Market Roundup

August 29, 2003

Intel Acquires Pallas' Cluster Group

By Charles King

News stories claiming that Intel had acquired the high-performance computing (HPC) product group from German software developer Pallas were confirmed this week by an Intel spokesperson, who stated the deal is expected to close in September. Financial details were not disclosed. The Pallas HPC group focuses on developing products for monitoring and improving the performance of server clusters, and is also finalizing a product for simplifying the use of grid computing environments. Systems using Pallas' solutions include the top four systems in the Top500.org supercomputer rankings. According to reports, Intel will acquire the 23-person HPC development group in Bruehl, Germany and its software solutions. The group will remain in Germany and become part of Intel's software and solutions group. Intel did not acquire Pallas' security and data management groups.

While acquiring a 23 person software development group hardly qualifies as a barnburner, the Intel/Pallas deal reflects a couple of issues worth further consideration. First, the deal punctuates the growing importance of clustering technologies, both in the HPC and supercomputer space and in a growing number of commercial sectors. While clustered server deployments have long been appreciated in research and university labs, a number of vendors including IBM and HP have found success in developing clustered solutions for a range of commercial applications that were once the sole territory of big box SMP servers. These commercial applications have been further energized by the continuingly evolving price/performance value offered by Intel's Xeon and Pentium processors, and to a lesser extent by Intel's Itanium offerings. By acquiring Pallas HPC development group, Intel is helping to ensure that new generations of its IA-32 and IA-64 processors are optimized for clustered applications before they ever leave manufacturing. This is likely to be good news for Intel and its ISV and vendor partners, as well as for a wide range of the company's customers.

More importantly, the Pallas deal is another step in Intel's transmutation to something rather different from its traditional role as a preeminent chip vendor. Intel is seldom considered in terms of software and in fact, several of the company's forays into this area, such as its Virtual Interface Architecture, have provided their share of problems. But as the performance of hardware components including processors continues to evolve, software has become a prime differentiator for IT vendors of nearly every stripe. Along with utilizing its own homegrown middleware and autonomic computing software to add value to its hardware products, IBM leverages its work with thousands of business ISVs to promote sales in specific industry and market sectors. Microsoft's efforts are key to the ongoing success of Dell and HP in both the commercial and business markets. While chip vendors have traditionally paid a great deal of attention to processor performance issues, a scattering of events including Intel's Pallas acquisition are signaling a new trend. In this case, Intel's focus on wider issues surrounding the performance of its products in clustered environments has Intel taking a longer view that would be more typical of a systems vendor. We regard this development as good news for Intel and its myriad partners, but vendors not fully onboard the IA bandwagon may be less than enthusiastic.

The Sageza Group, Inc.
836 W El Camino Real
Mountain View, CA 94040-2512
650·390·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Munich +49 (0) 89·4201·7144

sageza.com

Sun Sees the Light… and It Is Bright

By Jim Balderston

Sun Microsystems announced this week that it has added approximately 100 new companies to the list of certified vendors of its x86 hardware-compliant Solaris 9 OS offering. The company said that it has had overwhelming response from vendors seeking that certification, which allows Sun's flagship operating system to run on Intel-based computers, and reported that it has sold more than 250,000 seat licenses for the Solaris 9 x86 product. Sun officials said the interest in Solaris 9 x86 comes in the wake of two current influences in the marketplace: the prevalence of the Windows-targeting viruses and worms, and SCO's threats of lawsuits against UNIX users. The licensing fee for Solaris 9 x86 starts at $99.

Sun's decision to license Solaris for the x86 architecture is no small one; in fact it represents a complete about face for a company that has made a long and steady tradition of casting aspersions toward the entire Wintel oligarchy. While some people in Sun may regard this decision as an abandonment of the company's core principles, we see it as a sign that Sun is letting the reality of the market — and not internal theology — guide its strategic planning. In this light, Sun is demonstrating that it has a long way to go before it becomes the next SGI.

Sun has long been the most vocal proponent of 64-bit computing as the be-all/end-all of corporate IT, and its preaching on the subject — while colorful and dramatic — has had little impact on IT churchgoers. For now, much of the market appears to be very happy to move along with continually evolving 32-bit computing solutions. This is especially true for proponents of the growing range of clustered and grid solutions that allow racks of IA-32 servers to behave and perform like robust big footprint machines. In the present climate, asking — let alone expecting — customers to switch over wholesale to a 64-bit environment is more than a bit drastic. As a result, Sun and other 64-bit missionaries have been sailing into strong headwinds in their attempt to maintain meaningful market penetration. Sun's willingness to raise its Solaris 9 x86 platform out of obscurity and press it as a commercial offering apparently reverses this dynamic, allowing Sun and its resellers to sail with the wind at their backs, instead of in their faces. Further, Sun's x86 offering provides the company a means to offer end-to-end solutions to a wider range of businesses beyond Sun's traditional large enterprise clients. Solaris 9 x86 gives new customers the option of bringing Sun in the door without sending their existing IT investments out the window. At the same, Solaris 9 x86 offers existing Sun clients the means to leverage a wide range of robust, affordable x86 products without abandoning Solaris. While some would argue this move is long overdue from Sun, to our minds late is always better than never.

States & Cities Disappointed by DHS's Information Sharing Efforts

By Charles King

The General Accounting Office (GAO) released a report this week that concluded that the Department of Homeland Security (DHS) has been ineffective in coordinating its information-sharing efforts, leading to an atmosphere where clues about terrorist activities may go unnoticed. The Homeland Security Act (HSA) of 2002 requires the DHS to share information with state and local authorities. However, only 35% of the forty states that completed the survey said the federal effort was "effective or very effective" and a mere 15% of the large cities that participated in the survey said they had received information they needed from the DHS on the movement of known terrorists. The GAO report concluded that the DHS's efforts suffer from two major obstacles: the belief by many federal employees that fighting terrorism is primarily Washington's responsibility, and their concerns about sharing national-level evidence with state and local officials. Additionally, the DHS's lack of knowledge about existing state, local, and private-sector information-sharing programs has hindered the creation of an integrated, nationwide system. A spokesperson from the Department of Justice (DOJ) said the DOJ found the report "fundamentally incorrect and unsupported by reliable sources." However, Deputy Secretary of Homeland Security stated that the DHS agreed with the report's overall conclusions and officials from the Department of Defense indicated that they were in general agreement with the report.

In many ways, the failure of the DHS to follow the information mandate the agency received as part of the HSA is hardly surprising. Conceived by the DOJ and enacted by a compliant Congress in the difficult weeks following the Word Trade Center attacks, the HSA was not without controversy. Elements of the act sublimated fundamental constitutional rights, and in recent months a number of HSA provisions have come under attack by legislators who finally got around to reading the fine print of the Act they once vociferously supported. Opposition has become so overt that Attorney General John Ashcroft recently toured the country in an effort to drum up support to leave the HSA untouched. In a sense, the HSA and the DHS are both victims of their own legislated ambitions. Even as the HSA attempted to streamline legal issues according to the DOJ's brave new post-9/11 worldview, the DHS was given the unhappy mandate to effectively centralize security issues and information covering fifty cantankerous states, thousands of irritable towns and cities, and hundreds of millions of mouthy citizens. To be honest, herding this particular band of cats would not be a happy task under any circumstances.

So what is likely to be the eventual outcome of this foolishness? The DHS has suggested that the new enterprise IT architecture the agency will kick start next month, along with "internal and external interfaces and protocols" for information sharing the agency is developing, will help alleviate the problems illuminated by the GAO report. We sincerely doubt it. Considering the history of IT deployments, we expect that soon after the DHS's new architecture is deployed, it will be found to be incompatible with most of the state and local government IT infrastructures it is meant to support. By the time fixes are designed and put in place, the whole pile will be nearing extinction from an IT point of view and construction of a brand new solution will be deemed necessary. There is some small room for hope, though. By the time that second infrastructure is ready for prime time, in another decade or so, the internal and external interfaces and protocols the DHS discussed this week may nearly be ready for implementation.

Transparency vs. Security: The Eternal Struggle

By Jim Balderston

The Computer and Communications Industry Association has sent a letter to the Department of Homeland Security protesting the department's decision last month to purchase $90 million worth of Microsoft software for the department's new computer environment. The association, citing the recent outbreaks of the Blaster and Sobig.f worms and their impacts on the networks as a whole as a result of their attacking Microsoft Windows operating environments, argues that the DHS should consider more secure operating environments for its computer network and "lead by example." The CCIA, which represents a number of companies, including Sun, AOL, Intuit, and Oracle, has been active in filing motions, briefs, and other legal documents related to various legal actions against Microsoft, who is not a member of the CCIA.

The Holy Grail of standardized computing environments is one that many an IT manager has made his or her personal quest. They see such an environment as easy to manage, more cost-effective, and less complex overall. Information can move about freely in such an environment and its consistency alleges fewer headaches associated with the free flow of crucial information around the enterprise. Of course, such transparency comes with risks. If an environment is infected with something like the Sobig.f worm, there is little to stop it from spreading throughout a homogeneous operating system environment. This scenario is not a Microsoft-specific problem; it is one that can occur in any operating environment. Microsoft is the target of many virus writers because of its high profile and ubiquity in the marketplace. For many a virus writer, the goal of widespread havoc is primary, writing viruses for obscure, minimally deployed OS makes as much sense as a graffiti artist doing his or her work in a place where virtually no one will see the fruits of his/her labor.

> *We duly note the partisan nature of this letter, coming from a host of companies that compete with Microsoft and in many cases have made it known that the Redmond-based software giant is their mortal and eternal enemy. That said, we think the issues raised by the letter — especially as the lingering effects of the Blaster and Sobig.f worms continue to hamper email communications — are food for thought.*

We have noted in the past that the number of attacks on Linux-based environments continues to rise and we expect that as Linux's market share grows, so will these attacks. In this regard, size truly matters. One potential means of increased security may be heterogeneous IT environment deployments; viruses that infect one operating system may be stopped within the enterprise when encountering an OS that it is not written for. Such measures, of course, bring greater complexity to the IT manager's task list. We believe that that pursuit of the aforementioned

Holy Grail will and should continue going forward. At the same time, we would argue that this pursuit will come with additional demands for more sophisticated and reliable security at levels that many, if not most, enterprises have not taken or even contemplated to date. In our mind, the lessons of the Sobig.f and Blaster episodes is not that a single OS is more vulnerable than others, it is that the largest, most widely deployed OS was not properly secured by a large number of entities deploying it. Who is to blame for this insecurity is immaterial in our minds; the necessity of rectifying the situation — for Windows or any other OS — is the issue at hand.