



Solid-State Disks: A New Type of Storage for Blade Servers

By Jun Alejo

Jun Alejo is a Marcom Specialist at BitMicro Networks (Fremont, CA). You can reach him at jalejo@bitmicro.com.

Blade servers are transforming the server landscape because of their advantages in size, functionality, and total cost of ownership. IDC predicts they will represent nearly 30% of server unit shipments worldwide by 2008.

By separating CPU and memory from components such as cabling, power supply, network connectivity, and cooling systems, blade servers save space in data and telecom centers. Although this enhances scalability and ease of use for IT administrators, it poses design challenges when installing direct attached storage (DAS).

Since several blades already share a power supply, cooling system, and chassis, the logical approach is to use a low-power compact hard drive. For example, one could use the 2.5" form factor already employed in notebook computers. However, for enterprise applications, there is a better solution: flash solid-state disks (SSDs).

Flash SSDs are high-performance, rugged plug-and-play storage devices with no moving parts. Using flash memory chips for storage, they are available in the same standard form factors (2.5", 3.5", and PMC) and interfaces (Fibre Channel, SCSI, and ATA/IDE) as hard drives.

Flash SSDs versus Hard Drives

The key to finding the right DAS for blade servers is to get the best combination of cost and performance. For example, hard disks typically devour around 500mA, whereas flash SSDs consume a mere 50mA. The difference is insignificant in small numbers, but for huge server farms, the cost savings are obvious. Also, mechanical disk drives are guaranteed to operate correctly only within specified temperature ranges. As manufacturers introduce models with high spindle speeds, cooling has become a major issue. In fact, some suppliers offer a dedicated cooling fan or fan and heat sink combination. Unfortunately, the cooling systems of blade servers are shared, and there isn't any space for such add-ons.

Rugged Capabilities

Vendors are searching for better ways to cool densely packed blades. For example, Hewlett Packard's dynamic smart cooling initiative controls heat by focusing cooling on identified "hot spots." Meanwhile, IBM is working on liquid-cooled heat sinks for server processors and water-cooled cabinets. However, these ideas are still under development and are not available now.

A flash SSD generates far less heat than a hard drive since it has no moving parts. Hence it can operate over a wider operating temperature range. This ability makes flash SSD particularly suitable for telecom applications. Telecom carriers deploy gear in remote locations with unpredictable operating conditions, and they need highly reliable equipment.

A typical example of a flash SSD is BitMicro Networks' E-Disk PCI Mezzanine Card (PMC)-based plug-in module. Suitable for blade servers (with a PMC slot) that require a reliable direct-attached storage device, it features horizontal connectors that allow parallel fit onto a blade, giving plug-and-play advantages to system administrators.

Conclusion

Blade servers currently use DAS mainly for system boot and application storage, with a Fibre Channel interface for a separate SAN connection. Flash SSDs can improve system performance with faster access times, high I/O rates, and solid-state durability. With a great combination of performance and ruggedness, flash SSD is an ideal DAS solution for blade servers. ■

An Automated Approach to Securing Your Environment

By Sharon Chang

Sharon Chang is Senior Product Marketing Manager for Opsware (Sunnyvale, CA). You can reach her at schang@opsware.com.

All too often, we hear about viruses wreaking havoc due to outdated software or inconsistently patched servers. Unfortunately, the time and cost of keeping systems updated has made it impossible for most IT departments to completely safeguard their networks. Patch management for operating systems alone cost enterprises more than \$2 billion in 2002, mostly in staff time. Automation software strengthens network security by standardizing server builds and ensuring that labor-intensive IT tasks are done properly and consistently.

An automated approach reduces the time and cost of keeping systems up-to-date and increases the effectiveness of security solutions such as firewalls and intrusion detection. It allows administrators to systematize changes across all servers, regardless of location.

Automation software can also help IT departments catalog their assets. In practice, CIOs often don't know how many servers they have that are vulnerable to the latest virus. Securing an environment is much easier if you know where every server is, which applications are deployed, which require updating, and in what order you should apply patches.

You cannot secure a system without being able to track changes. For example, by tracking deviations from a baseline, automation systems can quickly identify what users – or unwanted intruders – have done to servers, how configurations have changed, which machines need to be locked down, and which backdoors need to be sealed firmly shut. If you cannot recognize changes, how can you identify a vulnerability or security breach?

You must also be able to execute changes quickly and correctly to all servers, regardless of where they are. Many times, seemingly well-guarded environments become vulnerable to attack due to human error in deploying patches or improper maintenance of remote servers.

And while point patch management tools can distribute patches, they cannot do the entire job by themselves. As outside agents, they lack the depth and breadth of coverage to substantially improve the end-to-end security of systems throughout their lifespan.

For example, last year a Windows RPC vulnerability was announced that only affected servers using a certain TCP/IP port. Organizations with IT automation systems could quickly identify which servers used that port and which should be unpatched. They could then actually perform the patching and port shutdown for the identified servers. In contrast, a point solution would not be able to identify the affected servers. It would most likely patch all the systems unnecessarily, typically shutting down critical applications.

Systems such as Opsware's IT automation software capture detailed knowledge in a "living blueprint" of a customer's environment. Hence they can apply changes precisely where needed. This capability is important in decentralized heterogeneous environments, where different versions of operating systems and endless combinations of hardware and software are running on servers located throughout the world. Keeping track of everything is only half the battle; ensuring that it is properly updated in a best practices manner is the other, unwieldy half.

Comprehensive automation strategies that consider people, processes, and technology can turn even the most complex environments into truly impenetrable targets. Automation systems complement perimeter line of defense systems by reducing the chance for human error, keeping systems up-to-date, and ensuring that patches are applied in a timely and uniform manner. Together, these two layers insulate your environment both against external attacks and against the unintended consequences of improperly applied patches. ■