Virtual server sprawl highlights security concerns

Ease of deploying virtual machines raises new risks

By Jon Brodkin

Network World |
APR 30, 2008 12:00 AM PST

Virtual server sprawl and various security problems are caused by how easy it is to create virtual machines.

LAS VEGAS -- Think server sprawl is bad now? Just wait till you experience virtual server sprawl. When users can clone a virtual machine with the click of a mouse, or save versions of applications and operating systems for later use, you're asking for trouble if IT doesn't maintain tight control, virtualization management vendor Embotics warned in a session at Interop Las Vegas Tuesday. (Look through our slideshow at other products shown at Interop.)

Server virtualization projects are driven by a desire for consolidation, yet the uncontrolled proliferation of virtual machines can result in the opposite, David Lynch, vice president of marketing for Embotics, said in a session called "Virtualization's Phantom Menace: Security."

RELATED: Hyperconvergence: What's all the hype about?

Physical servers and software resources are wasted by virtual sprawl, which also burdens IT with more manual processes and increased security risk, Lynch said.

"The risk of sprawl is a lot higher in the virtual world than it is in the physical world," he said. "When you think of how common sprawl is in the physical world, that means we're going to see it even more in the virtual world."

Virtual sprawl isn't defined by numbers; it's defined as the proliferation of virtual machines without adequate IT control, Lynch said.

One Embotics customer found itself with more than 5,000 virtual machines and suspected many of them were no longer needed. IT figured out which ones were useless simply by shutting them down and waiting to see if anyone would "yell," Lynch said. Few users noticed when virtual machines were eliminated. It turned out 70% of them were obsolete, but were still consuming network resources and software licenses.

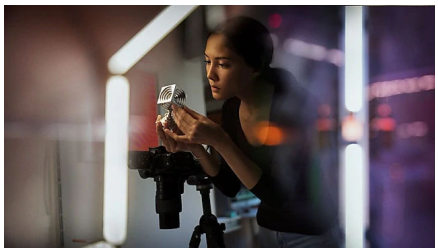
Offline virtual machines present their own problem, in that automatic patching systems don't recognize them, leaving them without critical updates, Lynch said. He recommended that IT shops set policies limiting the amount of time a virtual machine is allowed to stay offline. If it's offline for a period of, say, 30 days, just eliminate it, he said.

The central problem behind sprawl – that virtual machines are so easily generated that IT has trouble tracking how many there are, and when and where they are deployed – only serves to fuel the special security challenges that come with server virtualization.

Most security products today weren't built for the fluid environments of virtualization, Lynch said. Security problems you've already solved in the physical world have a way of cropping up again in the virtual one. The hypervisor is essentially another operating system being introduced into the data center, yet it was introduced without rigid inspection. "Hypervisors came in the back door as an operations tool under the guise of server consolidation," Lynch said. "It never went through the kind of inspection that other technologies have coming into the data center."

Given the hypervisor's access to multiple virtual machines, it's an obvious target for attackers. "If compromised, you can get access to a range of servers," Lynch notes.

The relatively small amount of code in a hypervisor makes it somewhat resistant to malware. But a recently found flaw in VMware's desktop virtualization software raises concerns about the safety of its server virtualization technology, Lynch argued, saying he expects major hypervisor-based attacks this year. Gartner analyst Neil McDonald has said more than 60% of virtual machines in production are less secure than their physical counterparts, Lynch noted.



IDC predicts that half of physical servers will be virtualized by 2011, Lynch said. So-called virtual appliances can be downloaded from VMware's Web site, and could ultimately become the most prevalent way to deploy software, Lynch said. But these appliances also raise new concerns. It's tough to know whether the virtual appliance downloaded over the Web actually comes from a trusted party, or whether updates come from a trusted source, Lynch said.

Virtualization in general requires a new approach to security, but progress on this front is slow and full of roadblocks for enterprises who might be fooled by industry claims, Lynch contended.

IT has to watch out for security vendors that simply take an application, drop it into a virtual machine and claim it's now "virtualization-aware," Lynch said.

Security could be built directly into the hypervisor, but hypervisor designers aren't necessarily security experts, Lynch said.

Some movement is afoot for security tools that are basically hypervisor plug-ins, he noted. IBM introduced an intrusion-prevention project related to virtualization, and VMware in February released a set of APIs designed to give security vendors more visibility into the hypervisor.

This essentially gives more insight into the "black hole the hypervisor guys have created," Lynch said. But unless VMware is really selective about its APIs, new risks could be introduced, he said.

"There's no such thing as private APIs," Lynch said. "They're out and about pretty much as soon as they're announced."

Learn more about this topic

Join the Network World communities on Facebook and LinkedIn to comment on topics that are top of mind.

IT Salary Survey: The results are in

Serious 10-year-old flaw in Linux sudo command; a new version patches it

Test and review of 4 Wi-Fi 6 routers: Who's the fastest?