuses on how technology solutions solve real world business problems. The firm's research concentrates on disruptive technologies, such as Cloud Computing, Service Oriented Architecture and Web 2.0, Service Management, Information Management, and Social and Collaborative Computing. We help our customers understand how these technologies are reshaping the market and how they can apply them to meet business objectives. The team provides direct customer research, competitive analysis, actionable strategic advice, and thought leadership. Additional information on Hurwitz & Associates can be found at www.hurwitz.com.



© Copyright 2011, Hurwitz & Associates

All rights reserved. No part of this publication may be reproduced or stored in a retrieval system or transmitted in any form or by any means, without the prior written permission of the copyright holder. Hurwitz & Associates is the sole copyright owner of this publication. All trademarks herein are the property of their respective owners.

175 Highland Avenue, 3rd Floor • Needham, MA 02494 • Tel: 617-597-1724
www.hurwitz.com