

# CDS CONNECTIONS

FALL 2007

## Stay Connected...

Partner Links  
CDSolutions  
In the neighborhood (Events)  
Cutting Edge  
CDS Bytes  
Customer Ties

## Edition 9

Reprint & Published by: CDS Marketing Editors, Guy Merola, VP Finance  
Jonathan Fernandes, Angelic Griego  
Naomi Lorenzo, Cheryl Bates,  
Kathy Brooks SE

**CDS** Connections is brought to you by Commercial Data Systems, Inc. (CDS). This quarterly publication is designed to provide our customers the latest industry trends, company updates, partner information, and highlight solutions that will impact how you do business. CDS provides 'relentless computing solutions' and the IT expertise 'you can trust'.

## Bytes

CDS welcomes three new systems engineers, Kevin Maekawa in Honolulu, Melanie Corn in Albuquerque, and Paul Ford in the DC beltway. Maekawa comes to CDS from Dell and has extensive Citrix experience. He will work onsite at Pearl Harbor Naval Shipyard. Corn's background includes Unix System Administration in the federal government space with agencies such as Lockheed Martin, Muse Technologies Inc, and Sandia National Laboratory. Ford's role within CDS is a PM/Sr. Technical Consultant with experience in Exchange, Active Directory and the National Guard's Distributed Training Technology Program.

Also new to CDS account management in Washington DC is Paul Waltrup who comes to CDS with extensive DOD experience and an MLS background. Troy Apostol has also joined Inside Sales in Honolulu; he will be reporting to new Inside Sales Manager, Malinda Garcia.

## CDS Releases New CDSolution: Virtualization Technology Enhancement

*Cutting Edge: By Charlie Rarick, CDS Product Manager*

### Open Systems End-to-End Virtualization

Commercial Data System (CDS) is pleased to announce the addition of a Server and Storage Virtualization practice to our CDSolutions portfolio. Developed in cooperation with Network Appliance, this solution provides a server-independent platform to reduce infrastructure, provide high availability, and simplify administration.

This architecture leverages Network Appliance storage and VMware's Virtual Infrastructure platform to provide virtual machines that increase performance; reduce power, cooling, and space requirements; and extend the same benefits of high availability to virtual machines that has traditionally only been available to data. This architecture can be used in both Fibre Channel or iSCSI environments, as well as leverage NFS and CIFS, to provide a comprehensive operating system, application, and data protection environment. VMware ESX servers are booted off Network Appliance storage, taking advantage of the high availability provided by Network Appliance's Data OnTap operating system, Write Anywhere File Layout (WAFL) file system, dual parity (RAID-DP), and pointer-based snapshot technology to increase performance and uptime. Virtual machines are also installed on shared storage to provide a centralized architecture and leverage VMware's Vmotion, High Availability (HA), and Dynamic Resource Scheduler (DRS). These provide the capability to rapidly migrate or restart your virtual machines, making available essential operating systems and applications.



### Benefits Include:

- \* High Availability
- \* Power, Cooling, and Space Reduction
- \* Rapid Backup/Recovery
- \* Open System Architecture
- \* Ease of Administration
- \* Application Availability

For more information about other CDSolutions visit [www.cdsinc.com](http://www.cdsinc.com).

## NetApp and Oracle Help Customers Prevent Data Corruption with SnapValidator for Oracle Database 10g

*Reprinted: By NetApp Press Relations*

Network Appliance recently announced the availability of SnapValidator for Oracle Database 10g across all of its modular storage platforms. NetApp is the only company to support the Oracle Hardware Assisted Resilient Data (HARD) Initiative across NFS, FCP, and iSCSI protocols.

SnapValidator for Oracle proactively checks and intercepts potential data corruption or loss, resulting in increased data reliability while helping to reduce risk and unplanned downtime. This end-to-end environments helps customers prevent data corruption before it starts.



Customers with database servers and storage devices often deal with added complexity and increased probability of corruption before data is written. NetApp and Oracle have added intelligence and database awareness to NetApp modular storage systems to provide customers unparalleled protection and validation for Oracle data and eliminate challenges associated with ensuring the accuracy of their data, including unplanned application errors, accidental human errors resulting in potentially copying data onto inappropriate storage resources, and intricate data backup and restore processes that make data susceptible to corruption or loss.

The Oracle HARD Initiative is a vaccine that helps customers prevent business data from becoming corrupted. It is cheaper, quicker, and easier to prevent an infection or corruption than to cure it. Our companies have tightly integrated SnapValidator with Oracle Databases to create a data corruption immune system that detects and eliminates corruptions before they happen. Customers that are dependent on the accuracy of highly sensitive data, particularly within financial services organizations, including major banks and brokerages, can leverage SnapValidator software to add an additional layer of protection, providing peace of mind that their transactions are accurate.

"We created SnapValidator for our customers who are responsible for making certain their Oracle data is unaltered and 100% accurate," said Patrick Rogers, vice president of Solutions Marketing at Network Appliance. "Our customers rely on our products with tight Oracle integration across our entire storage line, so they can remain focused on using their data rather than being preoccupied with its storage and movement."

## 12 Need to Know's about Sun and Microsoft

*Abbrev. Reprint; Submitted by Scott Grams, Sun Microsystems Marketing Manager*



Did you know that Microsoft and Sun Microsystems have a 10-year intellectual property licensing and technology collaboration agreement? Or that Sun offers Windows Server and support on x64 hardware? How about the fact that Sun provides additional utilities and value-added software offerings that leverage Windows servers? The following are 12 things you might not know about Sun and Microsoft:

1. Sun's unique systems offerings, combined with Microsoft's sought-after technology, are helping customers solve their most challenging IT problems. Working along side Microsoft, Sun is providing customers with new levels of scalability, performance, and efficiency, while continuing to provide customers with choice, innovation and value.
2. In 2004, Sun and Microsoft established a 10-year intellectual property licensing and technology collaboration agreement. Sun and Microsoft have expanded that strategic alliance by enabling cross platform virtualization for Solaris™ and Windows.
3. Sun has the industry's broadest line of x64 systems for our customers' Microsoft deployments. Sun's x64 servers give customers top performance, scalability, power efficiency, manageability, and longevity benefits that eclipse the competition.
4. With Microsoft SQL Server and Sun's scale up systems, we offer customers a true 64-bit, scalable database computing platform. Take advantage of a free database "Try and Buy" for SQL Server 2005 and Sun Fire™ X4600 server.
5. As a Microsoft OEM and Gold Certified Partner, Sun offers Windows Server and support on our x64 hardware and provides additional utilities and value-added software offerings leveraging Windows Servers.
6. Sun and Microsoft are collaborating on virtualization technology so Solaris runs well as a guest operating system on Microsoft and that Windows Server runs well as a guest environment on Sun's virtualization technologies. Sun and Microsoft continue to advance the worldwide deployment of the Microsoft Mediroom IPTV and multimedia platform on Sun servers and storage systems, speeding time-to-market for IPTV services.
8. Sun and Microsoft provide key Windows Certifications for Sun x64 systems and StorageTek™ storage arrays, bringing several archiving and retrieval solutions to Microsoft Exchange Server. Together, Sun and Microsoft are achieving world records for integer performance, Java™, Fluent and SPECcap graphics performance.
9. Sun provides customers with fully-integrated hardware and operating system service coverage with full Sun Services support to enable interoperability of Windows on Sun hardware.
10. Sun and Microsoft are a unique platform choice for fast media streaming and archival systems — meeting the security demands of video surveillance and high speed video processing, for collaboration and information-sharing solutions and a leading web application platform.
11. As customers look to consolidate their IT infrastructure on integrated, open, standards-based software systems, Sun offers a Windows Server ready software stack — the Java™ Enterprise System. Java ES helps enterprises reduce and simplify software and licensing costs, lower integration costs, and simplify administration across business units.
12. As a result of our customers and partners' stated need for combined Sun and Microsoft solutions Sun will deliver the software, systems and support to drive innovation across the industry.

## CDS Named Sun Microsystems Executive Partner

CDS has recently been named a Sun Executive Partner, the highest designation available to partners through Sun reselling programs.

Sun's partner advantage program has many competency, accreditation and certifiable curriculum paths, including expertise in both engineering and sales. Only resellers who are highly aligned, with proven capabilities to resell across the Sun business portfolio— Sun Systems, Storage, Software and Services are eligible for executive status. CDS will also provide engineering guidance throughout related projects, from architecture to installation and support.

### Program Requirements Include:

- Strategic Datacenter Elite
- StorageTek Elite
- Software Elite
- Service Delivery Specialty
- Sun Service Support/Delivery Audit certified

Commercial Data Systems is also positioned to sell Sun Microsystems on our own GSA schedule. CDS offers over 60,000 commercial-off-the-shelf (COTS) IT products and services from many manufacturers through our GSA schedule.

**Symantec** recently unveiled a "Healthcare Provider Solution", comprised of products, services and best practices to help healthcare providers protect and manage their critical infrastructure and ensure vital patient information is both protected and accessible.

"Symantec gives Baptist Health the confidence that our critical patient information is protected, and simplifies the management of our infrastructure to help us ensure compliance, better serve our patients and enhance employee productivity," said Allen Montgomery, Baptist Health South Florida, which serves approximately 100,000 patients annually. "We have saved close to \$2 million in IT administration costs, leaving more funding to focus on initiatives that directly benefit our patients."

Healthcare providers and their IT departments are increasingly applying automation to improve patient care quality and reduce costs. With the Healthcare Industry Solution, Symantec enables hospitals and provider networks manage IT risk and maximize IT performance by standardizing and automating their software and processes and over come their most critical business challenges.

 Commercial Data Systems

Connect with CDS

Toll Free: 1-800-527-2970  
[info@cdsinc.com](mailto:info@cdsinc.com)



Mainland HQ:  
4828 Hardware Dr. NE  
Albuquerque, NM 87109

Corporate HQ:  
50 S. Beretania Ste. C208-B  
Honolulu, HI 96812-2222



**Preview...**

\* The top 10 reasons Web sites Get Hacked

Web security is at the top of customers' minds after many well-publicized personal data breaches, but the people who actually build Web applications aren't paying much attention to security, experts say. That's a big problem, and it's one the nonprofit Open Web Application Security Project (OWASP) is trying to solve. An OWASP report called "The Ten Most Critical Web Application Security Vulnerabilities" was issued this year to raise awareness about the biggest security challenges facing Web developers. Below is a summary of OWASP's top 10 Web vulnerabilities, including a description of each problem and how to fix the flaws. For real-world examples, check out the entire list (inside).

**1. Cross site scripting (XSS).** The problem: The "most prevalent and pernicious" Web application security vulnerability, XSS flaws happen when an application sends user data to a Web browser without first validating or encoding the content. This lets hackers execute malicious scripts in a browser, letting them hijack user sessions, deface Web sites, insert hostile content and conduct phishing and malware attacks. *How to protect users:* Use a whitelist to validate all incoming data, which rejects any data that's not specified on the whitelist as being good. This approach is the opposite of blacklisting, which rejects only inputs known to be bad. Additionally, use appropriate encoding of all output data.

## Red Hat Enables Virtualization for HPC Servers

Abbren. Reprint; By Red Hat Press

Red Hat recently announced the availability of Red Hat Enterprise Linux 5.1, with integrated virtualization. This release provides a platform for both customers and software developers with virtualization capabilities complementing Red Hat's newly announced Linux Automation strategy.

Red Hat Enterprise Linux 5.1 virtualization delivers considerably broader server support than proprietary virtualization products, and up to twice the performance. This allows greater server consolidation and eliminates a key obstacle to deploying virtualization more widely.

Red Hat Enterprise Linux's deployment flexibility uniquely allows customers to deploy a single platform, virtual or physical, small or large, throughout their enterprise. By providing one platform that spans the broadest range of x86, x86-64, POWER, Itanium and mainframe servers, regardless of size, core count or capacity, customers can gain dramatic operational and cost efficiencies when compared to proprietary solutions. And fully integrated virtualization, included at no additional cost, amplifies these benefits. Notably, Red Hat Enterprise Linux 5.1 provides enhanced support for virtualization of Microsoft Windows guests, providing significant performance improvements for Windows XP, Windows Server 2000, 2003 and Windows 2008 beta guests.

"With Red Hat Enterprise Linux virtualization, customers can easily deploy any application, anywhere at anytime," said Paul Cormier, executive vice president, Worldwide Engineering at Red Hat. "Other virtualization products don't scale to support large numbers of cores or CPUs, which limit customers' ability to utilize their infrastructure, or force customers to deploy multiple virtualization platforms. With Red Hat Enterprise Linux, customers enjoy a flexible yet consistent application environment for all of their virtualization requirements: from small servers to mainframe-class systems, for Linux and Windows servers and for even the most demanding workloads."

Red Hat Enterprise Linux 5.1 is immediately available to customers via Red Hat Network, Red Hat's management and automation platform. Red Hat Network provides customers a common platform for managing both physical and virtual servers, eliminating the need for organizations to acquire, manage and train their staff on new tools to manage virtual servers. Red Hat Network allows customers to provision, monitor and manage their servers throughout the entire lifecycle.

## In the Neighborhood

### JANUARY

Seminar: "Open Virtualization," presented by Simon Mijolovic, CDS 1/29/08, TBA, ABQ NM

Tradeshow: NCSI Winter TX Series, 01/29/08-1/30/08, San Antonio, TX

### FEBRUARY

Tradeshow: FBC National Guard 02/01/08, Washington DC

Tradeshow: AFCEA West 2008 2/5/-2/7/08, San Diego, CA

Tradeshow: NCSI Ft. Belvoir, 2/7/08

TradeShow: FBC Camp Smith, 2/11/08, Honolulu HI

Tradeshow: Hickam Air Force Base, 2/12/08, Honolulu HI

Tradeshow: Ft. Shafter, 2/13/08, Honolulu, HI

Tradeshow: Schofield Barracks 2/14/08, Honolulu, HI

Tradeshow: Pearl Harbor 2/15/08, Honolulu, HI

Tradeshow: NCSI Norfolk 02/20/08, VA

Tradeshow: FDAE EXPO, Keesler Airforce Base, 2/27/08, Bloxi, MS

### MARCH

Tradeshow: NCSI Naval Surface Warfare Center Dahlgren, 3/5/08

Tradeshow: NCSI Dept. of Transportation, 3/11/08, Washington DC

Tradeshow: FBC White Sands Missile Range, 3/11/08, Las Cruces, NM

Tradeshow: NCSI Robins Airforce Base, 3/12/2008, Warner robins, GA

Tradeshow: FBC Los Alamos National Labs, 3/13/2008, Los Alamos, NM

Tradeshow: NCSI Ft. Mcpherson, 3/14/2008, Atlanta, GA

Tradeshow: DODIIS, 3/16- 3/20/08, San Diego, CA

Tradeshow: 1st Annual Global Civil Affairs Conference & Expo, 3/17-3/19/08, Fayetteville, NC

Tradeshow: NCSI DOE Headquarters, 03/25/08, Washington DC

Tradeshow: NCSI DOE Germantown, 03/26/08

Sun BlackBox Tour: Hurlburt Field, March TBA, Pensacola, FL

## HP Workstation Technology, Unveils Two Quad-core Models

One year after delivering its first workstations based on Quad-Core Intel® Xeon™ processors, HP said customers are experiencing performance increases of up to 400 percent, with double-digit gains in productivity and faster return on investment.(1,2).

HP followed up on this momentum with the unveiling of two upcoming eight-core workstations – the HP xw6600 and HP xw8600 – both powered by two next-generation Quad-Core and Dual-Core Intel Xeon processors.

"Customers can expect HP to be first to market with leading-edge workstation technology at a great value, while improving the customer experience," said John Thompson, vice president and worldwide general manager, Workstations, HP. "As part of our singular focus on satisfying the world's most demanding users of workstation technology, we offer more performance and robust capabilities with an eye towards designing for the environment."

Here is a sneak peek:

- \* Two next-generation Quad-Core Intel Xeon processor 5400 series or Dual-Core Intel Xeon processor 5200 series, based on Intel's new formula for creating chips (Intel 45-nm Hi-k metal gate silicon technology), which provide significantly better performance per watt than their predecessors and eliminate eco-unfriendly lead;

- \* Dual, full-performance PCI Express Gen2 x16 graphics slots;
- \* Memory capacity of up to 128 gigabytes in the HP xw8600;
- \* Storage capacity of up to 5 terabytes;
- \* HP workstations are 90 percent recyclable by weight and now come standard with more than 80 percent efficient power supplies, saving businesses money by reducing power requirements;
- \* Supports HP Remote Graphics Software, Performance Tuning Framework, tool-less chassis, and acoustic optimization technologies; and
- \* Form that is optimized for desk-side, desktop or industry-standard rack mount solutions.

The quad-core HP xw6600 and xw8600 Workstations are expected to begin shipping in mid-December.

## The Top 10 reasons Web sites Get Hacked (continued...)

By Jon Brodtkin, Network World, Abbren. Reprint Submitted by Mike Wysocki, Southwest Channel Sales Manager, F5 Networks

**2. Injection flaws.** The problem: When user-supplied data is sent to interpreters as part of a command or query, hackers trick the interpreter — which interprets text-based commands — into executing unintended commands. *How to protect users:* Avoid using interpreters if possible. "If you must invoke an interpreter, the key method to avoid injections is the use of safe APIs, such as strongly typed parameterized queries and object relational mapping libraries," OWASP writes.

**3. Malicious file execution.** The problem: Hackers can perform remote code execution, remote installation of rootkits, or completely compromise a system. Any type of Web application is vulnerable if it accepts filenames or files from users. The vulnerability may be most common with PHP, a widely used scripting language for Web development. *How to protect users:* Don't use input supplied by users in any filename for server-based resources, such as images and script inclusions. Set firewall rules to prevent new connections to external Web sites and internal systems.

**4. Insecure direct object reference.** The problem: Attackers manipulate direct object references to gain unauthorized access to other objects. It happens when URLs or form parameters contain references to objects such as files, directories, database records or keys. *How to protect users:* Use an index, indirect reference map or another indirect method to avoid exposure of direct object references. If you can't avoid direct references, authorize Web site visitors before using them.

**5. Cross site request forgery.** The problem: "Simple and devastating," this attack takes control of victim's browser when it is logged onto a Web site, and sends malicious requests to the Web application. Web sites are extremely vulnerable, partly because they tend to authorize requests based on session cookies or "remember me" functionality. Banks are potential targets. *How to protect users:* Don't rely on credentials or tokens automatically submitted by browsers. "The only solution is to use a custom token that the browser will not 'remember,'" OWASP writes.

**6. Information leakage and improper error handling.** The problem: Error messages that applications generate and display to users are useful to hackers when they violate privacy or unintentionally leak information about the program's configuration and internal workings. *How to protect users:* Use a testing tool such as OWASP's WebScarab Project to see what errors your application generates. "Applications that have not been tested in this way will almost certainly generate unexpected error output," OWASP writes. *Another tip:* disable or limit detailed error handling, and don't display debug information to users.

**7. Broken authentication and session management.** The problem: User and administrative accounts can be hijacked when applications fail to protect credentials and session tokens from beginning to end. Watch out for privacy violations and the undermining of authorization and accountability controls. *How to protect users:* Communication and credential storage has to be secure. The SSL protocol for transmitting private documents should be the only option for authenticated parts of the application, and credentials should be stored in hashed or encrypted form. Another tip: get rid of custom cookies used for authentication or session management.

**8. Insecure cryptographic storage.** The problem: Many Web developers fail to encrypt sensitive data in storage, even though cryptography is a key part of most Web applications. Even when encryption is present, it's often poorly designed, using inappropriate ciphers. *How to protect users:* Don't invent your own cryptographic algorithms. "Only use approved public algorithms such as AES, RSA public key cryptography, and SHA-256 or better for hashing," OWASP advises. Furthermore, generate keys offline, and never transmit private keys over insecure channels. It's pretty common to store credit card numbers these days, but with a Payment Card Industry Data Security Standard compliance deadline coming next year, OWASP says it's easier to stop storing the numbers altogether.

**9. Insecure communications.** The problem: Similar to No. 8, this is a failure to encrypt network traffic when it's necessary to protect sensitive communications. Attackers can access unprotected conversations, including transmissions of credentials and sensitive information. For this reason, PCI standards require encryption of credit card information transmitted over the Internet. *How to protect users:* Use SSL on any authenticated connection or during the transmission of sensitive data, such as user credentials, credit card details, health records and other private information. SSL or a similar encryption protocol should also be applied to client, partner, staff and administrative access to online systems. Use transport layer security or protocol level encryption to protect communications between parts of your infrastructure, such as Web servers and database systems.

**10. Failure to restrict URL access.** The problem: Some Web pages are supposed to be restricted to a small subset of privileged users, such as administrators. Yet often there's no real protection of these pages, and hackers can find the URLs by making educated guesses. *How to protect users:* Don't assume users will be unaware of hidden URLs. All URLs and business functions should be protected by an effective access control mechanism that verifies the user's role and privileges.