Virtualization and Mobility in Client and Server Environments

Eduardo Correia

Christchurch Polytechnic Institute of Technology, New Zealand

INTRODUCTION

A great deal of popular software is not designed for mobility (Griffiths, 2004). This is peculiar because many mobile users expect to have easy access to an information infrastructure that links up their mobile phone, laptop, personal digital assistant (PDA), and other devices, while the backend systems of organizations need to be agile, especially as the number, range, and diversity of services and associated technologies grow. Enter virtualization, a technology that has been part of computing for many years, but only fairly recently become mainstream (Intel, 2006; Singh, 2004). It makes use of a virtual machine monitor (VMM), a mechanism that frees up systems from many of the physical constraints of hardware, by adding a software layer that abstracts hardware, so that an entire machine, operating system, applications, and even data can be stored as a set of standard folders and files. While it is well established that this architecture enhances security and reliability (Rosenblum & Garfinkel, 2004), it also enables both users and systems, as this article shows, to be mobile and responsive to change, both in client and server environments.

VMware Workstation, Microsoft Virtual PC, and other virtualization software takes the form of a standard application that can be installed on physical computers. As Figure 1 shows, these applications provide a VMM, which enables one system (the guest) to run within the context of another system (the host). The VMM presents a complete set of virtual hardware to each guest virtual machine (VM) running within this environment. Just as ordinary computers access physical resources, such as memory, processors, hard disks, and network adapters, so too do each of the virtual or guest systems, only their hardware is an instance of a generic abstraction that the VMM generates for each of them. The VMM then mediates various calls made by VMs to access the physical hardware of the host machine. Whereas the standard computer has a single operating system with applications installed to it, a computer with virtualization software runs, in addition, within the VMM one or more operating systems, each with their own applications installed.

MOBILE VIRTUAL MACHINES

While virtual private networks enable users to work from remote locations, as if they are sitting at a machine on the local network to some extent, this approach has certain drawbacks. Users may wish to connect with machines that do not belong to the organization and therefore do not adhere to its policies and standards. Antivirus software may be out of date or updates not installed, for example. One solution is to provide a quarantine area that will allow a machine into the network, but restrict its access to resources until certain criteria have been met. Cisco Systems’ Network Admission Control (NAC) and Microsoft’s Network Access Protection (NAP) are examples of this kind of solution (Conry-Murray, 2005). Alternatively, network administrators can make use of the VMware Assured Computing Environment (ACE) to produce and deploy secure, fully built virtual machines that apply custom policies and adhere to certain specified standards (Burt, 2004).

The fact that it is in effect the VM that forms part of the network and not the physical machine means that it does not matter to the network administrators that these particular hosts may not have the latest antivirus signature files or applied recent updates, as this underlying (physical) system does not interact with the network and cannot influence it in any way. Naturally, the user’s physical machine could fail causing the VM itself to fail, but this will still not affect the network, and restoring the client machine is simply a matter