August 2014

PROSYS

Tech Outlook

Dive into Big Data

'Data lakes' built with EMC Isilon scale-out NAS and Hadoop analytics help organizations go with the flow.

In the age of "big data" many organizations are drowning in information but thirsting for knowledge. The "data lake" is an emerging concept driven by powerful data analytics and scale-out storage platforms that could control the rising tide and ensure the efficient use of all that data.

"The idea behind the data lake is actually very simple," said Matt Merriman, VP of Professional Services, ProSys. "It is a system built to store massive amounts of data in any format, combined with an analytics platform that can perform computations on the data in its original format.

"So, instead of placing data in a purpose-built data store, you just move it into a data lake in its native format. This eliminates the upfront costs of managing multiple silos of storage and makes the data available for analysis by anyone in the organization."

Organizations can build enterprise-grade data lakes today by combining EMC Isilon offerings with the Hadoop analytics engine. Isilon scale-out NAS storage is known for its prac-

continued on page 2

TECH OUTLOOK

PRSRT STD
U.S. POSTAGE
PAID
Tulsa, OK
Permit No. 2146

Dive into Big Data

continued from page 1

tically limitless scale, transcending the limitations of legacy file-based storage systems to optimize the flow of information and eliminate the risks associated with complex data migration schemes. Hadoop was designed to enable batch processing of unstructured and structured data at massive scale using commodity hardware.

"Isilon easily handles petabytes of data, and Hadoop deals well with data of any type — together, that's basically the very definition of a data lake," said Merriman.

What Makes Isilon Different

The traditional storage environment is made up of fixed storage containers that don't easily expand in response to data storage growth. In light of that, IT managers are forced to overprovision storage resources to ensure that essential services are not disrupted due to rapidly changing demands. The result is an enormous amount of waste — experts estimate that up to 50 percent of storage sits unused in the typical data center environment.

This model creates operational bottlenecks as well as excess costs. Fixed storage resources require constant oversight due to performance and reliability concerns, creating management inefficiencies that only intensify as storage volumes increase. This storage model also begins to defy traditional data protection techniques, such as mirroring and RAID, as storage capacity expands faster than data can be reconstructed.

Isilon resolves these challenges by focusing on the file system rather than storage hardware. Indeed, hardware is a commodity in an Isilon system, which can support Isilon-certified components from a variety of manufacturers.

Nearly all aspects of the storage system are provided in software by OneFS, the next-generation storage operating system that serves as the intelligence behind the Isilon scale-out NAS platform. With OneFS, the volume manager, file system and RAID are combined in a single file system and single point of management — a radical departure from traditional storage.

"Isilon is designed specifically to provide the capacity, throughput and data protection needed to support the big data environment," Merriman said. "Yet it is cost-effective and easy to manage, with automated, policy-based tiering and single-volume simplicity."

The Isilon Value Proposition

Isilon can scale on demand in terms of capacity, performance and throughput, without downtime or configuration changes. In an Isilon system, industry-standard hardware components function as nodes connected via an Infiniband high-speed interconnect. Each node is identical and therefore a peer, with OneFS running across all nodes to create a single, intelligent storage system.

"This architecture enables performance and capacity to be scaled out linearly by adding more nodes to the cluster — OneFS automatically joins the new nodes and redistributes data evenly across the cluster," said Merriman. "Isilon systems can start as small as 18TB and grow to more than 20PB in a single file system, increasing performance, availability and storage efficiency as it grows."

A single Isilon NAS cluster can support a mix of workloads simultaneously without sacrificing application performance or the specialized data protection required for long-

Hadoop Making Gains

Research from Wikibon indicates that new approaches to data management, most notably Hadoop and NoSQL, are making inroads in the enterprise. In a survey of 303 big data practitioners, 36 percent have deployed Hadoop to support either pilot or production workloads. The majority of Hadoop practitioners have shifted at least one workload from an existing enterprise data warehouse or mainframe to Hadoop.

Among the current obstacles to the success of big data analytics initiatives cited by survey respondents were difficulty transforming data into suitable form for analysis, difficulty integrating multiple data sources and difficulty integrating big data technologies into existing infrastructure.

"Through our research, Wikibon has identified a number of common barriers to successful Big Data analytics projects. Interestingly, many of the top barriers are not related to analyzing data per se, but preparing data to be analyzed," said Wikibon Principal Research Contributor Jeff Kelly. "There are also a number of non-technology barriers cited by respondents, including challenges 'selling' the value of Big Data analytics to reluctant end-users on the business side."

term data retention. Isilon SmartPools provides automatic storage tiering to ensure that data is stored in the best medium for maximum protection and cost savings. With SmartPools, multiple tiers of Isilon scale-out NAS nodes can exist within a single file system with a single point of management.

This functionality comes in a solution that is cost-effective and easy to administer. Organizations can choose the right storage for specific tasks — from analysis to reporting to archival — and one person can manage tens of petabytes as easily as 100TB. As a result, organizations can reduce operating costs while providing the agility and scale to meet changing business needs.

What's New

Two new Isilon platforms and an update of the OneFS operating system promise to further enable data lakes by providing improved performance and heightened agility over previous generations. The new products and capabilities, which include ongoing support for the Hadoop Distributed File System, provide advanced capabilities for ingesting, storing, protecting and managing massive amounts of unstructured data.

The latest version of OneFS includes SmartFlash, a flash-based cache that scales up to 1PB in a single cluster and enables customers to get to their data more quickly. The result is optimized performance with simplified management, 100 percent flash efficiency and reduced latency for traditional and next-generation workloads.

EMC also unveiled the Isilon S210 and X410. The Isilon S210 runs up to 3.75 million IOPS per cluster and provides flexible configuration and deployment, making it ideal for high transactional workloads in industries such as media and entertainment and financial services. The Isilon X410 offers a 70 percent increase in throughput with a 33 percent lower price per MBPS, and its versatility easily supports Hadoop analytics, high performance computing and enterprise file applications.

"The Isilon scale-out data lake is EMC's strategy to solve the world's biggest storage challenge —the growth of unstructured data created by traditional and next-gen applications," said Sam Grocott, Vice President of Product Management and Product Marketing, EMC Isilon. "This rollout of the new EMC Isilon software, platforms and solutions are designed to help our customers address these challenges while driving faster time to results and reducing costs."

Tech Outlook

Editorial Correspondence:
7360 E. 38th St.,
Tulsa, OK 74145
Phone (800) 726-7667
Fax (918) 270-7134

Change of Address: Send corrected address label to the above address.

ProSys locations

Atlanta, GA
(Headquarters)
Phone: 678-268-1300
Toll-Free: 888-337-2626
chash@prosysis.com

Atlanta, GA
(Integration Center)
Phone: 678-268-9000
Toll Free: 888-337-2626
twheless@prosysis.com

Austin, TX
Phone: 512-658-5847
Toll Free: 888-337-2626
jwestmoreland@prosysis.com

Birmingham/Montgomery, AL
Phone: 205-314-5746
Toll-Free: 800-863-9778
birminghamsales@prosysis.com

The Carolinas
Toll-Free: 888-337-2626
chash@prosysis.com

Knoxville, TN
Phone: 865-310-8843
Toll-Free: 800-863-9778
pmadden@prosysis.com

Lexington, KY
Phone: 859-887-1023
Toll-Free: 800-863-9778
dclemmons@prosysis.com

Louisville, KY
Phone: 502-719-2101
Toll-Free: 800-863-9778
dclemmons@prosysis.com

Miami, FL
Phone: 305-256-8382
Toll-Free: 800-891-8123
lspivack@prosysis.com

Mid-Atlantic
Phone: 800-634-2588 ext 2
midatlantic@prosysis.com

Nashville, TN
Phone: 615-301-5200
Toll-Free: 800-863-9778
dclemmons@prosysis.com

New England
Toll Free: 800-634-2588 ext 1
newengland@prosysis.com

New York/Metro
Toll Free: 800-634-2588 ext 3
nymetro@prosysis.com

Seattle
Phone: 425-939-0342
sballantyne@prosysis.com

Tampa, FL
Phone: 813-440-2410
800-891-8123
lspivack@prosysis.com

Washington D.C.
Phone: 703-351-5010
Howard.Klayman@prosysis.com

Virtual Work, Real IT Challenges

As virtual working becomes more prevalent, organizations need to ensure they have the right tools and processes to support remote employees.

Virtual working has become the reality of business today. The number of virtual workers — including telecommuters and mobile personnel — continues to increase dramatically, as employees take advantage of ubiquitous connectivity to free themselves from the confines of headquarters.

In February 2013, Yahoo CEO Marissa Mayer announced that the company would ban telework. In October 2013, HP decided to cut back telecommuting significantly. Nevertheless, a study released that same month by global human resources association WorldatWork found that 88 percent of companies offer some form of telework. Respondents said they believe workplace flexibility has a positive effective on employee engagement, motivation and satisfaction.

The Society for Human Resource Management (SHRM) in April released its 2014 National Study of Employers, which found that flexibility over when and where full-time employees work is on the rise. This includes options such as occasional telecommuting, which saw an increase to 67 percent from 50 percent in 2008.

Virtual working offers numerous benefits, including increased job satisfaction for employees and access to a larger talent pool for employers — 89 percent of survey respondents rated the opportunity to work remotely as an important fringe benefit. Time savings, increased productivity and the opportunity to focus on work rather than becoming distracted by office politics emerged as the top three benefits workers appreciate in remote collaboration.

However, organizations need to ensure that remote employees have the IT tools they need, and that IT teams are ready to support them. Of course remote workers need a PC or laptop and a reliable Internet connection. But they will also need strong collaboration tools and trusted access to applications and data. In addition, the organization needs to ensure that it has enough bandwidth to support remote users, strong security and solid help desk support.

Supporting Collaboration

While Yahoo's decision to ban telework was motivated in part by a sense that employees were shirking their duties, HP ostensibly wanted to increase "face time" within the organization. An internal company memo reportedly stated that the desire to "create a more connected workforce and drive greater collaboration and innovation" drove the new policy.

Without the right collaboration tools, virtual workers can feel isolated. A lack of direct communication remains

the biggest obstacle to efficient remote collaboration, along with hindered data accessibility and poor visibility into colleagues' activities. The right technology can overcome this roadblocks, however.

Unified communications solutions enable remote workers to use the company phone and conferencing systems as if they were in the office. Calls can be forwarded to the worker's home or cell phone, or a PC-based softphone utilized to serve as the worker's extension. Voice mail can be managed through an email client.

Video and web conferencing bring remote workers together for face-to-face communication and allow content sharing. Easy-to-use conferencing solutions support spontaneous, ad-hoc meetings among geographically dispersed teams, boosting productivity, cutting costs and enabling faster decisions.

The unified communications solution should also enable instant messaging for rapid communications with team members and other coworkers. Instant messaging is a subset of so-called "presence" technology, which enables workers to see who is available and the best way to communicate with them. Presence eliminates phone tag and enables remote workers to collaborate seamlessly — an instant message can become a phone call which can become a video conference with just a few clicks.

Enabling Access

Virtual workers also need access to applications and data. A virtual private network coupled with remote desktop protocol can enable remote workers to access their work PCs. However, this may not be the ideal solution for employees who only work remotely. A virtual desktop solution stores the user's desktop on a server in the data center so that it can be accessed from a wide range of devices.

With application virtualization, applications are centralized in the data center where they can be accessed by various devices or streamed to a PC for offline use. Application virtualization makes it possible for remote workers to access legacy applications that aren't web-based. Best of all, remote workers get the same performance as in-house users, even with bandwidth-intensive applications.

Of course, web- and cloud-based applications can be accessed by any employee with an Internet connection. Single sign-on solutions can make it easier for remote workers to access these resources and also improve security.

Whatever the solution, it must be easy to use and reliable. In addition, help desk personnel should be trained in supporting teleworkers. Remote employees should not have to troubleshoot IT problems in order to do their jobs.

The results of the WorldatWork and SHRM surveys underscore the growing demand for virtual work capabilities — whether employees are on the road or working from home — across both small and large enterprises. Given the prominent role virtual work is expected to play in the future of business, organizations should begin planning now to ensure that remote employees have the IT tools they need.

Federal Telework Benefits Taxpayers, Environment

Federal employees who worked from home during the four official "snow days" last winter saved the government about $32 million, according to Kate Lister, president of Global Workplace Analytics. But that savings is dwarfed by the potential for federal telework.

Based upon data released by the U.S. Office of Personnel Management in December 2013, Global Workplace Analytics updated its annual forecast for government-wide telework savings. The research indicates that if those federal employees both interested (87 percent) and eligible (47 percent) for telework did so about twice a week, taxpayers could save nearly $14 billion a year — nearly $16,000 per teleworker. In addition, greenhouse gas emissions could be reduced by the equivalent of planting 18 million trees.

The savings were calculated using Global Workplace Analytics' Federal Telework Savings Calculator, a model that includes more than 100 variables and more than 600 calculations. Using conservative assumptions, the calculator accounts for a wide range of telework impacts, including real estate and energy costs, turnover, absenteeism, productivity, healthcare costs, transit subsidies, continuity of operations, vehicle miles traveled, traffic accidents and more.

Legislation passed in 2000 required federal workers to telework "to the maximum extent possible." The absence of progress on that mandate inspired the 2010 Telework Enhancement Act, which added rigor to the earlier legislation. Yet the latest Status of Telework in the Federal Government report showed that less than 8 percent of federal employees who are deemed eligible for telework do so regularly. And while private sector telework grew 42 percent between 2006 and 2012, and state government telework grew 60 percent, federal telework declined 2.4 percent during the period.

If the federal government took steps to maximize the benefits gained from the 8 percent of federal employees who telework regularly, the savings could exceed $1.7 billion annually.

"The numbers are truly staggering," said Tom Harnish, senior scientist at Global Workplace Analytics and coauthor of the report. "Between the continual reminders from Mother Nature that telework is essential for continuity of operations, and the potential economic, environmental and employee impact, the public ought to be screaming for more telework in government and elsewhere."

The High Cost of Cybercrime

Despite the efforts of law enforcement, cybercrime remains a big business. Organizations of all sizes should be aware of the risks and establish policies and procedures to reduce the potential cost of a security breach.

Score two for the good guys. In June, a multinational task force of law enforcement agencies and security vendors was able to disrupt the Gameover Zeus botnet, which in two years had infected more than 1 million computers and had been used to steal millions of dollars from businesses and consumers worldwide.

In a related action, law enforcement officials from the U.S. and other countries seized servers used for the Cryptolocker ransomware, which encrypts files on victims' computers until a ransom is paid. According to the U.S. Department of Justice, Cryptolocker had infected nearly a quarter-million computers by April, mostly in the U.S., with victims estimated to have paid more than $27 million in ransom in the first two months after the malware emerged.

While law enforcement agencies are to be applauded for their efforts in disrupting Gameover Zeus and Cryptolocker, those threats represent only a fraction of the cost of cybercrime. According to a June 2014 report from the Center for Strategic and International Studies, cybercrime costs the global economy about $445 billion annually, representing almost 1 percent of global income. About one-third of those losses affect consumers, with the remainder impacting businesses.

And cybercrime is on the rise. The 2014 U.S. State of Cybercrime Survey, conducted by PwC and CSO magazine, found that 77 percent of companies had a cybersecurity event in the past year. More than a third said the number of detected incidents had increased over the past year, and more than two-thirds worried that cyber threats would impact their business growth.

Cybercrime doesn't just affect large enterprises — the vast majority of small businesses have fallen victim to some form of malware or other cyberattack. The fact is that small businesses are big business for cybercrime, and organizations must take steps to protect themselves.

Understanding the Costs

It's mindboggling to consider that cybercrime costs more than $1 billion each day. The Ponemon Institute's annual Cost of Cyber Crime Study helps to put that number into context

The 2013 study found that the average annualized cost of cybercrime incurred by a U.S. organization was $11.56 million, representing a 78 percent increase since the first study was conducted in 2009. The results also revealed that it takes 32 days on average to resolve a cyberattack, at an average cost of more than $1 million. The organizations surveyed experienced an average of 122 successful attacks per week, up from 102 attacks per week in 2012.

Cyberattacks have grown in sophistication as well as in sheer numbers in recent years. Cybercriminals share their techniques with one another, and hacking toolkits are readily available online. Take Crytolocker for example — there are a number of variants, including a worm-like version that spreads to removable drives. It's not clear if or how the disruption of the Gameover Zeus botnet will affect these variants.

Information theft continues to represent the highest external costs, at 43 percent. But business disruption and lost

productivity represent 36 percent of external costs, an increase of 18 percent from 2012. Recovery and detection account for 49 percent of total internal activity costs.

Cybercrime cost varies by company size, but smaller organizations incur a significantly higher per-capita cost than larger organizations. A 2011 Symantec/NCSA study found that cyberattacks cost small to midsize businesses (SMBs) $188,242 per incident on average. Nearly two-thirds of affected organizations were out of business within six months.

Small businesses are attractive targets for cyber criminals because they often lack the IT resources and budget to implement advanced security tools. Small businesses are not only more vulnerable than large enterprises but less able to identify and resolve security breaches.

Planning and Education Are Key

The most critical IT security issue facing SMBs is a lack of awareness and preparation. Experts say that 83 percent of SMBs lack a formal security plan, and more than 69 percent lack even an informal plan.

Organizations need to understand their security risks and have an action plan for responding to the inevitable cyberattack. Employees should be prepared to take steps to stop the attack and mitigate any damage.

The cyber security action plan should establish the roles, privileges and responsibilities associated with IT systems and data, the types of employees who are allowed to assume the various roles, and policies and procedures for assigning and revoking roles. The plan should also include processes for periodic review of roles and access rights.

Separation of duties creates checks and balances that can help reduce the risk of insider threats. At the same time, having someone who serves as steward for certain types of sensitive data can help ensure privacy, data protection and regulatory compliance.

Of course, security is not a one-step process. Organizations should monitor their systems and network constantly for potential security threats, respond quickly to alerts, and regularly review the log files of systems and security devices. Organizations that don't have the ability or bandwidth to do this in-house should partner with a reputable managed services provider.

Most importantly, organizations should educate employees about the potential threats and the steps they should take to prevent a security breach. Many cybercriminals take advantage of poor password practices and use social engineering to gain access to systems and networks.

Every person in the organization plays a role in effective cyber security. By simply establishing and enforcing a clear security policy and ensuring employees follow best practices, organizations can go a long way toward reducing the cost of cybercrime.

EMC²

BIG DATA.
BIG OPPORTUNITY.

Mining stored data is quickly becoming as important as managing it. EMC Isilon scale-out NAS fosters the convergence of data analytics with stored data. Isilon combines modular hardware with unified software to provide a storage foundation for in-place data analysis so you can find patterns in your data to predict behavior, create better products, innovate faster, increase revenue, or cut costs.

Contact ProSys to learn more.

PROSYS

www.prosysis.com 888-337-2626