SGI® Origin® 400 Chosen to Research Security of Virtual Machines and Virtualization Interoperability

One SGI® customer is expanding its efforts to understand the security implications and inter-operability in the area of virtualization. Virtualization allows computer systems, with powerful multi-core processors, such as the Intel® Xeon® processor, and large memory capacity, to be used more efficiently. Traditional IT infrastructure used one physical server to perform one or more server tasks, but with the invention of multi-core processors, additional cores are often sitting idle. With virtualization, multiple "virtual machines" (VMs) run on a single physical machine, allowing for better use of system processors and memory. Each virtual machine acts like it is a separate physical machine, but within the same single server.

SGI® Origin® 400 was chosen to conduct research in the security of virtual machines and the interoperability of different virtualization technologies. Working with SGI Professional Services, the customer has implemented a test bed containing multiple systems running VMware vSphere, Citrix XenServer, and Microsoft Hyper-V. Five Origin 400s were purchased, four with three servers, and one with four servers. Each system had the standard GigE switch and storage controller module (SCM), but was then supplemented by an additional switch and SCM to provide additional networking options and storage features. LUN copy and sharing software were also added to each Origin 400.

The Origin 400 is ideal for the task of testing virtualization interoperability and security for a number of reasons. Firstly, being able to run SGI Console Management across the network allows access to multiple servers from a single screen. This makes all the features of the Origin 400 accessible and easy to

use, allowing their scientists to spend their time doing research, rather than system administration. Faults are quickly identified by the management console, and the tool-less chassis allows for quick maintenance. Also, the features of the two built-in GigE switches, with four NICs available per server (with added mezzanine card) allow the customer to run four VLANs with ten free external ports available for many configuration options. This allows physical separation of host operating system, and three VLANs for the virtual machines as well as a separate, dedicated KVM, separate management function, from host O/S and VMs.

The storage flexibility also proved ideal for this customer's purposes. Each individual server has a pair of disks in RAID1 configuration to hold the operating system. Spare disks are available to serve as image repositories. This allows experimentation using the Origin 400 Storage Control Module to associate one of the spare disks with one of the servers, keeping the original data safe and outside of the experiment. Additionally, the disks can be configured as a second, or third, storage area that can be used to test things like VM failover and VM migration using JBOD or standard RAID levels. Since the Origin 400 allows disks to be abstracted, the customer found that they now have more disk than they need, even in mirrored RAID configurations; plenty of storage for backups and experimentation. The flexibility of prototyping and archiving available with the Origin 400 helps them to do their research effectively and efficiently.

![sgi logo]

Finally, being based upon Intel® Xeon® 5600 processors was appealing since it gave them access to the latest and greatest security features available such as Intel AES (Advanced Encryption Standard) technology and TXT, Trusted Execution Technology. The former allows for better than 50% speed improvement on encryption without the need for additional hardware or bogging down the CPU. TXT secures the computer at boot time by checking behaviors and launch configurations against the last known 'best' configuration, thereby trying to find attempts to alter this by programs trying to steal data or take control of the machine.

Because of their versatile test bed, the customer is able to test a large number of scenarios, including same-vendor clouds, VM interoperability, security best practices for virtual machines and the hypervisor, and virtual machine portability. Their research will benefit hardware, hypervisor, operating system and cloud technology vendors. This research will improve security networked systems, the stability of network services, and the safety of countless day-to-day interactions with the internet.

The customer also purchased an Octane® III workstation and six Rackable™ C1001 servers installed in a Mobirack™ Mobile Data Center.

sgi