SIGMA
A PIVOT COMPANY

SigmaUptime

volume 15 number 3

Flash Forward

All-flash storage arrays from NetApp accelerate applications and deliver IT services faster than traditional architectures.

Contents

4

Sigma Uptime

Editorial Correspondence:

10221 East 61st Street, Tulsa, OK 74133

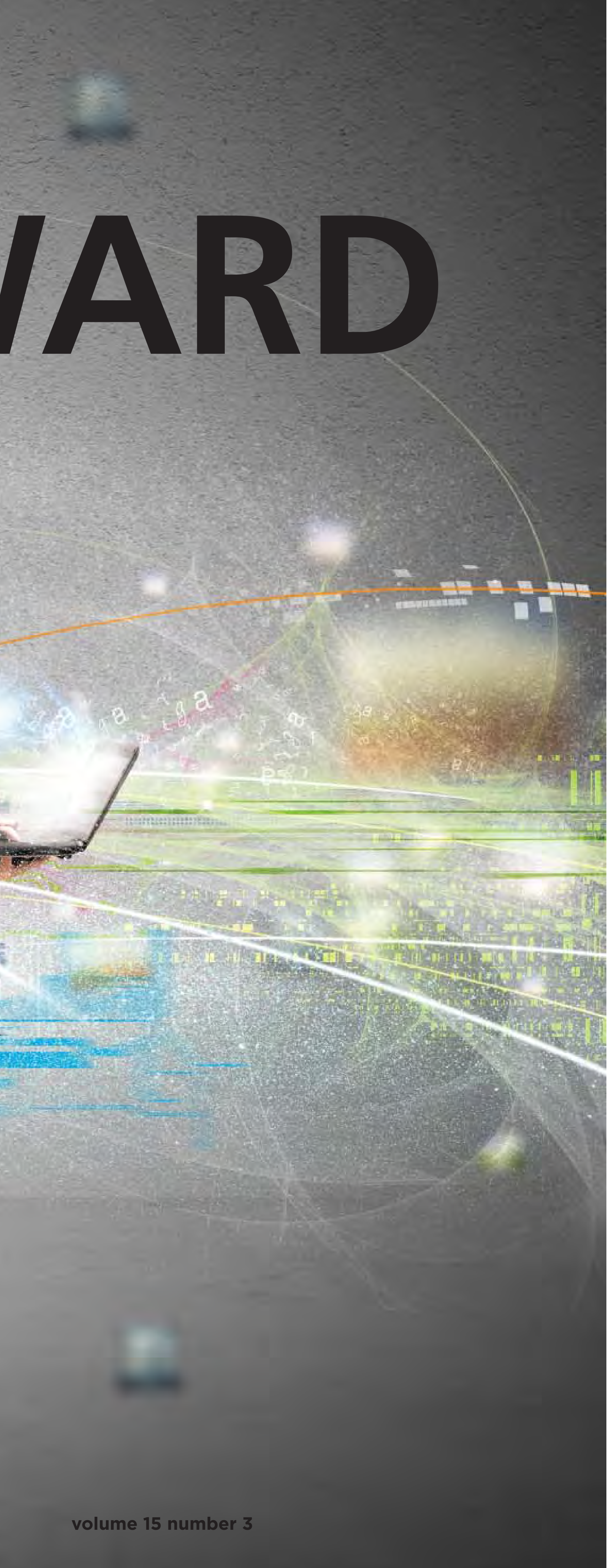
Phone (800) 726-7667 • Fax (918) 270-7134

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

Sigma UPTIME is published bimonthly by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.

FLASHFORW

WARD



With the addition of the SolidFire product line, NetApp is making all-flash storage arrays practical for all types of data center workloads.

An increased focus on cloud services, mobile computing and big data initiatives has changed data center workloads and strained traditional storage infrastructures. Beyond basic storage and access capabilities, organizations now require the ability to analyze and act on their information assets in real time. Hard disk drives simply weren't built for that type of performance.

"Today's mixed workloads create significant latency issues for traditional storage arrays because of the mechanical limitations of spinning disks," said Chris Norris, Practice Manager – Data Center Transformation, Sigma Solutions. "Over the past 10 years, network speeds, server speeds and processor speeds have all increased exponentially, but disk speeds are reaching their functional limits, which creates a serious bottleneck."

Solid-state drives (SSD) based on flash storage eliminate the mechanical overhead and can reduce data access times from milliseconds to microseconds, a factor of 1,000. Lower latency is essential to application performance across all industries, but until recently flash storage arrays were considered too costly for anything other than limited deployments such as improving the performance of individual applications.

"However, NetApp is changing the economics of flash," said Norris. "With the recent addition of SolidFire's product line, they've built a portfolio of solutions that make it practical for just about anyone to deploy all-flash arrays to handle mixed workloads throughout the data center."

A 'Radically Different' Architecture

NetApp was already among the major players in the all-flash array market before acquiring SolidFire earlier this year. The award-winning NetApp All Flash FAS product line is well-regarded among traditional enterprise infrastructure buyers, and the NetApp EF Series is designed

continued on page 6

continued from page 5

specifically for high-speed transactional applications with low-latency requirements.

However, NetApp co-founder Dave Hitz has noted that the SolidFire architecture is "radically different" than NetApp's other offerings, which is one reason SolidFire will remain a separate entity within NetApp for the foreseeable future. Designed from the ground up to make flash affordable for general workloads, SolidFire eliminates the dual-controller design of most storage arrays in favor of a shared-nothing architecture that delivers immense scalability, controls costs through automated management, and increases effective capacity with built-in data reduction technologies.

"Enterprises that think flash is still too expensive to deploy in their data centers are mistaken," said IDC's Flash Storage Research Director, Eric Burgener. "IDC believes that all enterprises should be using flash in at least some capacity in their data centers today for both performance and economic benefits."

Enterprise Strategy Group's 2015 report, "Quantifying the Economic Value of a SolidFire Deployment," compared a SolidFire system with a traditional storage vendor's reference architecture. The analysts found that SolidFire lowered operating expenses by 67 percent while avoiding up to 93 percent of performance-related issues with mechanical disks.

Built-In Value

SolidFire's Element operating system is the key to many of the performance and economic advantages.

"Traditional storage vendors often simply replace disk drives with flash drives in their storage arrays, but that just shifts latency issues from the media to the storage controller that moves data on and off of shared disks," said Norris. "If you add more capacity, you wind up actually reducing performance because of the additional burden on the controllers.

"SolidFire recognized this chokepoint and has eliminated the controller in its shared-nothing architecture. This not only bypasses a common point of failure, but makes it really easy to scale storage clusters. You just add new nodes — no controller upgrades are necessary, there is nothing to migrate, no settings to change and no interruptions to operations."

The Element OS also automates many of the time-consuming tasks typically performed by storage administrators, including storage provisioning management, monitoring and reporting. ESG's analysis found that this can lower operating expenses by up to 67 percent.

Additionally, Element includes storage-efficiency capabilities such as thin provisioning, compression and data de-duplication, which are often just bolted onto traditional storage architectures. In SolidFire nodes, data is compressed and de-duplicated inline, before it is ever written to flash. Embedded thin provisioning allocates storage capacity dynamically as an application needs it, immediately returning any free space for use by other SolidFire volumes.

"These features increase what SolidFire calls the 'effective capacity' of its systems by reducing the data footprint by five to 10 times inline before it's written to flash," said Norris. "This reduces the cost per gigabyte of data actually stored on the system, making it possible to use flash for just about any data center workload."

The SolidFire Family

For example, a four-node SF2405 system features 40 240GB SSDs, and offers up to 35TB of effective capacity and around 200,000 input/output operations per second (IOPS). The platform is targeted at IT departments and managers looking to accelerate the performance of individual applications or taking their first steps towards deploying a private cloud infrastructure.

The SF4805 doubles the density, with 480GB SSDs for 69TB of effective capacity and 200,000 predictable IOPS. The product is targeted at customers looking to eliminate traditional storage silos by consolidating a mix of application workloads within a single infrastructure.

The SF9010 platform is designed for large-scale public and private cloud infrastructures. At full scale with 100 nodes, the SF9010 is among the largest and fastest all-flash storage platforms on the market today, delivering 3.4PB of effective capacity and 7.5 million IOPS.

The most recent addition to the SF Series product line, the SF9605, is purpose-built for enterprises that require scale-out capacity and predictable performance to meet escalating demands for flexible and efficient IT service, delivery and consumption. It delivers 34.5TB effective capacity and 50,000 predictable IOPS, balancing capacity, cost and performance to meet the most complex use cases at scale.

NetApp also sells a software-only version of its technology called Element X, which is designed for white-box hardware and further extends the economic advantages of the SolidFire portfolio. While flash memory was generally more than $11/GB in 2012, SolidFire now claim prices lower than $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.

"The mechanical hard drive has been the workhorse of enterprise storage for decades, but in the very near future we may see it limited to use with select applications with specific production, demand and cost restrictions," said Norris. "By changing the economics of flash, the SolidFire line is helping to usher in a new era in which all-flash arrays will take on the majority of high-performance workloads and become the primary storage platform."

SOLIDFIRE
Now Part of NetApp

Storage Built for the Next Generation Data Center

Scale-out, all-flash storage that's highly available and easy to control — all with guaranteed performance.

Why SolidFire

The agility, efficiency, and scalability benefits demonstrated from cloud computing infrastructure have raised the bar on expectations for IT service delivery. The pressure is on IT to:

- Rapidly deploy applications and service
- Provide more agile and scalable infrastructure
- Increase application performance and predictability
- Enable automation and end-user self service
- Raise operational efficiency and reduce cost

SolidFire is architected from the ground up to be the storage foundation of next generation data centers.

SolidFire Benefits

Consolidate

Reduce cost and complexity by safely consolidating mission-critical applications onto a single storage platform.

Automate

Increase productivity with deep infrastructure integrations.

Scale

Dynamically scale storage resources to meet business demands.

Contact Sigma to learn more.

www.sigmasol.com
888.895.0495

SIGMA
A PIVOT COMPANY

Boosting Mobile Security

Virtual mobile infrastructure offers secure access to mobile apps and data.

Well-funded hackers with sophisticated tools make headlines and strike fear into anyone responsible for an organization's network and data security. Some of the more notorious groups include Russia's CyberVor gang, Iran's Tarh Andishan, the Syrian Electronic Army, Germany's Chaos Computer Club and the prolific Lizard Squad, not to mention infamous "hacktivist" groups such as Anonymous and LulzSec.

As scary as these groups sound, Stephen in sales and Ellen in engineering likely pose more imminent threats.

In its 2015 survey of 703 U.S. IT professionals involved in endpoint security for their organizations, the Ponemon Institute found that the biggest threats to network security usually come from careless employees using their own mobile devices to run commercial cloud applications while working outside the office.

"IT continues to battle malware at the endpoint, and 69 percent of our respondents say it increased in severity last year," said Dr. Larry Ponemon, chairman, Ponemon Institute. "While it is positive news that companies are making the security of endpoints a higher priority, to win the war they need to recognize the criticality of minimizing employee negligence and investing in technologies that improve the ability to detect malicious attacks."

A New Approach

To date, most IT organizations have attacked this issue with a mix of device and application management solutions that fall under the general umbrella of enterprise mobility management (EMM). These solutions attempt to manage and secure devices, applications and data on the device or in transit.

An emerging technology offers organizations a new weapon. Similar to desktop virtualization, Virtual Mobile Infrastructure (VMI) delivers secure access to mobile applications and an operating system that is running on a virtual machine (VM) in a remote data center. Any data associated with the application is stored there as well, thus eliminating the vulnerability of having data at rest on the device.

Employees are assigned a profile that is centrally managed and stored on secure company servers. Once employees install a lightweight client app on their devices, they can log in and access all their files and data, which are delivered through a secure, remote communications protocol. IT administrators can push security updates and modify employee profiles through a central management console. VMI can also be seamlessly integrated with EMM for heightened security.

Addressing New Threats

BYOD initiatives have created new opportunities for organizations, but they have also introduced security and application management challenges. In a January 2016 survey of 100 IT security management professionals, Avast found that while enterprise mobility programs have increased productivity, they have also led to a rise in datajacking — the hijacking of data from a mobile device. Seventy-two percent cited datajacking as the greatest security challenge related to enterprise mobility, followed by malware (67 percent) and employee compliance (58 percent).

To address these new threats, the National Institute of Standards and Technology (NIST) now recommends the implementation of VMI to strengthen an organization's remote-access data security. The NIST made the recommendation in March as part of an update to guidelines for telework security.

"Organizations are realizing that many data breaches occur when attackers can steal important information from a network by first attacking computers used for telework," said Murugiah Souppaya, author of the new NIST guidelines. "To prevent breaches when people are teleworking, organizations need to have stronger control over their sensitive data that can be accessed by, or stored on, telework devices."

Getting Started

As a nascent technology, VMI hasn't drawn much of a crowd yet. Six companies — Hypori, Remotium, Raytheon, Nubo Software, Trend Micro and Sierraware — have brought VMI solutions to market, each with a slightly different twist on how to execute the underlying virtualization platform. To date, all of these solutions have Android as the hosted OS, since Apple won't allow iOS to run on third-party hardware. However, some offer iOS client apps that would allow Android apps to run on iPhones.

It is widely expected that Citrix will also enter the market soon with a solution based upon technologies it acquired with the 2014 purchase of Virtual, a small virtualization startup that had developed a method for emulating both Android and iOS environments on remote desktops. Adding to the anticipation was the inclusion of a 50-minute presentation on VMI by TechTarget analyst Jack Madden during Citrix's annual Synergy conference last year.

"There are a lot of details we have to work out about virtual mobile infrastructure, but it's real and it's here and it works," Madden said. "There are unique problems that it can solve. There are unique use cases. There is a place for it. I think it has a future."

NETWORK TRAFFIC JAMS

Sharp surge in DDoS attacks is driving networks into the slow lane.

The legendary Woodstock music festival was a watershed moment in 1960s counterculture, famously known as "three days of peace and music." It is less well known for having created perhaps the worst traffic jam in American history.

County roads and interstate highways became virtual parking lots as more than a half-million people converged on Max Yasgur's farm in New York's rural Catskill Mountains. With traffic at a standstill, concert-goers simply abandoned their cars in the roadway and walked to the festival site. Performers had to be flown in and out on helicopters. Governor Nelson Rockefeller declared a state of emergency. The New York Times called it a "colossal mess."

Distributed Denial of Service (DDoS) attacks have much the same effect on computer networks — minus the music and fun.

DDoS attacks are designed to render servers and/or network resources unavailable by overwhelming them with traffic. This often involves the use of a botnet — a network of hijacked computers — to unleash a flood of traffic that saps bandwidth, clogs network connections and prevents legitimate traffic from getting through.

Some DDoS attacks are motivated by "hacktivism," a desire to disrupt commerce or bring down the web sites of government agencies or large organizations for political or philosophical purposes. Extortion, blackmail, revenge and competitive advantage are among other motives for attacks. Some hackers just do it for the "lulz" — their personal amusement. DDoS attacks don't require a particularly advanced skillset to execute, either. In fact, they are increasingly launched by so-called DDoS-for-hire services — cybercriminal operations that charge as little as $2 an hour to launch an attack.

Attacks on the Rise

Whatever the method or motivation, there has been a marked increase in the frequency, volume and sophistication of DDoS attacks. The Vatican, the Church of Scientology and the New York City government have all been hit recently, as have Amazon, PayPal, MasterCard and Visa, as well as the PlayStation and Xbox gaming networks.

In its Q4 2015 State of the Internet Security Report, Akamai reported that the number of DDoS attacks jumped 40 percent compared to the previous quarter and 149 percent compared to one year ago. Malicious actors are also notoriously persistent, with each target being attacked an average of 24 times. The annual Worldwide Infrastructure Security Report from Arbor Networks found that the average DDoS attack size increased 20 percent to 500Gbps, while more than half of respondents said DDoS completely saturated their Internet connectivity.

"The threat from DDoS and web application attacks isn't going away," said Stuart Scholly, Senior Vice President and General Manager, Security Business Unit, Akamai. "And malicious actors aren't backing down. They're hammering away at the same targets over and over again, looking for a moment when defenses may be down."

Internet of Things Targeted

It is no coincidence that the increase comes at a time when more and more devices are becoming interconnected through IP networks in the so-called "Internet of Things." As more devices become IP-enabled, it increases the number of devices that can be compromised and used in distributed attacks.

"By its very design, the Internet of Things is built with lightweight security," said Terrence Gareau, Chief Scientist, Nexusguard. "These devices rely heavily on shared libraries and a rapid development cycle. Because of their constraints, many IoT devices have limited options for firmware upgrades and other risk management features. The fact that they are also always online makes them highly susceptible to intrusion and attacks."

Some of today's attacks leverage an intimate understanding of the Internet routing topology. So-called Distributed Reflection and Amplification Denial of Service (DrDoS) attacks exploit common network protocols inherent in network devices. DrDoS attacks using these protocols can be difficult to trace back to the malicious actor because they often involve spoofing the origin of the attack. Requests to the victim are reflected to the primary target, making it appear that the target is being directly attacked by the victim.

Many organizations wrongly assume that their existing defenses will stop DDoS attacks, or believe their network will not be targeted. According to the results of a study conducted by Kaspersky Lab and B2B International, 43 percent of large enterprises and 28 percent of small businesses suffered a DDoS incident in the preceding 12 months.

Serious Damage

These attacks can cripple a business. According to the Kaspersky / B2B study, a DDoS attack can cost anywhere from $52,000 to $444,000 depending upon the size of the company. Beyond the financial impact of lost traffic, data, productivity and revenue, there are also costs involved to investigate, respond to and recover from an attack. Organizations in heavily regulated industries could be forced to deal with compliance violations. A poor user experience that makes it difficult for customers to access information and services or make purchases can result in lost business. Existing customers could even file lawsuits if services are completely unavailable.

According to the study, 61 percent of DDoS victims temporarily lost access to critical business information, 38 percent were unable to carry out their core business functions and 33 percent reported the loss of business opportunities and contracts. In 29 percent of DDoS incidents, a successful attack had a negative impact on the company's credit rating while in 26 percent of cases it prompted an increase in insurance premiums.

The rapid increase in this attack vector indicates that businesses, both large and small, need to take steps to protect vulnerable devices. Firewalls, intrusion protection and other devices may mitigate very low-level attacks, but high-volume attacks launched from large botnets can easily overwhelm the capabilities of traditional solutions. In fact, security devices can become the attackers' unwilling allies because they are unable to separate legitimate from illegitimate traffic.

As DDoS attacks have become more complex, sophisticated and frequent, organizations must rethink their security measures. A defense-in-depth posture with a combination of on-premises equipment and cloud-based mitigation offers the best protection against advanced DDoS attacks and will help keep network traffic moving smoothly.