Connect
Your Independent HPE Business Technology Community

Read it in **Print**
and **Online!**

The Connection

A Journal for the Hewlett Packard Enterprise Business Technology Community

A Guide to High Availability and an Approach to an Active/Active Environment in the OSS World

Not All Business Continuity Solutions Are Created Equal

PLUS

Women in NonStop

May – June 2017 { Volume 38, No. 3 }

XYGATE® SecurityOne™

Security Intelligence and Analytics for HPE Integrity NonStop™ Servers

Visibility

Faster Threat Detection

Improved Risk Management

Differentiate Noise from Actionable Incidents

Minimize the Impact of a Breach by Identifying it in its Early Stages

Reduce Mean
Time To Detection

Learn more at
xypro.com/SecurityOne

XYPRO®
Mission Critical Security

©2017 XYPRO Technology Corporation. All rights reserved.
Brands mentioned are trademarks of their respective companies

HPE NonStop Availability Stats and Performance

Continuous monitoring of application service-levels has been proven to be a key component of high availability systems. HPE NonStop Availability Stats and Performance (ASAP) provides continuous monitoring of service-levels and automated actions to maintain the highest levels of availability.

HPE NonStop Availability, Stats, and Performance software (ASAP) improves availability via service-level objective monitoring coupled with built-in service-level alerts, and automated recovery actions. For over 10 years, NonStop ASAP is the smart, affordable way to keep NonStop servers running non-stop.

- Monitor application and system resources
- Receive alerts via clients, events, email, & mobile
- Set user-defined goals
- Automate recovery actions
- Monitor and resolve issues quickly

Hewlett Packard
Enterprise

Contact your HPE representative for more info.
www.hpe.com/info/nonstop

#NonStopTBC

NonStop Technical Boot Camp 2017

November 13-15, 2017

Hyatt Regency San Francisco Airport

Pre-Conference Seminar on November 12, 2017

Table *of* Contents

{ Technology + Community }

Columns...

The Always On Operating System

The HPE NonStop operating system (OS) delivers fault tolerance through a share-nothing parallel processing architecture with multiple levels of error detection. Fault isolation and workload takeover capabilities provide application and database availability on both a local and global scale. As a result, HPE NonStop has the ability to detect, isolate and recover from failures without affecting critical applications and their users. We're here for you. All the time.

www.hpe.com/info/nonstop

Hewlett Packard Enterprise

intel®

A Note from Connect Leadership

Architecting your NonStop for High Availability. Seems almost like a joke, doesn't it? I mean, doesn't NonStop = High Availability? Someone in marketing came up with this, didn't they? Maybe I should take a second look at this…

I have been a NonStop professional for quite some time now. I think I have a pretty good handle on what it takes to configure my system for maximum availability, don't I? I monitor everything I can. From diskfiles to transaction rates. Processes to network interfaces. What am I missing? We invest in NonStop because it IS NonStop!

The more I focus on this, the more I realize it is outside of my control… OS upgrades. Power. Networking. Nature! There are any number of forces outside my control that can cripple my availability numbers! Arg!

The more I think about this, the more I recall any number of presentations I have attended at RUG meetings and the NonStop Technical Boot Camp. Dr. Bill Highleyman introduced me to a concept I found completely non-intuitive early on my career that I live by today: More parts CAN mean higher reliability!

In most cases, I would rather reduce the complexity of my enterprise. In this way, I can reduce a lot of things: Training, cost (sometimes), delivery time, documentation, etc. The list goes on. More often than not, in practice, I find that NonStop concepts, as complicated as they may seem, tend to lead to an increase in both complexity (minimally) and availability (maximally).

Every NonStop server I have had the pleasure of working on in my career has mirrored almost everything. Disk volumes, CPU's, even processes. All this has been engineered into the platform to reduce downtime, but it increases the complexity. Now that you have mirrored everything, what could possibly be left?

How about the entire system? The open source community has been using the HPE NonStop as a model for quite some time now! They now leverage tightly coupled inexpensive hardware with active database replication in a poor attempt to mimic our reliability. The scary part is that they are getting close! It will be decades before there is any real competition, and by that time we will have moved on to even greater availability, but until then, we should try and learn from them as well.

In the past, we have built monolithic processing hosts, a large system that handled all of our needs. Sometimes we even had the luxury of a hot backup! Moving forward, I challenge you to consider making that single system that runs on a single node into 2+ systems. Leverage active/active architectures, review different models, increase complexity and make 99.999% availability the OLD standard.

I am really excited about where NonStop is going. Smaller, faster systems. Virtualized for on-demand capacity and location. Co-locating with the "other" systems! I wonder what will happen when there are just as many NonStop VM's as there are Windows/Linux VM's running in the enterprise but with higher availability and a lot less staff.

Hm…..

Thanks.

Rob Lesan

Rob Lesan
XYPRO Technology
Connect Worldwide President

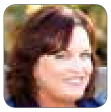
2017 Connect Board of Directors

PRESIDENT
Rob Lesan
XYPRO

VICE PRESIDENT
Michael Scroggins
Washington St. Community College

PAST PRESIDENT
Henk Pomper
Plusine ICT

DIRECTOR
Trevor Jackson
SOCAN



CHIEF EXECUTIVE OFFICER
Kristi Elizondo
Connect Worldwide

HPE LIAISON
Andrew Bergholz
Senior Director of Development of HPE NonStop

DIRECTOR
Navid Khodayari
Idelji

TheConnection

The Connection is the official magazine of Connect, an independent, not-for-profit, user-run organization.

Kristi Elizondo	CEO
Stacie Neall	Managing Editor
Mandi Nulph	Feature Editor
Kelly Luna	Event Marketing Mgr.
Joseph Garza	Art Director
Janice Reeder-Highleyman	Editor at Large
Dr. Bill Highleyman	Technical Review Board
Karen Copeland	
Thomas Burg	
Bill Honaker	
Justin Simonds	

We welcome article submissions to the *The Connection*. We encourage writers of technical and management information articles to submit their work. To submit an article and to obtain a list of editorial guidelines email or write:

The Connection
E-mail: sneall@connect-community.org
Connect
P.O. Box 204086
Austin, TX 78720-4086 USA
Telephone: +1.800.807.7560
Fax: 1.512.592.7602

We accept advertisements in The Connection. For rate and size information contact:

E-mail: info@connect-community.org

To obtain Connect membership and The Connection subscription information, contact:

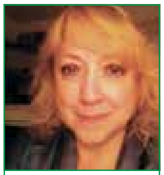
Connect Worldwide, Inc.
P.O. Box 204086
Austin, TX 78720-4086 USA
Telephone: +1.800.807.7560
Fax: +1.512.592.7602
E-mail: info@connect-community.org

Only Connect members are free to quote from The Connection with proper attribution. The Connection is not to be copied, in whole or in part, without prior written consent of the managing editor. For a fee, you can obtain additional copies of The Connection or parts thereof by contacting Connect Headquarters at the above address.

The Connection often runs paid advertisements and articles expressing user views of products. Articles and advertisements should not be construed as product endorsements.

The Connection (ISSN 15362221) is published bimonthly by Connect. Periodicals postage paid at Austin, TX. POSTMASTER: Send address changes to The Connection, Connect Worldwide, Inc., P.O. Box 204086, Austin, TX 78720-4086 USA.

© 2016 by Connect
All company and product names are trademarks of their respective companies.



Karen Copeland
Manager WW NonStop
Product Management
Mission Critical Solutions

News from HPE's NonStop Enterprise Division

NonStop Springs Forward

Ah, spring has finally arrived in Silicon Valley, after months of rain, skies are blue, the sun is shining, everyone's fruit trees and rose bushes are in bloom and people are beginning to talk about vacations. At HPE, the hardworking NonStop teams in Palo Alto have moved to new higher floors in Building 20 while we keep our shoulders to the grindstone so we can get product updates out to customers and meet schedules for future products. We just finished delivery of the L17.02 RVU at the end of March, followed by the latest J-series RVU, J06.21 this month, so we are now focused on the next release with even more updates to SQL/MX and the rest of our product line. Simultaneously we are supporting numerous events to talk about what NonStop can offer customers these days.

This spring has been one of the busiest times, starting with South America offering new NonStop events in Chile and Argentina for the first time that I can remember. The event in Chile was held at a winery and was very well received. You can read more about both events by viewing articles in this edition, "Chile NonStop User Meeting" authored by Jessica Nieves (OmniPayments) and Alfredo Villarroel (HPE) and the report on the "Argentina NonStop User Meeting" authored by Jessica Nieves (OmniPayments) and Fabian Manfredi (HPE).

Two events were also held in Asia the first week of May, "Indonesia HPE NonStop Technology Day" and the APJ NonStop Partner Conference followed. Partners like ETI-NET, Idelji, comForte, XYPRO and IDC were on hand to make presentations to an audience with almost twice the number of people expected including many people new to NonStop.

In the same week but much closer to our Palo Alto home, Wendy Bartlett presented the NonStop strategy and a security update at MRTUG near Chicago and OTUG in Columbus, Ohio. Turnout was high for both events, and there was a lot of give-and-take discussion throughout the HPE, partner and customer presentations.

However the largest and most sublime NonStop event of the year was in London! Everyone who attended the sold out eBiTUG event is still abuzz about it. There were keynote speeches by Jimmy Treybig, Andrew Bergholz and Dave McLeod and some amazing breakout talks. The most dazzling party of the show however was the event held at Aqua Shard hosted by our friends at CSP. Guests were given a beautiful sunset view of London with 360-degree views from the 31st floor with amazing food and drinks.

HPE's Discover 2017 in Las Vegas will be another grand event this year. It starts the 2nd week of June and NonStop will be there with our colleagues from the rest of the Mission Critical team. This year's Discover show is being combined with an HPE Global Partner event. If you are attending please drop by the Mission Critical area to say hello to our hardworking NonStop team.

In a shameless self-serving plug, I want to let people know that the week before Discover, I'll be in Dallas presenting at the N2TUG event to customers from Oklahoma and Texas. So there's plenty going on to keep everyone busy.

This edition of The Connection focuses on "Architecting your NonStop System for High Availability". While we all know that NonStop Systems come out of the box already architected for Fault Tolerance and the highest availability, there are of course ways to take the best advantage of what NonStop offers. In the case of Virtualized NonStop there are so many options for customers and ways to configure the systems that we have put a vetting process in place to work with customers and sales teams to ensure that final orders will work in the hardware environment that the end user is planning.

This month includes articles like "Dramatically Reduce Outage Costs with Advanced Business Continuity Solutions" from Keith Evans of Gravic and several articles on security such as "Welcome to the Layer Cake Son" by Steve Tcherchian from XYPRO where Steve looks as how security layers help you protect your system, and articles from the HPE SecureData team on FIPS certification and using tokenization to secure data in your POS networks. We're also including Sridhar Neelakantan' s short write up of a new product HPE is offering, NonStop In Memory Cache (or NSIMC) which some of you may want to check out. (It's a useful architectural addition to the platform at a nice price – free!)

So before you sail off on vacation for the summer, take a little time to check out what's happening with NonStop. We hope to see you at one of the NonStop user events so you can talk with us, our partners and your colleagues at other companies about the many ways NonStop can help you spring forward with your business.

Regards to everyone!

Karen

Karen Copeland
Manager, WW NonStop Product Management
Mission Critical Solutions
Hewlett Packard Enterprise

IT-Symposium 2017

GTUG NonStop Spring 2017 & Open VMS Spring 2017 April 25th - 27, 2017

"Digitalization" was the topic of the "IT-Symposium 2017", which this time took place at the "Robotation Academy" on the fairground of "Hannover Messe" (Hannover) and in Braunschweig, Germany. It was organized by the HPE User Groups Connect Deutschland e.V. and GTUG e.V.

Beside NonStop and VMS specific sessions and SIGs, (presented by customers, HPE and HPE software partners) there have been presentations from Thorsten Milsmann, HPE on "IoT" and Prof. Dr. Jana Köhler, University of Luzen on "Congnitive Services in industry". comForte21, ETINET and Xypro this time have been the exhibitors.

Further more the attendess had the opportunity to partiticipate at a interesting guided tour through the HPE booth at Hannover Messe, one of the biggest industry fairs in the world.

The "Welcome Reception" on April 25th at Hotel Landhaus Seela and the conference dinner on April 26th at Restaurant "Al Duomo" in the historic city of Braunschweig offered good opportunities for discussions and networking.

For more information and the published presentations please visit the websites www.connect-community.de and www.gtug.de.

GRAVIC®
Shadowbase

Would you bungee jump without knowing it was safe?

Then why take chances with your Business Continuity solution?

Many business continuity solutions are difficult or even impossible to effectively test. You'll never know if they work until you really need them. And by then, it's too late. Eliminate these risks by using an **HPE Shadowbase Active/Active** or **Sizzling-Hot-Takeover** business continuity solution. Then, you'll know for sure that your safety net will work.

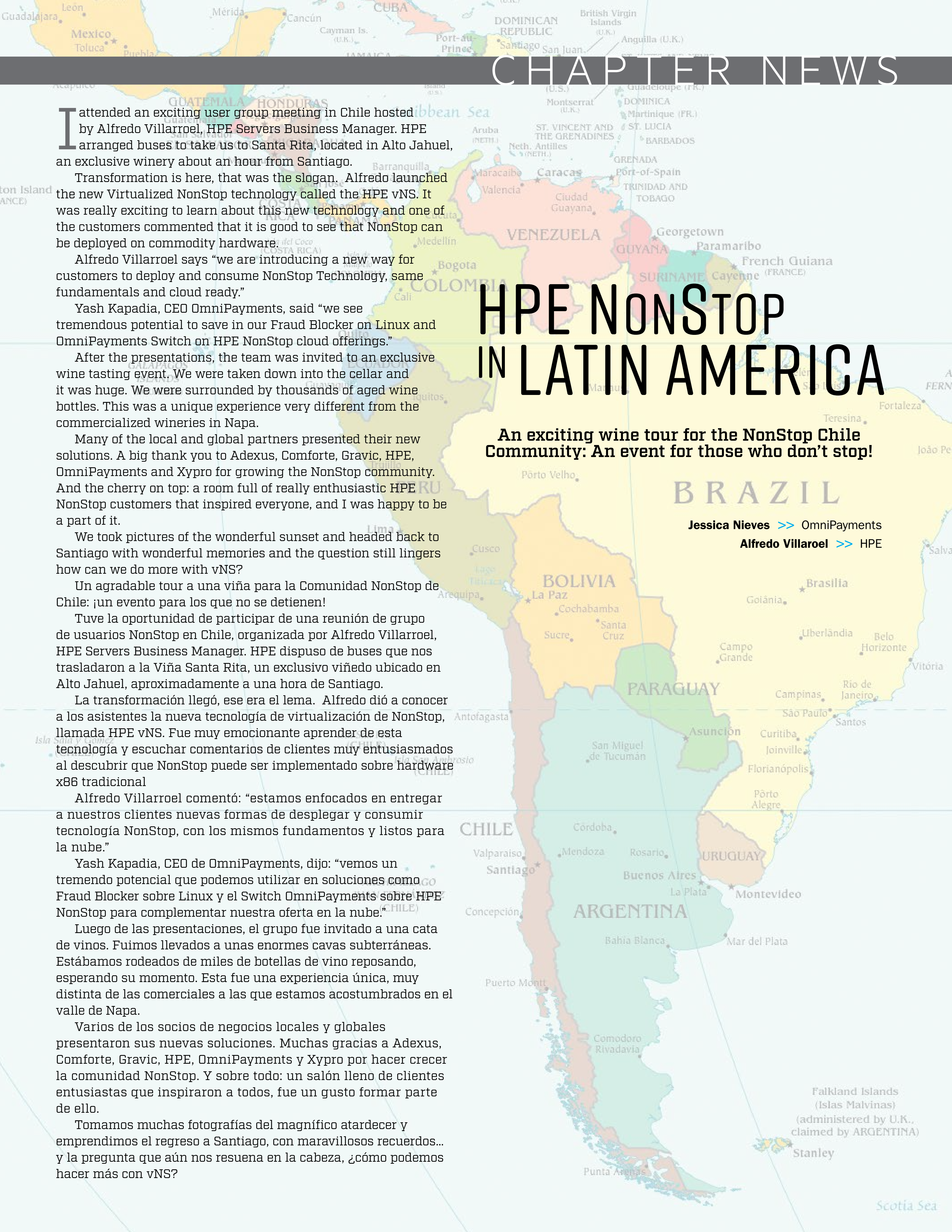
Don't cling to the cliff, contact us!

For more information, please see the Gravic white paper: *Choosing a Business Continuity Solution to Match Your Business Availability Requirements.*

ShadowbaseSoftware.com

Hewlett Packard
Enterprise
Silver
Partner
Technology Partner

©2017 Gravic, Inc. All product names mentioned are trademarks of their respective owners. Specifications subject to change without notice.



HPE NonStop in LATIN AMERICA

An exciting wine tour for the NonStop Chile Community: An event for those who don't stop!

Jessica Nieves >> OmniPayments
Alfredo Villaroel >> HPE

I attended an exciting user group meeting in Chile hosted by Alfredo Villarroel, HPE Servers Business Manager. HPE arranged buses to take us to Santa Rita, located in Alto Jahuel, an exclusive winery about an hour from Santiago.

Transformation is here, that was the slogan. Alfredo launched the new Virtualized NonStop technology called the HPE vNS. It was really exciting to learn about this new technology and one of the customers commented that it is good to see that NonStop can be deployed on commodity hardware.

Alfredo Villarroel says "we are introducing a new way for customers to deploy and consume NonStop Technology, same fundamentals and cloud ready."

Yash Kapadia, CEO OmniPayments, said "we see tremendous potential to save in our Fraud Blocker on Linux and OmniPayments Switch on HPE NonStop cloud offerings."

After the presentations, the team was invited to an exclusive wine tasting event. We were taken down into the cellar and it was huge. We were surrounded by thousands of aged wine bottles. This was a unique experience very different from the commercialized wineries in Napa.

Many of the local and global partners presented their new solutions. A big thank you to Adexus, Comforte, Gravic, HPE, OmniPayments and Xypro for growing the NonStop community. And the cherry on top: a room full of really enthusiastic HPE NonStop customers that inspired everyone, and I was happy to be a part of it.

We took pictures of the wonderful sunset and headed back to Santiago with wonderful memories and the question still lingers how can we do more with vNS?

Un agradable tour a una viña para la Comunidad NonStop de Chile: ¡un evento para los que no se detienen!

Tuve la oportunidad de participar de una reunión de grupo de usuarios NonStop en Chile, organizada por Alfredo Villarroel, HPE Servers Business Manager. HPE dispuso de buses que nos trasladaron a la Viña Santa Rita, un exclusivo viñedo ubicado en Alto Jahuel, aproximadamente a una hora de Santiago.

La transformación llegó, ese era el lema. Alfredo dió a conocer a los asistentes la nueva tecnología de virtualización de NonStop, llamada HPE vNS. Fue muy emocionante aprender de esta tecnología y escuchar comentarios de clientes muy entusiasmados al descubrir que NonStop puede ser implementado sobre hardware x86 tradicional

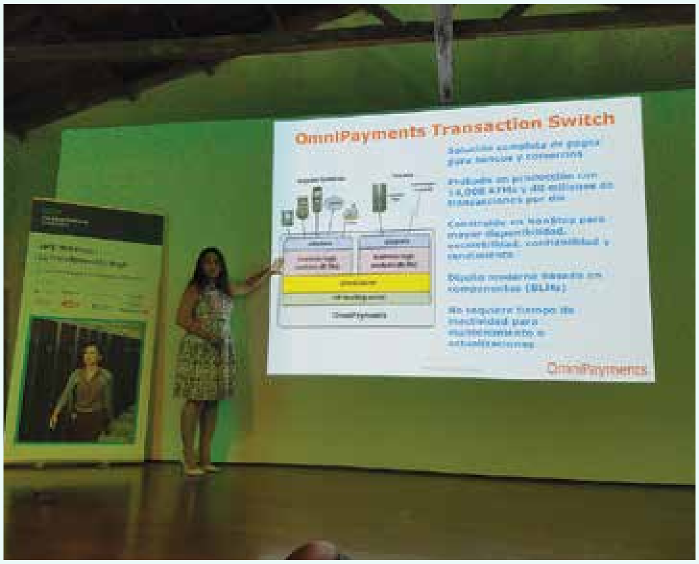
Alfredo Villarroel comentó: "estamos enfocados en entregar a nuestros clientes nuevas formas de desplegar y consumir tecnología NonStop, con los mismos fundamentos y listos para la nube."

Yash Kapadia, CEO de OmniPayments, dijo: "vemos un tremendo potencial que podemos utilizar en soluciones como Fraud Blocker sobre Linux y el Switch OmniPayments sobre HPE NonStop para complementar nuestra oferta en la nube."

Luego de las presentaciones, el grupo fue invitado a una cata de vinos. Fuimos llevados a unas enormes cavas subterráneas. Estábamos rodeados de miles de botellas de vino reposando, esperando su momento. Esta fue una experiencia única, muy distinta de las comerciales a las que estamos acostumbrados en el valle de Napa.

Varios de los socios de negocios locales y globales presentaron sus nuevas soluciones. Muchas gracias a Adexus, Comforte, Gravic, HPE, OmniPayments y Xypro por hacer crecer la comunidad NonStop. Y sobre todo: un salón lleno de clientes entusiastas que inspiraron a todos, fue un gusto formar parte de ello.

Tomamos muchas fotografías del magnífico atardecer y emprendimos el regreso a Santiago, con maravillosos recuerdos... y la pregunta que aún nos resuena en la cabeza, ¿cómo podemos hacer más con vNS?


OmniPayments Transaction Switch
Solución completa de pagos para bancos y comercios
Probado en producción con 14,000 ATMs y 40 millones de transacciones por día
Construido en NonStop para mayor disponibilidad, escalabilidad, confiabilidad y rendimiento
Diseño moderno basado en componentes (BLMs)
No requiere tiempo de inactividad para mantenimiento o actualizaciones
OmniPayments

Jessica Nieves, OmniPayments, After over 14 years of technical experience in the transaction processing industry, managing banking delivery channels, and payments systems, she joined OmniPayments. Jessica now leads OmniPayments Client Services and Operations.

Alfredo Villarroel, HPE. Mr. Villarroel has direct responsibility for the NonStop Servers business in Chile. He has previously held various positions at HPE, from field support engineer through District Manager before moving to sales, beginning his career as a Tandem (HPE NonStop) support engineer back in 1999.

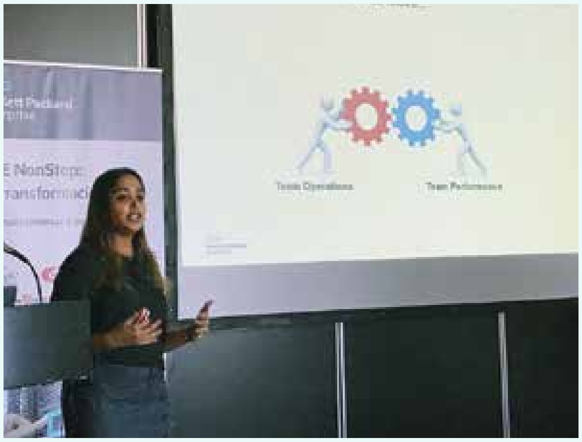
NonStop User Group meeting in Argentina

Jessica Nieves OmniPayments and Fabian Manfredi, NonStop BM Hewlett Packard Argentina

After Santiago I flew to Buenos Aires and enjoyed spectacular views of the Andes. The Argentina NonStop User Group event was perfectly timed right after the Chile NonStop User Group event.

Fabian Manfredi, NonStop Business Manager, HPE Argentina, kicked off the event at a splendid hotel with panoramic views overlooking the scenic Puerto Madero. Fabian launched the vNonStop in Argentina and it drew a lot of attention. The room was packed with customers and partners, a very good turnout for the Argentina NonStop user community.

Fabian Manfredi says “vNonStop will open new markets for us and our NonStop Partners on Retails and Small Banking in Argentina.”



Evento de los Usuarios NonStop en Argentina

Jessica Nieves de OmniPayments y Fabian Manfredi, Gerente de Negocios NonStop de Hewlett Packard Argentina

Luego del evento de Santiago de Chile, tomamos un vuelo a Buenos Aires donde tuvimos una espectacular vista de la Cordillera de Los Andes. El Evento de Usuarios NonStop de Argentina estuvo perfectamente sincronizado luego del Evento de Usuarios NonStop de Chile.

Fabian Manfredi, Gerente de Negocios NonStop de Hewlett Packard Argentina realizó la apertura del evento en un explendido hotel ubicado en la zona residencial de Puerto Madero donde disfrutamos de una excelente vista panorámica. Fabian llevó adelante el lanzamiento de vNonStop en Argentina lo que generó una importante atención de la audiencia. La sala estaba completa de clientes y socios de negocio NonStop, una participación muy buena para la comunidad de usuarios NonStop en Argentina.

Fabian Manfredi expresó: “vNonStop abrirá nuevos mercados para HPE y nuestros socios de negocio NonStop en el mercado de Retail y pequeños Bancos en Argentina.”

Fabian Mandfredi is an HPE Business Manager for the NonStop Servers business in Argentina, Uruguay and Paraguay. After 10 years working at one of the biggest NonStop customers in Argentina, in 1998 Fabian joined HPE as a Pre-Sales resource, and two years later became Product Manager and Sales Specialist of NonStop managing the south region of Latin America.

The Zero Outage Industry Standard Association

Dr. Bill Highleyman >> Managing Editor >> Availability Digest

As an organization's IT infrastructure can involve a complex ecosystem of technologies from a variety of vendors, there are often differing levels of service-level agreements in place which can lead to critical defaults and security issues.

The Zero Outage Industry Standard Association (www.zero-outage.com) is focused on minimizing the risk of users suffering from IT outages. It is creating IT principles that will help users to confidently make use of systems and services that are less likely to be affected by crashes and outages. As one who deals extensively with highly available systems, it is clear to me that a standards organization dealing in reducing outages is sorely needed by the industry. However, I am not sure that this association is going to achieve its goals. At least so far, its outlook is much too generic.

Launched in November, 2016, the Association is headquartered in London, United Kingdom. Its founding members include Brocade, Cisco, Dell EMC, Hitachi Data Systems, Hewlett-Packard Enterprise, Juniper, NetApp, SAP, SUSE, T-Systems, and IBM. There are many other large organizations with a stake in IT availability, and I wonder why they have elected not to participate.

Zero Outage is currently in the process of defining what is required to achieve a zero-outage IT environment. IT failures can result from technical defect, human error, or flawed, inconsistent, or ineffective organizational processes. The Association seeks to standardize the quality of IT platforms, people, processes and security throughout the IT life cycle.

Zero outage industry standards reflect several parallel trends:

The ongoing digitalization of the enterprise.

The growing importance to businesses of being able to maintain uninterruptible services to their customers.

The real cost to businesses caused by service interruptions and outages.

The desire among industry manufacturers to find new commercial opportunities and ways of boosting productivity in an increasingly competitive marketplace.

The Zero Outage Industry Standard Association

As Association members point out,

"Digitization is in full swing: Machines communicate with each other, processes are becoming more efficient, and automation is an integral part of the process. But this can only work if the IT behind it runs smoothly. A failure, even for a few minutes, can have fatal consequences. If production bands are stopped due to IT problems, companies are threatened with image losses and costs of millions."[1]

The digital world is increasingly dependent on IT. A technical defect, human error, or erroneous process execution can be a threat to a company's everyday operations. Zero Outage intends to specify consistent error response times, employee qualification levels, and asset security and platform requirements in order to help companies minimize errors, increase availability, ensure security, and operate cost-effectively.

Zero Outage is providing a framework of best practices and standards to enable the delivery of secure, reliable, and highly available end-to-end services and solutions. The goal is to safeguard quality and reliability at all levels and to maximize the availability and customer satisfaction with IT services by improving stability and security.

The Zero Outage Initiative intends to focus on:

- Establishing consistent error response times.
- Improving security and platform guidelines.
- Specifying training and qualification requirements for IT personnel.

From my own personal experience in dealing with highly available systems, I think that Zero Outage should focus on additional items such as:

- The quality of devices in redundant systems.
- The proper architecture of redundant systems.
- Proper failover procedures.
- Failover testing (often not done or done only partially by organizations).
- The frequency of failover testing (many organizations rely on faith and hope rather than on proper testing).

Stephan Kasulke, senior vice-president of global quality at IT service provider T-Systems, is the Association chairman. He stated:

[1] The Zero Outage Industry Standard Association website https://www.zero-outage.com.

"As an organization's IT infrastructure can involve a complex ecosystem of technologies from a variety of vendors, there are often differing levels of service-level agreements in place which can lead to critical defaults and security issues."

Zero Outage's IT standards will help bring into conformity the requirements of SLAs from different vendors.

Zero Outage Design Principles

Zero Outage's priority is on existing technologies, not new technologies. In order to create a Zero Outage framework, it is important to establish agreement on what Zero Outage Design Principles mean. This has been the initial focus, and the Association's current positions on this topic are as follows:

What do Zero Outage Design Principles mean?

The Association must describe the necessary combination of features and services in conjunction with IT-elements in order to contribute to a Zero Outage service. They include the Zero Outage Design Principles needed to achieve the anticipated standard. For instance, principles will be compiled for becoming a Zero Outage cloud environment.

Two varying perspectives on Zero Outage Design Principles

Two types of Zero Outage Design Principles exist:

- General Zero Outage Design Principles that suit all IT elements, such as the high availability of power supplies.
- Specific Zero Outage Design Principles for specific IT elements, such as LAN storage devices.

Zero Outage Design Principle Phases

Within each Zero Outage Design Principle, there are three phases:

The Plan Phase:

During the Plan phase, Zero Outage requirements that are to be met by all platforms, such as redundant design, are established. A Validation Plan to ensure these requirements are met is prepared.

The Build Phase:

The Build Phase follows a deployment plan that must be prepared. Proper tests at the end of the deployment are specified to ensure the introduction to service has been correct. Support is provided for a period after the Build Phase to ensure systems continue to operate properly. (It is here that the failover procedures should be specified and tested.)

The Run Phase:

The Run Phase includes normal life-cycle management activities, such as update, change, and patch management.

Design Principles for the Run Phase

It is during the Run Phase that test procedures can be provided to certify compliance with the Zero Outage Design Principles. The Principles include:

Zero Outage Design Principles for IT Elements:

Redundant power supplies and interfaces with battery back-ups
Non-disruptive upgrades, patches, and changes
A health-check procedure for providing system status
Online replacements without disruption
Redundant cable paths, virtual paths, and drive paths
Redundancy and resiliency checks
Absence of single points of failure in the architecture
Failover procedures and tests

Zero Outage Design Principles for Storage Devices:

Online procedures for hardware replacement
Up and down capacity scaling
Online implementation of updates, patches, and changes
Check procedure for missing data replication or backup
Securing traceable purging data from replaced disks

Zero Outage Design Principles for Network Elements:

Redundant routing engines
Redundant cards and ports
Redundant links
Geo-redundancy via WAN
In-building redundancy (e.g., fire protection)

Summary

The Zero Outage Industry Standards Association is a work in progress. The major companies involved have been active in the organization only for a few months as of this writing. At this point, they are still in the process of defining Zero Outage Design Principles. However, the goal is impressive. If the Association can produce reasonable standards for zero outage IT systems, businesses and consumers will have scored a major win against the costs and inconvenience of IT failures.

However, the Association's attempts at defining principles are currently much too generic. As I mentioned above, zero outage principles should include additional factors such as requirements for redundant systems and failover procedures and testing.

Acknowledgement

Information for this article was taken from the web site of The Zero Outage Industry Standard Association www.zero-outage.com.

Dr. Bill Highleyman brings years of experience to the design and implementation of mission-critical computer systems. As Chairman of Sombers Associates, he has been responsible for implementing dozens of real-time, mission-critical systems - Amtrak, Dow Jones, Federal Express, and others. He also serves as the Managing Editor of The Availability Digest (availabilitydigest.com). Dr. Highleyman is the holder of numerous U.S. patents and has published extensively on a variety of technical topics. He also ghostwrites for others and teaches a variety of onsite and online seminars. Contact him at billh@sombers.com.

Women in NonStop: *Tissa Richards*

Mandi Nulph >> Marketing Coordinator >> NuWave Technologies

In this edition of Women in NonStop we spoke with Tissa Richards, founder and CEO of Network Kinetix, about her professional journey and the future of security in NonStop.

Mandi Nulph: Let’s start off with who you are and your background.

Tissa Richards: I am the founder and CEO of Network Kinetix. We're still in stealth mode in terms of not having a very loud presence online and at trade shows, but we are working with channel partners, partners like HPE, and with customers in deployment on our product. We'll probably come out of stealth mode in the next 12 months, once we get some solid reference studies that we think will be able to launch that in a really loud way.

I came out of a security and enterprise software background initially, after 20 years in Silicon Valley. I decided when I started Network Kinetix to relocate out to Austin where there is a lot of growth and innovation happening.

Mandi: What has been your professional journey so far?

Tissa: I think I always thought I would be a lawyer when I was younger, or maybe in public relations, because I like the power of words and talking for a living. I found myself working in technology doing global program management, branding, and product management. I was working with a combination of Fortune 500 companies and startups in Silicon Valley.

I really stumbled into starting my own company. I think if you had predicted this for me a few years ago, I would have gotten a real kick out of it because it’s not in my risk profile. As with a lot of classic startups, the idea for Network Kinetix was born in a bar with a conversation about a big, fundamental problem that wasn't being solved. That conversation sparked a moment of insight into an elegant solution–if we could give it a try, maybe there would be something there. Next thing you know, you're self-funding a company, you have a team of people working for you and you've got partners like HPE! Then you start getting outside investors, you start getting customers, the patent office is issuing patents, and three years later, you suddenly realize, “wow, maybe you do have it in you to be entrepreneurial.” But it happens really fast, and it's a lot of fun–it’s a whirlwind.

Mandi: How would you say your experience working as a woman in the tech industry has been so far, especially as someone who owns her own company?

Tissa: A lot of women feel that there are issues being a woman in technology. You hear things like being "manterrupted" and "mansplained to", but frankly, that has never happened to me. I’m frequently the only woman in the room and I don't care. I don't notice, and I don't think the other people in the room notice. My gender hasn’t hindered me from successfully raising money for the company or bringing industry luminaries onto our advisory board. As an example, Jimmy Treybig, who founded Tandem, has joined our advisory board and has been an incredible mentor to me personally, as well as to the company. For me, there is no difference being a woman in technology or being a man in technology, as long as you are hardworking, ethical, and straightforward. I know a lot of women don't agree with that, but I’ve been very fortunate that that has been my experience my entire career. I have never, ever been made to feel different. I have only been made to feel like a contributor to whatever I have been working on.

Mandi: You just mentioned Jimmy Treybig, but have you had any other mentors in your career?

Tissa: I've had several mentors, and they have all been from really different places. My relationship with Jimmy was unexpected and something I don’t take for granted. It was one of those meetings where you think, "Oh this is great! It's a once in a lifetime thing!" But he saw something in the company that convinced him to stay with us. I think Tandem had a similar journey as a startup that we are having with Network Kinetix. Tandem was a complete paradigm shift when it was first started. Nobody had ever thought about fault-tolerant, failover computing. They had to educate people and create a market that then took off rapidly and still endures today in NonStop. I think that what we are doing is similar in terms of changing a paradigm, and it can be frustrating to have to educate people before you can begin the sales cycle. It’s nice when you have people who have “been there, done that”, and have been entrepreneurs themselves, so they know the grind.

I also have great mentors from my previous roles in Silicon Valley. It's not a direct relation to what I do every day in my professional life today, but they are so successful in what they do and it's surprising how useful their mentorship has been. I think that's an important lesson: don't try to find a mentor who only does what you do. They have been some of the most valuable people in my career.

Mandi: Do you have any advice for people who are coming into the technology industry, whether they are joining an existing company or want to start their own?

Tissa: The most important thing, if you are fortunate enough to be able to do it, is internships. Do as many internships as you can, and you must be really bold. For my first internship, which I firmly believe launched many of my subsequent jobs and opportunities, I literally had to walk up to a general manager at a very large public relations firm and tell him that I needed it. There were no more open internship positions left, but I talked my way into it. I think you have to be really ballsy, because you are negotiating and advocating for the whole rest of your life. You may not have a lot of confidence at that age, and you don't even know what you're good at yet, so it doesn't matter. You just have to get out there and know that somehow, you'll figure it out.

The other thing is not to be afraid to ask people to mentor you. It can be kind of embarrassing, because early on you may not even know what you are asking them to mentor you in, but people don't mind. Especially when you're up front about it, which is, "I think you could really teach me a lot, would you be willing to help me?" I think a lot of people, especially good people, are willing to pay it forward and help--you just have to ask.

And, as you get further in your career, make sure you pay it forward. If someone asks you to meet with a young person just starting out or exploring their career paths, do it. Or if someone works up the nerve to ask you to mentor them, really consider it. Think about what mentors have meant to you in your career and life and take the time to return that gift.

The last piece of advice is that you don't necessarily have to know what you want to do or what you're good at. I'm a great example. I started a technology company, but I'm not a technologist. I'm not an engineer. I can't cut code. But we now have attracted a lot of technologists to our advisory board and to support the company.

Every five years or so you realize, "I wouldn't have been doing this five years ago, but everything I've done in the past five years has built me up to it." So, don't be afraid if you don't know where it's leading you. It's leading you somewhere.

Mandi: Thank you for your time, Tissa! That is all very interesting and exciting.

Tissa: Thank you for the opportunity!

To learn more about Network Kinetix and Tissa Richards, visit www.nuwavetech.com/blog

Mandi Nulph is NuWave's marketing coordinator. NuWave specializes in HPE NonStop middleware, including their newest product, LightWave Server™, which allows you to expose your existing Guardian or Pathway servers as industry-standard REST services. With a degree in Mass Communication and Journalism, she boasts 10 years of professional experience writing and editing for a variety of publications, as well as an extensive career in marketing. She volunteers to help interview companies making innovations in the NonStop space for a variety of trade publications.

CONNECT
Your Independent Hewlett Packard Enterprise Technology User Community
MEMBER

UPDATE YOUR PROFILE TODAY!

http://bit.ly/2jKRaph

www.connect-community.org

You Know NonStop

You want to know that your information is accessible, yet secure. You also want to be able to get the most out of your hardware investment quickly and easily. We don't think that's too much to ask.

NuWave offers quick, easy, secure integration for your NonStop servers. Our products can connect your servers to virtually any platform, anywhere, using REST or SOAP services, allowing you to get the most out of your systems.

You choose NuWave for all of your NonStop middleware needs, because you know NonStop.

Why NuWave Middleware?

✓ ***HIGH QUALITY***

✓ ***LOW TCO***

✓ ***EXCELLENT SUPPORT***

Learn more about NuWave middleware at
www.nuwavetech.com/middlewareguys

NuWave
THE MIDDLEWARE GUYS

Government Agencies Require the Same Data Protection as the Private Sector

Marcelo Delima >> **Global Product Marketing Manager** >> HPE Security - Data Security

Our world runs on data. From consumer information (health files, banking and financial data, education records, and more) to research findings and classified national security information, we generate an ever-increasing volume of critical, sensitive data. Criminals target much of this information, and cyber-attacks against enterprises and governments globally continue to grow in frequency and severity. A U.S. federal government agency data breach announced in June 2015 involved the greatest theft of sensitive government data in the history of the United States. Data targeted in the breach included personally identifiable information such as Social Security numbers, as well as names, dates and places of birth, and addresses. Worse, the hack went deeper than initially realized, and likely involved the theft of detailed security clearance-related background information. The estimated number of stolen records is 21.5 million, with an estimated cost of more than $1 billion.

How did it happen? The agency maintained an unsecured and unencrypted database for security clearances. A 2006 agency report states that this "Data Repository" is premised on a "shared-disk (shared-data) model," and that "all of the disks containing databases are accessible by all of the systems." An official at the Department of Homeland Security (DHS) testified that the attackers most likely gained valid user credentials to the systems by a phishing attack through social engineering. The breach also consisted of a malware package that installed itself within the agency's network and established a backdoor. From there, attackers escalated their privileges to gain access to a wide range of the agency's systems.

The damage is not limited to the agency. Whatever entity successfully breached the agency system potentially gained pass-through access to other extraordinarily sensitive national security data. Whether perpetrated by lone operators or state-sponsored actors, data theft is a constant, and protecting data is of the utmost importance. It's not a question of if you will be hacked; it's a question of when. And it's vital to be prepared.

The government challenges

Government customers have some of the same challenges faced by private sector corporations, including:

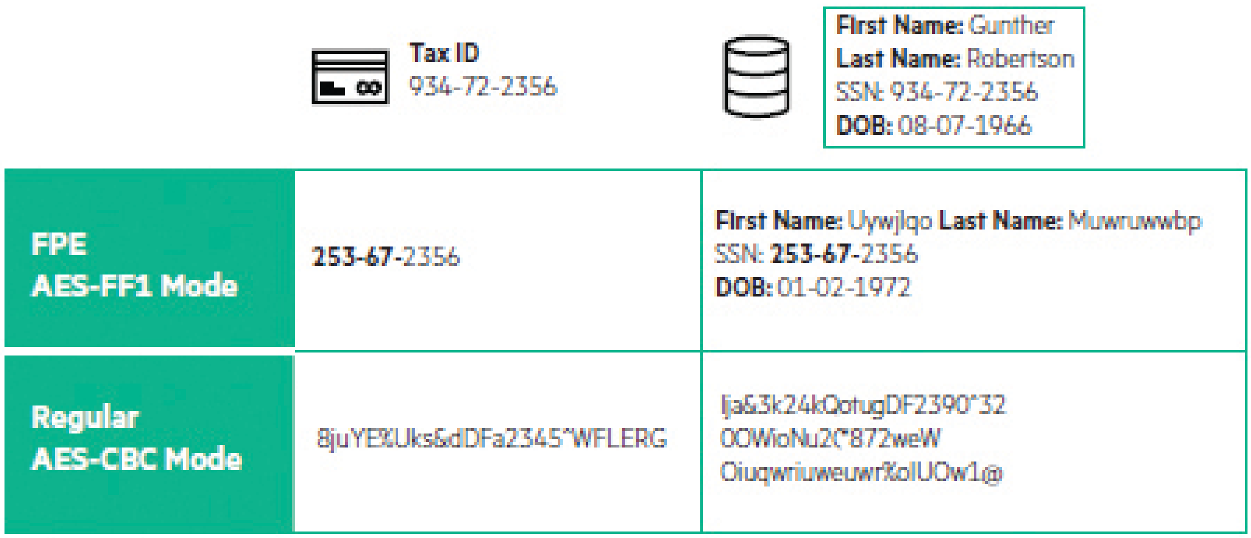
- The exponential growth of high-value and personally identifiable information from citizens, employees, and anyone with any business with the government.
- The difficulty of adding security to legacy applications and platforms with limited native data security options.
- Gaps in data protection from the over-reliance on data-at-rest, network and endpoint security.
- The need to leverage rich data for analytics and share data between agencies and with contractors.
- Compliance with privacy and data protection legislation such as General Data Protection Regulation (GDPR), The Health Insurance Portability and Accountability Act (HIPAA).
- The need to adopt innovations such as cloud and IoT.

HPE SecureData provides an end-to-end data-centric approach to enterprise data protection. It is the only comprehensive data protection platform that enables you to protect data over its entire lifecycle—from the point at which it's captured, throughout its movement across your extended enterprise, all without exposing live information to high-risk, high-threat environments.

HPE SecureData includes next generation technologies, Hyper Format-Preserving Encryption (FPE), Hyper Secure Stateless Tokenization (SST), HPE Stateless Key Management, and data masking.

A comprehensive approach to end-to-end encryption

HPE SecureData with Hyper FPE has the ability to "de-identify" virtually unlimited data types, from sensitive personally identifiable information (PII), to IDs, health information or classified data, rendering it useless to attackers in the event of a security breach. This allows government agencies to securely leverage the de-identified data for big-data analytics, and collaborate with shared data between other agencies or contractors. It also provides accelerated encryption speeds that



	Tax ID 934-72-2356	**First Name:** Gunther **Last Name:** Robertson SSN: 934-72-2356 **DOB:** 08-07-1966
FPE **AES-FF1 Mode**	**253-67**-2356	**First Name:** Uywjlqo **Last Name:** Muwruwwbp SSN: **253-67**-2356 **DOB:** 01-02-1972
Regular **AES-CBC Mode**	8juYE%Uks&dDFa2345^WFLERG	Ija&3k24kQotugDF2390"32 0OWioNu2(*872weW Oiuqwriuweuwr%olUOw1@

Figure 1. Format-Preserving Encryption (FPE) versus regular AES Encryption

enables government agencies to adopt new technologies such as the cloud or Hadoop or invest in innovations such as IoT, all while lowering the risk of disclosing sensitive personal data or compromising high value data.

A major challenge faced by federal agencies, including those attacked by nation state adversaries, is the dependency on legacy applications and platforms with limited native data security options. HPE SecureData helps build data security into both new and decades-old legacy applications, de-identifying high-value data classes; for example, protecting classified information, or eliminating reliance on using Social Security Numbers for business processes. Security assurance is increased, while unleashing utility of data for secure adoption of big data analytics, Hadoop and other new applications and solutions.

Hyper FPE: encryption and masking—how we do it

Traditional encryption approaches, such as AES CBC have enormous impact on data structures, schemas, and applications as shown in Figure 1. Hyper FPE is NIST-standard using FF1 mode of the Advanced Encryption Standard (AES) algorithm, which encrypts sensitive data while preserving its original format without sacrificing encryption strength. Structured data, such as Social Security, Tax ID, credit card, account, date of birth, salary fields, or email addresses can be encrypted in place.

Traditional encryption methods significantly alter the original format of data. For example, a 16-digit credit card number encrypted with AES produces a long alphanumeric string. As a result, database schema changes are required to facilitate this incompatible format. Hyper FPE maintains the format of the data being encrypted so no database schema changes and minimal application changes are required—in many cases only the trusted applications that need to see the clear data need a single line of code. Tools for bulk encryption facilitate rapid de-identification of large amounts of sensitive data in files and databases. Typically, whole systems can be rapidly protected in just days at a significantly reduced cost. In fact, Hyper FPE allows accelerated encryption performance aligning to the high volume needs of next generation Big Data, cloud and Internet of Things, and supports virtually unlimited data types.

Hyper FPE de-identifies production data and creates structurally valid test data so developers or users can perform QA or conduct data analysis—all without exposing sensitive data. The HPE SecureData management console enables easy control of policy and provides audit capabilities across the data life cycle—even across thousands of systems protected by HPE SecureData. Hyper FPE also provides the option to integrate access policy information in the cipher text, providing true data-centric protection where the data policy travels with the data itself.

HPE Stateless Key Management: transparent, dynamic

HPE Stateless Key Management securely derives keys on the fly as required by an application, once that application and its users have been properly authenticated and authorized against a centrally managed policy. Advanced policy controlled caching maximizes performance. HPE Stateless Key Management reduces IT costs and eases the administrative burden by:

- Eliminating the need for a key database, as well as the corresponding hardware, software and IT processes required to protect the database continuously or the need to replicate or backup keys from site to site.
- Easily recovering archived data because keys can always be recovered.
- Automating supervisory or legal e-discovery requirements through simple application APIs, both native and via web services.
- Maximizing the re-use of access policy infrastructure by integrating easily with identity and access management frameworks and dynamically enforcing data-level access to data fields or partial fields, by policy, as roles change.

Hyper SST (Secure Stateless Tokenization)

Hyper SST is an advanced, patented, data security solution that provides enterprises, merchants, and payment processors with a new approach to help assure protection for payment card data. Hyper SST is offered as part of the HPE SecureData platform that unites market-leading encryption, tokenization, data masking, and key management to protect sensitive information in a single comprehensive solution.

Hyper SST is "stateless" because it eliminates the token database, which is central to other tokenization solutions, and removes the need for storage of cardholder or other sensitive data. Hyper SST uses a set of static, pre-generated tables containing random numbers created using a FIPS random number generator. These static tables reside on virtual "appliances"—commodity servers—and are used to consistently produce a unique, random token for each clear text Primary Account Number (PAN) input, resulting in a token that has no relationship to the original PAN. No token database is required with Hyper SST, thus improving the speed, scalability, security, and manageability of the tokenization process. In fact, Hyper SST effectively surpasses the existing "high-octane" SST tokenization performance.

NIST validation brings FPE to Government

HPE SecureData is the first data protection platform to earn FIPS 140-2 validation of its Format-Preserving Encryption (FPE) technology under the new National Institute of Standards and Technology's (NIST) AES FF1 Format-Preserving Encryption (FPE) mode standard. This enables public sector customers, when operating in strict FIPS mode, to take advantage of true FIPS-validated cryptography and build compliance programs for regulations such as the Cybersecurity Act of 2015 data security requirements, DFARS CUI, and General Data Protection Regulations (GDPR).

Key Government Benefits

With the HPE SecureData FIPS validation, government agencies and contractors can now use a standardized data security product with extensive enterprise deployments, neutralizing data breaches while liberating analytics and innovation. Key benefits include:

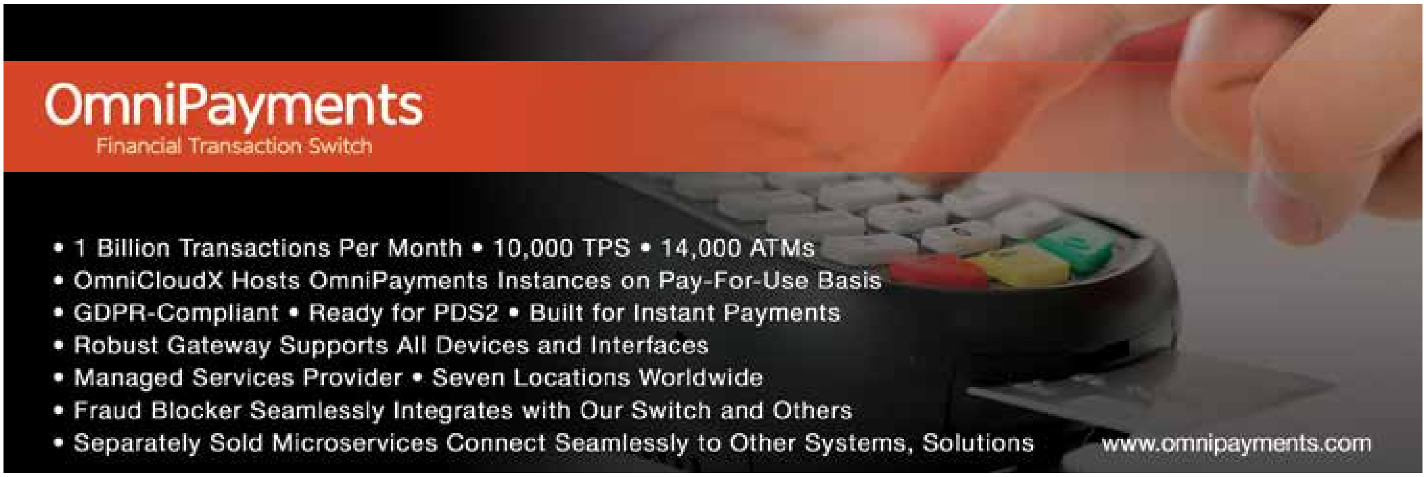
- Protect all kinds of structured high value data: personally identifiable information (PII), personal health information (PHI) or Classified data types.
- Enable agencies to share data (data portability), improve citizen services and collaborate with other agencies and contractors.
- Layer data-centric security into decades old legacy systems and applications.
- Expand access to de-identified data, drive big data analytics.
- Adopt innovations such as cloud, Hadoop and IoT.
- Address specific requirements in legislations such as Cybersecurity Act of 2015, DFARS CUI, GDPR or HIPAA.
- Protect foreign citizen data with Unicode latin 1 support.
- FIPS validated solution and NIST standardized technology.

Conclusion

Government agencies set the high bar for protecting both their sensitive data and citizen data across multiple platforms and applications, both legacy and modern. With the HPE SecureData FIPS validation, and the NIST validation of AES FF1 Format-Preserving Encryption (FPE), government agencies and private contractors can leverage the same powerful technology that has transformed cybersecurity in the private sector. A standardized data security technology with extensive enterprise deployments, neutralizing data breaches while liberating analytics and innovation.

In his capacity as Global Product Marketing Manager at HPE Security – Data Security, Marcelo focuses the US Federal market sector among other responsibilities. Marcelo has over 16 years of experience marketing secure technology solutions for highly regulated enterprises and government agencies. In his career Marcelo has held marketing leadership and management positions in technology organizations large and small in Silicon Valley.

NonStop Resources
Watch for a special advertising section coming soon...


OmniPayments
Financial Transaction Switch

- 1 Billion Transactions Per Month • 10,000 TPS • 14,000 ATMs
- OmniCloudX Hosts OmniPayments Instances on Pay-For-Use Basis
- GDPR-Compliant • Ready for PDS2 • Built for Instant Payments
- Robust Gateway Supports All Devices and Interfaces
- Managed Services Provider • Seven Locations Worldwide
- Fraud Blocker Seamlessly Integrates with Our Switch and Others
- Separately Sold Microservices Connect Seamlessly to Other Systems, Solutions

www.omnipayments.com

Dramatically Reduce Outage Costs with Advanced Business Continuity Solutions

Keith B. Evans >> **Shadowbase Product Management** >> Gravic, Inc.

Disaster Recovery is Not Business Continuity

In today's business world, consistent access to real-time online transactional data is a competitive advantage. To realize the advantage, this data must be available at any time, all the time, from anywhere, and it must be current. The corollary to this advantage is that the inability to access or update this current data, or the loss of data, carries a significant business cost, possibly measured in many thousands of dollars per second, or even lives lost. In some cases, absolutely no data loss nor application downtime can be tolerated. These requirements necessitate an application service that is continuously available, in other words an *IT infrastructure* that is continuously available, and an adequate business continuity plan in place to assure application service continuity with access to current and complete data under both planned and unplanned circumstances.

Stuff Happens

Whether it be fire, power failure, software error, malfeasance, or some other cause, the fact is that events will occur which lead to unplanned outages of IT services. It is a matter of when, not if. Studies[1] show that the average business revenue lost per hour of downtime across a range of industry segments is about US$1.4M. The U.S. Bureau of Labor reports that 93% of companies that suffer a significant data loss are out of business within five years. Outages will ultimately happen, and they can be very damaging (even fatal) to the business. Consequently, for those critical IT services necessary for the business to function, steps must be taken in advance to ensure availability of those services and the data they depend on no matter the cause or duration of the outage.

HPE NonStop systems – more so than many other platforms – and the mission-critical applications that run on them, must have a business continuity plan in place. NonStop systems are highly fault-tolerant, but they still represent a single point of failure. Hence, there is a need for a business continuity plan to enable operations to survive, despite the loss of a NonStop system or an entire datacenter. Such plans typically include multiple geographically distributed NonStop systems with at least some form of online data replication between them. The question is, are these plans adequate? While you may think so, that belief could be based more on hope than on reality. A recent survey[2] reports some disturbing results:

- Only 36% believe they utilize all best practices in datacenter design and redundancy to maximize availability.
- Only 38% agree there are ample resources to bring their datacenter up and running if there is an unplanned outage.
- 68% agree that availability has been sacrificed to improve efficiency or reduce costs.
- 71% believe at least some unplanned outages could have been prevented.

These findings, which illustrate that not enough attention and resources are being applied to outage prevention, are borne out by the fact that all of the respondents have experienced a complete datacenter outage, with an average of one outage per year and an average duration of 91 minutes.[3]

A study conducted by IBM[4] finds that perceptions of the business

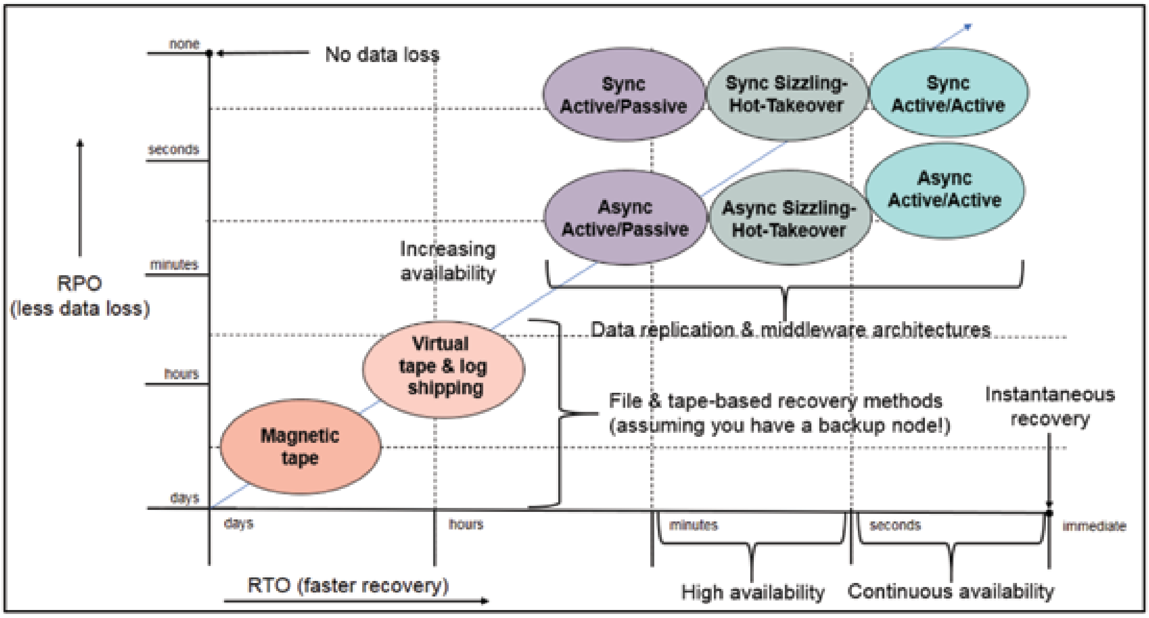


Figure 1 – The Business Continuity Technology Continuum

[1] Network Computing, The Meta Group, Contingency Planning Research
[2] Ponemon Institute, Cost of Data Center Outages
[3] Ponemon Institute, Study on Datacenter Outages
[4] IBM Global Reputational Risk and IT Study

continuity plan often differ from reality, with 82% of respondents confident or very confident about their level of outage protection, yet only 65% have 24x7 expert technical support coverage. This same study also found that only 78% perform regular failover testing, and only 67% have a fully documented disaster recovery plan.

While everyone acknowledges that outages do happen, are costly, and need to be protected against, there is substantial evidence that IT departments are not applying sufficient resources to business continuity in practice (even though they might think otherwise). The first lesson is to take a thorough and objective look at your business continuity plans, asking if they are adequate and will they work, or do you just hope they will?

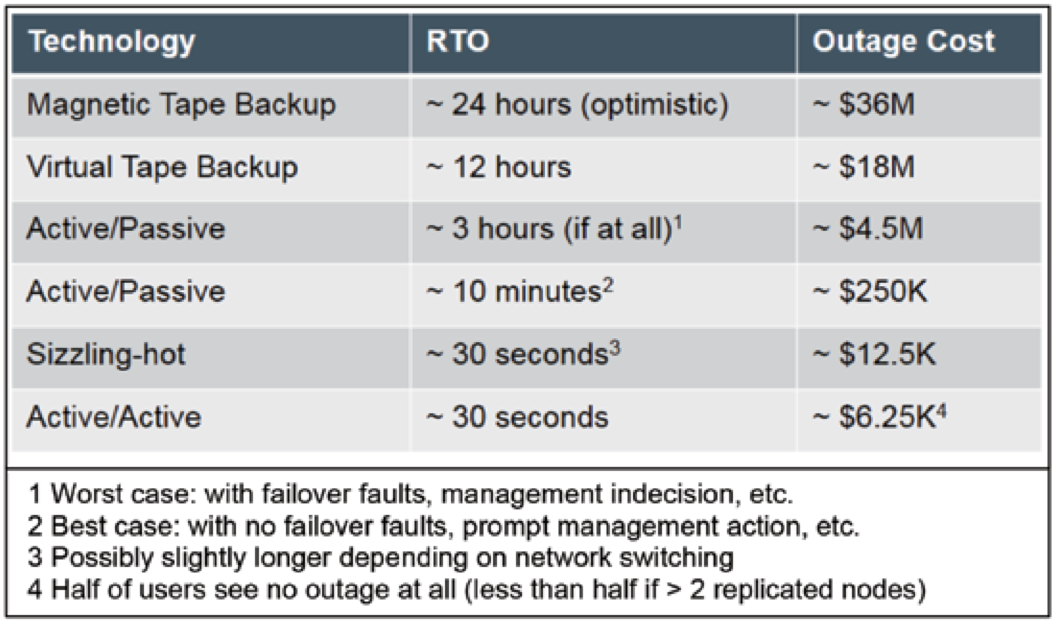
Not All Business Continuity Solutions Are Created Equal

In implementing a business continuity plan, there are a range of solution architectures and technologies available which provide differing levels of protection, from magnetic tape backup to active/active data replication (Figure 1). Key metrics for evaluating recovery solutions are: one, how long will recovery take, or the Recovery Time Objective (RTO), and two, how much data will be lost, or the Recovery Point Objective (RPO).[5]

Figure 2 shows some estimated RTO times and costs based on the business continuity technology employed. This table clearly demonstrates that tape-based solutions are insufficient for the purposes of providing adequate availability to mission-critical applications. The table also shows that active/passive data replication architectures are inadequate; this inadequacy bears more explanation.

Active/passive business continuity architectures describe multiple geographically distributed systems, in which one system is active (being used to process online business transactions), and data from that system is replicated to remote standby (passive) systems in near real-time. Replication is uni-directional (one-way) from the active to the standby system. The standby systems are not running mission-critical online applications; they may be used for ad-hoc query and reporting, or for other non-update type services. In ideal circumstances, this architecture may seem to provide adequate protection against service outages, but there are many potential issues that make it an unsatisfactory solution:

- **Difficult to test**. In order to test a failover plan the active system must typically be taken out of service and workload transferred to the standby system (i.e., application services to the end users are disrupted). Because the standby system is not running the business applications at the time of the takeover (i.e., it is not a known-working system), it is possible it will take several hours before it can be brought into service. Once upon a time there may have been an overnight or weekend maintenance outage window where this length of application outage was acceptable, but in today's always-on world, this outage duration is increasingly not the case. Even if such a window does exist, it is not always possible to complete the testing within that timeframe. When the testing period is over, there is also the risk that the active system may not be able to be brought back online in time as operations fail-back to the original system. For all these reasons, very often failover plans have not been sufficiently tested, and when they are actually needed, the failover does not go smoothly (so-called failover faults occur), and restoring service takes much longer than expected.
- **Management indecision.** Because there is an uncertainty as to whether the failover will be successful, senior management is usually required to authorize the fail-over action (as opposed to trying to restore the failed active system, if that is possible). Locating the necessary management personnel, apprising them of the situation, and having them reach a decision takes time, further prolonging the outage.
- **All users are affected.** When an outage of the active system occurs, all users are denied service until either a failover is effected or the active system is restored.
- **More data loss at failover.** Along with the unavailability of services, data loss accounts for the majority of the costs associated with unplanned downtime. In an active/passive architecture, all of the updates are being performed on one system. If that system fails, then all of the data in the replication stream that has not been successfully delivered to the standby system will be lost (known as the replication latency).[7] This amount of data loss is far more than will occur in the most advanced architectures.
- **Standby database open read-only.** Even if the business applications are actually up and running on the standby system (but not processing transactions), the database may only be opened read-only. Hence, when the failover occurs, all



Technology	RTO	Outage Cost
Magnetic Tape Backup	~ 24 hours (optimistic)	~ $36M
Virtual Tape Backup	~ 12 hours	~ $18M
Active/Passive	~ 3 hours (if at all)[1]	~ $4.5M
Active/Passive	~ 10 minutes[2]	~ $250K
Sizzling-hot	~ 30 seconds[3]	~ $12.5K
Active/Active	~ 30 seconds	~ $6.25K[4]

1 Worst case: with failover faults, management indecision, etc.
2 Best case: with no failover faults, prompt management action, etc.
3 Possibly slightly longer depending on network switching
4 Half of users see no outage at all (less than half if > 2 replicated nodes)

Figure 2 – Estimated Outage Times and Costs by Business Continuity Technology (Financial Application, Average Outage Cost $1.5M/Hour)

[5] See Chapter 6, RPO and RTO, Breaking the Availability Barrier: Survivable Systems for Enterprise Computing, AuthorHouse: 2004

of the applications must be somehow notified (or restarted) and the database reopened for read-write access. This process complicates application programming, and can be time consuming, extending the outage.

- **Standby database inconsistent.** While replication is occurring, the standby database may be inconsistent ("fuzzy"), which could limit utilization of the standby system for query processing. This inconsistency will happen, for example, if the replication engine does not preserve the source application's transaction boundaries when replaying the data into the standby database.

Due to these issues, recovery times for an active/passive system will often be on the order of several hours, and data loss may be significant, resulting in outage costs of millions of dollars (Figure 2). Worse, if a serious failover fault occurs, it is possible that the standby system may never be able to be brought into service; the mission-critical application is down and stays down, denying service to users for a prolonged period. An active/passive architecture is therefore insufficient protection for a mission-critical application.

But Some Business Continuity Solutions Are "More Equal" than Others

However, there are alternative business continuity solution architectures and technologies which may be deployed today that do not suffer from these issues; the first is known as sizzling-hot-takeover (SZT). This architecture looks much the same as an active/passive architecture (all transactions are routed to and executed by a primary system, with data replication to a standby system), but it has one big difference – the standby (passive) system is "hot." The business applications are all up and running on the standby system with the database open for read-write access, the only difference between it and the active system is that it is not processing online transactions that update the database (it can be processing read-only queries). An SZT architecture has several important benefits:

- **It greatly reduces risk.** When a primary outage does occur, failover will be to a known-working standby system with a running application, thereby obviating failover faults. It also removes management indecision issues since the standby system is known to be operational.
- **It greatly improves RTO.** The application is already running, in full read/write mode, on the standby system. It is ready to receive user requests at any time. No delay is required to bring the application up for processing.
- **It simplifies testing.** A feature of SZT is that because the applications are hot and the database open for read-write access, it can be tested, end-to-end, at any time even while the production system is in full operation. To verify the end-to-end operation of the standby system, occasionally send it a verification test update transaction. Taking an outage of the active system is not needed, so there is no concern whether the standby system will come up or the testing will cause damage to the production environment.
- **The standby database is consistent.** Replication products that support standby applications opening the database read/write typically maintain transactional database consistency, so there are no data consistency issues with using the standby system for query processing.
- **It is easier to recover the failed system.** Although all updates are being executed by one system, bi-directional replication is in place between both systems. When the failed system is restored, it is straightforward to recover it and bring the databases back into synchronization.

Overall, an SZT architecture improves RTO and failover reliability significantly, decreasing recovery times and outage costs substantially (Figure 2). But it does still suffer from the fact that all users are affected when a primary system outage occurs, and incurs more data loss than fully active/active architectures. Nevertheless, this architecture represents an excellent solution when the application cannot run in full active/active mode for some reason, and it is not more complex to implement than an active/passive architecture.

Application Availability – It Doesn't Get Any Better Than This

Next we turn to active/active architectures. In an active/active configuration there are two or more geographically separated systems, each running online business transactions and updating their local copy of the database, with data replication occurring between each system. Replication is bi-directional (two-way) between each active system.

Note that both systems are using replicated copies of the same database, and are running the same applications, with the transaction workload apportioned between them. As shown in Figure 1, active/active solutions provide the absolute fastest takeover times (RTO), with minimal data loss (RPO), because only half the data in the replication pipeline is lost in an outage of one system. Recovery times are measured in seconds to sub-seconds, and because half of the users see no impact at all, outage costs are half those of the active/passive and SZT architectures (Figure 2).

If the SZT and fully active/active business continuity technologies offer such great benefits versus active/passive architectures, why doesn't everyone use them? Good question. Compared with active/passive, there are really no additional complexities or limitations with an SZT architecture. It is just an incremental extension of the active/passive model, which needs a replication product that allows the standby database to be open for read/write access and can be configured for bi-directional replication. An SZT architecture should be considered the absolute minimum configuration for mission-critical applications.

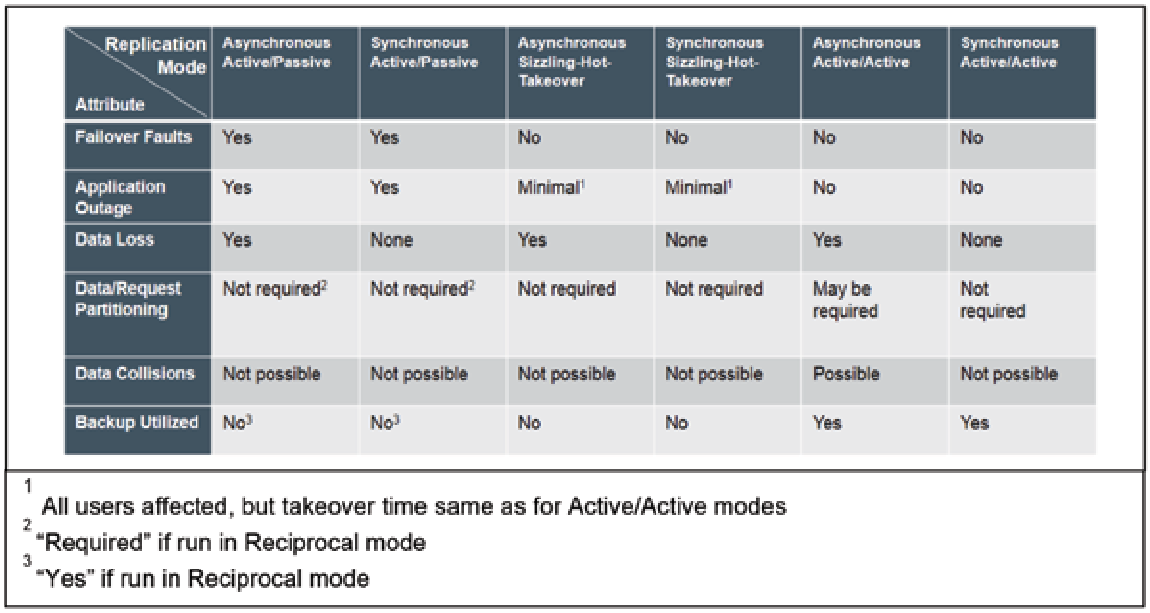
Active/active solutions on the other hand can suffer from complexities which do not arise in active/passive or SZT modes. Principal among these complexities is the possibility of data collisions. Because the same logical database is being updated on multiple nodes, and the same business applications are executing on those nodes, it is possible for a transaction to be executed simultaneously on each system which updates the same record in each copy of the database. When that change is replicated to the other system, each will overwrite its update with that from the other system, and consequently both databases will be incorrect.

There are two potential solutions to this problem. The first is to avoid the possibility of data collisions altogether, which can be done by partitioning either the data or the applications, with transactions routed to the appropriate system, such that the same record will never be updated on both systems at the same time. For example, transactions for customer data records with names A-M are executed by one system, and those for names N-Z by the other system. One downside of this approach is that not all business services are amenable to partitioning in this way. The other is that the workload may not be evenly distributed between each system, under-utilizing capacity and affecting response times.

The second solution is to route the requests to either system based on load (the so-called "route anywhere" model) and subsequently detect and reconcile any data collisions which do occur. Data replication solutions which support active/active modes generally include automated mechanisms for detecting data collisions, which are resolved using pre-defined rules (e.g., the transaction update with

[6] Network Computing, The Meta Group, Contingency Planning Research

[7] See Chapter 3, Asynchronous Replication, Breaking the Availability Barrier: Survivable Systems for Enterprise Computing, AuthorHouse: 2004



Replication Mode / Attribute	Asynchronous Active/Passive	Synchronous Active/Passive	Asynchronous Sizzling-Hot-Takeover	Synchronous Sizzling-Hot-Takeover	Asynchronous Active/Active	Synchronous Active/Active
Failover Faults	Yes	Yes	No	No	No	No
Application Outage	Yes	Yes	Minimal[1]	Minimal[1]	No	No
Data Loss	Yes	None	Yes	None	Yes	None
Data/Request Partitioning	Not required[2]	Not required[2]	Not required	Not required	May be required	Not required
Data Collisions	Not possible	Not possible	Not possible	Not possible	Possible	Not possible
Backup Utilized	No[3]	No[3]	No	No	Yes	Yes

[1] All users affected, but takeover time same as for Active/Active modes

[2] "Required" if run in Reciprocal mode

[3] "Yes" if run in Reciprocal mode

Figure 3 – Pros and Cons of Replication Technologies and Architectures

the more recent timestamp wins). This approach does not suffer from the workload distribution issue, but may not be feasible where there is no easy way to automatically resolve the collision (or where collisions cannot be tolerated by the application at all).

One Business Continuity Solution to Rule Them All – Synchronous Replication!

But what is necessary for those business services where application or data partitioning is not possible, and data collisions and/or loss of any data cannot be tolerated? Up until now this discussion has been all about asynchronous replication, where the replication engine sends data to the standby system asynchronously from the database updates made by the application. In this mode, when a failure occurs data can be lost and data collisions can occur in active/active route anywhere architectures, during the replication latency interval mentioned above. Synchronous replication resolves all of these issues. It is the business continuity solution which provides the greatest protection against the many impacts and costs of unplanned outages.

With synchronous replication, application data updates are not committed (made visible and permanent) by either system unless the updated data has been replicated to the standby system. This replication guarantees that no data is lost in the event of an outage of the system performing the update (known as zero data loss, or ZDL). Hence the costs arising from data loss simply do not occur with synchronous replication.

Additionally, in an active/active environment, it is not possible for data collisions to occur because the updated data records are locked on both systems before any changes are committed on either system. The same simultaneous update situation is instead manifested as a transaction deadlock (caused by a distributed lock collision), which is easily resolved by the data replication engine (one lock/transaction wins, the other loses and should be resubmitted by the application similar to any other error that the application receives that requires request resubmission). There is never any visible data inconsistency.

In summary therefore, synchronous replication further reduces outage costs by avoiding any data loss, and by eliminating data collisions, opening up the benefits of active/active architectures to any application. It is the pinnacle of business continuity replication solutions.

For comparison, Figure 3 gives a summary of the most significant characteristics of each of the various replication architectures discussed.

Time for Reassessment?

Even though you may already have a business continuity plan in place, it may not be adequate, well-tested, or well-supported. Worse, it may be providing you with a false sense of security, and will fail when called upon. If this plan relies on an active/passive replication architecture, there are significant issues with this approach which could hamper a fast and successful takeover in the event of an outage. The key point is that you can avoid this risk, since there are other replication solutions readily available, such as SZT and active/active architectures, which mitigate the issues with active/passive, and with better TCO. Further, for the highest levels of availability with no data collisions and zero data loss, synchronous replication may be utilized (a new release, ***HPE Shadowbase ZDL,*** is now available which supports synchronous replication and zero data loss). If your business is relying on an active/passive or asynchronous solution for business continuity, take another look at whether or not it really provides a sufficient guarantee of protection against the impacts and costs of downtime and data loss. Chances are that it doesn't, and now is the time to consider moving to one of the other higher levels of business continuity solution.

Mr. Evans earned a BSc (Honors) in Combined Sciences from DeMontfort University, England. He began his professional life as a software engineer at IBM UK Laboratories, developing the CICS application server. He then moved to Digital Equipment Corporation as a pre-sales specialist. In 1988, he emigrated to the U.S. and took a position at Amdahl in Silicon Valley as a software architect, working on transaction processing middleware. In 1992, Mr. Evans joined Tandem and was the lead architect for its open TP application server program (NonStop Tuxedo). After the Tandem mergers, he became a Distinguished Technologist with HP NonStop Enterprise Division (NED) and was involved with the continuing development of middleware application infrastructures. In 2006, he moved into a Product Manager position at NED, responsible for middleware and business continuity software. Mr. Evans joined the Shadowbase Products Group in 2012, working to develop the HPE and Gravic partnership, internal processes, marketing communications, and the Shadowbase product roadmap (in response to business and customer requirements). A particular area of focus is the newly patented Shadowbase synchronous replication technology for zero data loss (ZDL) and data collision avoidance in active/active architectures.

A Guide to High Availability and an Approach to an Active/Active Environment in the OSS World

Ki Roth >> Business Development >> Lusis Payments

There's no time for downtime, and it's crucial that your Nonstop hardware platform is at the ready 24/7. Lusis Payments has years of experience with open systems and brought our experience to Nonstop and OSS a few years back. One of the key architecture features of an SOA Nonstop environment relates to reliability and high availability, with the agility and the scalability users need. A versatile design and architecture provides the same high availability Nonstop users are accustomed to for continuous online processing plus Active/ Active and Active/Passive environments. This allows payment applications to be streamlined across multiple servers without sacrificing speed or accuracy which creates a robust, reliable platform with guaranteed delivery each and every time.

Some elements of high availability are provided by the architecture of the hardware platform, such as fault tolerance, clustering, and remote backup. Lusis has experience with these different architectures and their respective pros and cons. We have integrated several functions to minimize any constraints introduced by these disparate architectures.

Fault Tolerance

In a fault tolerant system, there are minimum requirements. A) The software must not cause an application to stop either during normal processing or when making frequent, everyday changes to the system, such as adding an ATM, a network interface, a financial institution, or even for version changes or bug fixes. B) The software must make its own provisions through its configuration or architecture for those hardware elements that are not fault tolerant, such as older communication cards.

Cluster with a single Application Database and Application Synchronization

In the case of high availability clusters, the hardware is replicated. The application resides on each server and is either permanently active or automatically activated if the primary server fails. The database is seen as one entity by the application. Stopping software on a server is an event that seriously disrupts its operation: reconnection of ATMs, reconnection of network resources, loss of in-flight transactions. As a consequence, point A) above must be assured as a minimum. Point B) can be assured by a mirrored architecture.

The software must also ensure:

- The transparency of the database, which could be located on multiple nodes
- Central management of technical operations

For application synchronization, each occurrence of the application has its own database, and all instances of the database are synchronized by an application notification mechanism. For the same reasons the software must assure point A) above. The software must also ensure sending of notifications, a guaranteed delivery mechanism, forced posting of notifications and technical management of this message flow.

The SOA Contribution

Alongside various hardware architectures, a properly architected SOA environment provides a number of robust and proven technical approaches to provide software with 'no single point of failure':

- The application can be configured to be highly redundant:
  - o Service-level redundancy uses multiple instances of a given Service in an application process.
  - o Process-level redundancy uses multiple copies of a given Process, each with one or more instances of a given Service.
- The SOA's modular design allows application processing to be decoupled into functional modules, giving the following advantages:

Each module is simpler and therefore more robust.

o The modules themselves may be replicated either within or across processors to accommodate the throughput required.

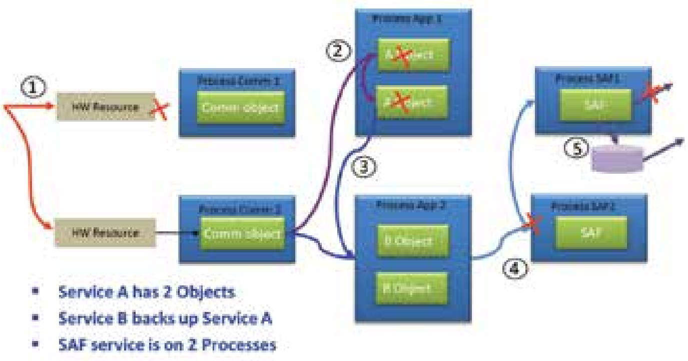
- A High Availability solution supports redundancy at the site level:

- A copy of each transaction can be sent, in the form of a notification message with guaranteed delivery, to the remote site in either an Active/Active or an Active/Passive configuration.

- The technical management of the environment incorporates centralized functions for controlling the entire technical environment:
  - Automatic monitoring of modules
  - Restart commands
  - Dynamic warm-boot commands
  - Stop and start commands by process, by service or by a group of services, to ensure changes can be made without stopping the entire application.

Intra-Application High Availability

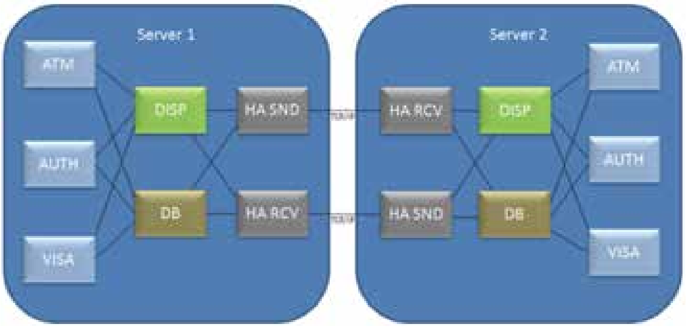
The diagram below presents the inherent software high availability provided in an SOA architecture, as described above, by configuring multiple processes and services and employing an alternative routing capability to ensure maximum opportunity of guaranteeing delivery of a message.



1. System resource becomes unavailable and therefore uses a backup route
2. Routing to the element responsible for a pool of software resources
3. Routing to the backup pool B after an incident in Pool A
4. Sending a notification advice with guaranteed delivery Store and Forward (SAF)
5. SAF the advice then retries if there is a delivery failure

Inter-Application Ultra High Availability

Inter-Application Ultra High Availability can be provided using data replication tools. It can also be accomplished thru the application's own specialized High Availability components integrated within the payments platform to provide an alternative Active-Active solution for two servers, as shown in the diagram below.

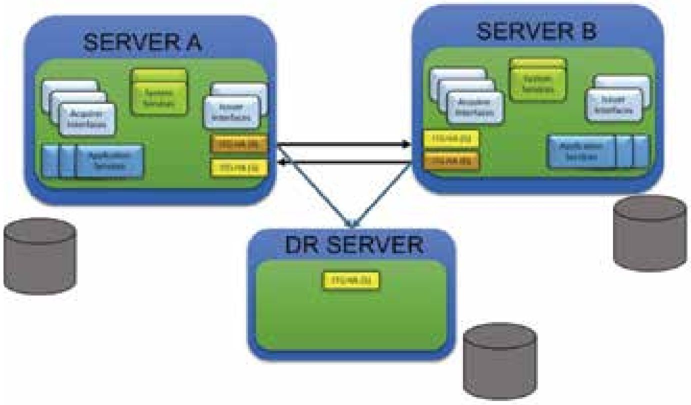


HA SND sends advices to the remote server. HA RCV receives the advices from the remote server. For an Active/Active environment, there is one copy of HA RCV and HA SND on each of the servers. These components are responsible for keeping updated a set of data (tables) on both payment servers. To do this, both payment servers contain two secured communication channels (including SAF capabilities) responsible for exchanging activity advices and status advices.

This additional capability provides the opportunity to streamline current payments platforms as well as reducing the overall TCO for running the authorization system. A SOA based payment platform can be unique by providing both an authorization system and a high availability capability integrated within the same architecture. This will assist both in reducing the ongoing costs and simplifying the management of upgrades as a result of data evolutions.

Inter-Data Center High Availability

In addition to providing the capability for two systems to replicate data between each other in one data center, this mechanism can also be used to replicate data between different systems located in different data centers, as described in the diagram below.



The above diagram shows two local systems replicating data between each other and replicating data to a remote cold/warm standby DR server in another datacenter. The two production systems described could be in different datacenters, providing ultimate flexibility in deploying the system to customers' specific requirements

The previous sections have described the flexibility and configurability that can be designed into an SOA open system application irrespective of the capabilities or configuration of the hardware platform on which it is deployed: on a single node, in a single datacenter or in multiple datacenters.

Implementation of the High Availability components can also provide further flexibility and automation. For example, one option would be to deploy a 3rd cold standby datacenter if required.

Therefore, given the capabilities described above, a properly designed architecture/modules, plus the deployment of Nonstop high availability hardware will provide both the 99.999% availability expected of the system and the required capacity for increasing transaction volumes.

Ultra-High Availability

Ultra-High availability is provided by:

- The capacity to do multi-instances services
- The capacity to implement application services on several systems with the same level of key information
- The capacity to easily provide Active/Active systems.
- The capacity to change configurations without stopping the application
  - Adding processes
  - Update services parameters.

A service runs as a thread inside an application process. For each process, the definition of each service contains a parameter defining the number of instances of the service inside the process. Each instance manages its own queue of events (among which are application requests, responses and notifications). To benefit from multi-cores and multi-CPU architectures it is necessary to instantiate more than 1 thread to run per service. Distribution of the message load is the responsibility of a dispatcher process, which maintains counters for all registered service instances.

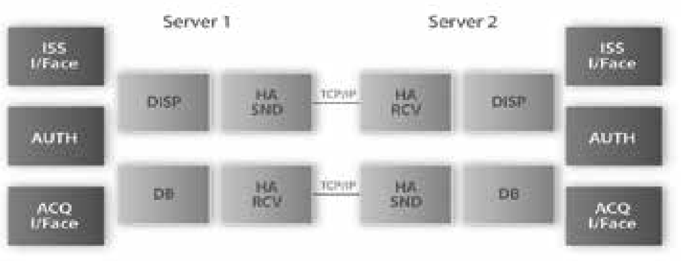
High availability components oversee maintaining an up to date set of data on both payment servers to allow each server to process data flows without any restrictions:

- Authorization data
- Terminal contexts
- Dynamic network and terminal keys

This can be realized without any third-party replication tool. As it is using only messaging features, servers can use different operating systems or even different data models (and databases).

Each server contains at least 2 communication channels in charge of exchanging activity advices (from ATM management, network protocols management and authorization management) and status advices (from ATM management) from one system to the other:

- HASND (High Availability SeNDer process): In charge of sending local system activity advices to remote system.
- HARCV (High Availability ReCeiVer process): In charge of processing remote system activity advices to maintain local database up to date



Both systems are completely symmetrical

The application uses the equivalent of “0120”, “0320” and “0820” messages to notify data from one system to another (and vice versa).

Key data elements are:

- Authorization management
  - o Hot cards
  - o Authorisation activity
  - o False PIN
  - o True PIN after False
- ATM management
  - o Status advices
  - o Terminal contexts (counters….)
- Network management
  - o Encrypted keys

Time of updating the distant system needs to be within 50 milliseconds. Configurations are synchronized via scripts.

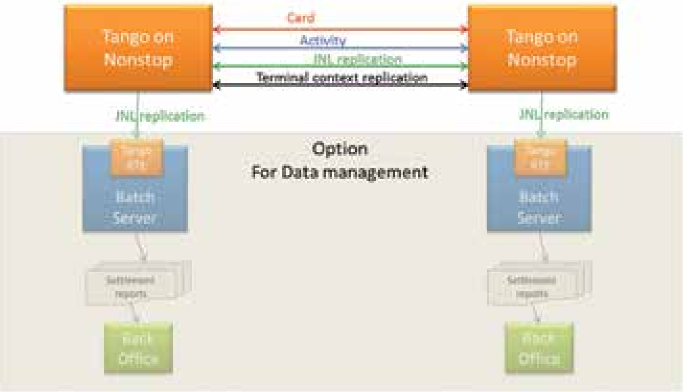
A Real-Life Example

To demonstrate how the above theory is implemented let’s take a look at the TANGO architecture from Lusis Payments, although there may be similar solutions available on the market.

For Active/Active

High Availability mechanisms and Interoperability allow simple Active/Active systems integration. RTE package (Remote TANGO Environment) contains the Inter-TANGO process sets. Authorization activity, terminal contexts (ATMs and POS devices), merchant, and customer data are synchronized through real-time TANGO messages. For instance, any given terminal can connect to any of the Application servers to provide functionalities to customers with 24/7 availability.

The following schema shows a TANGO fully synchronized DUAL server including an interaction with a remote TANGO batch server that provides safe access to application real-time history at no risk to the real-time transaction flows. This remote server can also host batch extraction activity.

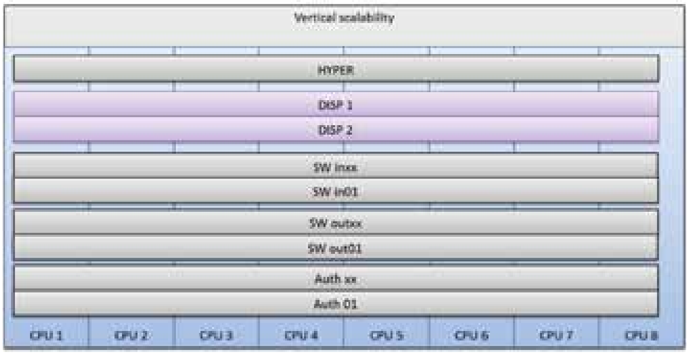


Active redundancy mode

Service is instantiated with a unique name. Several processes host this unique service in parallel. They run on different CPUs and process transactions in load balancing mode, as routing is based on service name. The Hypervisor launches several (minimum of 2) instances of a process at start-up - all are active. The Dispatcher sends transactions over running processes via round-robin with a priority on less loaded processes in the queue. Sizing ensures that if one CPU fails, all the remaining processes can handle the transaction flow.

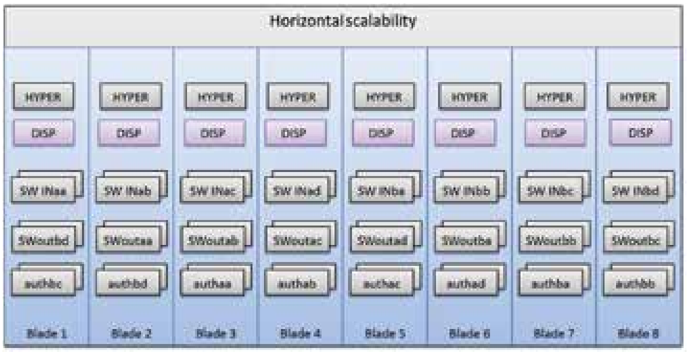
CPU backup mode

The Service is initiated with a unique name. A Unique process is first launched at start time on the first CPU and processes transaction as long as it is present. If a CPU fails, the hypervisor launches the back-up process – configured to run on another CPU. This mode is used when a constraint (external resource, sequence, …) makes use of ‘active redundancy’ mode impossible. Initial process is launched on one CPU and processes all transactions.



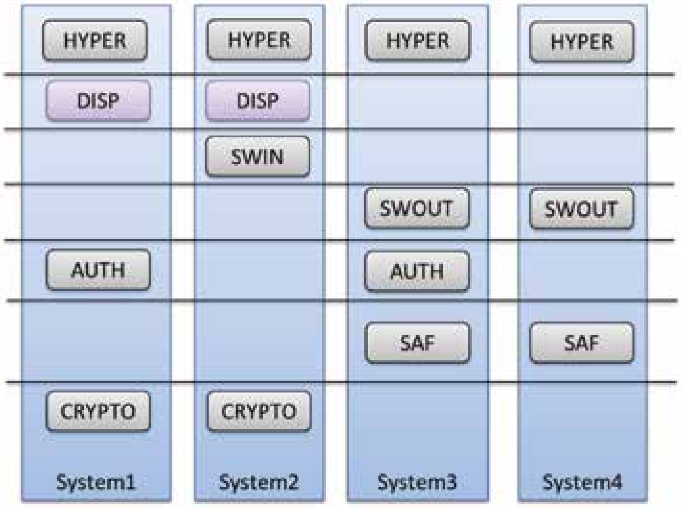
Vertical scalability

Adding CPU and memory in an existing system is a classic way of improving Server capacity without touching the application. All modern Operating Systems can balance process execution on numerous CPUs or CPU cores. Nonetheless, certain OS’s may have a very efficient balancing algorithm at the process level but poor balancing at the process threads level.



Horizontal Scalability

New Hardware is now promoting distributed CPU power inside Blade server architectures and high performance interconnection between servers. A solution with high modularity and process organization allows full benefits for such architectures and can seamlessly replicate services on different hardware, either using a centralized Dispatcher registration for services spread over different hardware, or using distributed sub-systems dialog using inter- product functions.

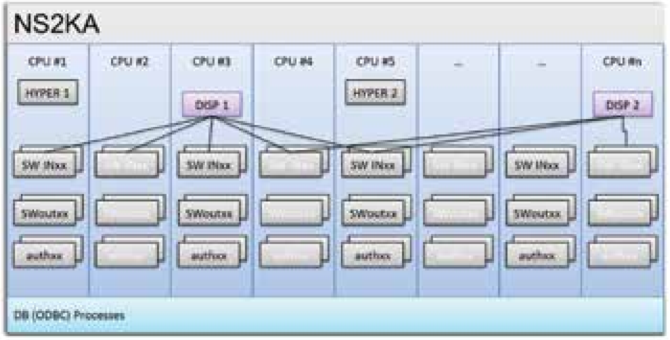


Functional Scalability

All functions being executed in isolated services, the repartition of services on the Hardware and the number of instances that will run the service are highly configurable and can grow by simple configuration changes.

Scalability Example on NonStop

The following schema illustrates the combination of all types of scalability that can be achieved on an HP NonStop with processes spread over logical CPUs executing different sets of services.

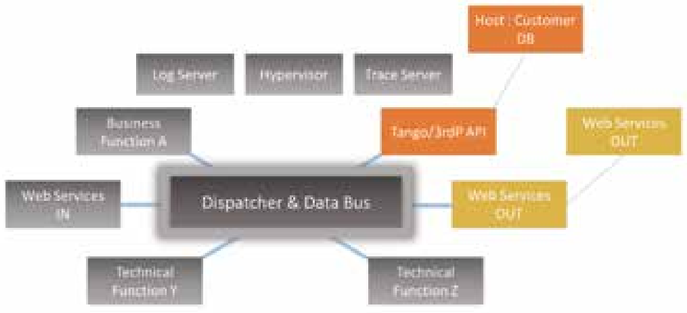


Cooperating with Third Party Applications

Interoperability with third party applications can be managed through integration of APIs or message interfaces when available. In the latter case, this reduces the introduction of a new interface module:

- Providing Perl and Python libraries and C, C++, XML and Java APIs
- Interacting with Java applications by building hybrid Java objects

For example, the high availability solution would interface with the customer database in the Bank's back-end using Web-Service to execute VISA Address Verification Service; or a bank API is used to connect to an external Fraud detection application. The following schema shows how external third party applications can integrate into the services architecture of a high availability solution.



Conclusion

There are many different methods of High Availability and whether to go with an Active/Active environment is a difficult decision to make. At the end of the day each organization must weigh the different factors, some of which are risk assessment, value, resources, time and intrinsic visibility to determine what is best for their situation and ultimately their customer base.

Ki Roth has been with Lusis Payments for over 3 years in a Business Development role. One of his main objectives has been to build awareness for the TANGO solution in the financial sector. Ki has worked in the NonStop space since 1997 when he began working for a large payments software company based in Omaha NE. Over the years, each of his employers have brought solutions that run on the HP NonStop platform. The value that NonStop brings to the market, make it easy for Ki to promote applications that build on the NonStop fundamentals of reliability, stability and high availability. Today TANGO runs on the OSS layer of the platform and uses the SQL/MX database when performing transactional processing.

lusis
Payments

The Challenge of Protecting Payment Data Streams End-to-End

Trish Schaefer Reilly >> HPE Security – Data Security

In today's environment of heightened regulatory requirements and increasing risk of cardholder data breach, it is critical for merchants, payment processors, and acquirers to protect payment data anywhere it moves, anywhere it resides, and however it is used. In payment acceptance systems, including EMV (Europay, Mastercard and Visa) terminals, payment data is commonly left unprotected during the authorization and settlement processes. Payment data is also left unprotected during routine and necessary back-office business processes such as fraud screening, chargeback processing, and recurring payment processing. Traditional methods for protecting payment data are often inflexible, expensive, and difficult to implement.

HPE SecureData Payments securing sensitive data end-to-end

HPE SecureData Payments protects payment data at all points, from swipe/dip through to the payment processor, end-to-end. It eliminates the traditional complexities associated with payment device key injection, key management, payment application changes, and enables a true end-to-end architecture that can be rapidly deployed even in the most complex environments.

PCI Compliance Alignment

HPE SecureData Payments can reduce the cost of complying with PCI DSS—a direct result of reducing the number of changes necessary to implement payment data protection while eliminating payment data from databases and applications. By incorporating HPE Secure Stateless Tokenization with HPE SecureData Payments, service providers, merchants, and enterprises are able to secure back-end data, removing data from PCI audit scope while complying with the latest PCI DSS requirements for cardholder data protection. HPE Secure Stateless Tokenization maintains token schemes across regions with no communication between them, eliminating the need for a central key management database as well as database replication. By tokenizing card numbers immediately at the source, clear data is eliminated from the transaction process.

As providers move to point-to-point encryption (P2PE) validations, HPE SecureData Payments enables service providers to expand their reach by offering a complete P2PE v2 validated solution. With HPE SecureData Payments cardholder data is protected from the earliest point of entry in such a way that decryption keys are not available at POS devices or any other intermediate systems, significantly reducing potential attack areas. HPE SecureData Payments communicates with validated, authorized payment terminals sending secure payment transactions for processing to the back-end system. The back-end host incorporates an integrity check on the cryptographic functions, creating host logs based on crypto changes. This enables management and control of the complete system and payment transactions.

Innovation in cryptography provides end-to-end encryption without massive changes

HPE SecureData Payments is a complete payment transaction protection framework, built on two breakthrough technologies encompassing encryption and key management: HPE Format-Preserving Encryption (FPE) and HPE Identity-Based Encryption (IBE). These two technologies combine to provide a unique architecture that addresses the complexity of retail environments with high transaction volume.

HPE Format-Preserving Encryption

With HPE Format-Preserving Encryption (FPE), credit card numbers and other types of structured information are protected

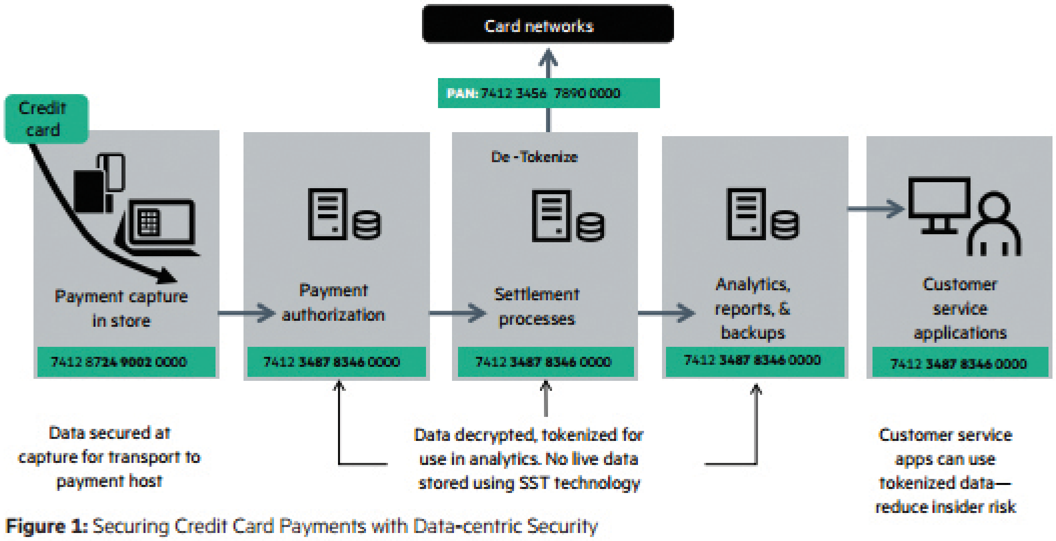

Card networks
PAN: 7412 3456 7890 0000
Credit card
De -Tokenize
Payment capture in store
Payment authorization
Settlement processes
Analytics, reports, & backups
Customer service applications
7412 8724 9002 0000
7412 3487 8346 0000
7412 3487 8346 0000
7412 3487 8346 0000
7412 3487 8346 0000
Data secured at capture for transport to payment host
Data decrypted, tokenized for use in analytics. No live data stored using SST technology
Customer service apps can use tokenized data—reduce insider risk

Figure 1: Securing Credit Card Payments with Data-centric Security

By protecting the data itself, HPE SecureData Payments eliminates security gaps that exist between networks, databases, and applications when protected with point security solutions are used.

without the need to change the data format or structure. In addition, data properties are maintained, such as a checksum, and portions of the data can remain in the clear. This aids in preserving existing processes such as BIN routing or use of the last four digits of the card in customer service scenarios.

HPE Identity-Based Encryption

HPE Identity-Based Encryption (IBE) is a breakthrough in key management that eliminates the complexity of traditional Public Key Infrastructure (PKI) systems and symmetric key systems. In other words, no digital certificates or keys are required to be injected or synchronized. HPE IBE also enables end-to-end encryption from swipe-to-processor and swipe-to-trusted-merchant applications.

With point-of-sale (POS) solutions that use legacy symmetric encryption, encryption keys must be reset annually for each POS device through a process called key injection. This procedure is expensive and cumbersome, as merchants must take POS devices offline while new keys are injected. With HPE SecureData Payments, because encryption keys are securely generated on demand and not stored, POS devices are not subject to key injection and key rotation. This function happens systematically, eliminating labor-intensive key management processes and costs.

HPE SecureData Payments compatibility

- Robust host side capabilities and broad platform support: HPE SecureData Payments Host SDK can be deployed on a wide variety of platforms including HPE NonStop, Windows®, Linux®, UNIX®, z/OS, and Stratus. HPE SecureData Payments is the only data protection solution available that natively runs on Nonstop (OSS and Guardium) and Stratus VOS, enabling maximum protection and efficiency.
- Unified, complete end-to-end data security: HPE SecureData Payments enables merchants and service providers to protect their entire payment stream and reduce PCI audit scope from the end-user to back-end systems by offering a variety data protection needs for m-commerce (in-app) payment data (mobile), e-commerce/in-browser payment data, device-based encryption of payments data (P2PE), and protect PCI data stored for post-authorization needs.
- Stateless key management: HPE SecureData Payments does not require digital certificates or keys to be injected or synchronized with the host. Because encryption keys are securely generated on demand, POS devices sufficiently protect card data without the need for key injection or key rotation, which can be labor-intensive and expensive to administer.
- Integrated with an industry-leading pioneer: HPE SecureData Payments is the only off-the-shelf integrated solution with a PCI-HSM and FIPS validated secure root of trust (HPE Atalla HSM) to protect payment data, payment authorization and fraud prevention. The integrated solution extends end-to-end data protection through the combined, integrated solutions of HPE SecureData Payments and HPE Atalla Hardware Security Module (HSM). By joining data-centric data protection with a tamper-reactive hardware security module, companies are able to neutralize data breaches by protecting data, rendering it useless to attackers.
- Multiple integration options: Processors and merchants can choose to integrate using SDKs, Web services, and/or command line tools for quick and simple deployment. End-to-end encryption can easily be combined with HPE Secure Stateless Tokenization (SST) to provide merchants with a complete solution for PCI audit scope by protecting data stored for post-authorization needs.
- Integrated POS systems: HPE SecureData Payments solution is integrated into a variety of payment terminal devices and platforms, giving organizations the flexibility to select one or more payment vendor(s) for the required business needs. For a complete list of payment partners, visit voltage.com/partners.
- Scalability and performance: Flexible, scalable architecture that handles quickly scales eliminating the need for merchants to self-manage payment transactions. The platform delivers complete control over end-to-end payment security stream for the omni-channel business requirements.

How secure is secure?

To ensure compliance with PCI DSS best practices and requirements, Coalfire, a well-known cyber risk management and compliance organization, conducted independent technical assessments of HPE SecureData Payments to verify HPE SecureData Payments meets the current PCI DSS standards.

End-to-End Data Security for the Payments-driven Market

HPE SecureData Payments is part of the HPE SecureData portfolio for protecting sensitive data in-motion, in-transit and at-rest. HPE SecureData Payments is a complete payment transaction protection framework built on a flexible and highly scalable architecture, including a common back-end infrastructure that protects system and device payment transactions for ecommerce (mcommerce), mobile payments, card on file (CNP) and the associated PII payment stream data.

Protect the full payment stream—more than just the credit card number—and the associated PII payment stream information, including payment data from POS devices, terminals, browsers and mobile devices. By incorporating data-centric endpoint protection with HPE SecureData Web and HPE SecureData Mobile, enterprises and service providers are able to protect the full payment lifecycle.

HPE SecureData Payments provides unique benefits:

- Diminishes the liability exposure of a breach while meeting card (PCI) requirements
- Complies with the Payment Card Industry Data Security
- Standard (PCI DSS and PCI P2PE) and data privacy laws
- Easily expands to accommodate new payment methods transparent to the user
- Enables seamless omni-channel business, with complete control over end-to-end payment security independent of the payment or service provider solution
- Ensures customer cardholder data is never in the clear at any point in the transaction flow (from the dip, swipe, keyed, or NFC) through to the protected backend
- Flexible, scalable architecture with common back-end infrastructure that protects payment transactions and associated PII/PHI payment stream data

Trish Schaefer Reilly has over 18 years of product marketing and management experience. She has a broad range of expertise in marketing, defining and managing varied technology platforms including: security, data storage, encryption, key management, big data, analytics, virtualization and cloud services for the enterprise and channel for multiple industry verticals. Trish has played a prominent role in building demand and resources within database, security and licensing organizations focusing on the protection of data. Trish brings a unique, broad perspective both to the challenges facing the industry today and the difficulties that experience making critical technology decisions.

Future Dates Spell Problems for IT

Dr. Bill Highleyman >> **Managing Editor** >> Availability Digest

Two major date rollover events are on the horizon for IT systems. They are known as Y2038 and Y2042. Either one of these events could cause applications that use dates beyond the rollover events to crash. And there are many such applications. For instance, life insurance policies and home mortgages can extend decades into the future, well past the rollover dates.

The Y2038 problem is a direct result of the common use of 32-bit date/time fields. The Y2042 problem results from the representation of time in IBM z/OS mainframes.

Though these dates are more than two decades in the future, beware! Time passes quickly, and the longer one waits to correct an application, the more difficult it may be.

Shades of Y2K

It wasn't very long ago that we faced a similar problem. For decades, applications had used a two-digit date field. The year 1983 was simply stored as '83.' This was done because back then memory was very expensive, and any savings in memory were actively sought after.

The two-digit data field worked fine until we approached the year 2000. Were we going to store the year 2003 as '03'? Wouldn't that be treated as 1903?

Massive amounts of effort went into reprogramming applications to move from a two-digit date field to a four-digit date field. I was personally heavily involved in this effort. My company, The Sombers Group, joined a consortium of four other companies to help organizations plow through their applications so that they could become Y2K compliant. The consortium provided a specific project methodology, a complete set of software conversion tools, and experienced resources to fix Year 2000 related problems.

The consortium was called Four2000 and its tools included:

- *Application Repair Methodology for the Year 2000 from Leardata.* This tool performed a business and technical impact assessment and prepared a detailed project plan.
- *Q2000* from Questicon helped determine the project's scope and identified every line of code to be fixed.
- *OPTA2000* from TANDsoft was used to identify and test application procedure calls to system time and date functions without having to modify the operating system time and date.
- *VersaTest* from SoftSell simulated the production environment for integration testing.
- Finally, The Sombers Group provided ongoing application development to enhance applications while maintaining Y2K compliance.

Probably the most expensive task of a Y2K fix was testing it. General industry estimates put the test of costing in the range of 45% to 65% of the total Y2K project cost.[2] Testing began with the creation of a Master Test Plan. This test plan included several levels of testing – unit testing, system testing, user testing, and performance testing. The testing effort was extensive enough that it required full support from corporate management.

Y2038

The Y2038 Problem

The Y2038 problem is an issue for computing and storage systems in which time values are calculated or stored as 32-bit signed integers. Most 32-bit Unix systems store and manipulate time in this format. Typically, in these systems, time is interpreted as the number of seconds since January 1, 1970.

Using this technique, times cannot be encoded past 03:14:07 UTC on January 19, 2038. Times beyond this time will wrap around and be stored as a negative number. Systems will interpret the wraparound time as December 13, 1901, rather than January 19, 2038.

My Own Experience with Y2038

I myself was a victim of Y2038 years ago. One day as I logged onto my e-mail, I received an insidious error message that said "MAPI Spooler shut down unexpectedly." Then Microsoft Exchange crashed. No matter what I did, I was dead in the water.

Calls to the Microsoft help desk resulted in the advice to reinstall Exchange. That didn't work, so I bought Outlook '97. Same result. I next called Outlook '97 support. The very knowledgeable technician with whom I spoke said that if the system date were set to later than the Year 2038, the MAPI Spooler would crash. I then realized that my clock battery had died a couple of weeks ago, and I had forgotten to reset my computer's system date. Sure enough, it was set to the year 2099. Resetting it instantly cured the problem.

The 32-Bit Time Field Problem

The use of 32-bit date/time fields is extensive. There is a major use of embedded systems with such fields. Examples include cell phones and internet routers. These systems rely on storing accurate times and dates. They are increasingly based on Unix-like operating systems that use 32-bit date/time fields. In fact, some Android devices crash and will not restart if their time is changed past 2038.

Programs that run in 32-bit environments but that work with future dates will have to be fixed earlier. For example, a program that works with dates twenty years in the future will have to be fixed no later that 2018.

[1] Y2038/Y2042 Are Business Risks – You Need to Know Today, Softdate; undated.

[2] Year 2038 Problem, Wikipedia.

64-bit systems are generally immune from this problem unless they have 32-bit systems embedded in them. Linux uses a 64-bit time field for 64-bit architectures only. 64-bit time fields introduce a wrap-around date that is twenty times greater than the estimated age of the universe!

In 2011, an amusing example of the Y2038 problem occurred when the Congressional Budget Office's economic forecasting software was found to be incapable of running economic analyses past the year 2037. Congressman Paul Ryan reported to the media:

> "I asked CBO to run the model going out and they told me that their computer simulation crashed in 2037 because CBO can't conceive of any way in which the economy can continue past the year 2037."

COBOL systems of the 1970s to 1990s vintage, of which many are still in operation, will fail on dates after 2038. The MySQL database's built-in timestamp will return 0 after 03:14:07 UTC on January 19, 2038.

There is no universal solution for the Y2038 problem. Any change to the date/time data type will result in code compatibility problems in any application.

But won't all new systems sold in the future have a 64-bit date-time field? Indeed, virtually all new servers, desktop, and laptop computers being sold today have 64-bit hardware and operating systems, as do some high-end cell phones and tablets. However, the hardware and operating systems are only part of the Y2038 issue. One must also consider the application software, peripheral hardware, device drivers, file systems, databases, communication protocols, web servers, and embedded systems. Also, 64-bit systems may be running embedded 32-bit software.

Furthermore, 32-bit CPUs will continue to proliferate due to factors such as power usage and the higher cost and complexity of 64-bit CPUs.

Testing the Y2038 Fix

Finally, testing the Y2038 fixes made to applications probably will be as extensive as the Y2K testing we described earlier. A Master Test Plan must be developed which will specify the unit and system testing of each application module affected by Y2038. This must be coupled with a deployment plan that sets forth how the newly modified applications will be deployed into service.

As with Y2K, the development of the testing and deployment plans and their execution may well be the major part of the Y2038 project. It is imperative that the Y2038 modifications be thoroughly tested before they are deployed to ensure that all applications will behave properly.

There is one shortcut that can be considered, and that is to exempt non-mission-critical applications from exhaustive testing. Rather, the modified versions can simply be put into production; and any problems that arise can be fixed through the normal bug-fixing procedures.

Y2042

Y2042 is due to a limitation in the representation of time on IBM mainframes running z/OS. In the z/OS operating system, time is represented as a 64-bit integer showing the number of microseconds since January 1, 1900. This integer rolls over on September 17, 2042.

IBM has defined a new 128-bit time format that is available on its new hardware. However, many applications and computer languages continue to rely on the 64-bit format.

Time Testing Utilities

There are utilities available for testing your applications for time-rollover problems. TANDsoft (http://www.tandsoft.com/files/products/OPTA2000.html) provides OPTA2000 for clock and time-zone simulation and testing for HPE NonStop systems. Softdate (http://www.ddvtechnologies.com) provides time simulation for IBM z/OS, Linux, Unix, and Windows systems.

Summary

The Y2038 and Y2042 date/time rollovers are not that far away. Most of us will still be working two decades from now when these will impact our systems and applications. Now is the time to begin to analyze the impact these rollovers will have on us and to take action to mitigate any serious consequences.

[3] Testing the Year 2000 Fix, Tandem Connection; July 1997.

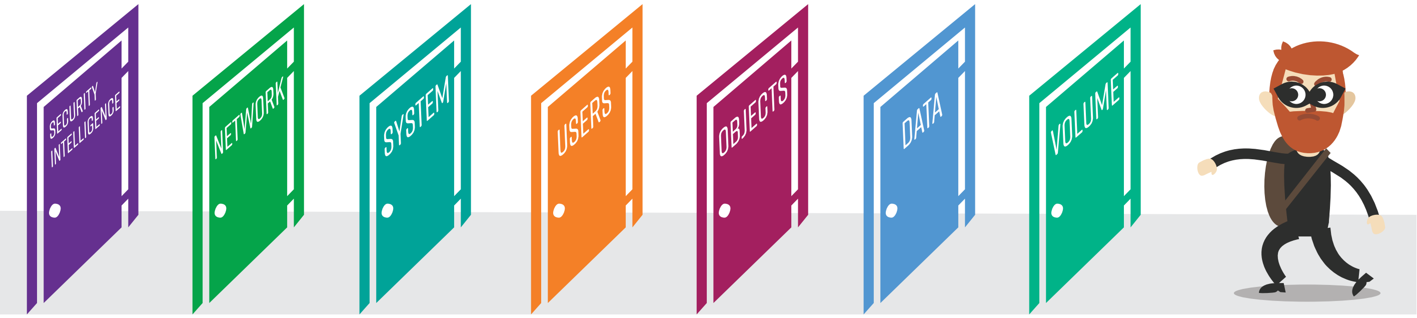
[4] Y2038.com

Dr. Bill Highleyman brings years of experience to the design and implementation of mission-critical computer systems. As Chairman of Sombers Associates, he has been responsible for implementing dozens of real-time, mission-critical systems - Amtrak, Dow Jones, Federal Express, and others. He also serves as the Managing Editor of The Availability Digest (availabilitydigest.com). Dr. Highleyman is the holder of numerous U.S. patents and has published extensively on a variety of technical topics. He also ghostwrites for others and teaches a variety of onsite and online seminars. Contact him at billh@sombers.com.

FUTURE LEADERS OF IT
Interested in investing in next year's future leaders?
Make an investment that is certain to show a return for years to come!
DONATE TODAY!

GET SMART!

CONTROL KAOS WITH **LAYERED SECURITY**



Steve Tcherchian >> **Chief Information Security Officer** >> XYPRO Technology Corporation

I recently came across reruns of a TV show from the 60's called "Get Smart". In the opening sequence of the show, the lead character, Maxwell Smart, played by Don Adams, must pass through nearly a dozen doors, or layers of security in order to access his job at "Control" where the secrets are stored.

I spend a lot of time discussing security strategy and requirements with colleagues, customers and the HPE NonStop user community in general. Over the last 10 years that I've been working in the NonStop space, it's become clear that the traditional approach to security – applying a single layer of security or a solution that meets a certain requirement, has some serious shortcomings. History has shown time and time again that although a single focused solution can be useful in stopping a particular attack, in the long run, more patient and advanced adversaries will find this approach to security merely an inconvenience. I'm amazed at how often I hear "That's good enough for us" speaking about a particular approach.

"We use multi-factor authentication."
"We use encryption."
"We scan our systems."
"Our servers aren't connected to the internet."
"Our auditors have not mentioned that."

No one is suffering from the illusion that there's a silver bullet that will effortlessly make an organization 100% secure. More importantly, the perimeter itself is dissolving. Punting security to an external group and relying on firewalls, IDS/IPS and authentication controls by themselves to protect a system is irresponsible and actually leaves unexpected holes in the system. Identifying your assets and building your security strategy around those assets is the only true way to mitigate risk. Identification is key. If you don't know what you are protecting and why you are protecting it, it becomes difficult to deploy the right security measures.

Layered security takes the military concept of "Defense in Depth" and applies it to cyber security. The idea is simple; a single solution may stop a certain type of attack, but if an attack does get through, the layers behind them are set up to continuously slow down and stop the attacker. For example, a castle may have a moat, a protected door, a perimeter wall, guards and guard towers, inner walls and a highly secure, highly protected safe that contains the crown jewels. The same strategy should be applied to how critical digital assets are secured.

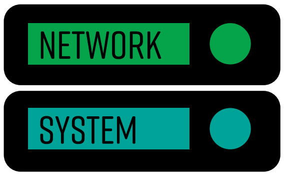
Hardening the NonStop server is no different. Structure your security solutions to best manage your risk. The goal is if an attack gets past a single layer or solution, the subsequent layers are purposefully set-up to slow down and narrow the field of attack.

XYPRO's approach to HPE NonStop security is this: we took the same layered, defense in depth strategy and deconstructed all those layers to identify where the system or data is most at risk on the NonStop server. We apply the strategy based on the risk involved, the type of data we're aiming to protect, and how different layers can interact with each other for risk mitigation. We ended up with the layers illustrated below. In this introductory article, we'll identify and explain all the layers. In future articles we'll discuss the importance of each layer in depth.

The Network Layer

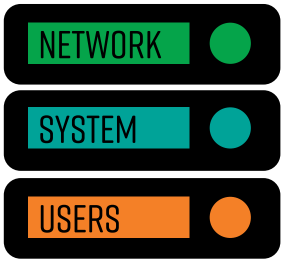
The Network layer is the outermost layer of the system and most likely to be targeted first. This layer is essentially your system's perimeter, where applications are exposed and data is in motion, communicating with other systems and endpoints. Unlike subsequent layers, the system does not necessarily need to be compromised for an attack to be successful at this layer. Therefore, it's critical to ensure all data flowing in and out of the system at this layer is properly protected using secure protocols such as TLS, SSH, SFTP etc… and ensuring no suspicious ports or services are available for external fingerprinting or other reconnaissance activity. Implementing security at this layer will cause a potential attacker to look elsewhere.

The System Layer



The system layer controls who is allowed to have access into your system. This is where logon controls are set up, credentials are validated and additional integrations, such as Multi-factor Authentication and other authentication providers are implemented. An often overlooked but eq ually important understanding is access isn't only for users or logging into the system. Processes, objects and subsystems also need to properly authenticate themselves to access system resources and data. Think of this layer as the front door to your house. A thief would typically need valid credentials, or keys, to proceed any further. Although hardening your defenses here is a must, assume a motivated and patient adversary will bide their time and eventually get the keys they are looking for. And not to mention those pesky insider threats who may already have validated access to the system. How do you slow them down once they penetrate this layer?

The User Layer

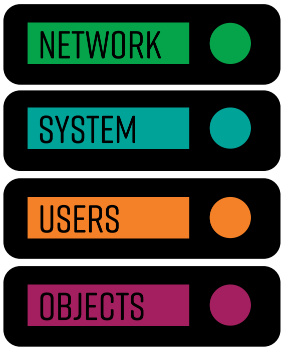


The user layer approach takes the position that users shouldn't have unchecked permissions on a system, even after they've been granted access. Assume an attacker was road-blocked at the Network Layer, but was able to compromise a user's credentials at the system layer and logged on to the system. Deploying a proper layered strategy at these next two layers will ensure access to the "Data in Use" is properly controlled and managed. Once granted access to a system, users shouldn't have free reign to browse and run applications and utilities as they please (although I have seen this happen more than I'm comfortable admitting). Controlling what a user can access in terms of utilities and system locations based on their role, job responsibilities and other factors is a critical approach to executing a proper security strategy. Role Based Access Control (RBAC) is a familiar concept to most security administrators. RBAC is deployed at this layer.

Let's look at an example. Your organization has a database administrator who, for their job function, should only have access to SQLCI and no other applications or utilities. Using RBAC, you restrict their access to the utility needed to execute their job duties and deny access to everything else. That way, if their credentials are compromised at the system layer, their ability to access utilities and programs will be tightly controlled. It is very important to note as part of this process, that their access be monitored via proper audits. We'll discuss this later.

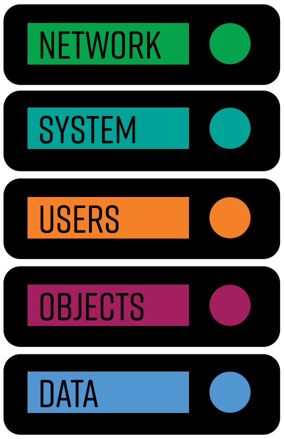
XYPRO's XYGATE Access Control takes RBAC a step further, by restricting control to the subcommand level within utilities and programs. So, unless a user is explicitly granted access to run a utility or program, or even a subcommand within a utility, they will be denied. Further controlling what a malicious user may or may not do if they get down to this layer

The Object Layer



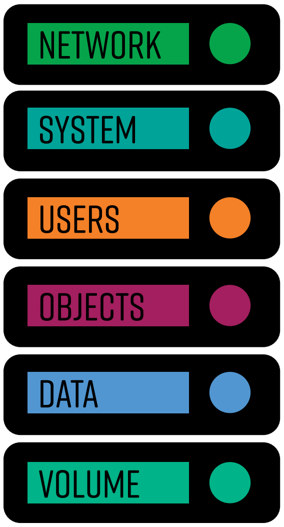
The object layer will ensure access to resources is granted only to authorized users. Resources may include files, volumes, subvolumes, databases and other objects. Building on the previous layer that restricted access based on actions, protection at the object layer will ensure an authorized user running an authorized application can only access authorized objects.

The Data Layer



The data layer is where the core of your data resides. The crown jewels of what an attacker would be after. Examples of these would be data stored within files, databases and other data repositories containing critical business data, payment card data, customer data and other critical data necessary for your operations. This is typically referenced as "Data at Rest". If an attacker made it this far, your last line of defense would be to make the data completely unrecognizable. There are several solutions that exist such as HPE SecureData Transparent Data Protection encryption solutions. These solutions tokenize or encrypt data at rest, so even if the data was exfiltrated, it would be of no use to the thief.

The Volume Layer



To protect the volume layer, often considered a physical layer of security, HPE also offers solutions that protect data at rest at the disk level. One solution is Volume Level Encryption (VLE). An important point to keep in mind, VLE only protects against physical threats. If someone were to walk into your data center and walk out with a hard drive containing critical data, using VLE, that drive would be unusable to them. VLE does not protect application access to the data once the system is on and running. This concept shifts around a bit in the vNonStop world, but the objective is still the same.

Hewlett Packard
Enterprise

Discover 2017

Accelerating next

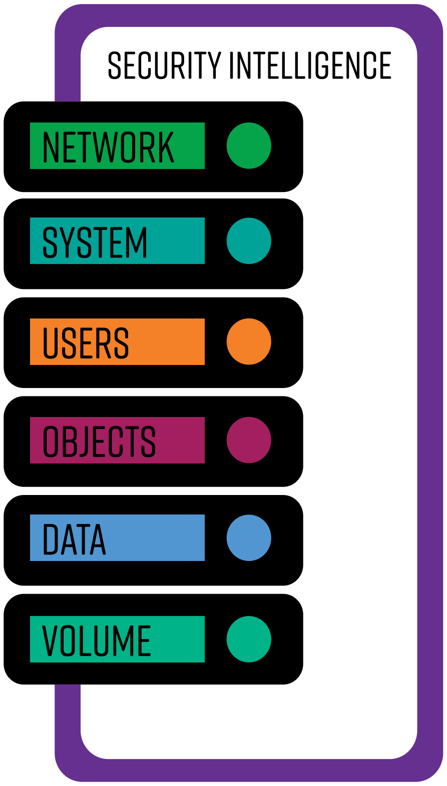
Las Vegas June 6 – 8

Prepare for a world where everything computes

The next wave of market leaders will possess the vision and technological agility to turn ideas into reality faster than the competition. Accelerate your digital transformation.

hpe.com/discover

Audit and Monitoring



Implementing controls without auditing and monitoring is ineffective and can ultimately be the Achilles heel that sinks a security strategy. Generating audit records at every layer for critical activities and reviewing those in a timely fashion will help gain insight into a security strategy like never before. Security intelligence and analytics are no longer buzzwords. Solutions like XYGATE SecurityOne and other analytics platforms give you views into your data and what is happening on your systems like never before. What was traditionally a very tedious and time consuming activity with little result can tilt the scale in your favor and slow down or even stop a costly breach. At the end of the day, data is king. You can add defenses at every layer, but without generating the data to know what is happening at those layers, you're flying blind and cannot ensure your defenses are working the way you intended. As part of this process, ensure the operating systems and applications are patched and updated regularly.

Back to Get Smart…… The reason I found the TV show so relatable to this article (aside from the very appropriate title) is the character works for a secret U.S. government counter-intelligence agency named CONTROL which is appropriate to all of the differing security layers for controlling access to computers and their data. CONTROL's nemesis is KAOS who are an international organization of evil and represent the chaos of all the various threats against computers and their data. The fit was perfect with the opening to the show depicting agent 86 passing through many layers of security protecting their secrets and intelligence information. Agent 86, with his many layers of security, provide him with a 100% success record of detecting and averting disasters.

A motivated attacker will always find a way. Using a layered security approach to risk management can slow their advances enough to allow you to counter their moves. Without a strategy in place to address what happens when they get through, you are gambling, and hoping an attack will stop once they hit the first obstacle you throw at them.

Technology continues to evolve. The skill level & creativity of attackers also continues to evolve. Organizations and merchants need to up their game and their security strategy to keep up with the challenges of the current landscape. This not only benefits the organization, but more importantly provides the necessary assurance to customers that their critical data is being responsibly handled and protected in the most secure way possible.

We'll be taking a deeper dive into the importance and risk at each layer in upcoming blogs and articles and discuss how to map solutions to set up your strategy to best mitigate your risk. Stay tuned!

Steve Tcherchian, CISSP, PCI-ISA, PCI-P is the CISO and SecurityOne Product Manager for XYPRO Technology. Steve is on the ISSA CISO Advisory Board and a member of the ANSI X9 Security Standards Committee. With almost 20 years in the cybersecurity field, Steve is responsible for XYPRO's new security intelligence product line as well as overseeing XYPRO's risk, compliance, infrastructure and product security to ensure the best security experience to customers in the Mission-Critical computing marketplace.

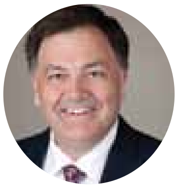
SPEAK NOW.
BE HEARD.

Submit your Advocacy request to: **http://bit.ly/21tsMGf**

HILTON WORLDWIDE | CONNECT+

HILTON ELEVATED DISCUSSIONS by Hilton Worldwide

We're very pleased to announce the long-anticipated launch of **Hilton Elevated Discussions**, a growing collection of short videos of customers and Hilton Worldwide subject experts sharing insights on specific topics that are relevant to the Connect+ audience. Currently we have 25 clips that include the ROI of meetings and events, procuring grants and sponsorships, negotiating Wi-Fi, effective contracting, planning hybrid live/virtual meetings, and much more.
To view the content, please visit **Hilton Elevated Discussions**



To learn more about Hilton Worldwide's unique suite of customer solutions, please contact:
Rocco LaForgia
Director of Sales Technology Associations
p. 212-820-1715 e. rocco.laforgia@hilton.com

Hilton HOTELS & RESORTS | WALDORF ASTORIA HOTELS & RESORTS | CONRAD HOTELS & RESORTS | CURIO A COLLECTION BY HILTON | DOUBLETREE BY HILTON | EMBASSY SUITES | Hilton Garden Inn | Hampton | HOMEWOOD SUITES BY HILTON | HOME2 SUITES BY HILTON | Hilton Grand Vacations | HILTON HHONORS

©2014 Hilton Worldwide

HPE NonStop In-Memory Cache

Sridhar Neelakantan >> **Product Manager** >> NonStop Enterprise Division (NED)

Introduction

HPE NonStop In-Memory Cache (hereafter referred to as NSIMC) is a shared data store that helps applications running on different CPUs, nodes of a NonStop system or even on other platforms to exchange information among themselves. NonStop is well known for its shared-nothing architecture. This design helps improve the availability of services because the failure of a CPU does not affect the applications on other CPUs since their memory areas are isolated from each other. However at the same time, there are situations where it also becomes essential for the applications to have the ability to share information across CPUs/nodes/platforms. To satisfy this need, NonStop Enterprise Division (NED) has released a new product HPE NonStop In-Memory Cache on the NonStop X systems running the L-series software. The key characteristic of the product is that it offers a shared information store without compromising on the NonStop fundamentals of continuous availability and very high data consistency.

This article describes the salient features of NSIMC and concludes with a list of where to get further information.

Description of NSIMC

HPE NSIMC is based on the open source data server Redis® (www.redis.io). Redis is a popular in-memory NoSQL[1] data structure store used by applications serving across many domains / industry verticals. It is used widely in the cloud-computing space, and has a proven track record of handling high transaction rates. The open source software has been deep-ported in order to impart NonStop characteristics.

Redis version 2.8.9 has been chosen as the base version for porting on to NonStop. Thus the NSIMC version on NonStop is also called NSIMC 2.8. It is fully integrated with the NonStop OS and provides a rugged in-memory repository for data elements in a variety of formats.

NSIMC is a "server" that caters to "client" applications that implement the business logic. Figure 1 shows how applications and the NSIMC server communicate. The client invokes "commands" on the server to create, read, update and delete (CRUD) data elements. Many client libraries that are available for several different languages. See https://redis.io/clients for a comprehensive list of client libraries. Out of these, the client Hiredis has been tested on NonStop.

Data Types and mode of communication

NSIMC supports several data structure types viz. Bitmaps, Hashes, HyperLogLogs, Lists, Sets, Sorted sets and Strings. More data types are envisaged in future versions. Multiple operations are possible on these data structures such as appending to a string, incrementing the value in a hash, pushing an element to a list, computing union or intersection of sets, getting the member with highest ranking in a sorted set and so on.

The commands are sent using REdis Serialization Protocol (RESP) as shown in Figure 1. This is an ASCII text based protocol that uses TCP/IP sockets between the client and the server. Multiple commands can be sent by the client and the server will execute all of them together in one atomic operation called a NSIMC transaction[2] and return a response.

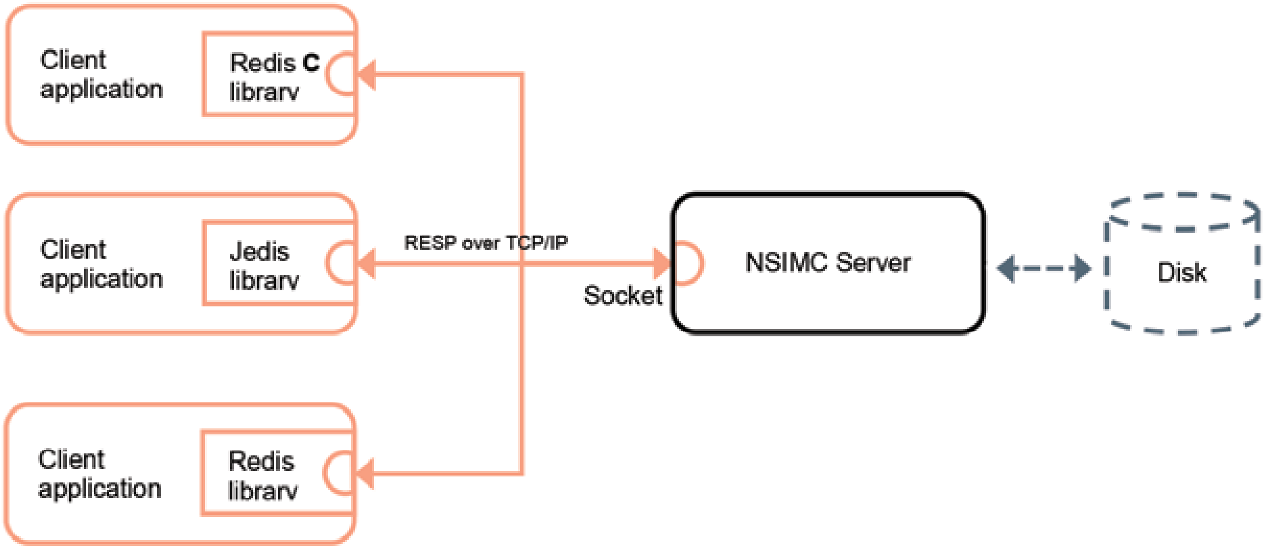


Figure 1. HPE NSIMC client-server model

[1] Not only SQL

[2] Note that HPE NSIMC transactions are not same as HPE NonStop Transaction Management Framework (TMF) transactions

The HPE Partner Ready for Technology Partner Program

Expand your customer base

Increase market share

Accelerate revenue growth

Join today
hpe.com/partners/technology

Hewlett Packard
Enterprise

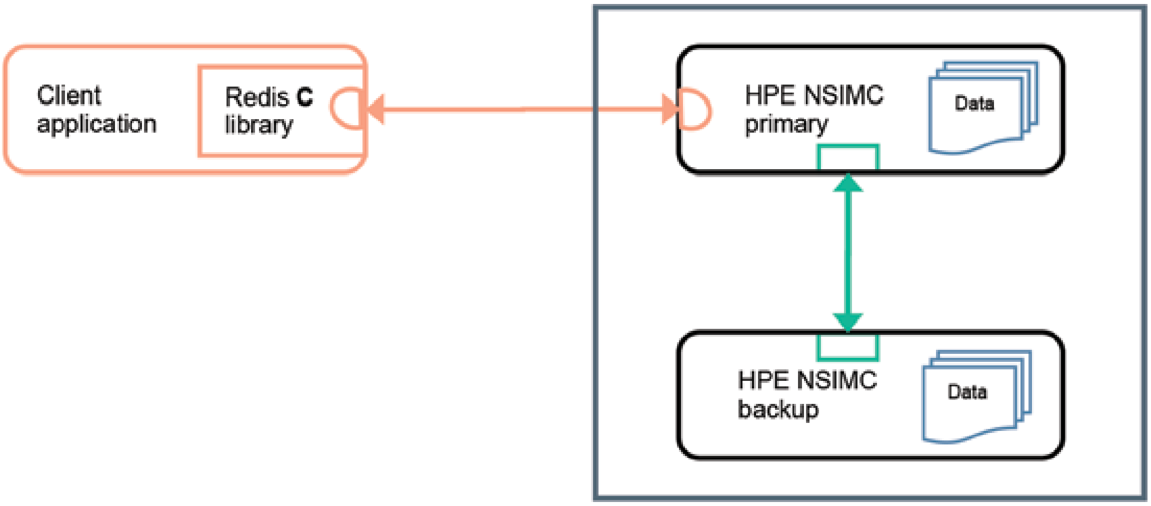


Figure 2. HPE NSIMC—NonStop Process Pair

Continuous Availability and Data Consistency

HPE NSIMC is implemented as an HPE NonStop Process-Pair (NSPP). The backup process takes over when the primary process fails and becomes the new primary. There is no loss of the stored data elements. Figure 2 shows the HPE NSPP architecture. The backup takes over as the new primary when the erstwhile primary fails. The backup has an exact copy of the data set managed by the erstwhile primary. Thus an NSIMC server is always available and there is no loss of data stored in the cache.

Persistence of data

For persisting the cache data in the non-volatile memory, the NSIMC supports the Redis database (RDB snapshot) facility. RDB stores a snapshot of the cache contents in to the non-volatile disk storage at specified intervals (Figure 1) if so configured. The open source Redis offers one more method of persistence called Append Only File (AOF). RDB and AOF have their own pros and cons. The combination of NSPP mode and RDB snapshot provides near zero data loss on NonStop. Thus the RDB snapshot method is the preferred and the only supported mechanism on NonStop for data persistence.

Eviction of old/stale data elements

HPE NSIMC provides a configurable approximation of theoretically Least Recently Used (LRU) algorithm. Beyond a configured maximum memory size, when a new data element is attempted to be stored, the algorithm tries to evict the least recently used data element from the cache. One can configure policies that decide how the algorithm chooses to pick the LRU element to evict.

NSIMC as a message broker between clients

Client applications can be publishers and subscribers of messages where the NSIMC server plays the role of a broker among them. Publishers push messages into channels from which the subscribers receive them. Publishers can push messages into multiple channels. Similarly, subscribers can receive from multiple channels. It is to be noted that messages passed between clients are not stored in the cache. They disappear after the subscribers consume them. The NSIMC server also supports a configurable setting to publish the internal server states such as key expiry, command execution & key eviction etc into channels.

Master-Slave configuration

There is one more mode of configuring NSIMC for increasing the data consistency – the Redis master-salve configuration. A master NSIMC server replicates its data elements in one or more slave servers. In case the master goes down then the slave takes over as the new master. Upon addition of a new slave, the data from the current master is replicated to the new slave. However on NonStop, the NSPP mode provides a higher factor of data consistency and hence master-salve mode is not required.

Scripting facility

NSIMC provides a built-in scripting language, Lua. It provides commands that can execute scripts written in Lua version 5.1 from within the context of the NSIMC server. Execution of a script is atomic. While a script is being executed, no other NSIMC command or script will be executed. Scripts can be used to execute multiple commands sequentially without the client having to send every command across the socket and thus save time.

Conclusion

In summary, NSIMC is a powerful in-memory shared data store that can serve many use cases. Effective use of the NSIMC server can open up several new avenues for NonStop applications. Diverse data types, ability to persist, built-in scripting language, message broking functionality and other features extend the scope of the NSIMC to well beyond a simple heap memory space. NSIMC is available to download from HPE NonStop Scout. Look for the T-number T1300L01^AAA or later after logging in to NonStop E-services Portal (NEP). Current product version as of 2017 May is NSIMC 2.8.

For more information

More details are available in the NSIMC data sheet. The NonStop In-Memory Cache User Guide is available on Hewlett Packard Enterprise Support Center web page.

Redis® and the Redis logo are the trademarks of Salvatore Sanfilippo in the U.S and other countries. Redis is open source software released under the terms of the three clause BSD license. You are advised to refer Redis license and trademark information (https://redis.io/topics/ license).

Sridhar Neelakantan works in NonStop Product Management. He manages middleware and JavaTM based products on NonStop. The middleware products he is responsible for are the ported binaries of Java SE (NSJ), NSJSP, NSASJ, NSMQ, TS/MP, the TMF, iTP WebServer, NonStop SOAP 4, XML parsers and CORBA. He also manages a set of products, that fall under the manageability domain, such as OVNM, OVNPM, SST Ops Bridge, ATM & POS Transactions Analyzers. He has been in HPE & with NonStop for a bit more than 5 years. Sridhar works in the Bangalore, India office of HPE. His email address is sridhar.neelakantan@hpe.com

Back*for*More

Richard Buckle >> CEO >> Pyalla Technologies, LLC.

The NonStop community continues to remain loyal to the NonStop system and for good reason. Nothing better has come along. Let's not mince words, NonStop is the premier fault-tolerant, 24 x 7, best-suited platform in support of the most demanding mission-critical applications. With that said, is it time to pull back the curtain a little and look at NonStop, and its well-known attributes, within the context of what is happening today.

This is a reference to not only what is happening with a number of proprietary offerings but with open source projects as well. When there is so much energy in support of standards, open, and yes, the biggest combination of both, clouds – how does NonStop continue to differentiate itself from what it would appear that the rest of the world is doing? To some in the industry, NonStop is tracking closely to IBM's mainframe and sharing similar problems when it comes to identity and yet, looking at the numbers it would appear that NonStop isn't beset with as many problems as its counterpart at IBM.

I am probably not alone within the NonStop community when it comes to having to listen to the latest industry analyst telling me about stepping out from NonStop to embrace something far more modern. To put aside championing traditional approaches to computing and instead, focus my energy on evangelizing what's truly revolutionary. And what is that, exactly? Well, it's all about open source projects tackling everything from the OS to database to development frameworks. When was the last time you checked-out the projects being worked on under the Apache banner, for instance? Not to discount the wisdom of my learned colleagues within the industry analysis business, but for the most part they continue to take the easy way out!

Take for instance the argument about not being able to recruit NonStop programmers. What complete nonsense and in all reality an argument a CIO can make to the board and yet, dig deeper, and what does "programming NonStop" really involve? There are many within the NonStop community that swear about the fantastic performance of Java applications on the new NonStop X just as they continue to embrace online development platforms like Eclipse. You don't program NonStop – you exploit it to your advantage using regular programming languages tools and frameworks!

As for the other argument about NonStop lagging other systems when it comes to performance, NonStop managers Karen and Andy have done an amazing job in a relatively short period of time to absolutely quell any disquiet that may have existed about performance as compared to previous iterations of NonStop. The message coming from NonStop product management, "There is just nobody complaining today about how their applications run on NonStop X. Nobody!" Embracing the Intel x86 architecture not only meant making an even bigger bet on standards and openness, it also meant leveraging a much faster engine and the NonStop user community is starting to realize just how beneficial to them this is proving to be.

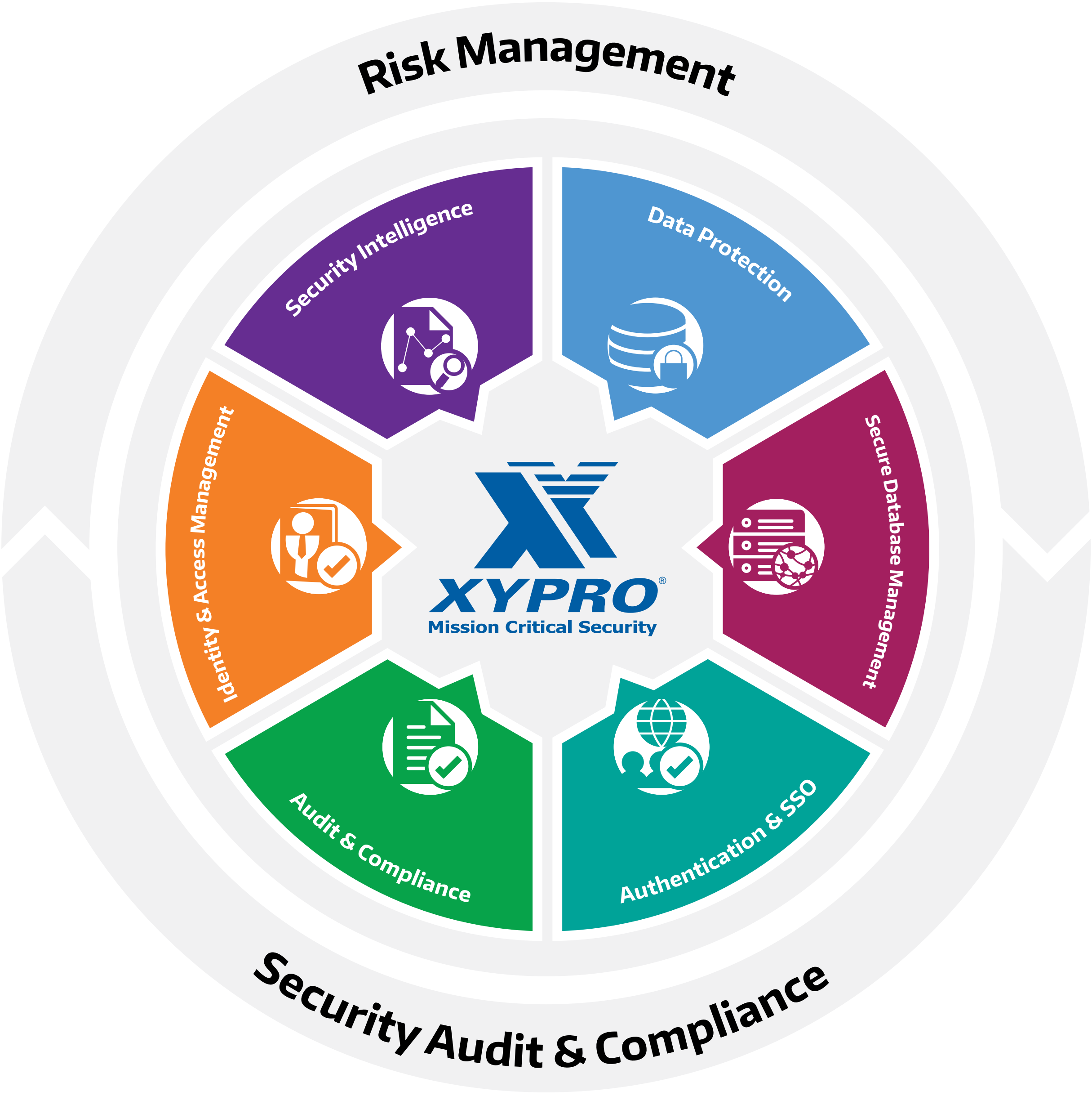
The theme of this issue of The Connection is Architecting your NonStop system for High Availability. Well, NonStop is High Availability out of the box! Industry analysts such as IDC say that NonStop, out of the box, stands alone atop their chart as being leader of the category, Availability Level 5. That's it. The top tier with only very special configurations of multiple IBM mainframes under a Parallel Sysplex banner comes close but at a price you just don't want to read about it and the complexity of the stacks configured in support of Parallel Systplex approach levels of absurdity that look to many IT professionals as though you needed to tap the powers of Star Wars' dark side. On the other hand, nothing new here – we all should know this without any further consideration.

Oftentimes overlooked when discussing the merits of NonStop today is the integrated stack the NonStop team provides. Yes, from the metal to the fanciest user interface, there's just one stack making up NonStop and it does all work out of the box. A similar case cannot be made for almost no other environment. Take for instance, the recent experiences of one developer who documented his woes on LinkedIn. "I'm currently looking to learn Hadoop and in order to make it useful, I've got to download and install various components from various vendors and configure accordingly," the author of the post began.

"With a NonStop environment, that is all taken care of," the post noted. It then makes the more pertinent point and one that is often repeated by developers working with NonStop systems, of how advantageous to development this NonStop integrated stack really is when the author rails on readers to make sure that, "CIO's need to know that developers can go immediately to programming their application solution and not be delayed in doing that because they're trying to build the development environment that they'll be working in."

When it comes to architecting your NonStop system for high availability then with NonStop deployed you are already ahead of the game. You are essentially well past high availability right out of the box. Something programmers of all skill levels can leverage immediately even as the performance improvements can be readily seen. And yes, productivity is even better that can readily be achieved with other systems as yes, NonStop is unarguable the premier fault tolerant system every business should turn to when time comes to run their mission critical applications.

Security Solutions for your HPE NonStop Environment


Risk Management
Security Intelligence
Data Protection
Identity & Access Management
XYPRO
Mission Critical Security
Secure Database Management
Audit & Compliance
Authentication & SSO
Security Audit & Compliance

Exceeding your HPE NonStop security, compliance & encryption needs for over 30 years

Learn more at
www.xypro.com

XYPRO®
Mission Critical Security

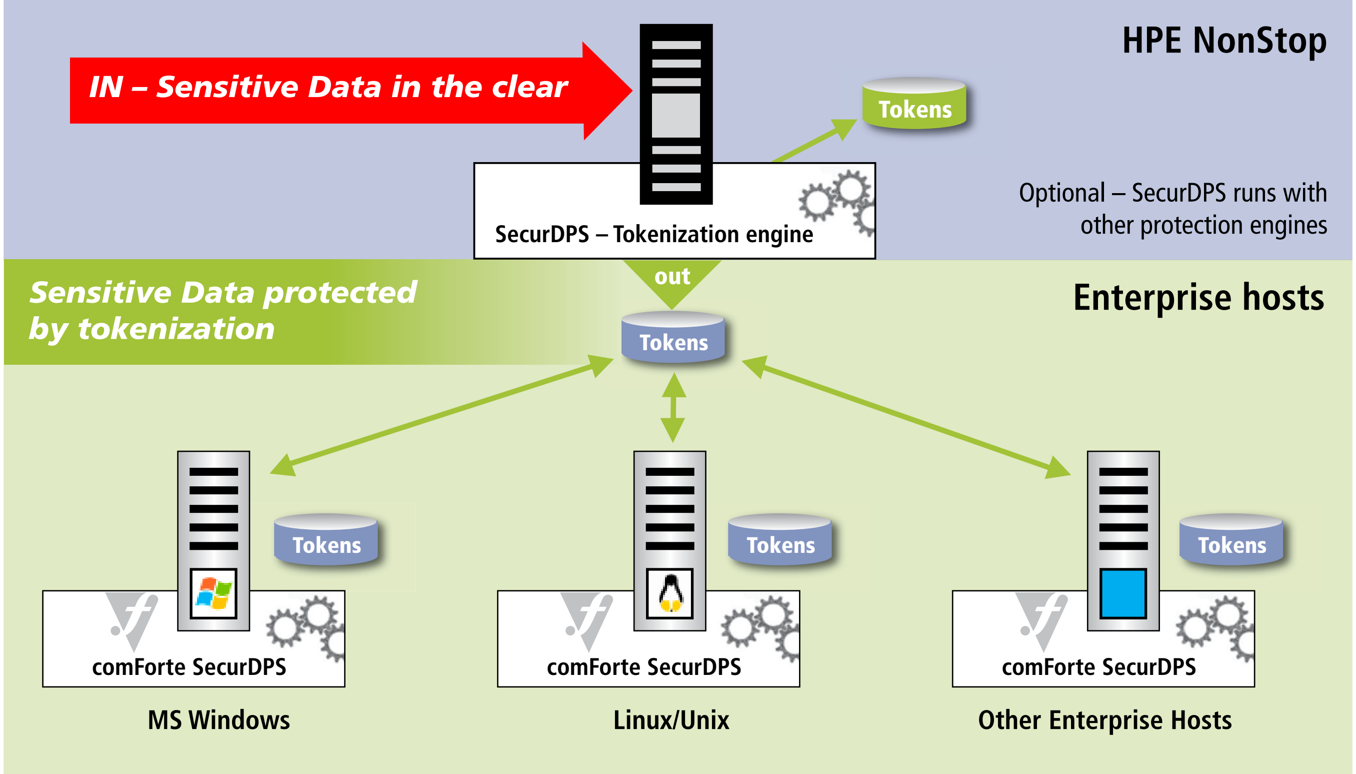
©2017 XYPRO Technology Corporation. All rights reserved.
Brands mentioned are trademarks of their respective companies

SecurDPS Enterprise Data Protection

Data-centric approach for enterprise data protection across heterogeneous platforms

- ☑ Protect sensitive payments and customer data
- ☑ Includes tokenization and encryption
- ☑ Neutralize impact of data breaches
- ☑ Reduce compliance audit scope and costs
- ☑ Enable PCI compliance and tackle GDPR legislation
- ☑ Integrates transparently with no software changes required

Already protecting millions of PANs for customers today


HPE NonStop
IN – Sensitive Data in the clear
Tokens
SecurDPS – Tokenization engine
Optional – SecurDPS runs with other protection engines
out
Sensitive Data protected by tokenization
Enterprise hosts
Tokens
Tokens
comForte SecurDPS
MS Windows
Tokens
comForte SecurDPS
Linux/Unix
Tokens
comForte SecurDPS
Other Enterprise Hosts

Learn more at comforte.com/SecurDPS

comforte® better always on

NonStop is a trademark of HPE. All other trademarks are acknowledged. *©2017 comForte 21 GmbH. All rights reserved.* *Feb.24_2017*