November 2014

PROSYS

Tech Outlook

Flash Point

EMC XtremIO all-flash storage arrays help organizations achieve full operational and performance advantages of virtualized environments.

Virtualization techniques that allow multiple operating systems to run on a single server have had a profound effect on the modern data center. Increased server utilization, scalability and flexibility have opened the door for large-scale social, mobile, big data and cloud initiatives. However, these benefits have also brought undeniable disruption to storage infrastructures.

Servers hosting multiple applications are running mixed workloads that create random input/output (I/O) for the storage array. This random I/O is difficult for spinning disks to handle, requiring additional seeks and rotations that add precious milliseconds to the read/write process.

"It's the 'I/O blender' effect," said Matt Merriman, VP of Professional Services, ProSys. "When data is requested, a hard drive must rotate its platters to the location where that data resides. In a one server/one application arrangement with sequential I/O operations, this rotation is manageable. But In a virtualized environment, tens or hundreds of virtual machines are sending random I/O requests at the same time. In that situation, the disk heads are almost constantly rotating back and forth looking for data, which creates a huge performance bottleneck.

"The typical answer has been to add more spindles, provision more disk space and create storage silos to meet the different performance and capacity requirements of various ap-

continued on page 2

TECH OUTLOOK

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

continued from page 1

plications. But that's just not sustainable. This approach wastes storage capacity and physical space while increasing the management burden and the power required to spin all those disks. In the end, you can end up doubling your cost per gigabyte of storage."

The No-Spin Zone

EMC's XtremIO all-flash storage arrays effectively neutralize the I/O blender effect, making them an attractive alternative for Tier 1 storage. Unlike hard-disk arrays with spinning magnetic disks, flash arrays — also known as solid-state arrays (SSAs) — have no moving parts and thus eliminate the mechanical chokepoints of hard-disk drives (HDD).

XtremIO flash arrays actually excel at random I/O performance. Since they don't have to spin or rotate, they essentially have direct access to all data locations simultaneously. They are equally fast on random workloads as on sequential ones, producing huge gains in I/Os per second (IOPS) compared to HDDs. A single flash drive can deliver tens of thousands of IOPS – the equivalent of an entire midrange disk array.

Additionally, all-flash arrays save on power, cooling and physical space, all of which are in short supply in many data centers. Per IOPS, flash uses around 600 times less energy than disk. Some data center operators have reported up to 90 percent reductions in power and cooling costs when replacing disk with flash.

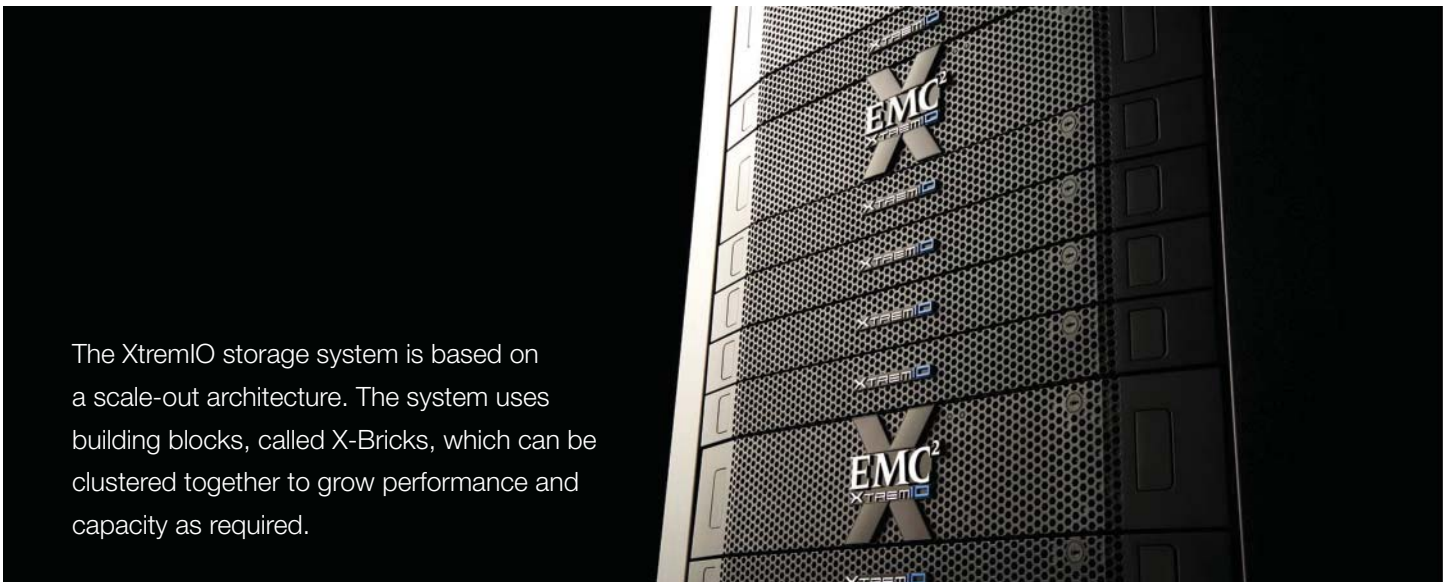
Industry experts say that all-flash arrays will bring dramatic improvements to data center performance while expanding use cases for enterprise application data. Gartner says the SSA market grew by 182 percent in 2013 and predicts that all-flash arrays will account for 20 percent of high-end storage arrays by 2019. IDC forecasts revenues from all-flash arrays will triple to more than $1.6 billion by 2016.

"Modern data centers have raised the stakes for storage vendors, requiring them to be more agile, scalable and cost-effective than ever before. They've also led to a surge in demand for all-flash array solutions that can deliver on these business needs better than legacy arrays," said Eric Burgener, research director for IDC's Storage Practice. "All-flash arrays … meet storage performance requirements with generally far fewer storage devices than traditional spinning disk-based arrays, requiring significantly lower power consumption, floor space and backup infrastructure that translate to a compelling economic proposition."

Hybrid Issues

While flash is indisputably faster, more powerful and more space efficient than disk, until recently price was a barrier to using it across an entire array. This led most storage vendors to try incorporating a small amount of flash into disk arrays to help resolve performance issues while still keeping costs manageable. In these hybrid arrays, flash is incorporated as a cache or tier alongside disk drives, with a caching algorithm deciding which media is the most appropriate landing spot for data.

While the hybrid architecture delivers some performance gains, it also creates significant challenges. Chief



The XtremIO storage system is based on a scale-out architecture. The system uses building blocks, called X-Bricks, which can be clustered together to grow performance and capacity as required.

among them is the potential for a so-called "cache miss" due to latency differences between the two media.

"The problem is that caching algorithms cannot predict with 100 percent certainty which data will be accessed by an application," said Merriman. "If the algorithm makes the wrong prediction, a cache miss occurs and data must be read from back-end storage — which dramatically increases latency for that operation and makes storage performance unpredictable."

Dropping prices for solid-state disks have made all-flash arrays far more practical. While flash memory was generally more than $11/GB in 2012, manufacturers now claim prices as low as $3/GB. In an even more important measure — price per unit of performance (IOPS) — flash really shines, testing at levels about 40 times cheaper than disk.

Purpose-Built Arrays

Most approaches to delivering flash today involve taking an existing array design that was optimized for disk and retrofitting it for flash. This approach doesn't deliver the full capabilities of solid-state storage. The software and controller architectures in arrays designed for disk don't scale to deliver on the full potential of flash.

EMC was among the first vendors to recognize that flash requires a purpose-built array that aggregates flash into one large pool and implements flash management services across the entire array. XtremIO arrays are created from building blocks called X-Bricks that can be clustered together to increase capacity and performance as needed. Each X-Brick is a high-performance, high-availability SAN appliance with 10TB or 20TB of storage and even greater logical usable capacity. The XtremIO storage cluster is managed by the powerful XIOS operating system, which ensures the system remains balanced and always delivers the highest levels of performance without any administrator intervention.

"What I find most compelling about XtremIO is the unique architecture," said Laura Dubois, Research VP of Storage at IDC. "Core functions such as granular metadata processing, shared in-memory metadata handling and content-based data placement are enablers to XtremIO's impressive sustained IOPS metrics while offering core services — including de-duplication and copy data services. The other standout capabilities with this system are native inline de-duplication, in-memory metadata-only copy and a scale-out architecture. These are attributes not all of the all-flash array solutions on the market offer."

Tech Outlook

Copyright © 2014 CMS Special Interest Publications. All rights reserved.

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.

Some parts of this publication may be reprinted or reproduced in nonprofit or internal-use publications with advance written permission. Tech Outlook is published monthly by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.

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

Backup Plan

SMBs without sound data backup strategy are flirting with disaster.

It's human nature to take a reactive approach to problem resolution. You probably don't repair your roof until it leaks during a thunderstorm, service your air conditioner until it breaks down on a 95-degree day or inspect your hot water heater until you've been surprised by an ice-cold shower.

But waiting for a disaster to start backing up your data properly? That is an exceptionally dangerous tactic.

Too many organizations — particularly small and midsized businesses (SMBs) — simply don't have a data backup strategy in place. According to a study by AVG Technologies, owners and managers of SMBs spend more time straightening up their desks or ordering business cards than they do on backing up data. Although 30 percent believe more than half of their data is sensitive, one in four don't even require a weekly backup.

Consider the Options

The biggest challenge faced by SMBs is limited IT personnel. Many IT solutions are designed for large enterprises that have plenty of IT resources, and data backup is no exception. SMBs need a data backup solution that is easy to deploy and manage, and makes it simple to restore data and applications. Fortunately, much of the data backup technology built for the enterprise has been simplified for SMBs.

There are three general categories of onsite backup options available:

Tape. Tape provides a low-cost, reliable option and is most commonly used for archiving data that is rarely accessed or that is retained for regulatory compliance purposes. Despite tape's reputation for being somewhat of a dinosaur, newer solutions have brought increased longevity, capacity and transfer rates. Tape is easy to move offsite to keep data secure, but retrieving data can be a slow process.

Disk. Although more expensive than tape, disk-based backup is fast, efficient and reliable. Data de-duplication has made disk-based data backup a viable option for SMBs by reducing the amount of data to be backed up. However, disks reside in the data center, which can increase power and cooling costs and require offsite redundancy.

Network-attached storage (NAS) appliances. This is an appealing option to SMBs because of its relatively low cost and high storage capacity. NAS allows for real-time backups while eliminating software licensing costs. However, NAS appliances can't be detached from the data center and moved to remote location for safe keeping. One option is to back up data on a NAS appliance and then move that data to tape each day.

Embracing Cloud Backup

Another option is to move data backup to the cloud, which provides virtually limitless storage capacity. Carbonite's 2014 Report on the State of Data Backup for SMBs indicates SMB owners are beginning to recognize the gaps in their data protection, and view the cloud as a good solution. In the survey of 500 IT professionals at companies with fewer than 100 employees, 56 percent said they have chosen the cloud for off-site backup.

Today's remote backup systems require no capital investment for equipment and makes data backup an operational cost. Software encrypts data for security purposes and automatically backs it up to remote servers. The service provider maintains and monitors the data backup plan, and because data is saved at a different location, it's always accessible. Because cloud-based data backup is susceptible to performance issues, many organizations will implement a hybrid solution, keeping primary storage onsite on disks or NAS appliances and moving secondary storage and data backup to the cloud.

The beauty of the cloud is that it can be used for more than data backup. Cloud-based data archival allows organizations to move rarely accessed data offsite. Primary storage, which has traditionally been kept in a local stor-

age system, can be moved to the cloud and accessed whenever needed. A cloud service provider can also host a secondary storage environment that stores replicas of primary data. SMBs that want to share data without investing in file servers should explore cloud-based secondary storage.

Planning is Key

Still, cloud backup isn't for everyone. While a service provider generally has more redundancy and better security and support than most SMBs, security can't be taken for granted. It does no good to outsource data backup if that data isn't secure or easy to access. A service provider should also be able to provide high performance without bandwidth restrictions, and be vetted to ensure they understand and adhere to regulatory requirements.

For some organizations, the right approach may be a mix of onsite and offsite backup to gain the highest levels of control and security. To develop an effective backup strategy, SMBs must invest the time, talent and effort to properly evaluate their data infrastructure, their budget and manpower restrictions, and their data availability requirements. Key steps in the planning process should include:

• **Analyze the current state of data in your organization.** How much data do you create? What data is stored? Where is it stored? How often is this data accessed? Is data being backed up now? If so, how often?

• **Identify goals.** What is your recovery time objective (RTO) – the time it will take to recover data? What is your recovery point objective (RPO) – the maximum age of data that you'll need to recover? Make sure your expectations for RTO and RPO are in line with your business processes and requirements.

• **Prioritize.** What are your mission-critical data assets? These should be the priority in any data backup strategy.

• **Create a plan.** How can you achieve at least two levels of redundancy in different geographic locations? How often will data be backed up? How can that data be accessed? What are the technological requirements?

• **Test.** Are you certain that backup processes are functioning properly and data can be recovered?

The bottom line is that organizations can't afford to react to disaster. Plan for it with a smart data backup strategy. Cloud backup is increasingly a good option because it makes the process simple and cost-efficient, but each organization must engage in careful planning will ensure a strategy that makes good business sense.

Virtualization Exacerbates Backup Woes, Survey Says

Server virtualization enables consolidation, higher resource utilization, cost savings and improved efficiency. However, virtualization also creates new backup challenges.

Traditional backup processes are ill-suited to the virtualized environment, with consolidated server loads and extreme data redundancy. Multiple virtual machines (VMs) sharing the same physical hardware have fewer resources available for backup. At the same time, there is more data to be backed up thanks to redundant operating system images, application profiles and data.

A recent survey of 500 small and midsized business (SMBs) across the U.S. and Europe found that they are experiencing significant issues with the cost, complexity and lack of capabilities of their data protection for virtual environments. The survey from Veeam Software found that 85 percent are experiencing cost-related challenges with backup and recovery, 83 percent with lack of capabilities and 80 percent with complexity.

Other key findings include:

• Recovery of SMBs' virtual servers is only a little faster than physical servers, at 4 hours and 21 minutes compared to 4 hours, 51 minutes.

• Recovery of individual files such as emails takes up to 12 hours, 8 minutes.

• Sixty-seven percent of SMBs' backup tools use agents, which can add to complexity — 76 percent of those SMBs encounter problems such as difficulty managing agents, slow performance and both backup and recovery failing too often.

• Sixty-three percent of SMBs believe their backup and recovery tools will become less effective as the amount of data and servers in their organization grows.

• 41 percent of SMBs stated that downtime in the event of an IT failure costs $150,000 or more per hour, meaning that outages can cost these organizations $600,000 or more based on the recovery times given.

• More than 1 in 6 (17 percent) recoveries of backed-up machines cause SMBs problems, increasing recovery times and the cost of downtime. This is not surprising considering only 8percent are tested.

• Currently, an average of 33 percent of SMBs' virtual infrastructure is not backed-up.

• Fifty-five percent of SMBs are planning to change their backup tool for virtual servers.

NAC Gets High Marks

Survey indicates network access control is perceived as most effective defense against cyber threats.

Mobility, convergence, 802.11ac wireless standards, BYOD and increased access to wireless LANs are all elements of a fundamental change in how networks are used today. These changes have contributed to decreased visibility into how networks are being accessed.

The multitude of devices and connections in use today offer demonstrated productivity and collaboration benefits, but they also create multiple avenues for introducing viruses, worms and other malware into an organization. This has increased the likelihood of unauthorized access — consider the recent high-profile password breaches at eBay, Adobe and Home Depot.

In fact, more than 60 percent of respondents to a recent, large-scale security survey report they were breached in 2013. A quarter of them cited a lack of employer investment in adequate defenses as a factor.

That's why many organizations have begun implementing endpoint security solutions — also known as network access control (NAC) — that make devices prove they're secure before they are allowed to connect to the network. NAC was rated the highest of all security technologies in its potential to defend against today's cyber threats in the "2014 Cyberthreat Defense Report," a survey of more than 750 security decision makers and practitioners in organizations with 500-plus employees in North America and Europe.

The survey was conducted by CyberEdge Group in conjunction with nine other information security companies. It was designed to complement Verizon's annual Data Breach Investigations Report.

Question and Verify

NAC solutions provide role- and location-based user authentication and require a minimum acceptable security posture for all devices using the network infrastructure. Before allowing a user to access the network, NAC asks who they are, where they are located and what device are they using.

Based upon the answers to those questions, the NAC solution authenticates the user, determines the user's access permissions, determines what endpoint security policies are applicable, and ensures that the policies are enforced through quarantine or remediation. All of this activity is tracked through an audit trail.

Network-based policy enforcement can take many forms, including dedicated gateway, DHCP manipulation, 802.1x authentication, and port- and VLAN-based enforcement on switches. In addition to ensuring that the right users have access to the right data, NAC solutions also verify that unauthorized individuals cannot access sensitive data. If a security breach is detected, NAC solutions can notify the appropriate individuals and use self-remediation and automated remediation to help contain the damage.

These factors made NAC the highest-rated defense solution in the Cyberthreat Defense Report. Participants were asked to rate various solutions on a scale of 1 to 5, with 5 being highest. NAC received the highest marks at 3.71. Enterprise mobility initiatives have contributed to the fairly widespread adoption of NAC.

Improving Awareness

In the report, one quarter of organizations noted they are conducting full network scans weekly or daily, indicating a greater understanding of the tremendous value of continuous monitoring. However, 52 percent of responding organizations conduct full network vulnerability scans quarterly or annually. Alarmingly, one in five organizations admitted to rolling the dice by doing nothing to assess the state of their transient devices between regularly scheduled active scans. This provides a large window of opportunity for a successful cyberattack against the transient device.

Fifty-one percent of survey respondents said NAC is their most-used means of detecting vulnerabilities and security misconfigurations within transient laptops and mobile devices between full-network vulnerability scans. In addition, 77 percent of respondents said they are using or plan to use NAC for mobile security, and 53 percent said they use it to detect host security misconfigurations.

Growing demands for network connectivity, combined with increasingly sophisticated threats, have raised the stakes for security professionals. NAC is a vital tool for improving security by improving network visibility into user, device and application access.

"It is obvious from our research that NAC is an important weapon within many organizations' arsenals — and for good reason," said Steve Piper, CEO of CyberEdge Group. "Many of our respondents saw it as a versatile tool that could support protection efforts ranging from BYOD policy enforcement to configuration management."

Secure Access for Wired, Wireless and VPN

Cisco Identity Services Engine (ISE) gives you a single policy control point for the entire enterprise, enabling secure wired, wireless and VPN connectivity. Cisco ISE is used to provide secure access and guest access, support BYOD initiatives, and enforce usage policies. Cisco ISE is designed to support up to 250,000 active, concurrent endpoints – more than any other product in the marketplace – to ensure seamless onboarding, roaming, and network access control throughout a distributed enterprise network.

Contact ProSys to learn more.

PROSYS

Cisco Gold Partner

www.prosysis.com
888-337-2626

Copyright © 2014 Cisco Systems. CIS-119

EMC²

STORAGE. **UNLEASHED.**

Welcome to the 100% Flash Storage Array from EMC XtremIO.

XtremIO finally delivers the breakthrough scale-out architecture, consistent performance, data reduction, thin provisioning, and manageability you've been waiting for in an enterprise flash array. More than its individual features, XtremIO allows you to completely rethink your old assumptions about shared storage. Workload consolidation, dynamic provisioning, production & test/development storage consolidation, zero maintenance windows, and more are now real opportunities as you unlock the full business value of flash across your data center.

Contact your ProSys representative for more information about using EMC XtremIO to solve your data storage challenges.

PROSYS

www.prosysis.com
888-337-2626

© Copyright 2014 EMC Corporation. All rights reserved. EMC-48