

*Read it in Print
and Online!*

The Connection

A Journal for the Hewlett Packard Enterprise Business Technology Community

**2 Powerful Ways to
Protect Sensitive Data
on NonStop Systems**

**NonStop System
Console Care
and Feeding**

PLUS
**Women in
NonStop**

XYGATE® SecurityOne®

Security Intelligence and Analytics
for HPE Integrity NonStop™ Servers



Visibility

Minimize the impact of a breach by identifying it in its early stages

Faster Threat Detection

Improved Risk Management

Separate Noise from Actionable Incidents

Reduce Mean
Time To Detection

Learn more at
xypro.com/SecurityOne

 **XYPRO®**
Mission Critical Security

Monitor 100% of Your Processes. In 100% Real Time.

Not sure why your NonStop system isn't performing the way you want? Use RPM to find out why ...

HPE's NonStop Real-Time Process Monitor (RPM) is efficient, low-cost, real-time monitoring software that continuously determines what's consuming resources.

Engineered specifically for NonStop servers, NonStop RPM helps you monitor 1000s of CPUs, IPU's and millions of processes letting you know instantly when any process is using excessive resources. So you can fix bottlenecks before they become full blown problems.

Here's your chance to keep your NonStop infrastructure more non-stop than ever.

Technology for better business outcomes.



Hewlett Packard
Enterprise

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

JOIN THE CONNECT BOARD OF DIRECTORS

Now accepting applications for 2017

<http://bit.ly/CWWBOD18>



Applications are now open for the Board of Directors for Connect Worldwide. Volunteer your time to further our mission of advocacy, community, philanthropy and education. This is your opportunity to lead the Hewlett Packard Enterprise community, partners, and customers into the future.



We're sorry, but HPE employees are not eligible to run for these open positions. If you are interested in learning about other ways that you can volunteer with Connect, please visit our [volunteer opportunities](#) page.

Inside *the* Connection



{ Technology + Community }

08 News from eBITUG

10 News from N2TUG 2017

14 NonStop Innovations:
Women in NonStop

Mandi Nulph

16 Crashing the (Third) Party:
The Supreme Court and Privacy

Karen Martin

19 Achieving Scalability for
Mission-Critical Systems in
the Cloud

Dr. Bruce D. Holenstein

Dr. Bill Highleyman

Paul J. Holenstein

24 2 Powerful Ways to Protect
Sensitive Data on NonStop
Systems

Jonathan Deveaux

28 How HPE is Making
Blockchain Resilient

Dr. Bill Highleyman

32 NonStop System Console
Care and Feeding

Wendy Bartlett

34 HPE Shadowbase Software
Enables Operational Analytics
for Commodity Big Data

Keith B. Evans

38 Secure Communication
Through VPT the Virtual
Private Tunneling

Jürgen Overhoff

40 A Web Application
on NonStop

Wolfgang Breidbach

Sven Breidbach

45 Security: A Critical Piece of
NonStop SQL Management

John Furlong

Columns...

05 **A Note from
Connect Leadership**

ROB LESAN

07 **News from HPE's
NonStop Enterprise
Division**

KAREN COPELAND

12 **ADVOCACY
Not Only the Y2038
Problem - There's a
Y2028 Problem**

DR. BILL HIGHLEYMAN

48 **Back for More...**

RICHARD BUCKLE

#NonStopTBC

NonStop Technical Boot Camp 2017



November 13-15, 2017

Hyatt Regency San Francisco Airport
Pre-Conference Seminar on November 12, 2017



A Note from Connect Leadership

Security


We love to hate it and often choose to ignore it. Security is the one job that no one seems to want. It can be one of the toughest jobs around. No one ever looks forward to a call from IT Security... As difficult as security can be, it is also the most rewarding position I have ever held. I have worn quite a few hats in my NonStop career, but none of them have granted me the level of satisfaction that this one does.

You all know how complicated the NonStop enterprise is! Between the file systems (Guardian and OSS), to user management (how about those aliases!), regular audits (both internal and external) and finally to compliance to any number of standards, security is a full time job that most of us have on top of our other responsibilities.

Please, always remember these things:

1. Security is everyone's job!
2. Compliance does not always mean security and vice versa.
3. Security is not a product, but a set of processes, products and people.
4. Don't try to work around security. Understand why protections are in place and ask for access when necessary.
5. Be nice to your security staff! Most of what they do is enforcing enterprise policy, it isn't personal!

Never fear ladies and gentlemen. HPE and your NonStop partners spend THEIR days and nights worrying about these things to help YOU sleep better at night.

Now, stay off those exception reports!  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.

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

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

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.

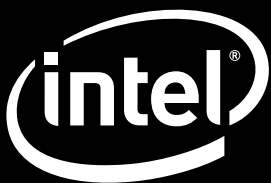
© 2016 by Connect
All company and product names are trademarks of their respective companies.



The Always On Operating System



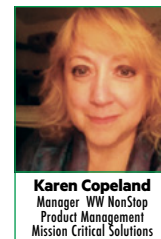
**Hewlett Packard
Enterprise**



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

News from HPE's NonStop Enterprise Division



The NonStop Summer, Could It Get Any Hotter?

Summer has come roaring in with record heat waves in Silicon Valley as well as the rest of the country. The kids are out of school and everyone's packing up to go to the beach or camping or more exotic vacations. In the meantime, NonStop servers keep running businesses around the world without fail, so people can take time off with confidence that their business will have smooth sailing while they're gone.

HPE's Discover 2017 in Las Vegas this year was a little smaller than past events run by HPE and everyone I talked to told me this was a relief as it was easier to navigate the show floor and to find the NonStop booth. We had good traffic at the booth this year and talked to a number of companies who were new to the capabilities of NonStop systems and were amazed at the demo we were presenting. We also have a proof of concept port of R3's Corda that runs on NonStop demonstrating Blockchain capabilities in a fault tolerant environment. This demo, hosted by our Pointnext group and the Financial Solutions team, had a lot of interest from customers and partners at the show. If you attended, we hope you thoroughly enjoyed the event.

This issue of The Connection Magazine focuses on Security. I capitalize it because it's a serious matter for every business these days. Protecting data protects the confidence of customers and clients to do business with you. A breach shakes that confidence and can drive customers away, especially if their personal information is stolen and surfaces later on the dark web. The violation of being breached is still every business's worst nightmare.

NonStop with its unique OS architecture has some advantages. With the additions of improved network security and additional authentication and access control options as well as encryption and tokenization for data at rest, the NonStop platform has come a long way in recent years in terms of the options that you can choose to protect your business and the data it collects.


In this issue you can read about "2 Powerful ways to protect sensitive data on your NonStop systems", by Jonathan Deveau of comForte Inc. He writes about how to protect your data when it's in motion and when it's at rest and some choices now available for NonStop from both HPE and partners. Although we now include products on every commercial system that are aimed at helping customers both better secure their systems and monitor security-related events, they can't help you if you don't actually use them.

An interesting article by Wolfgang Breidbach, simply titled "A web application on NonStop", describes how easy it was for a Bank Verlag developer to prototype and secure a payments-

monitoring application based on JPATHSEND, JSP and TMF. Our own Wendy Bartlett has provided an article on how to protect and secure your NonStop System Console in "NonStop System Console Care and Feeding". The NonStop System Console is an important device for accessing and managing your NonStop system and because it runs Windows Server can still be vulnerable to viruses if protection software is not kept up to date. In addition, an article on the differences between Virtual Private Networks (VPNs) and Virtual Private Tunnelling (VPT) from Juergen Overhoff, of ITP-Panorama, Inc. explains the difference and why VPN is losing popularity and VPT is gaining ground.

This issue rounds out its contents with two articles on Business Continuity. "Achieving Scalability for Mission-Critical Systems in the Cloud" by Dr. Bruce Holenstein and Paul Holenstein from Gravic, Inc. and Dr. Bill Highleyman from the Availability Digest continues the conversation about Mission Critical environments by talking about designs for scaling applications and bursting into the Cloud for additional resources using data replication to ensure data availability. A second article called "HPE Shadowbase Software enables Operational Analytics for Commodity Big Data" by Keith Evans from Gravic, Inc. describes how a government customer can mine NonStop application data for real-time analysis using Shadowbase capabilities to keep the analytics systems up to date.

We hope you find this issue of The Connection Magazine valuable and want to remind you that if your company has concerns about Security on your NonStop systems, there are services available to help you analyse your risks and advise you on what to do to better protect your system and your data. Contact your NonStop sales representative for options in this area if you think you need it.

Wishing you all a great Summer, if you are taking an vacation, enjoy your time off and stay cool (maybe spending some time in the computer room is sounding better than usual)! 

Regards to everyone!



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



eBITUG has set the bar for European NonStop User Group events according to Dr Michael Rossbach at the closing ceremony.

The event had a perfect mix of HPE, Partner and Customer sessions with 3 parallel tracks providing something for all the 250+ delegates.

HPE set the theme talking about what had been planned 12 months ago, what had been delivered and what is coming next. Customers and Partners not only enjoyed the openness of the future sessions but how HPE has delivered on the strategy and the relevance to cloud strategies and data lakes for the new IT. Deployment options, continual integration and DevOps were all part of how NonStop participates in IT's Transformation. The enhancements to capability, portability and deployment of SQL/MX along with the use of micro-services frameworks supported the modernisation theme for developers along with new HPE and Partner capabilities for business continuity data replication and also data integration on and off platform.

Customers presented on their migration to NonStop X, a cornerstone to the adoption of Virtualised NonStop and Cloud deployment.

Payments vendors outlined new solutions for card issuing, prepaid cards and electronic benefits payments as well as payment SaaS.

There was a large focus on securing NonStop platforms, payment

solutions and software subsystems in line with PCI-DSS and general industry concerns over security. Choice was plentiful and sessions covered forthcoming requirements as well as tool capability.

Management services and solutions also took centre stage with automation tools and cloud analytics demonstrating once again a modern platform.

Daimler discussed their world-wide dependency on NonStop for vehicle manufacture and how their plans for the future would remove paperwork making systems even more critical.

1:1 meetings and NDA sessions with HPE as well as Virtualised NonStop demos rounded out the event as well as the second under 40s SIG meeting following the one last year at TBC.

It was great to see that Jimmy Treybig (Venture Capitalist and Tandem ex-CEO) not only presented the Keynote on Industry Disruption for Enterprise companies but supported the event by being present throughout both days of the conference.

The social events during the conference were also heavily attended giving a great opportunity for networking and enjoying London during a very pleasant couple of days weather.


BITUG and GTUG are working to share experiences and ideas to maintain the momentum of a European NonStop User Conference in future. 

Photo credit: CORP'ix Photography





News from N2TUG 2017



On June 1st of this year, The North Texas and Oklahoma NonStop Users Group (N2TUG), in conjunction with the local HPE NonStop Sales team and a great bunch of sponsors, held our 2017 event at the Gaylord Texan resort in Grapevine, Texas. We started the day with a breakfast buffet while people registered.

The theme of the event, *Mission: Virtual, Lone Star Style*, came about partly from the design of the resort.

The opening remarks, given by the N2TUG planning committee (President Bill Honaker of XID Software and Liaison Diane Funkhouser of HPE), discussed how the legacy of the Republic of Texas was a vibrant one. Throughout this exciting venue, one will find vistas reminiscent of San Antonio, the Texas Hill Country, Lone Stars, old bridges, and oil wells. When I saw it, I thought of a 'Virtual' tour of the state of Texas. And the term 'legacy', as it applies to solutions platform such as NonStop, describes things with a strong foundation that allows for positive growth. The latest great innovation from the NonStop division of HPE, Virtualized NonStop, is a great example of extending the platform's strong legacy.

Next up, Karen Copeland, HPE's Manager of NonStop Product Management, presented the keynote address with 'NonStop for your future'. After reminiscing and sharing some pictures of her growing up in Central Texas, she gave the attendees updates on HPE's mission critical solutions, focusing on the family of NonStop systems. She shared her team's vision of the NonStop Cloud and what is planned for the near future, not only on

Virtualized NonStop, but on the strategic direction and product enhancements for NonStop SQL/MX as well as other exciting directions that her team is targeting.

After our first break, Jim McFadden from our Platinum sponsor, Network Technologies International, presented 'The Evolution of Data Replication'. His enthusiastic presentation included announcements about their latest EVOLUTION, VISION, and LiveLink support offerings. Our Platinum Sponsors are one



of the key reasons we continue to be able to bring a great event to the local NonStop community at no cost to its attendees, and N2TUG really appreciates NTI!

The event's Happy Hour sponsor, XYPRO, followed as CISO Steve Tcherchian gave the audience a lot to consider with his talk 'Security Defense in Depth'. While he started by discussing the challenges faced by all businesses today, he presented very powerful strategic

directions that can be used to keep your company's information safe.

Shawn Sabanayagam from Tributary Systems finished our morning presentations with 'Cloud Backup and Data Management Solutions', with concrete examples of the flexibility that's available to NonStop customers, as well as users of other Enterprise systems, today. He also touched on ways to manage all of your archives.

We then stepped out of our meeting room into the open atrium area of the Gaylord to enjoy a lunch buffet, giving people time to chat while enjoying a nice meal. I'm only sorry that the food was so good that apparently nobody stopped to take any pictures!

Tom Miller from HPE led off the afternoon speakers by updating us on the status of NonStop MQ Version 8, which is currently in 'Beta' release. He gave the crowd some expectations of the upcoming product rollout.

Idelji's Khody Khodayari gave a great demo of the latest Operations and Performance Management products and services. He focused on both 'Web ViewPoint Plus', a browser-based tool, and the 'Remote Analyst' service, and also mentioned other available products.

Jessica Nieves of OmniPayments talked about their OmniCloudX service, after giving an overview of the OmniPayments product. She provided highlights of the available features as well as a report on the performance characteristics of the products.

Paul Hostenstein of Gravic updated us on the latest Synchronous Replication features of HPE Shadowbase. After laying



the groundwork of concepts such as RPO and RTO, Active/SZT/Passive, and Asynchronous/Synchronous, he compared the costs and benefits of each in a very informative presentation.

Fernand Lussier of [ETI-NET](#) started his talk about the life cycle of archive media by talking about vinyl records. He gave very clear examples of the real reasons that storage media formats are a key strategy driver for your archives, while providing useful guidelines in how to build that strategy.

Gabrielle and Vince Guerrero from NuWave gave demos of exposing NonStop services using the REST technologies of their LightWave product. The highlights of the presentation used an Amazon Echo, during which Vince demonstrated a couple of novel ways to use your 'legacy' NonStop in a truly 'modern' way.

Marty Edelman, representing comForte, discussed using the Escort product to modernize NonStop applications. He also took the time, as a Giants fan, to try to stir up some NFL rivalries.

Finally, Budd Matlock from [QSA](#) talked

about how to securely enhance your backup catalogs using the Q/Tos catalog and the Qtos GUI solutions, also mentioning other products in their portfolio.

After such an exciting and whirlwind tour of the ways that HPE and the NonStop vendors are extending the legacy of NonStop, we all needed some time to unwind. What better way than with a 'Happy Hour'? Well, in typical NonStop fashion, we opted for 2 hours! And in typical Texas fashion, we provided that in a part of the venue called the 'Mission Plaza' area. The design of that plaza is reminiscent of the historic district of San Antonio; it was very much like being on the shores of the Riverwalk. The attendees networked while enjoying hors d'oeuvres and beverages provided by the sponsors. A generous array of door prizes was given away, including 2 drones! There are some fun images of Happy Hour in the pictures accompanying this article, so please check those out.

We are pleased to report that we had our largest turnout ever, with a total of 84 attendees representing 19 customer companies and 15 sponsors. Along with

the breakfast, lunch, daytime breaks and the happy hour, quite a bit of good business happened that day in addition to the usual socializing and catching up with friends. The venue seemed to encourage that networking, and we may very well use it again.

That venue, by the way, is close to the airport (and therefore convenient to the out-of-towners), and it's on the shores of Lake Grapevine. Evenings were filled in the hotel's ample sports bar watching NHL and NBA playoff action, or in one of the great restaurants on site.

Diane and I also wish to thank all of our sponsors for making it possible. In addition to the speakers mentioned above, the other sponsors were: [Connect Worldwide](#); [IR](#); [Odyssey](#); [NonStop Insider](#); and [XID Software Inc.](#)

By now I'm certain that those of you who couldn't be there are feeling sorry you missed this year's event. We are looking forward to seeing you next year! [CS](#)



Not Only the Y2038 Problem – There's a Y2028 Problem

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

In our article “Future Dates Spell Problems for IT” in the March, 2017, issue of the Availability Digest, we pointed out that many systems might crash on January 19, 2038, due to the overflow of 32-bit date/time fields. Though most applications should be corrected by then to avoid this problem, there are old legacy applications still in use that are not easily modifiable. For many, the source code is lost and the original programmers have all moved on. These applications are at risk for this fault.

For many systems, such a catastrophe might occur a decade earlier, in the year 2028. But this will occur for a completely different reason - a Y2K temporary fix that has become all but temporary.


Y2K was a big problem for many programs. Written years ago, these applications used a two-digit year field to save memory space, which was at a premium when these programs were written. The year ‘1967’ was stored as ‘67.’ But as the year 2000 approached, the year 2000 would be interpreted as the year 1900. All later years in the 21st century would be treated as 20th century years.

Massive efforts were launched to modify applications to move from a two-digit year field to a four-digit year field. However, some clever individuals came up with another technique. Since the calendar repeats itself every 28 years, it was only necessary to roll the calendar back 28 years. That is seven years to get the weekdays synchronized, times four to account for the leap year. The year 2000 became the year 1972. The year 2017 became the year 1989. The application then only had to be modified to add 28 to the year. For instance, if the year was stored as ‘89,’ the modified application would interpret this as $1989 + 28 = 2017$.

This was a much easier change to the applications in many cases. For instance, data stored in the database could still use two-digit dates. If a full Y2K correction were implemented, all database structures that stored a date would have to be modified to use a four-digit year rather than a two-digit year.

Unfortunately, this algorithm breaks down in the year 2028. The year 2027 is stored as the year 1999, or as ‘99’ in the two digit format. The next year is stored as ‘00,’ which the application interprets as the year 1900. Adding 28 gives the year 1928 instead of the year 2028. At this point, application programs will fail. Imagine what happens if you try to calculate interest from the year 2027 to the year 1928? In fact, CNBC reported that the Congressional Budget Office’s computer program crashed when it reached the year 2027 as it calculated forward government spending.

Clearly, these applications will have to be corrected before they start using dates beyond 2027. They will have to finally be modified to use a four-digit year. Using the Year 2028 fix bought companies a 28-year reprieve, but time will catch up to them.

Many people are saying that this won’t be a big problem since most computers in use today will have been replaced by 2028. However, the Y2028 problem is not a computer problem. It is an application problem, and the applications must be retired or fixed. For those unmodified applications that are still around by the year 2028 (or earlier if the applications are performing time-forward computations), beware the Y2028 bug. It could deliver a painful bite. 

¹ Future Dates Spell Problems for IT, Availability Digest; March 2017.
http://www.availabilitydigest.com/public_articles/1203/dates.pdf

² Y2K28 Problem: All Computers Will Crash in 16 Years, Godlike Productions; July 28, 2012.
<http://www.godlikeproductions.com/forum1/message1939123/pg1>

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. Find his books on Amazon. Contact him at billh@sombers.com.



**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

Women in NonStop:

Lisa Partridge on XYPRO, Her Journey, and What's Next in NonStop

Mandi Nulph >> Marketing Coordinator >> NuWave Technologies



In this edition of Women in NonStop, we had the opportunity to chat with Lisa Partridge, CEO of XYPRO. We discuss her long tenure with the company, how she got her start in NonStop, and how she sees young people playing a role in the future of the NonStop space.

Mandi: Explain your role in your company for those who might not be familiar with you.



Lisa Partridge

Lisa: My current role, starting in 2014, is as CEO of XYPRO. I participated in the management buy-out from the original founders of XYPRO. They were ready to retire and I took over as CEO. I had been working as president for quite some time before that, and had been working with XYPRO for over 25 years at that time. I've spent the majority of my adult life working for XYPRO in a variety of roles.

Mandi: What has been your professional journey leading up to XYPRO and your path since you've been there? What did you think you were going to get into when you were younger versus what you ended up doing?

Lisa: When I was in high school I thought I was going to get into politics or political science. I certainly never aspired to be a software salesperson, that's for sure.

I did spend time living and working in the UK, and it was there that I started doing some receptionist work at Tandem Computers in London. I worked at Tandem during a very exciting time when it was coming up in the 80s. I worked in the banking district at a very fast-paced office. I thought I was going to be there for a short period, but I ended up staying there for some number of months and eventually ended up being recruited as a junior salesperson by someone who started Insider Technologies. So, I was one of the first four or five original employees of Insider Technologies.

Mandi: What do you like best about working for XYPRO and in the NonStop space?

Lisa: Well, I think even how I ended up at XYPRO is illustrative of why I like it very much. Insider Technologies in London was distributing XYPRO products in the European territory. I ended up at XYPRO to take on more training and get more in-depth education about the products, and I never ended up leaving! They liked the way I did things, and I liked the way they did things. I was given a lot of opportunities to do things that I would not necessarily be able to do in other circumstances. They taught me literally everything I know about the NonStop platform and gave me a lot of space to find my own voice as a salesperson.

We were a small company, so I literally was the only person selling the XYGATE security suite at the time. I had to learn everything. I had to give technical and sales presentations, and I was first-line technical support when the customers called because I helped write the documentation. They all had my home number because there were no cell phones, there was no email, there was nothing. It was all done the old-fashioned way, with phone calls, letters written on paper, faxes, things like that. I learned from the ground up about all aspects involved in being a software development and sales company. I think that's just invaluable experience that allows you to take on responsibilities that might not normally have been given to someone my age at the time.

Mandi: Did you have any role models or mentors who have helped you along the way?

Lisa: The founders of XYPRO, Dale and Sheila, were excellent role models. They were a husband and wife team. Dale started the company with a partner of his, and they were of course former Tandem analysts who started a software company supporting the NonStop/Tandem platform. He was a very good teacher. I got some serious thrown-in-the-deep-end knowledge very quickly about how the product worked because I had to answer questions.

Sheila was an excellent role model because Dale asked her to come in and help run the company. So, from learning to deal with people, being responsive to employee needs, and communications skill and style, I learned a lot from her. She came from a marriage and family counseling background, so there was a lot to learn as far as listening, taking things in, and making decisions once you thought out the options and weighed the pros and cons. I still often think about that when I have to make decisions, because it's my full responsibility now, and I sit back and make a list like Sheila

would have done when it was her job to make those decisions. I am also very lucky to do this all in the NonStop/Tandem space. It's a very supportive, family-oriented community, in the sense that we're all part of the same family.

It's also visibly very strong in contributions by women. I never felt like there weren't role models for me in the Tandem space. I was often the only woman salesperson in a given situation, but I only had to look around. Even when I was working in London as a receptionist, there were sales managers there who were women. Patty Fennell worked there. She had a very senior position, and was a very strong, thoughtful person, so I got to see her confidence level. Then, when I came to the states, you've got Wendy Bartlett, Karen Copeland, Meg Whitman, Rita Wells, and so many other exceptional women in this industry. You don't look around and go, "Hmm, how strange." You look around and think it's normal. In fact, I don't even really think about whether I have it more difficult than the men in the NonStop space. I'm very privileged that I haven't felt like I've been held back or had to work harder than the guys, because I think I've had the privilege of being surrounded by very prominent women from the beginning.

Mandi: I've heard the same sentiments from the other ladies that I've talked to. That they haven't felt challenged by their gender at all in this industry.

Lisa: Yes, I would agree.

Mandi: Do you feel like it's important for more women to jump into the NonStop space? Do you think that maybe technology can be an intimidating space to try to come into?

Lisa: I wouldn't necessarily isolate the NonStop space as being challenging for women to join. At XYPRO we have a lot of female employees in the engineering department. My director of engineering is a woman, one of my development managers is a woman, the lead business analyst is a woman, our VP of human resources is a woman. I don't think that was necessarily an on-purpose thing that we did, to make sure we hired women, but there are a lot of very capable women applying for most of the jobs we advertise. So, I think we have a beautifully diverse group of people, and it's not just gender diverse, it's diverse in every way.

Mandi: Do you have any advice for young people, men or women, who are trying to figure out what their career path is going to be and are thinking about technology?

Lisa: Back in the day, we used to judge a resume by how long people had spent at certain jobs. If they job hopped too much that was usually a warning sign, but we're really learning that the younger generation don't really want to be tied down to one place. They want to move around and try different things, so we've really tried to focus on giving them that opportunity, internally. I think that sometimes you have dissatisfaction with how your career is going is because it's not happening fast enough.

I'm a real avid follower of a motivational speaker named Simon Sinek, and he has a great analogy. He says a lot of people stand at the bottom of a mountain and they look at the top of the mountain as where they want to get to. Some people get to the top of the mountain very quickly and some people take a long time to get to the top of mountain, but you can't forget you must actually climb the mountain, however you do it. If young people are trying to find their bliss or their release in life, or what exactly they want to get involved in, give things a bit of a chance. Six months at one place is not going to give you a sense of whether this might be something you want to do long term. Talk to your managers. Have a dialogue back and forth with them because a happy employee produces so much more than someone whose feeling like they're not getting to spread their wings.

When you're new, you do have to spend some time doing the job you were hired to do and doing it well, and then I promise you opportunities will come to you. I've been very, very lucky; I've luckily been given a lot of opportunities and was smart enough to know when to take advantage of them. Working hard is the most important thing—do your job, absolutely do your job, and good things will happen.

Mandi: Thank you for giving us the opportunity to learn a little bit more about you and your background!

Lisa: My pleasure!

To learn more about what is new at XYPRO, their commitment to NonStop, and what they have planned, visit NuWave's NonStop Innovation's blog at www.nuwavetech.com/blog for a follow-up interview with Lisa.

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.



**UPDATE YOUR
PROFILE TODAY!**



<http://bit.ly/2jKRaph>

www.connect-community.org

Crashing the (Third) Party: The Supreme Court and Privacy

Karen Martin

Introduction

The Supreme Court recently agreed to hear *Carpenter v. United States*¹. This will require them to consider whether the warrantless seizure and search of historical cellphone location data is permitted by the Fourth Amendment. Their decision may change the rules for disclosure to law enforcement of records related to customers' communications collected by cellphone service providers, internet service providers, and other third parties. It may have a significant effect on everyone's privacy.

Courts have traditionally made a distinction between the contents of a message or conversation, and the information needed to deliver that message. A letter is protected under the Fourth Amendment; the address written on the envelope is not. A conversation spoken over a phone line is protected, the phone numbers used to connect the call are not. In the past, this distinction was relatively straight forward – information sealed inside an envelope or package is private, but we cannot reasonably expect information written on the outside of a package or envelope to remain private.

Electronic communications over mobile devices, however, pose a problem. They generate vast amounts of metadata – information about the communications. Metadata includes to/from phone numbers, email addresses, date, time and location of transmission and reception, the amount of data sent, the length of a conversation, and more. Some of this data is more sensitive than the limited data needed to send postal mail or make landline calls.

Consider for example, a man who suspects his wife is being unfaithful. If she tells him that her boss has just called her back into work, and leaves the house late one evening, he might

wonder if she were really going to work. If he could choose to either hear a recording of the conversation or be told the caller's phone number, he would obviously prefer to hear the conversation. If he were offered a choice between learning the phone number or tracking the movements of his wife's phone, however, he would likely choose the location data. Clearly, data is more sensitive than metadata, but some types of metadata are much more sensitive than others.

Now that conversations, messages, photos and files are flowing across the Internet and through cellular networks, service providers are accumulating much more metadata, and the scope of this information is raising some serious privacy concerns. *Carpenter v. United States*, gives the Supreme Court the opportunity to address those concerns. Their decision may force a major change in the level of privacy afforded to metadata.

Fourth Amendment Background

The Fourth Amendment states, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." Over time, Fourth Amendment cases have established that:

- contents of letters and packages are protected; addresses are not protected;²
- people are protected from warrantless searches and seizures in which they have a "reasonable expectation of privacy";³
- warrantless wiretapping violates the Fourth Amendment;⁴
- information voluntarily shared with a third-party, such as a bank or telephone service provider, is not protected – the "Third-Party Doctrine".⁵

¹ *Carpenter v. United States*, 819 F.3d 880 (6th Cir. 2016)

² *Ex parte Jackson* 96 U.S. 727 (1878)

³ *Katz v. United States* 389 US 347 (1967)

⁴ *Katz*

⁵ *Smith v. Maryland* 442 US 735 (1979)

⁶ https://www.law.cornell.edu/wex/probable_cause_retrieved_6/12/2017

⁷ 18 U.S.C. Chapter 121 §§ 2701–2712

The Amendment does allow limited access to specific protected information with a warrant. To obtain a warrant, the government must show probable cause, and describe the place to be searched, or the person or things to be seized. According to the Legal Information Institute, probable cause usually means “a reasonable basis for believing that a crime may have been committed (for an arrest)” or that “evidence of the crime is present in the place to be searched (for a search).”⁸

The Stored Communications Act (SCA)⁹, passed by Congress in 1986 as part of the Electronic Communications Privacy Act, specifically addressed Fourth Amendment issues with electronic communications. Just as the contents of a letter are protected, but the address on the envelope is not, the SCA grants stronger protection to the contents of communication than to the metadata. The government may need a warrant to compel disclosure of the contents of some electronic communications, but only needs a court order stating that the information is relevant to an ongoing investigation to receive metadata. This is a much lower standard than that required for a warrant – no probable cause is needed and no specificity is required.

Carpenter v. United States

The case the Supreme Court will consider concerns Timothy Carpenter, the mastermind behind a series of robberies of Radio Shack and T-Mobile stores in the Detroit area. He was convicted of six robberies and sentenced to 116 years in prison. The evidence against Carpenter included cellphone location records collected over several months by his cellphone service provider. The records, which the FBI had obtained without a warrant, showed that Carpenter’s cellphone had been in the vicinity of the crime scenes during the robberies. Carpenter appealed his conviction, claiming that the use of this location data violated his Fourth Amendment rights.

Privacy vs. Security

The law must strike a balance between an individual’s right to privacy and a society’s right to security. The recent massive changes in electronic communications suggest the Supreme Court may need to reassess whether we need to shift policy to maintain a reasonable balance. The proliferation of metadata is the main issue, with location data specifically causing great concern. As Justice Sotomayor’s stated in her widely cited concurrence in *United States v. Jones*⁸, “...people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their internet service providers; and the books, groceries, and medications they purchase to online retailers.” She goes on to express doubt that people are really willing to make this tradeoff between privacy and convenience.

And yet, people do make this tradeoff. In the last 30 years, cellphones have changed from a luxury to a necessity. They have also transformed from mobile phones into mobile computers. Cellphone service providers, internet service providers, Google, Apple, Amazon, and scores of other third parties are recording massive volumes of data about our communications, which provides a disturbing amount of information about our behavior and interests.

Most of us are aware that our phones’ locations are tracked. We could avoid tracking by turning them off or leaving them behind. Yet we are increasingly dependent on them. According to the Pew Research Center⁹, as of January 2017, 95% of adults in the United States own cellphones of some kind, and 77% own smartphones. Approximately 10% use smartphones as their primary online access at home. In 2014, the Pew Research Center reported that 50% of survey respondents considered “details of your physical location over time” to be very sensitive information.¹⁰


Apparently, we would like to have a reasonable expectation of privacy for any location data our internet connected devices generate. Given the scope of the tracking data available from our devices, it may be the case that warrantless disclosure has become a potentially serious invasion of privacy. The Supreme Court now has an opportunity to address that question.

Possible Outcomes

Predicting a Supreme Court decision can be extremely difficult, but we can safely say that they will either uphold the Circuit Court’s ruling, or they will not. If they agree with the Circuit Court, cellphone location data will continue to be released to law enforcement with court orders rather than warrants. If the Supreme Court disagrees with the Circuit Court’s ruling, their opinion could be narrowly focused on the protection due to location data, or it might be broadened to consider all metadata, or even the Third-Party Doctrine itself.

The Supreme Court does generally favor targeted, incremental changes, which suggests they may only consider location data. In *Jones*, the Supreme Court ruled that installing a GPS tracking device on a suspect’s car was an unreasonable search, which suggests that they might consider location data to be particularly sensitive. The circumstances in *Jones* were, admittedly, very different from *Carpenter*. *Carpenter* “voluntarily” shared his location information with his cellphone service, a third-party. *Jones* did not know the tracker was on his vehicle and did not voluntarily share the information with a third-party. It is possible, however, that the Court would find that the availability and scope of location data has reached a point that potentially violates Fourth Amendment rights.

Alternatively, the Supreme Court’s decision in *Carpenter* could address the Third-Party Doctrine, itself, which would potentially have far greater implications than an opinion targeting only the protection afforded to location data. Given the wealth of information that we “choose” to share with third parties, perhaps we need to require warrants showing probable cause and asking for specific narrowly targeted information, before third parties disclose data to the government.

Those are just a few possibilities to consider while we wait for the Court’s decision. Unfortunately, one thing is almost certainly true: no matter what the Supreme Court decides in *Carpenter v. United States*, the privacy debate will not end. As technology evolves, the balance between individual privacy and public safety will continue to shift, and laws and regulations will need to evolve as well. 

Editor’s Note: This general-interest article seems particularly pertinent to those of us managing Enterprise data for our companies. It occurred to the Connection staff that this doesn’t just apply to location data!

⁸ *United States v. Jones* 526 US 227 (1999)

⁹ Mobile Fact Sheet, Pew Research Center, <http://www.pewinternet.org/fact-sheet/mobile/> retrieved 6/14/2017

¹⁰ Rainie, L., The State of Privacy in Post-Snowden America, 10/21/2016 <http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/> retrieved 6/14/2017

Who are The Middleware Guys?



Learn more about LightWave Server and how you can integrate your NonStop with nearly any device, including the Amazon Echo, at www.nuwavetech.com/echo

At NuWave, we know middleware.

We have specialized in HPE NonStop middleware for over 15 years, and our software architects have been developing NonStop middleware for decades. We eat, drink, and sleep middleware, so you can be sure you're getting the best.

Our products help you get the most out of your NonStop servers by integrating them with other platforms, and you won't find higher-quality, more intuitive NonStop software for the price.

Why NuWave Middleware?

- ✓ **HIGH QUALITY**
- ✓ **LOW TCO**
- ✓ **EXCELLENT SUPPORT**

LightWave Server: Use REST services to access your NonStop applications from nearly any modern platform

LightWave Client: Access public or private REST services from your NonStop

SOAPam Server: Use SOAP Web services to access your NonStop applications from nearly any platform

SOAPam Client: Access public or private SOAP Web services from your NonStop



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

NuWave
THE MIDDLEWARE GUYS

Achieving Scalability for Mission-Critical Systems in the Cloud

Dr. Bruce D. Holenstein >> President & CEO >> Gravic, Inc.
Dr. Bill Highleyman >> Managing Editor >> Availability Digest
Paul J. Holenstein >> Executive Vice President >> Gravic, Inc.

In our previous paper, “Improving Reliability via Redundant Processing,”¹ we discussed the reliability and the availability of mission-critical systems. We noted that ‘reliability’ is the probability that a system will produce correct outputs. ‘Availability’ is the probability that the system is operational. Reliability and availability are two of the three pillars of mission-critical systems. The third pillar is scalability, leading to the acronym RAS.

In this article, we look to add scalability to mission-critical systems. Scalability means that the system capacity can be expanded easily, and without taking an outage, if the workload on the system increases. Likewise, the system capacity can be scaled back if the workload diminishes.

Modifying system capacity based on a fluctuating workload precludes replacing the servers and databases with different hardware to match a new workload. Such an approach is very expensive and time-consuming, taking perhaps months to order, install, and test new hardware. Certainly, the scale-up or scale-down of the system will lag far behind the workload fluctuations, which might occur on an hourly or daily basis.

Rather, the system architecture must be flexible from a scalability viewpoint. Capacity must be able to increase or decrease easily, perhaps on a daily or weekly basis. For instance, a retail application may need additional capacity as the holiday season approaches. Once the holidays are over, the excess capacity can be retired.

A straightforward approach to achieving scalability is to burst the application to a cloud. Clouds comprise multiple physical servers, each capable of supporting several virtual servers. Thus, an application that suddenly needs additional capacity can be extended to a cloud and given access to one or more of the cloud’s virtual servers. When the application’s excess capacity needs have diminished, the application releases the virtual server resources that it consumed in the cloud.

Other ways to achieve such scalability include active/active systems and Pathway Domains. We look at these techniques first, and then move on to scalability using cloud resources.

¹ Improving Reliability via Redundant Processing, The Connection; March/April 2017.

Active/Active Systems

What Is An Active/Active System?

An active/active system comprises two or more servers and two or more copies of the application database. Each server has access to a copy of the database (Figure 1). The databases keep synchronized via bidirectional data replication. Whenever a change is made to one database, that change is replicated immediately to the other databases in the system.

Therefore, any server in the active/active system can process any transaction and achieve the same result that would occur if any other server had serviced the transaction in the system.

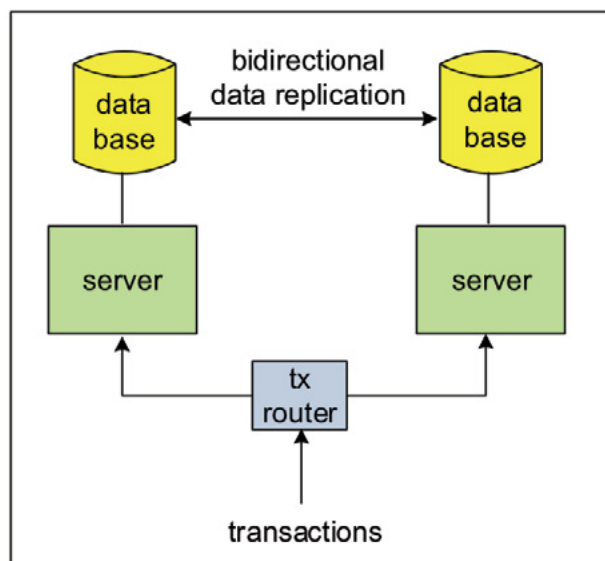


Figure 1: An Active/Active System

Consequently, an active/active system provides continuous availability. If a server fails in an active/active system, further transactions are simply routed to surviving servers. Recovery is so fast that users will be unaware that an outage took place. To restore a server to service, it is rebooted with the application(s), attached to a database copy, and added back into the transaction-routing facility.

To achieve continuous availability, there must be at least two copies of the application database in the system. If there are only two servers, each server typically will have its own copy of the database, as shown in Figure 1. To improve availability, each server in a two-server configuration also has access to the database on the other server in case it loses its own database, as shown in Figure 2.

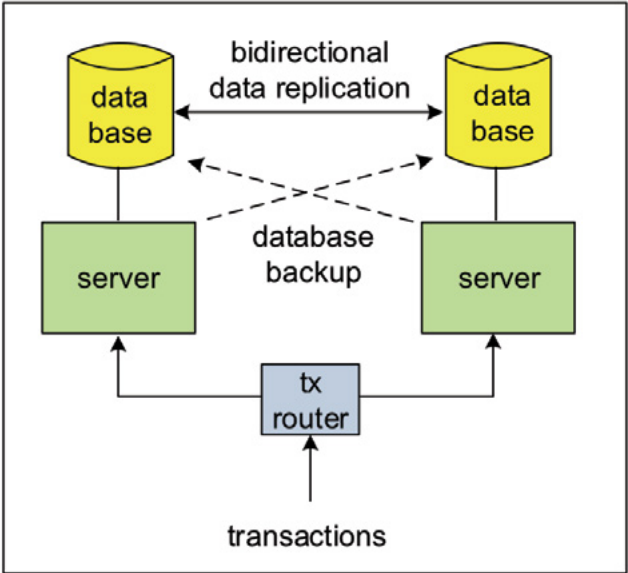


Figure 2: Active/Active System with Database Backup

Active/Active Systems Are Inherently Scalable

Capacity can be added to an active/active system by adding additional servers, as shown in Figure 3. Each server must have access to a copy of the database so that a transaction can be sent to any server. If there is excess capacity, some of the servers can be retired and moved to other applications. Consequently, an active/active system is scalable, both in terms of adding capacity and in terms of reducing capacity.

In general, there is only a need for two copies of the application database to ensure continuous availability, though more copies can be provided. Each of the multiple servers in the active/active

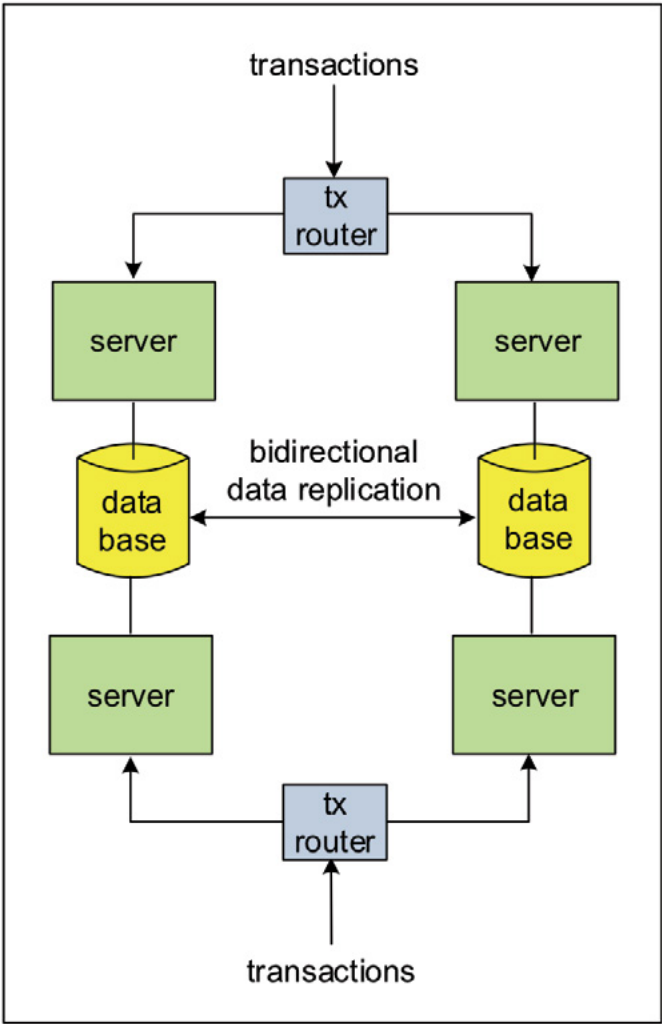


Figure 3: Scaling an Active/Active System

system must have access to at least one copy of the application database. However, if access is provided to only one database, the attached server becomes inoperable if the database fails.

System availability can be improved by giving every server the capability to reconnect to an operational database. Thus, if a database fails, the affected servers can reconnect to another copy of the database and then continue to operate.

Scaling an active/active system can be accomplished with no

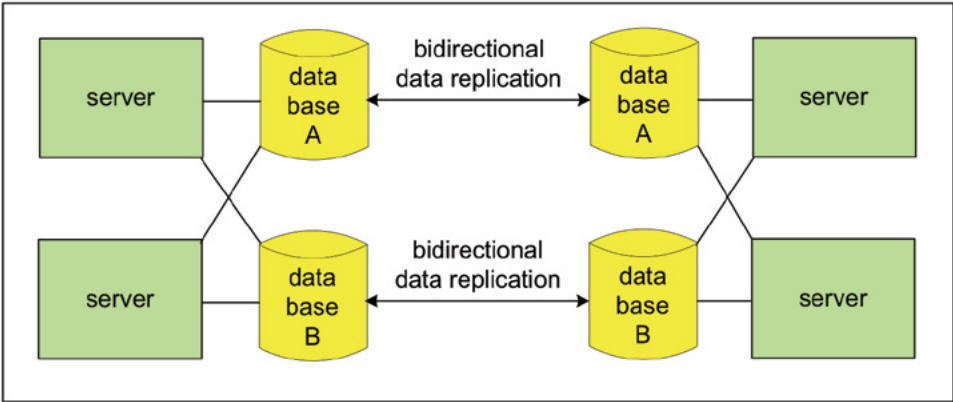


Figure 4: Active/Active System with Direct Access to a Partitioned Database

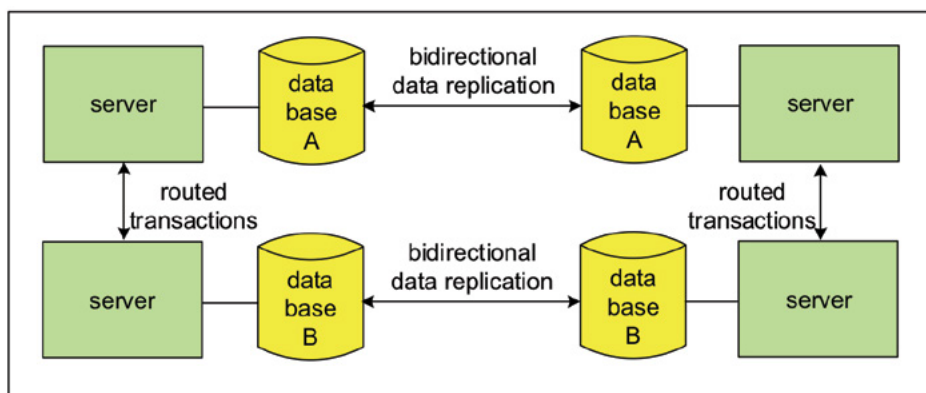


Figure 5: Active/Active System with Indirect Access to a Partitioned Database

downtime. If a server is added to increase capacity, it is brought online and allowed to attach to a copy of the database. Then the transaction routing table is expanded to include the new server, and it can begin to process transactions along with the other servers.

If a server is removed from the system to decrease capacity, its identity is first removed from the transaction routing table. Next, the server completes the processing of any transactions with which it already is involved. Only then, is the server shut down and removed from the active/active system.

Scaling an Active/Active Database via Partitioning

The database in an active/active system can be scaled via partitioning. Many application databases are large and partitioned across several disk volumes. As with a single database disk, every partition must be redundant. There must be at least two copies of each partition to maintain availability of the system in the event of a disk failure.

Every server in the active/active system must have access to all partitions. One method of access is shown in Figure 4. Each server attaches to one copy of every database partition (partition A and partition B in Figure 4). In this way, each server has direct access to the entire database.

An alternative technique is for a server to access a copy of an unattached partition by routing requests to a server attached to the partition, as shown in Figure 5.

Pathway Domains

What Is Pathway?

A software facility known as 'Pathway' provides the facility for fault tolerance and scalability for application programs in HPE NonStop systems. Applications written in a Pathway environment provide fault tolerance and scalability with little effort on the part of the application programmer.

Pathway Architecture

Pathway applications comprise a collection of server classes, as shown in Figure 6. A server class contains one or more identical stateless application servers (processes) designed to process a particular transaction (or set of transactions). Typically, a server in a server class receives a transaction from a requesting client and routes the database updates to the appropriate databases. The HPE NonStop Transaction Management Facility (TMF) is responsible for maintaining the Atomicity, Consistency, Isolation, and Durability (ACID) properties of the transaction as it updates the database. NonStop systems support three databases -

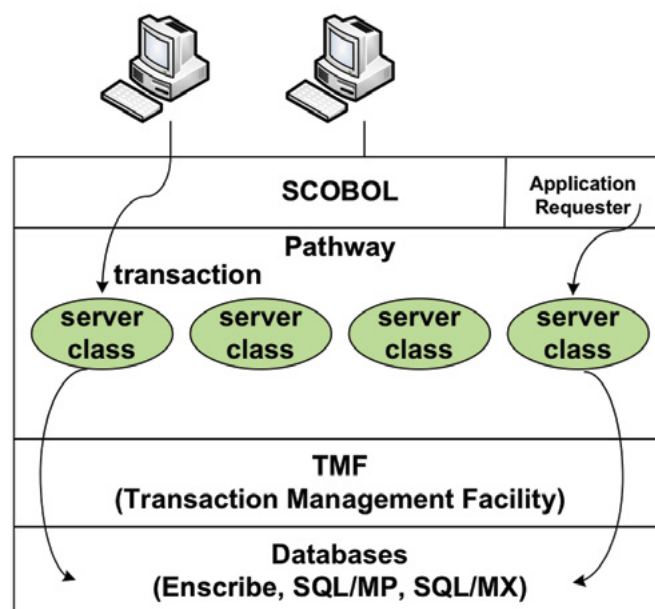


Figure 6: A Pathway Environment

Enscribe, a relational file system, SQL/MP, a SQL database, and SQL/MX, a newer SQL database that complies more closely with the ANSI SQL standard.

Pathway Scalability

The server classes provide the scalability of the Pathway environment. The servers in a server class can be spread among several processors in a NonStop system, with transaction requests automatically distributed between them. If a server class becomes overloaded, Pathway can spawn additional server processes for the server class. If the load on a server class falls to the point where not all of its servers are needed, it terminates some of them.

Communication between processes in the NonStop system is via interprocess messages, where there is no common memory used. Therefore, there is no fundamental limit to the expandability of a system, which is a near-linear function of the number of processors in the system. In fact, it is possible to link up to 255 systems (4,080 processors) in a cluster; each additional processor increases the system capacity by 98% of that processor's capacity, (which is not the case for symmetric multiprocessor (SMP) systems).

Pathway Domains

While Pathway provides scalability across a single NonStop system, Pathway Domains enables scalability across multiple NonStop systems². Multiple identical Pathway environments can be configured as a Pathway Domain that behaves as a single, large Pathway application. Any of the Pathway environments within a domain can be taken down for maintenance while the remaining environments within the domain continue processing work with no interruption. This ability enables online updating of server code and rebalancing of Pathway environments without planned outages. It also relaxes the configuration limits of a single Pathway system, removing barriers to scalability. Server classes are replicated across all Pathway environments in the domain, and requests are automatically load-balanced across the domain.

Since a remote Pathway environment can be configured as part of a domain, a logical Pathway server class can span multiple (up to four) NonStop systems. This configuration allows a NonStop node in a domain to be taken down for maintenance while the application remains available on other nodes. Pathway automatically routes requests only to the available nodes in a domain. This routing also increases scalability because a Pathway application can span multiple NonStop nodes, which may actually be part of a bigger ServerNet or Infiniband cluster containing hundreds of NonStop processors. So if a Pathway application reaches the scalability limits of a single NonStop system, simply distribute it across multiple NonStop nodes using Pathway Domains.

Of course, since each server node in the Pathway Domain must have access to the application database, each system is provided access to a copy of the database. The database copies are kept synchronized via bidirectional replication.

Bursting to the Cloud for Scalability

With the advent of cloud technology, a new method of scalability has evolved. Applications can scale internally as described above; but if they need further capacity, they can be burst to a private cloud³, a public cloud, or a hybrid mix of private and public clouds. A copy of the database must be in the cloud or be available to applications running in the cloud.

When an application requires more capacity than is available via its physical servers, a copy of the application can be sent to the cloud. The cloud spawns virtual servers on which the application can run. As the application demands even more capacity, the cloud provides further virtual server resources. If the capacity needs of the application diminish, the cloud releases some of the assigned resources. In this way, the application is scaled to handle its workload.

Clouds, whether public or private, comprise inexpensive commodity hardware, which supports scalability quite well. However, how does one support the reliability and availability aspects of RAS in clouds? Though not dealing with clouds, we explored reliability and availability to a great extent in our two-part paper “Improving Availability via Staggered Systems,” published in the November/December 2016 and January/February 2017 issues of *The Connection*.⁴ By staggering the start time of a system and its backup, the probability distributions of failure will not line up. Therefore, when one system is most likely to fail, the other system is much less likely to fail. If the starting times are not staggered, the times

for the peak probability of failure will align; and increase the likelihood of both systems being down at the same time.

When bursting an application to the cloud for scalability, an important technique to guarantee reliability and availability is to run redundant systems in a Validation Configuration. In this architecture, redundant arrays of inexpensive computers (RAIC) are deployed in a cloud (public or private), as shown in Figure 7. As discussed in our previous paper, “Improving Reliability via Redundant Processing,” each RAIC system in a redundant pair periodically exchanges ‘indicia.’ An indicium is a representation of the current state of the system. Each system in the redundant pair compares the indicia sent by its mate to its own indicia. If the indicia agree, the systems are behaving properly; and processing continues. If the indicia do not agree, the systems are halted; and diagnostics are run to identify the faulty system.

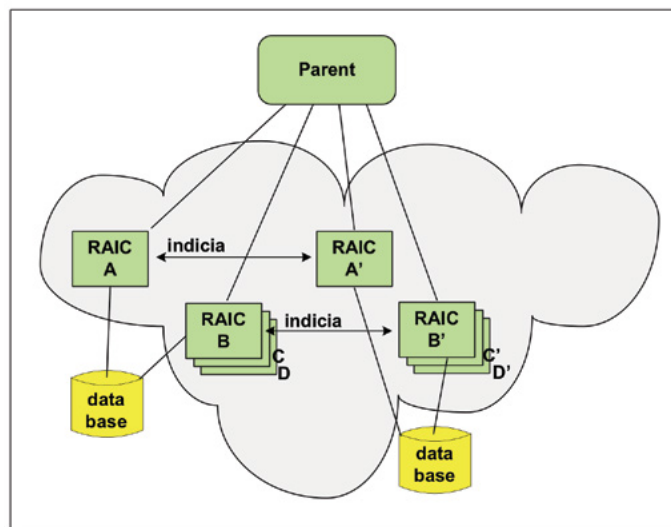


Figure 7: Bursting to a Single Cloud for Scalability

Figure 7 shows the RAIC systems running in the same cloud. To protect against cloud failures, RAIC redundant pairs could be run in separate clouds, as shown in Figure 8. Bursting to multiple clouds is most effective from an availability perspective if the clouds are provided by different vendors, such as Microsoft Azure, Amazon AWS, or the Google Cloud Platform. However, it requires that the application be written for deployment in multiple clouds.

Summary

Applications often require additional capacity during critical times. Scalability is an inherent and important attribute of mission-critical systems. Both the servers and the database must be scalable. Active/active systems can provide scalability to servers as well as to the database. However, adding physical servers and disk systems to achieve greater capacity is typically not feasible, especially if the additional capacity needs are temporary.

Scalability can be achieved via the use of Pathway Domains that span multiple NonStop systems, providing significant scalability. It can also be achieved by bursting applications to RAIC servers in one or more clouds. RAIC servers use inexpensive commodity hardware and can be reused between applications,

² See for background HP Pathway Domains and Data Replication – Perfect Together!, *The Connection*; September/October 2014.

³ See for background Adding High Availability to the Cloud, *The Connection*; July/August 2014.

⁴ Improving Availability via Staggered Systems Part 1: MTTF- Mean Time to Failure, *The Connection*; November/December 2016.

Improving Availability via Staggered Systems Part 2: Mitigating Redundant Failures via System Staggering, *The Connection*; January/February 2017.

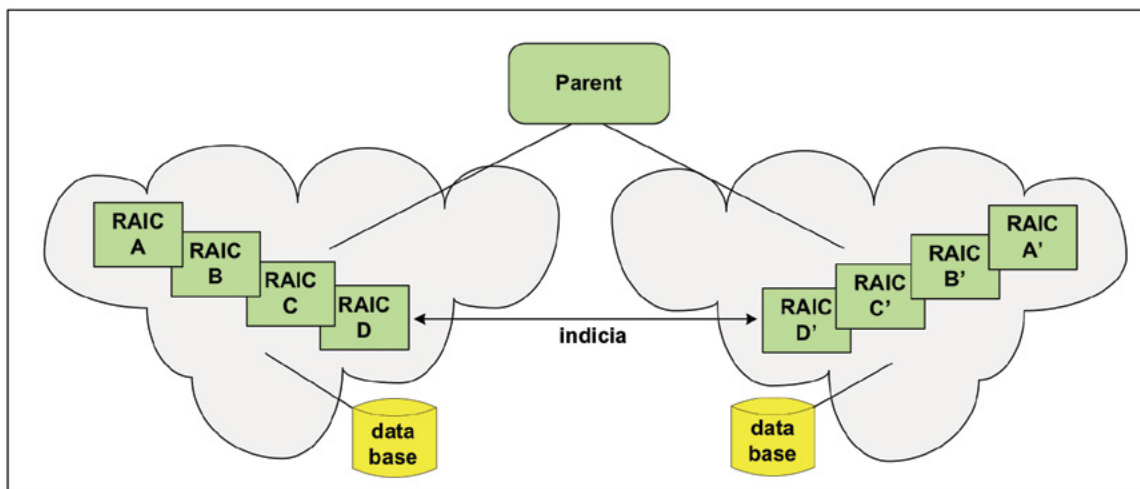


Figure 8: Bursting to Multiple Clouds for Scalability and Reliability

as scalability needs change, thus providing an economic cloud platform for scalability-on-demand.

R	Reliability	Use Validation Configurations that match indicia to ensure that there are no data errors
A	Availability	Provide redundancy in all critical components. Use staggered starts to eliminate correlated failure modes.
S	Scalability	Use Pathway Domains to span NonStop systems. Burst applications needing additional capacity to a cloud.

We find that the attributes of RAS can be achieved as follows:

For HPE NonStop users, maximizing the RAS for mission-critical systems can now be accomplished by leveraging the new Virtualized NonStop technology. [SD](#)

Dr. Bruce D. Holenstein, President and CEO. Dr. Holenstein leads all aspects of Gravic, Inc. as President and CEO. He started company operations with his brother, Paul, in 1980, and is presently leading the company through the changes needed to accommodate significant future growth. His technical fields of expertise include algorithms, mathematical modeling, availability architectures, data replication, pattern recognition systems, process control and turnkey software development. Dr. Holenstein is a well-known author of articles and books on high availability systems. He received his BSEE from Bucknell University and his Ph.D. in Astronomy and Astrophysics from the University of Pennsylvania.

Dr. Bill Highleyman is the Managing Editor of The Availability Digest (www.availabilitydigest.com), a monthly, online publication and a resource of information on high- and continuous availability topics. His years of experience in the design and implementation of mission-critical systems have made him a popular seminar speaker and a sought-after technical writer. Dr. Highleyman is a past chairman of ITUG, the former HP NonStop Users' Group, the holder of numerous U.S. patents, the author of Performance Analysis of Transaction Processing Systems, and the co-author of the three-volume series, Breaking the Availability Barrier.

Paul J. Holenstein is Executive Vice President, Gravic, Inc. He has direct responsibility for the Gravic, Inc. Shadowbase Products Group and is a Senior Fellow at Gravic Labs, the company's intellectual property group. He has previously held various positions in technology consulting companies, from software engineer through technical management to business development, beginning his career as a Tandem (HPE NonStop) developer in 1980. His technical areas of expertise include high availability designs and architectures, data replication technologies, heterogeneous application and data integration, and communications and performance analysis. Mr. Holenstein holds many patents in the field of data replication and synchronization, writes extensively on high and continuous availability topics, and co-authored Breaking the Availability Barrier, a three-volume book series. He received his BSCE from Bucknell University, a MSCS from Villanova University, and is an HPE Master Accredited Systems Engineer (MASE). To contact the author, please email: SBProductManagement@gravic.com. Hewlett Packard Enterprise directly sells and supports HPE Shadowbase Solutions (www.ShadowbaseSoftware.com); please contact your local HPE account team.

2 Powerful Ways to Protect Sensitive Data on NonStop Systems

Jonathan Deveaux >> Manager – Marketing and Partner Development >> comForte Inc.

When it comes to protecting personal data, many individuals use good security hygiene to minimize the potential of their data getting into the wrong hands: shred documents with names, addresses, social security numbers or Tax IDs; activate fingerprint technology on mobile phones; cover the pin-pad at ATMs when withdrawing money.

What are companies doing to protect YOUR data as it passes through or remains on their systems?

But, when it comes to Enterprise Data Protection, what are companies doing to protect YOUR data as it passes through or remains on their systems?

Proof that many organizations still struggle with this question is the fact that data breaches are more prevalent in the news – websites like https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf for healthcare related breaches, and <https://www.databreaches.net/> for data breaches in general, frequently list companies who have had sensitive customer or employee records exposed or lost.

As the writer of this article, I chose to conduct a small experiment – List companies that I used or visited in the past week, and determine if they have ever lost customer data, including mine. My list contains LinkedIn, Twitter, and Yahoo

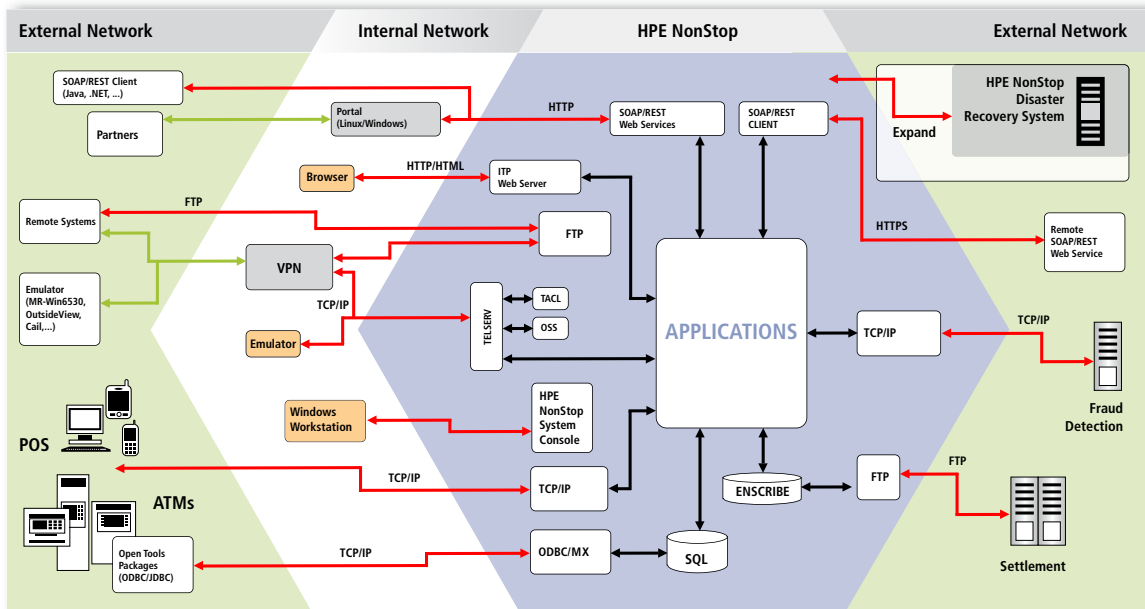
Mail, retail stores such as Target, CVS, and Sprouts, and entertainment websites including Netflix and ESPN. 7 of the 8 companies on my list have experienced a data breach in the past of some sort! A variety of data was reported as exposed or stolen – user ids and passwords, some personal data such as addresses, and also credit card numbers. What does this list look like if you conducted the same experiment?

These companies are not alone. According to <http://breachlevelindex.com/> there have been **over 7 billion records exposed or stolen since 2013** – thousands of companies around the world have been breached! That is a serious number, especially when some studies show that each lost or stolen record containing sensitive data can cost an organization almost \$160 per record. This number could go higher, once the final amounts from the brand damage, customer loss, and potentially from falling share prices are calculated.

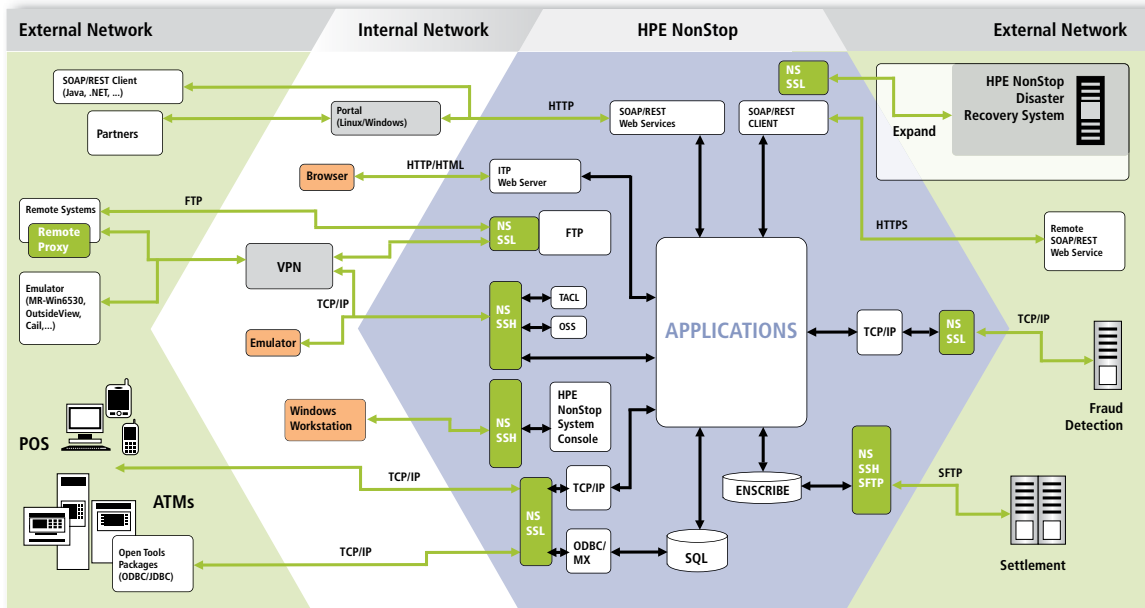
It is not as if companies are doing nothing to prevent data breaches. Typically, most organizations have pretty good perimeter security of some kind – routers, firewalls, network segmentation, etc. And many companies use Intrusion detection and anti-virus protection as well. Unfortunately, hackers and attackers still get through, and, unintended incidents and accidents happen as well.

Another approach is to take a deeper look at data protection around data in motion, and data at rest – in these 2 areas, enterprises can enable strong security technology to protect data. This means encrypting the connections of data flowing to and from each NonStop, and tokenizing or encrypting the data where it resides (most likely in files and databases). Both help reduce the likelihood of data being changed, captured or stolen by intruders, and even if data is accidentally exposed outside of the secured area, the data is rendered useless.

Example of **unsecured** Data in Motion with HPE NonStop



Example of **secured** Data in Motion with HPE NonStop



Protecting Data In Motion

When data is exchanged between systems, user names, passwords, files, and sensitive application data are exposed. As companies expand their business, so does the need to communicate with more systems over the internal network and over the internet. This need increases the challenges to secure these connections. By enabling encryption, companies can make sure that no data is transmitted between systems “in-the-clear” or ensure that no ‘clear text’ data is viewable by unauthorized users.

Both HPE NonStop SSL and HPE NonStop SSH software provide strong encryption of connections to and from your NonStop systems and are included in the NonStop L-series Operating System (included in the NonStop Security Bundle for J-series).

The HPE NonStop SSL software provides strong, reliable encryption to protect transmitted data over internal and external networks. NonStop SSL encrypts the segments of network connections at the transport layer – basically it encrypts the data packet before it is sent, and decrypts the data packet for

use after it arrives on the destination system. The NonStop SSL software should probably be renamed to “NonStop SSL/TLS” as the software secures connections for all versions of SSL and TLS up to and including TLS 1.2. Extra security from strong ciphers including 256-bit AES (Advanced Encryption Standard) among others are included.

When a shared communication line is used between systems, data protection is still needed. The NonStop SSH (Secure Shell) software provides communications security in this case for applications connectivity, system administration, and file transfers. NonStop SSH supports various ciphers including AES and has public key authentication support for key sizes of up to 2048 bits.

We have created 2 example diagrams that show some common connections around NonStop systems, for data in motion – one diagram shows sample connections of unprotected data in motion, and another is showing the same connections, but secured by NonStop SSL and NonStop SSH. These diagrams are only examples, with the intention of showing how a variety of connections can be secured. Check out the HPE NonStop Security Hardening Guide for recommendations, best practices, and options if tighter control over data protection is needed.

Protecting Data at Rest

Even though data in motion is encrypted via NonStop SSL or NonStop SSH to the NonStop system as described above, the data is decrypted when it arrives for use by the application. Therefore, data is exposed and ‘in-the-clear’ so the application on the NonStop system can use the data as expected. Most applications have a requirement to store the data – most likely in a file or database. Therefore, to ensure the data does not reside in a file or database ‘in-the-clear’, the data should be protected via tokenization or encryption.

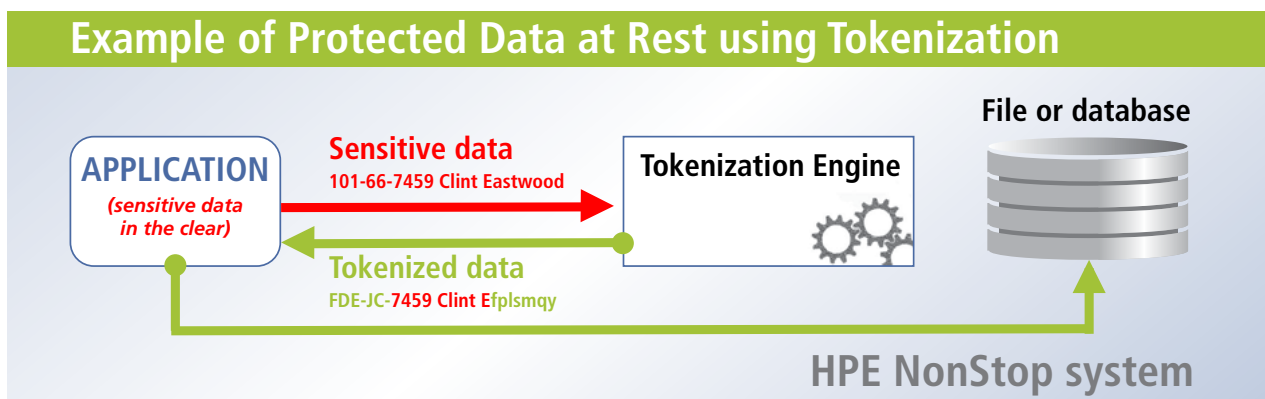
So, what can be done to protect credit card numbers, personal info, social security numbers, healthcare records and other sensitive data? To accomplish this, there are several licensable options available by HPE, HPE Security, and 3rd Party vendors such as comForte, XYPRO, and possibly others. Depending on requirements, either tokenization or encryption will in most cases help minimize data exposure and risk of a data breach and help reduce compliance burden.

Encryption involves the process of scrambling original data by using an encryption algorithm, into a cipher text, so that the cipher text cannot be easily descrambled without using the proper encryption key. On HPE NonStop systems, there are various technology choices available, however this article does not intend to delve into the options. For the sake of discussion, it is worth mentioning that some options include encrypting the whole disk volumes, encrypting columns of data in SQL tables, or encrypting only certain fields of data. Typically with encryption, there is some level of key management required – issuance of keys used to encrypt and decrypt the data, rotating keys, etc. Some solutions offer options which reduce operational stress around managing keys. HPE or the 3rd Party vendors will have more information for encryption cases which fit your needs.

With tokenization, data is replaced with a surrogate value (a token), which is also created by an algorithm. The token created is a mix of characters and numbers and in most cases, the token value resembles the format of the original data, in terms of field length and other characteristics. The application takes the surrogate value and writes that value to the file or database.

A key difference between tokenization and encryption of data at rest becomes apparent when the data needs to be used.

With encryption, the encrypted data will in most cases need to be decrypted before it can be used by an application. For example, if data from a payment application resides in a



database and is encrypted, then the post-processing application expecting to use the payment original data, will need to decrypt the data before it can process the data.

But with tokenization, since most tokens resemble the format and characteristics of the original data, the post-processing application can use the tokenized data since the format remains the same. In cases where the original data is actually needed, a detokenization step is required using the algorithm in order to generate the original data.. HPE and the aforementioned 3rd Party vendors have more information based on requirements.

Both methods accomplish the goal of protecting the data at rest, and this provides organizations with solid options for keeping sensitive data from being exposed due to a data breach.

What's driving businesses to protect sensitive data?

There are many reasons why data protection is a key topic of discussion for many companies.

Meeting compliance and passing regulatory requirements are top drivers. PCI-DSS (The Payment Card Industry - Data Security Standard) and HIPAA (Health Insurance Portability and Accountability Act) are two common and well known organizations who create data protection guidelines in the payments and healthcare industries respectively.

Compliance is a heavy burden for many organizations from a cost and time perspective. Fines can be issued for failure to comply, which can be anywhere from the tens of thousands of dollars for the first-time offense, to millions of dollars (February 2017 - Memorial Healthcare System has paid the U.S. Department of Health and Human Services \$5.5 million to settle potential HIPAA violations - <https://www.hhs.gov/about/news/2017/02/16/hipaa-settlement-shines-light-on-the-importance-of-audit-controls.html>). Failure to comply may also lead to a shutdown of business operations, as these organizations have the authority to shutdown an organization if they determine they are not able to protect sensitive data.

Reducing compliance burden isn't the only driver, though. LinkedIn, Target, Yahoo and others listed at the beginning (as well as most companies for that matter), have a desire to build trusted customer relationships. This is another driver, which in turn leads to customer loyalty and customer retention. Letting

customers know they care about their data, and have put in place the means to protect data is one way to build and retain trust – even after a previous data breach. Some people may think that their data is safer with a company after a data breach, as “now they are doing something about it!”

Another driver motivating companies to protect sensitive data is to stay competitive, and to gain new or future business. Some organizations will only work with companies with the ability to send data that is already protected, rather than having to carry the burden of protecting the data themselves. Companies who have the ability to protect data in this aspect will be in a better position to satisfy this requirement.

In essence, data protection helps to


- Secure business with existing customers
- Drive additional revenue from new customers
- Increase top-line growth

It is no surprise that successful organizations today are starting to treat data protection as a strategic asset rather than a liability.

Protecting data in motion and data at rest, provides companies with the ability to secure their most valuable asset – data – especially in critical areas where the data is most vulnerable.

The first step is simple – turn on NonStop SSL and NonStop SSH, which are included with the NonStop Operating System (L-series, and in the NonStop Security Bundle for J-series). Work with your HPE solution architects to review all of your connections and ensure you enable encryption to protect data as it is transmitted between systems.

Regarding data at rest protection, explore options by HPE, HPE Security, and the 3rd Party vendors. Ask for references, setup a proof of concept (or proof of value as they are now called), and determine which functions fit the common or unique requirements for your NonStop systems.

Take action and do something to protect sensitive data today. NonStop systems have been associated with running mission critical applications – now, it is data-centric protection that must become mission critical in order to minimize risks of a data breach and maintain high customer expectations! 

For more info check out:

<https://www.comforte.com/products/protect/secure/dps/>

.....

Jonathan has been at comForte Inc for almost 2 years, but has been associated with NonStop systems since the mid-90's. He has worked on the customer side of NonStop systems while at Bank of America and First Data Resources, and on the vendor side at IR and comForte. Jonathan has held various positions in Sales, Management, Marketing, and Product Management. Contact Jonathan at J.Deveaux@comforte.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!



How HPE is Making Blockchain Resilient

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

Blockchain. Oh, no! Another new technology about which I know nothing. That statement summarized my feelings about blockchain until I heard a presentation from HPE's Matt Riesz at the May 2017 NYTUG meeting in Berkley Heights, New Jersey (USA). Matt is a superb speaker. His clear, concise explanation of how blockchain works elevated my understanding from total ignorance to a "not nearly as dumb as I thought I was" level. This article is based on Matt's presentation.

Matt also explained how HPE has partnered with R3, the provider of the Corda open-source distributed ledger technology (DLT) platform, to bring resilience and scalability to DLT applications. R3 leads a consortium of more than 70 of the world's largest financial institutions in the research and development of blockchain database usage within financial systems. It was the consortium's efforts that brought Corda into fruition.¹

At the recent HPE Discover conference in Las Vegas, R3 demonstrated Corda, now in public beta, running on Integrity NonStop.

What Is a Blockchain?

A blockchain is a secure, append-only distributed database that is created by a collection of untrusted or semi-trusted parties. The distributed nature of a blockchain allows parties to engage in transactions without a trusted central authority. A copy of the blockchain is made available to all involved parties.

Transactions are organized into blocks. Each block contains a timestamp and a link to the previous block. A checksum in each block header is calculated based on the block contents and on the checksum of the previous block. Thus, blockchains are inherently resistant to modification of the data within a block. Once recorded, the data in any given block cannot be altered retroactively without the alteration of checksums in all subsequent blocks. This makes blockchains suitable for the recording of transactions that must maintain their integrity. Oftentimes, users will ignore new transactions until several new blocks have been appended to the blockchain to ensure that the transactions they are accessing are secure.

Blockchain systems assume that some parties engaged in a transaction may be dishonest. These systems need only a majority of participants to be honest. Any party involved in a blockchain may create a new block to be added to the chain. However, all

parties involved in the blockchain vote on any new block that is to be added. If a majority of the parties do not agree that the block is valid, it cannot be added.

Marc Andreessen has said that the blockchain's distributed consensus model is the most important invention since the Internet itself. Marc is the co-author of Mosaic, the first widely used Web browser, and the co-founder of Netscape.

Others have said that the blockchain will transform value exchange as profoundly as the Internet transformed information exchange.



The First Blockchain Use – Bitcoins

Blockchains were introduced with Bitcoins. Bitcoin is a cryptocurrency. No physical bitcoins exist. Rather, transactions take place directly between users without an intermediary. The transactions are recorded in a public distributed ledger, a blockchain. Since the system works without a central repository, bitcoins are the first decentralized digital currency.

Bitcoins are stored in a digital wallet, which may be either in the cloud or on someone's computer. Bitcoins are totally anonymous. There is no need for either the buyer or the seller to provide identification. Only the digital wallet ID is exposed. People can transfer bitcoins with each other via their digital wallets using either mobile apps or their computers.

¹ R3 has explained that Corda, although inspired by blockchain architecture, is itself not a traditional blockchain platform.

² Just in – Exciting news about HPE and Blockchain

<https://community.hpe.com/t5/Alliances/Just-in-Exciting-news-about-HPE-and-Blockchain/ba-p/6967334#.WVVnahPyui4>

Bitcoins can be bought and sold on bitcoin exchanges. The largest bitcoin exchange, Mt. Gox, went belly-up in 2014 after hackers stole almost a million bitcoins from it.

Bitcoins currently move about USD \$185 million via 220,000 transactions a day. The total value of all outstanding bitcoins is approximately USD \$10 billion.

Blockchain's Rapid Evolution

Blockchain is effectively a Distributed Ledger Technology (DLT), and DLTs are transforming business models in the Financial Services Industry (FSI). FSI is making significant investments in proof-of-concepts to support blockchain business cases.

However, current DLT vendors cannot support scalable, enterprise-grade solutions. Their implementation models have proven to be too slow for rapidly evolving business and technology demands. They also are not mature enough at this time to meet the enterprise and governance requirements of security, risk, manageability, and performance, among other prerequisites. DLT technology must meet the pace of change required by an organization.

Hurdles to DLT Adoption

What is required is an open and modular application framework for the development of blockchain applications rather than the fragmented set of platform providers and point solutions that exist today. Performance, scalability, and resiliency are below enterprise standards with high numbers of single points of failure. These challenges must be met by robust blockchain foundational services such as accelerated smart contract virtual machines and highly available environments such as HPE NonStop servers. There is no blockchain-specific infrastructure or reference architecture at this time that provides a fault-tolerant environment to run blockchain workloads at scale.

What's more, the small startups that currently dominate the blockchain market do not integrate well if at all with existing technologies and standards. As such, it has been difficult to engage business units, partners, the industry, regulators, and others for support and funding.

The R3 Consortium

A major player in the blockchain world is R3. As we mentioned in our introduction, R3 in conjunction with its consortium of financial institutions created Corda, an open-source distributed ledger platform. Corda is a distributed ledger in that it is distributed across multiple platforms and is shared with multiple participants. Each participant has access to at least the part of the ledger with which it is engaged, and participants collectively can assemble an entire ledger.

Corda is especially attractive to the financial industry because it can handle very complex transactions and restricts access to transaction data. The aim of Corda is to provide a platform with common services to ensure that any services built on top of it are compatible with the network participants.

How HPE Can Help

One of the interesting aspects of blockchain is that it is by its very nature resilient to faults. If a node fails for any reason, all of the other nodes have a copy of the chain so that it never disappears.

By comparison, Corda, being a SQL database, does have some possible fault-tolerant issues. For instance, if a node dies, so does its portion of the distributed ledger.

Enter HPE NonStop, which has both a highly resilient and

high-performance database, SQL/MX, and a continuously available platform. HPE has announced that it has entered into a partnership with R3 to bring Corda to Mission-Critical HPE Systems.² "HPE and R3 will bring Distributed Ledger Technology to workloads that must run at enterprise scale. A proof of concept created in collaboration with HPE Labs, HPE Mission Critical Systems, and R3 has demonstrated R3 Corda running on the HPE Integrity NonStop platform, delivering the resiliency and scalability enterprise customers need as they bring their DLT applications into production."

Via such partnerships, HPE can accelerate the selection of blockchain applications based on business demands. It can enable Line of Business leadership to incorporate DLT solutions that will address enterprise business goals. As with any new technology, there are risks; but HPE is well-positioned to evaluate the challenges of a blockchain approach and to propose viable risk mitigations.

From the R3 perspective, HPE Integrity NonStop offers a proven reference architecture, one that delivers reliability, performance, and scalability improvements as compared to other platform implementations. HPE offers educational, advisory, and implementation services augmented by Blockchain-as-a-Service offerings. In addition to R3, it maintains a multi-platform ecosystem with partners such as Ethereum and Microsoft.

Ethereum is a full distributed blockchain implementation backed by a tradeable cryptocurrency. It offers availability with predictable performance and resilience. It uses accelerated cryptography, shared memory, and an enterprise-grade support ecosystem.

The Corda Distributed Ledger

HPE NonStop with R3 Corda uses an enterprise-grade message bus (HPE NSMQ) and a persistent data store (SQL/MX). It provides linear scaleout and is suitable for physical and virtual NonStop platforms.

Corda provides the fundamental services of a blockchain but is not itself a blockchain. A blockchain involves a specific architecture for implementing distributed ledgers. Corda has a different physical implementation. The storage method for Corda is ANSI SQL rather than blockchain. This allows the ledger to be queried with common query tools, though the data in the Corda ledger is encrypted. One would need the encryption key in order to query the data in Corda.

Corda does not require each state change to be broadcast to all nodes. Unlike blockchains, it is designed from the beginning as a distributed ledger to offer more robust and flexible storage of complete smart contracts.

With Corda, there is no unnecessary global sharing of data. Only those parties with a legitimate need to know can see the data within an agreement. Corda explicitly links human-language legal prose documents to smart contract code for choreographed workflow between firms without a central computer. It enables regulatory supervisory observer nodes. Transactions are validated by parties to the transaction rather than by a broader pool of unrelated validators.

A Corda smart contract is an agreement automated by computer code working with human input and control. The rights and obligations of the contract are legally enforceable, ensuring that the financial agreements are rooted firmly in law.

A Summary Comparison of Blockchain and Corda

The table (on page 30) summarizes the comparative attributes of blockchain and Corda:


Property	Private Blockchain	Corda
Data replication	Broadcast to all bitcoin miner nodes	Only participant nodes hold data
Data protection	Cryptographic chain of blocks	Cryptographic chain of records
Data structure	Flat/unstructured	SQL/structured
Reliability - platform	Transparent node failure	Node failure disruptive/outage
Reliability - data	Data corruption transparent	Avoided if using RAID
Scalability	Scale-up; no real scale-out	Scale-up and scale-out
Parallelism	Not fully used	Fully used
Transaction consistency	Eventful - BASE	Immediate - ACID
Consensus	BFT ³ & various - system wide	BFT & various - private
Transaction validation	Bitcoin miners	Notary and participants
Smart contracts	Add-on to architecture	Built into architecture - Java VM
Performance	Can be burdened by miner time	Potentially better than blockchain
Cryptocurrency	Bitcoin or other	None

Distributed Ledger Technology has applicability in several areas, including:

- Financial – funds transfers, clearing/settlement, brokerage, mortgage.
- Medical – record keeping/sharing.
- Insurance – claims processing, document handling, liability insurance.
- Government records – property transfers, titles, licenses, elections/voting.
- Retail – gift cards, loyalty programs.
- Legal – digital notarizations, certificates, smart contracts.
- Education – records, grades, curriculum/course registration.
- Transportation – document tracking, digital signatures, fraud prevention.
- Energy – opportunities at electrical ‘grid-edge.’
- Libraries/documents/publishers – document handling and tracking, ties to payments.
- Smart contracts – two-party/multi-party.
- Controlled permissions – broad or restricted permissions for different party members.
- Provenance of creative assets – publicly verifiable registry [music, arts, patents].

Summary

R3's Corda is designed specifically for the Financial Services industry, a major consumer of Integrity NonStop's ability to quickly scale resources for real-time, high-volume transactions. R3 brings to the new partnership its expertise in distributed ledger and blockchain technologies. What it relies on from HPE is NonStop's acclaimed fault-tolerant environment, an impressive suite of HPE and partner solutions, and a large customer base that looks to HPE for assistance as new DLT applications are brought into production.

We once again want to thank HPE's Matt Riesz for the use of his blockchain slide presentation as the foundation of this article. 

This article has been reprinted from the July 2017 issue of The Availability Digest.

³ BFT – Byzantine Fault Tolerance, the characteristic of a system that tolerates the class of failures known as the Byzantine Generals' Problem for which there is an unsolvability proof.

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. Find his books on Amazon. Contact him at billh@sombers.com.

NSU40 Update

After a worthy start at the NonStop Technical Boot Camp in San Jose, NSU40 is still going strong, having had its most recent meeting in London at the eBITUG conference. Jimmy Treybig, founder of Tandem Computers, attended the NSU40 meeting in London and stressed, among other things, how NonStop should be presented as a solution and not a technology. It was great advice to a group that is looking for new ways to market the solution to the next generation. The meeting was a success with the entire Board present to take feedback from the room and promote discussion.

Besides the eBITUG meeting and the website going up (www.NSU40.com) several months ago, the group is starting to produce educational videos as a way to modernize the current NonStop educational resources. The first one will be a simple intro to NonStop and is expected to debut over the summer.

Another idea the group is looking into is a NonStop Hackathon as a way to get people outside the NonStop world exposed to NonStop technology, and promote new ideas on the platform. Details of this are in the early stages but expect to see more information very soon.

More news to come at a later time but if you have not done so already, please register at the website, www.NSU40.com, to share ideas on the forum and get on the mailing list!

Merlon SQLXPress

Now the best NonStop SQL database management solution is also the most secure!



Performance•Efficiency•Security

SQLXPress 3.50 includes comprehensive security controls

Auditing

Access Control

Session Encryption

Code Integrity

SQL Injection Protection

Multi-Factor Authentication

Complete HPE NonStop
Database Management Solutions

Learn more at
xypro.com/SQLXPress





NonStop System Console Care and Feeding

Wendy Bartlett >> Distinguished Technologist >> HPE

This May a ransomware cryptoworm known as WannaCry, which encrypts data on systems running the Microsoft Windows OS and demands ransom payments in the Bitcoin cryptocurrency, was launched against hundreds of thousands of systems in a worldwide cyberattack. The cryptoworm leveraged a Windows vulnerability that had recently had patches released for newer Windows versions. WannaCry's impact was relatively high because many system owners had not yet installed the patches or were running versions of Windows that were old enough that they were unsupported, including Windows Server 2003.

I won't touch on the discussion about the discovery and subsequent handling of the underlying vulnerability here, but you can read more about it in the WannaCry Wikipedia article (https://en.wikipedia.org/wiki/WannaCry_ransomware_attack) or by searching the web.

Writing the Hotstuff (HS03356A) about the WannaCry impact on NonStop systems was a good reminder to me that we need to keep emphasizing the importance of keeping your NSCs, which run various versions of Windows Server, current with respect to Microsoft's security updates. It also provided the impetus for us to update and republish the NSC security policy and configuration best practices, which are now available in a combined white paper as part of our manuals collections at www.hpe.com/info/nonstop-docs.



Tips for keeping your NSCs well secured

The new white paper goes into detail, but here are the highlights on how to keep your NSCs from being security victims.

Don't mistake an NSC for an ordinary Windows server...

Your NSCs are a key part of your NonStop server infrastructure, and you need to carefully control:

- Physical access
- Network access
- User accounts
- Installed software

Keep your consoles physically secured, and restrict network access to what is required by your business.

Apply the same considerations to creation and management of user accounts, access control and audit as you do to your NonStop servers: configure for minimum privileges and verifiable individual accountability. Don't treat your NSCs as general-purpose PCs. Don't install additional software packages besides antivirus products and software firewalls, such as different browsers or Microsoft Office.

Don't mistake an NSC for an ordinary Windows server, but...

- It still needs regular patch (and OS) maintenance
- It may be able to fit into your corporate management infrastructure for Windows-based workstations, e.g. Microsoft System Management Server, if certain conditions can be met

Your options for installing security and OS updates will vary depending on your environment, but you need to put the appropriate policies and practices in place to make sure that you perform updates regularly and without accidentally introducing malware - for example, having it hitch a ride on a USB memory stick used to install updates.

By the way...

NSCs are not the only hardware in the NonStop environment running Windows. The BackBox Virtual Tape Controller (VTC) and Virtual Tape Repository (VTR) both run Windows Server and need regular updates, but there are special conditions that you need to consider in order to not disrupt regular operations. See the NonStop Security Hardening Guide and Hotstuff HS03356A for more details.

NSC security references

In addition to the NSC Security Policy and Best Practices guide and the NonStop Security Hardening Guide, see the NSC Installation and Configuration Guide. Happy reading!

Security documentation news

We've been working hard at updating and augmenting our security guides and white papers over the last couple of months, and the following documents either are newly available or are in review internally and will be published soon.

At www.hpe.com/info/nonstop, under the Portfolio tab:

- NonStop Security Overview (updated)

In the NonStop manuals collections at www.hpe.com/info/nonstop-docs:

- NonStop System Console Security Policy and Best Practices (updated/combined)
- NonStop Security Hardening Guide (updated) [↗](#)

.....

Wendy Bartlett is a Distinguished Technologist in HPE's NonStop Enterprise Division, and focuses on dependability – security and availability - for the NonStop server line. She joined Tandem in 1978. Her other main area of interest is system architecture evolution. She has an M.S. degree in computer science from Stanford University. Outside of work, Wendy is a dedicated choral singer and enjoys spending time hiking, in the gym, and just hanging out with her husband, Joel. She lives in the San Francisco area.

Protecting the Enterprise and Ensuring Security at the Speed of Innovation

Protecting the enterprise—or government agency—has become a never-ending and mission-critical initiative, as cyber-attacks continually grow in frequency and scope. How do you balance security with innovation?

September 11-13

Register: <http://bit.ly/2tjRvay>

HPE Shadowbase Software Enables Operational Analytics for Commodity Big Data

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

Introduction

The growers of a major U.S. commodity deliver about eight billion pounds of produce per year to consumers. The produce is cultivated at thousands of independent farms throughout the country, and samples used for quality analysis and control are delivered to one of ten regional classification centers run by a large U.S. government agency.

Major commodity producers are shifting towards *precision agriculture* (also known as *satellite agriculture*), which takes the guesswork out of growing crops, shifting production from an art to a science. Precision agriculture is achieved through specialized technology including soil sensors, robotic drones, mobile apps, cloud computing and satellites, and leverages real-time data on the status of the crops, soil and air quality, weather conditions, etc. Predictive analytics software uses this data to inform the producers about such variables as suggested water intake, crop rotation, and harvesting times.¹

The analyses benefit the growers as a means to improve their products via changes in produce quality, soil moisture content, manufacturing upgrades, etc. The analyses are also used for pricing the commodity product on the open market. However, the analyses can be time-consuming, and the testing equipment can sometimes provide erroneous results as it drifts out of calibration. By the time results are available and are manually reviewed, much of the product has already been distributed to the marketplace; and some of it may have been incorrectly classified.

In early 2016, the agency undertook a major project to create a system that allows quality-control procedures to be performed in near real-time. The new system also provides for aggregation and historical analysis of the quality control information from all ten classification centers. The system's applications employ Online Analytical Processing (OLAP) utilities. Major goals of the project were to distribute data using the OLAP tools in a shorter time frame, to provide immediate notification if any of the testing

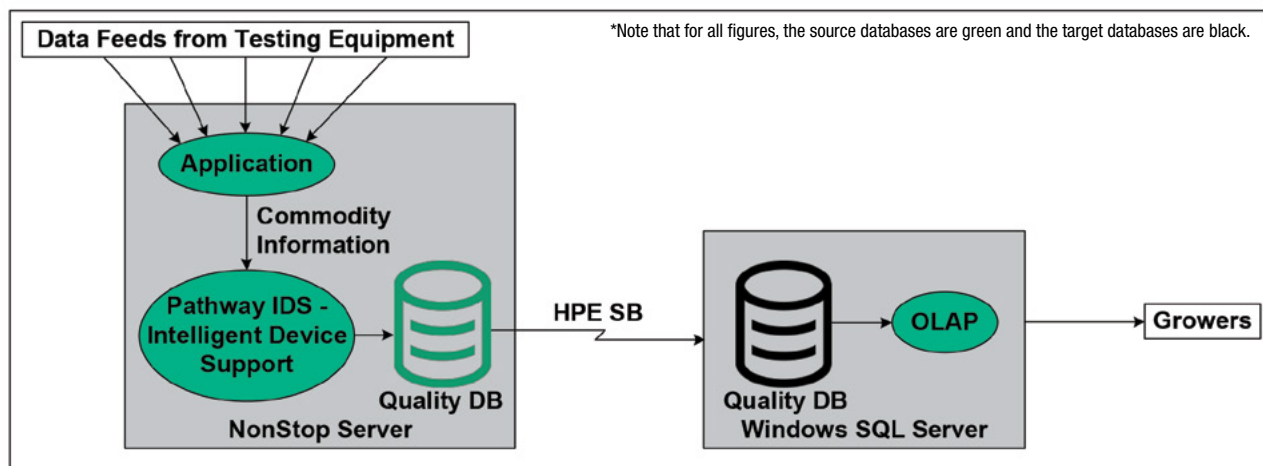


Figure 1 – A Regional Classifying Center

¹ For more information, please visit: <http://bit.ly/2kYVJa>.

² A data lake is a storage repository that holds a vast amount of raw data in its native format until it is needed.

Power Outages

The information on commodity quality is also sent by the CS to the futures market, where the crop is bought and sold. The spot price for the commodity on the futures market is set every day at 2 PM, and is partially determined by the quality control information. If a regional classification site loses power from Mother Nature (as the agency often faces) or otherwise goes offline, under the current configuration, samples are sent to another site for processing.

When power returns or the systems are brought online again, the systems are restarted and the Shadowbase software picks up right where it left off. For some systems (not configured with HPE Shadowbase), manual management intervention is required to restart them, creating a time delay, and minor inconvenience.

The central office is the only location with true disaster recovery enabled. However, the agency is considering adding disaster recovery to other systems in order to dramatically increase uptime through a more resilient, zero downtime infrastructure.

equipment became uncalibrated, and to improve the delivery and richness of feedback to growers eager to provide the highest possible product quality.

The HPE Shadowbase data replication engine plays a major role in this system since it automatically moves data from the testing equipment to the multiple OLAP quality analysis applications. Testing results can be immediately validated because the OLAP enabled quality measures occur at the same time. HPE Shadowbase software also creates an up-to-date *data lake*² of the classifying centers' output for historical analytical processing.

A Big Data Problem

As the produce is harvested, it is bundled into millions of 500-pound bales, and a sample read from both sides of each bale (with its own unique identifier) is sent to one of the agency's regional testing centers. The agency performs its tests under strictly controlled environmental conditions. The temperature is held at 70° Fahrenheit, and the humidity is fixed at 68%. Several quality measurements are made on each sample, including uniformity, color, moisture content, particle content, purity, and tensile strength. Consequently, over a 100 million measurements are made on the commodity throughout a single growing season.

Historically, the measurement data was printed on green-bar computer paper, and required an analyst to review the results. In addition to the sheer enormity of the printed output, small anomalies were hard to identify and isolate, especially in real or near-real time.

The lengthy time frame between samples being delivered to the agency and the analyses results being distributed to growers is due to the enormity of the processing of the samples and the sheer number of measurements. This delay leads to a significant problem if a manual review of the quality control data – where area directors would have access to commodity samples from each site – shows that some of the commodity has been improperly classified after much of the product has already been delivered to the marketplace.

In addition to growers' eagerness to receive faster, more informative evaluations of their crops, the merchants to whom growers sell their produce advocate near real-time quality analyses as well. For the merchants, price-setting is based on product quality and availability. The quicker the quality and volume can be determined, the faster an equitable price can be set for sale on the open market.

It was clear to the agency that a solution was needed to permit near real-time analysis of the immense number of measurements made during every testing procedure, and to return results rich in useful information to the growers and merchants in a timely manner. The answer was the implementation of a large, distributed OLAP system, which could distill the data to a manageable size, with the ability to quickly identify any aberrations as the testing results flowed through the system. The agency selected the HPE Shadowbase data replication engine to move data from one processing step to another in the distributed system, thus integrating several separate applications into a cohesive whole. This case study explores the use of data replication, application integration, and big data analytics to unlock the value of enormous amounts of operational data.

Analyses in the Regional Classification Centers

The first step in data distillation takes place in the regional classification centers. Each center is equipped with an HPE NonStop system and a Windows SQL Server environment, as shown in Figure 1. The centers use a variety of testing devices to measure the characteristics of each sample. The data from a center's testing devices is sent to its supporting NonStop system.

Next, the NonStop system processes the data via a local application running in a Pathway environment. The data is entered into a SQL/MP Quality Database by Pathway Intelligent Device Support (IDS). From there, it is replicated by the Shadowbase data replication engine (HPE SB) to a Windows SQL server environment for further analysis. The Windows system runs an OLAP application that analyzes the quality-control data for the region. The results of these analyses occur in near real-time and will immediately alarm if any results are out of band from the expected ranges, or if the equipment fails an internal validation test. The results are also returned to the growers via a customized SQL Server-generated view, for guidance in making crop improvements, and to the markets for immediate pricing input. All results indicating there is a problem with a particular batch are flagged for further, immediate review by the agency's team of analysts.

Throughout the agency, thirteen pairs of NonStop/Windows systems are deployed (a single pair's configuration is shown in Figure 1). One pair is located at each of the ten regional sites; one of these sites is collocated with the Central Site (CS), described below. Three pairs are used by the CS: one pair aggregates the data from all the regional sites; another serves as the QA system, and the third is the development system. A disaster recovery system is located about 500 miles away, and can be placed into service should one of the regional systems go down.

TIBCO Spotfire (Figure 2) is a data visualization and analytics software product that runs on an HPE ProLiant server. The agency uses Spotfire to monitor and manage the systems in the regional

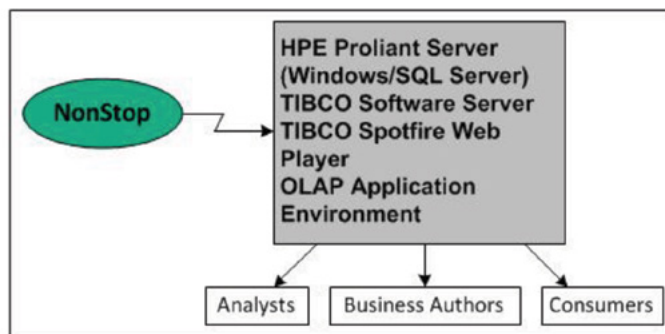


Figure 2 – Spotfire

³ According to Investopedia, "Futures contracts are made in attempt by producers and suppliers of commodities to avoid market volatility." Read more at: <http://www.investopedia.com/terms/f/futuresmarket.asp>.

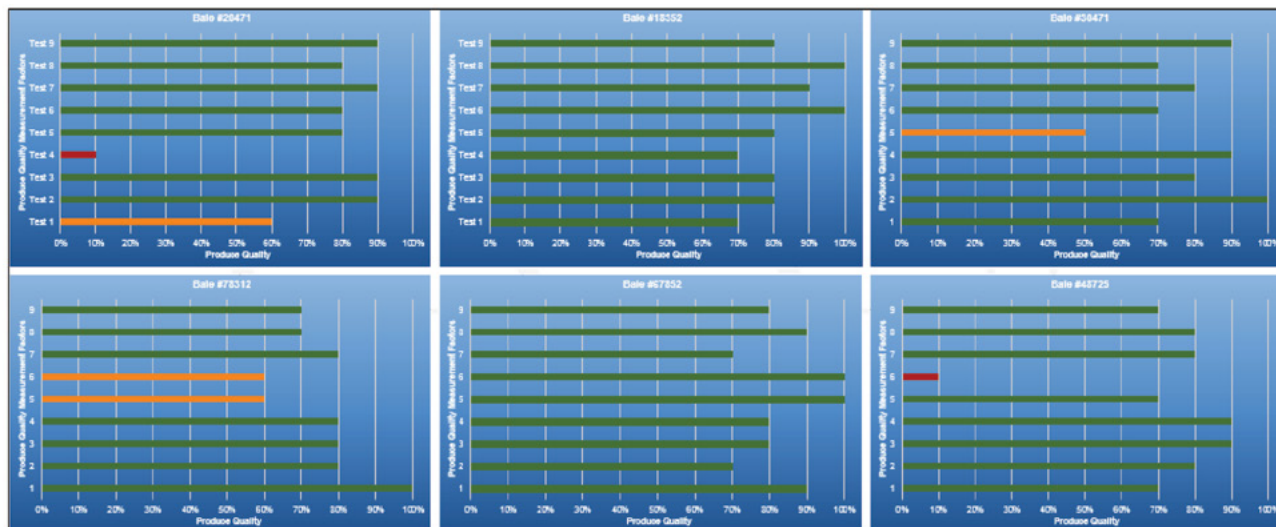


Figure 3 – Produce Quality Dashboard

offices in order to provide a visual dashboard showing the status of the various systems. Spotfire highlights testing results that return out-of-band values. The OLAP software allows the users to point and click, honing in on the raw data for review. Spotfire ensures all systems are working properly and that accurate quality control results are returned to the growers in real-time and before the commodity is shipped.

Spotfire defines three classes of users – analysts, business authors, and consumers – each with a specific role. One problem faced by the agency³ is that the testing equipment drifts out of calibration over time. Analysts ensure the testing equipment is properly calibrated and that the systems being monitored by Spotfire are working properly. Spotfire indicates the operational status of each system via a series of colors: green means the system is operating properly; yellow means that the system is operating, but it may not be producing accurate results due to improper calibration of the testing equipment; and red means that the system is down, for example, not responding (Figure 3). As a consequence, the health and proper calibration of the testing equipment is continually monitored, and can be recalibrated immediately if it starts to drift or otherwise fails.

Business authors can create and modify the rules that Spotfire supports for analyzing the data, and they can change the graphical and dashboard displays presented by Spotfire. Consumers are the growers and manufacturers who are the end users of the quality control information (e.g., for improving their product or for determining the price they should pay for any particular lot of product). This system also leverages the consumer demand as market feeds, pricing the commodity on the spot market.

The Central Site (CS)

The quality control information generated by the Quality Databases at the regional offices is consolidated and integrated via Shadowbase data replication to the agency's Consolidated Quality Database (CQD) at the CS, which is located in the heart of the growing region. It is organized in a classic hub-and-spoke architecture (Figure 4). The CQD is a SQL/MP database running on a NonStop system (Figure 5).

The CS also houses a Windows/SQL Server environment for processing the aggregated CQD. Shadowbase replication keeps this database up-to-date as the data changes in the regional classification centers. An OLAP application on the Windows/SQL Server environment processes the consolidated data's quality measures for the entire commodity crop in a manner similar to the

regional offices.

The regional offices save their data for five years, while up to fifteen years of consolidated data is saved at the CS. In effect, the CQD is an aggregated data warehouse of the quality control information from all ten Regional Classification Centers over several years, allowing for both tactical near-term analyses and strategic long-term analyses. For instance, the agency can look at trends over time for production quality, quantity, and so forth.

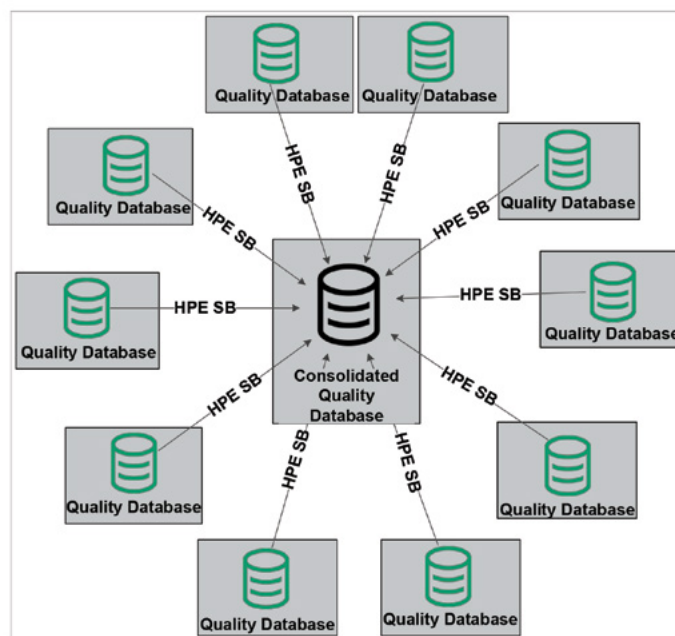


Figure 4 – Consolidated Quality Database

The consolidated information is sold to wholesalers. Typically, they are mills that are looking for specific crop quality parameters to optimize processing procedures and make accurate pricing decisions.

The Many Roles of HPE Shadowbase Data Replication Engine

The commodity application described above is an excellent example of big data analytics using data integration and application integration. Data must be copied between systems and aggregated at the CS. Multiple applications must also interoperate with each other, each extracting quality control

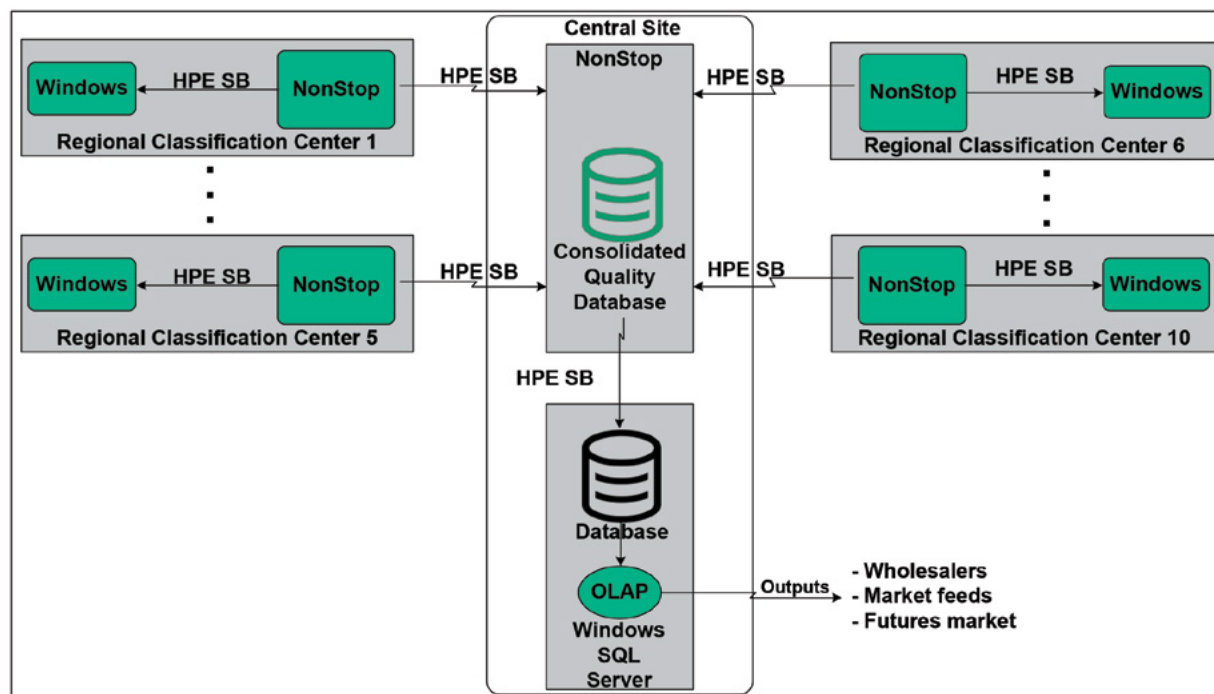


Figure 5 – Central Site (CS)

information from the test data and sending the information to the next application. The Shadowbase data replication engine plays a major role in this solution:

- It replicates test data from the NonStop systems in the agency's regional offices to the Windows SQL Server environments in those same offices for OLAP analysis.
- It replicates the test data to the CQD at the CS.
- It replicates quality control information from the CQD at the CS to a Windows SQL Server environment at the CS for overall OLAP quality analysis, enabling the agency to monitor the crop as a whole.

Conclusion

The commodity quality control system integrates applications to extract meaningful data from a mass of test and product quality data, or Big Data. Extraction is efficient thanks to a series of OLAP processors. HPE Shadowbase software plays a key role

in the system by integrating distributed applications through replication of data between the applications. With the right tools, the system can also determine where the commodity with certain quality control parameters (such as tensile strength) was grown and shipped.

The solution has dramatically improved the reporting of the quality metrics for the crop, immediately alarming the users when the parameters are not met. It provides for near real-time tactical reporting of crop metrics to the growers (for production analysis), manufacturers (for manufacturing analysis), and markets (for accurate pricing), and provides historical analysis for strategic purposes.

HPE Shadowbase software (built by Gravic, sold by HPE) is available from HPE and globally sold, supported, and provided service by Hewlett Packard Enterprise. Contact your local HPE Representative for more information. [CD](#)

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.



Secure Communication Through VPT the Virtual Private Tunneling

Jürgen Overhoff >> President >> ITP – PANORAMA Inc.

Millions of dollars are spent to make computer centers and applications safe. The threat from intruders is growing every day. They are trying to steal data, gain control over power plants or blackmail after encrypting data on workstations and servers. All successful attacks to IT systems are coming today through VPN connections [Virtual Private Network]. This tells us that VPN, the current standard is not secure enough.

Weak point 1: Authentication is happening on the server after a user has been passing the firewall. Complex software on servers is trying to separate *good from bad*. Cases in which the checks have failed we read in the news media.

Weak point 2: Direct Network-Network coupling is making “Man in the middle” attacks possible. This means connections are unsafe. This can be any access to the IT, the opening of a car door, the connection between car and vendor or a hotspot in cities, airports or a restaurant.

Weak point 3: Exchange of IP-Addresses allows hackers to locate used devices and target systems for their attacks.

Weak point 4: PCs accessing the IT need installation of a *Network Card and Communication Software*. In a network with thousands of users, the costs of setting up hardcoded user workstations is time consuming and very expensive. Administration is labor intensive and very costly. How many, in a network of thousands of users are losing

valuable time every day while their PCs are down? Until they are getting a replacement, they cannot work online.

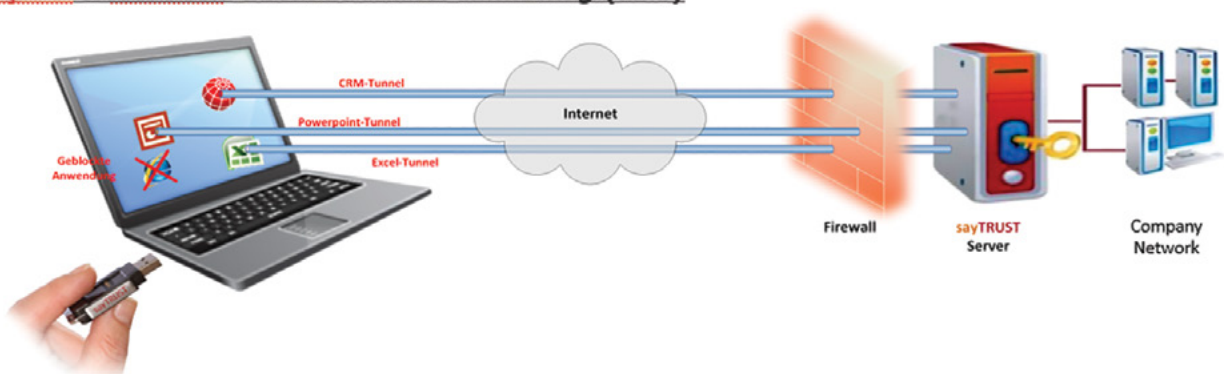
From experience, you know that over time a better successor is replacing solutions that we tend to defend because we are used to them. However, evolution moves on. One can delay better solutions, but not stop them.

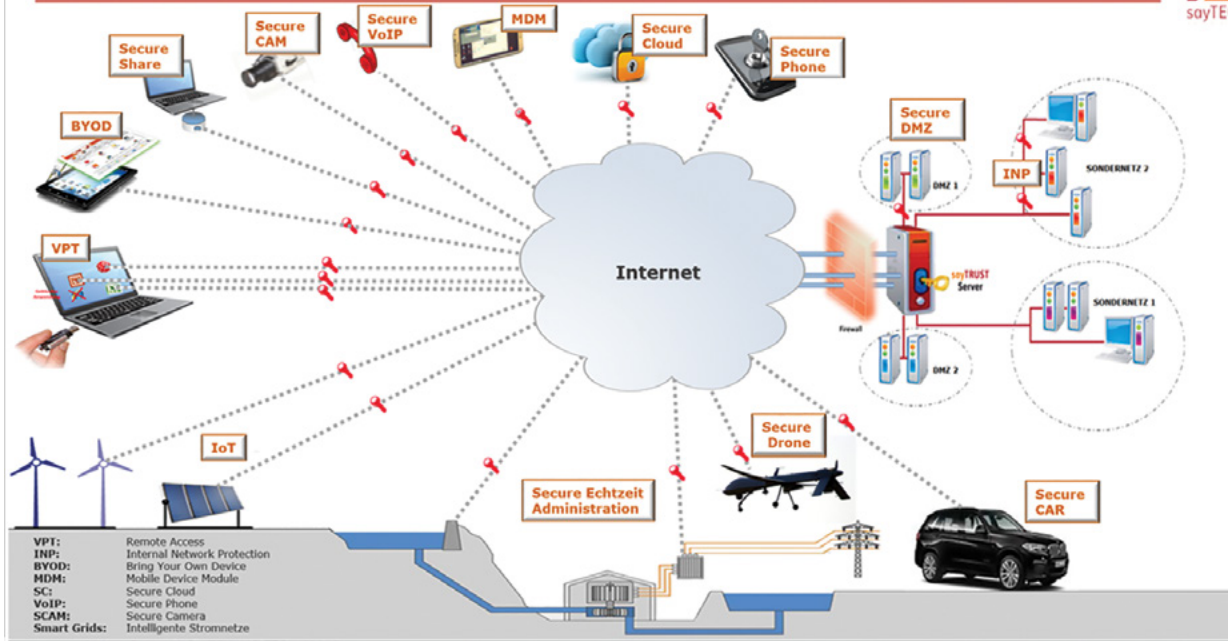
So, what would it mean to you, if there would be a solution that can solve the weak points mentioned above? What, if the better solution would be even less expensive to operate? Ready to having a closer look at VPT Virtual Private Tunneling?

So, why will VPT replacing VPN?

1. An *Access Stick* that contains all communication software allows to build up a communication from any PC or laptop with Internet connection. In cases that a user's device fails, he/she can use any other one. This is limiting downtime to a minimum.
2. VPT has moved the authentication to the used device. Only users who pass the authentication can build a communication with the target system. Three levels are available. (Certificate, Biometric and PIN)
3. Only the processor and the RAM of the device are used to build the tunneled connection, ignoring all other applications and data on the used device.

sayTEC's solution: Virtual Private Tunneling (VPT)





4. The certificate defines applications a user is supposed to work with on the target system. The user menu shows only these applications.
5. Functions on a PC can be blocked by the user's certificate. This can be access to the Internet, copying data, start of specific applications during an active communication session.
6. The connection from the used device to the target computer are protected by three level security. [Certificate, Diffie-Hellman Perfect forward 2,048 BIT key Secrecy]
7. For each application, a separate connection is built.
8. Only data related with the use of applications dedicated to a user can enter the communication link.
9. Taking-off, the Access Stick from a PC or laptop does not leave a single Byte left that could reveal that the device was used for a communication.
10. All these facts lift the safety of communication to the level that is technically possible theses days.

VPT works also from smart phones and tablets.

Phone calls are secure in a private network. The user has access to a phone book on the server that shows only contacts that he or she is supposed to call. After finishing, nothing shows on the device that there was a call.

Communication from hotspots is as safe as from an Internet Cafes.

In addition to all of the benefits that VPT (Virtual Private Tunneling) has above VPN, it is faster to install, easier to administer and roll-out and user friendly.

Use case 1: Hospitals The risk that a "man in the middle" intrudes a connection when a doctor is using a tablet while accessing sensible data when visiting patients disappears. By certificate, doctors can see more data than nurses can.

Technical staff of vendors of e.g. X-ray systems are accessing servers that control the systems as well as the systems itself. It is important to know that the connections are secure and the rest of the IT of a hospital is invisible and inaccessible.

Use case 2: Financial Institutions VIP customers of banks and investment brokers can build a safe connection when placing orders or analyzing data.

There is no need for downloading sensible data from the servers to laptops for consulting customers at their location.

Use case 3: In-house Security Within an enterprise, access to applications and data can be restricted. This can be depending on the position of an employee within the organization or the information he or she needs to do the job.

Within the IT center, servers or groups of servers can be restricted as far as access is concerned to limit the traffic and the group of users.


Use case 4: Power plants are connecting various sources of energy production and consumers. Recent attacks show how important it is to secure these networks. Particularly if a control center is managing the entire system real-time.

Use case 5: All industries A sales director can access more applications than area managers can and these more than account managers can. All can access the companies IT from wherever they are with smart phones, tablets, laptops or PCs, whatever is available at a given time.

Use case 6: Transport and logistic services provider use worldwide complex highly integrated IT environments. Large numbers of carriers and customers are linked in a global network. Breaking in and manipulating such systems can be catastrophic.

Use case 6: Cloud computing is growing at impressive rates. The fear is not so much whether the data are safe in the cloud, but how secure the communication with the cloud is.

These are only some of the cases where safe communication is having highest priority. Airlines, Cities, Government agencies, all industries, you name it. Now, you know that there is a way to make IT communication safe. The point is not whether you believe it or not. You will only know after trying.

For more information please visit www.sayTEC.eu or contact Juergen.Overhoff@sayTEC.eu Distributers welcome. 

Juergen Overhoff spent his entire business career in IT. There are very few jobs he did not own at hardware vendors, computer centers, user's side and software vendors. At present times, Juergen is President and owner of ITP-PANORAMA Inc. and member of the board and co-owner of sayTEC AG. He is devoted to quality and productivity of software maintenance and modernization and also in to security.



A Web Application on NonStop

Wolfgang Breidbach >> Bank-Verlag GmbH

Sven Breidbach >> Bank-Verlag GmbH

If you try to talk to other people in the IT world about HPE NonStop you are very often confronted with buzzwords like legacy, outdated and others of that sort. We never met anybody outside the NonStop world thinking of these systems as „modern“ or „flexible“. Even many people working on NonStop do not know much about the capabilities of the system and this is not depending on their age. Our impression is that those who are aware of at least most of those capabilities sometimes feel like the people in the well-known little Gallic village surrounded by the big Roman Empire. Fortunately there seems to be some immigration into that village like the U40 SIG.

But let us have a closer look at what is going on in one of the houses within that village the house with the Bank-Verlag logo at the front.

A few years ago we introduced a first version of Bank-Verlag's monitoring tool which was working with open-source Nagios at that time. During the last years the functionality of the monitoring tool itself has been massively extended and nearly all of the boring daily work is done automatically.

Bank-Verlag is doing card authorization with a multi-active application, that means that the application is able to support more than just 2 active systems, we have tested the application with up to 6 active systems.

Within card authorization the Bank-Verlag application has 3 main functions:

1. Accept the transaction from the acquirer, forward it to the card issuer, get the answer from the issuer and reply to the acquirer.
2. Do stand-in authorization in case the issuer is not responding and we are allowed to do stand-in.
3. Act as the issuer for some banks.

In addition there is a bunch of other functions like blacklist processing, importing card data, producing statistics, data exchange and so on.

The Bank-Verlag authorization application is defined as critical for the German payment infrastructure, so this application needs a very intense monitoring. We again set up a home-grown tool acting as a user-exit of the standard monitoring.

Here are a few sample problems that might occur:

1. Too many timeouts for an issuer
2. Too many reversals
3. Too many transactions with defined answer codes

There are many of these directly measurable criteria.

All these problems are monitored, the parameters are set in cooperation with the issuers. In case a value is out of range a message is created and an e-mail is sent to the issuer.

The problem we had was on the acquirer side, we only see the transactions arriving at one of our systems, we do not see transactions lost in transport. We just might see that the number of transactions is too low or, in case of an attack, too high. So we needed to create something like estimated numbers and check if the actual number of transactions is within the expected range.

This is the point where Sven enters the stage. He is studying media informatics at the Technical University Cologne and he had to do a project as part of his studies. And very soon the idea was born: Create a prototype of a web-based GUI to make visible what is actually going on in the authorization application (Remember: We are situated within the Gallic village and are aware of the modern tools on the NonStop!). For the database access we could use Pathway servers which are either already available or can easily be created using already existing source code.

The GUI itself would be using ITP Webserver and JSP.

Bank-Verlag and the University agreed and so the project could start.

As described before the first request was creating an overview of the incoming transactions.

But the first problem we had to take care of was security. Bank-Verlag is PCI/DSS certified so a security concept is a must. That is the point where some Safeguard functionalities proved as very useful. We are using the already existing users and aliases. Every user or alias can be a member of up to 32 groups. So we decided to use the Safeguard groups for the application security, a little table contains the functionality and the groups allowed to use this functionality. For the groups we are not using the 256 Guardian user groups but the so called file-sharing groups, which have numbers above 255 and can be named with up to 32 bytes. This concept was accepted by the security group. Technically we put all the security things into one Pathway server.

The next step was making some proposals for the look and feel of the GUI, starting with some drawings on paper and switching to some static HTML pages afterwards. The whole thing was discussed with the operations people and as a result we got a very good concept.

The next step was creating the Pathway servers and the logon page. Here again we could make good use of a very old functionality called DDL. We defined all the requests to and the replies from the Pathway servers within DDL and with the tool ddl2java (part of Jtoolkit) you can easily convert the definitions to JAVA and in addition ddl2java creates all the functions needed.

Jtoolkit also contains a pretty good example for using JPATHSEND and TMF from a JAVA program.

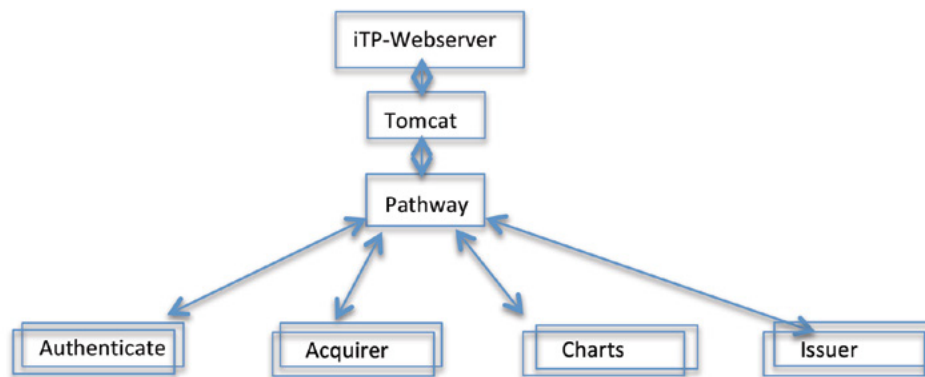
Unfortunately there is no example using JPATHSEND and TMF together with JSP. In addition we found out that JSP needs some additional libraries for JPATHSEND and TMF and again nothing could be found in the manual but fortunately all the information could be found searching the support center. A little manual "Creating a JSP application using Pathway servers" would be really useful and create more acceptance.

Let's go back to the GUI. The best news was that there is no detailed NonStop knowledge necessary, only the very few lines containing TMF and JPATHSEND functions are NonStop specific. For the development Sven used a standard Windows PC with Eclipse and Maven installed.

Some of the previously mentioned libraries have to be copied to the PC.

The result of the development is a .war file, similar to any other web application. And this file is brought to the NonStop and placed into the correct directory ...webserver/servlets/webapps. JSP will find the file automatically and deploy it. Again this is not NonStop-specific.

Let us now have a look to the structure of the application:



At this time we have 4 Pathway serverclasses:

- Authenticate for all the security stuff
- Acquirer for the incoming messages
- Issuer for the routed transactions
- Charts for the graphical presentation

For every request the Authenticate server is asked if the user is authorized for this function.

Because Bank-Verlag is a German company the following screenshots are in German.

We created a pretty conventional logon-screen. As usual the logon will be rejected if the userid or password is wrong or if the password is expired.



Login

Benutzername

Passwort

Anmelden

A successful logon leads to the menu page (Übersicht means overview):



This page contains a counter for an automatical logoff after 10 minutes without activity.

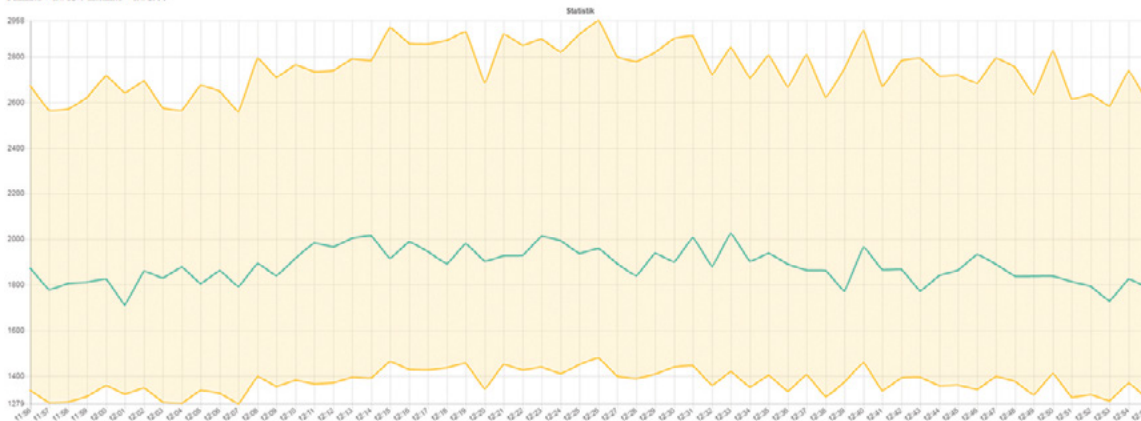
The overview of the incoming POS-transactions has been anonymized and serves as a sample for all overview pages. We are collecting this data on a 1 minute base, so the page is actualized every minute. The timeframe for the data collection can be selected by the user.

Netzbetreiber	Gesamt	StandIn	geroutet	Storni	Routingfehler	Systemfehler	erfolgreich	Timeout	Keine Verbindung
Provider 03	449	1	436	1	0	0	442	0	0
Provider 04	4	0	4	0	0	0	4	0	0
Provider 05	159	0	150	0	0	0	153	0	0
Provider 07	23	0	23	0	0	0	22	0	0
Provider 08	29	0	28	0	0	0	28	0	0
Provider 10	13	0	12	0	0	0	13	0	0
Provider 14	50	0	50	0	0	0	50	0	0
Provider 15	636	0	615	1	0	0	626	0	0
Provider 16	152	0	148	1	0	0	150	0	0
Provider 18	154	0	150	0	0	0	154	0	0
Provider 19	161	0	161	0	0	0	155	0	0
Provider 20	34	1	31	1	0	0	32	0	0
Provider 22	642	2	613	5	0	0	636	0	0
Provider 24	94	0	88	1	0	0	94	0	0
Provider 25	103	0	93	5	0	0	103	0	0
Provider 26	73	0	70	0	0	0	73	0	0
Provider 27	56	0	53	1	0	0	55	0	0
Gesamt	2832	4	2725	16	0	0	2790	0	0

Similar pages are available for incoming ATM transactions and for the issuer routing. This was the state, when the original project ended. Finally it had been possible to create a complete application rather than the planned prototype. Even during the prototype phase it has proved very useful during several network changes and a major maintenance window of one of the biggest German banks.

But the work on the GUI is not finished yet.

The next picture again shows the POS transactions as the blue line. We compare again the values one week ago and if that day was a holiday we take the values 2 weeks ago. With the actual configuration we would accept 25% less and 50% more transactions than one week ago. So as long as the blue line is within the yellow area, the numbers would be within range.



While this article is created, the work on the GUI is continued, there are lots of ideas and wishes.

Finally we want to summarize our experiences and the lessons we have learned during the project:

- Creating web-based application on a NonStop is similar to creating those applications on other systems, only the very small parts concerning Pathway and TMF are specific.
- If you want to replace your SCOBOL applications by web applications there is no need for detailed NonStop knowledge. There is no need to change any of the servers. You just need the DDL definitions of the interfaces.
- The acceptance of web GUIs is much better than that of old „green-screens“.
- There is very little need for training, people are used to web applications
- There is no need to install any specific client soft- or hardware, the web GUI can even be used on a smartphone.
- For the security stuff you can easily use Safeguard functions.
- Even on a NS1200 system we did not have any performance problems except during startup of JSP the application did not cause any significant load.

Wolfgang Breidbach has more than 40 years IT industry experience, spent in a variety of roles. Currently he is responsible for the NonStop-Systems at Bank-Verlag. Wolfgang joined Bank-Verlag in 1985, he was deeply involved in setting up the company's IT infrastructure and migrating the Bank-Verlag from a publishing house to an IT service provider. He was responsible for setting up the DR concept of Bank-Verlag. He has set up two DR sites and has been responsible for the HP Integrity NonStop early adopter program in 2005 and and the migration to Integrity NonStop immediately afterwards. Since 2009 he has designed and developed Bank-Verlag's own NonStop monitoring tool because Bank-Verlag decided to use Nagios as the central monitoring server. In 2012 he lead the replacement of Bank-Verlag's 2 production systems by NB54000C systems without any outage visible to the customers. Today he is responsible for 4 NonStop systems running various applications.

Sven Breidbach is studying media informatics at TH Cologne and created the web part of the new GUI. Meanwhile he is working part time at Bank-Verlag.


SPEAK NOW. BE HEARD.



Submit your Advocacy request to: <http://bit.ly/SpeakNowBeHeard>

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

Security: A Critical Piece of NonStop SQL Management

Merlon SQLXPress Delivers New Security Protection for NonStop SQL



John Furlong >> Director, Software Development - Merlon >> XYPRO Technology

Data is the lifeblood of mission-critical applications, and HPE NonStop customers rely on the powerful capabilities of NonStop SQL databases to store, analyze and manage that data. Therefore, NonStop customers need to ensure that NonStop SQL databases are well-organized, using efficient queries, and running at peak-performance.

To do that, NonStop database managers need powerful database management tools and often, highly-privileged access rights. However, providing database managers unrestricted privileged access poses serious risks. With privileged access comes increased threats from malicious insiders (one of the most difficult to detect and resolve security threats), catastrophic user error and compromised credentials.

Previously, NonStop customers didn't have a choice between database management functionality and security controls. Now, with the release of Merlon SQLXPress 3.50, you can have the most functional graphical database management solution for NonStop SQL and strong security protections.

Secure NonStop SQL Database Management

Merlon SQLXPress 3.50, released in June, is the culmination of a multi-year project to make it the most secure database management solution available for NonStop SQL, period.

SQLXPress 3.50 includes a comprehensive set of security controls, including:

- Support for Multi-factor Authentication
- Auditing
- Access Control
- Session Encryption
- Code Integrity
- SQL Injection Protection

Support for Multi-factor Authentication

SQLXPress requires a user to logon using either a Guardian user name, or a Safeguard alias name, together with a valid password.

The SQLXPress client logon dialog supports PCI DSS 3.2 multi-factor authentication (MFA) requirements by prompting the user for a verification code, or passphrase. Using this in conjunction with XYGATE User Authentication (XUA), which is already present on your HPE NonStop server, means you're now up-to-date with the very latest in PCI 3.2 MFA compliance requirements.



Auditing

The SQLXPress Security Administrator can configure the level of audit data that is collected by the audit subsystem.

The audit subsystem records the actions of SQLXPress users in an audit trail and contains detailed information on each user action, including: date and time, user logon name, PC device identification, SQL statement text, SQL parameter values, outcome details, and much more.

Audit trail data is extracted to an SQL database for reporting purposes. A rich set of audit reports is available, from activity summary reports down to individual actions. Reports can be filtered by time of day, user, PC, and SQL object name.



Audit data is useful for security administrators. It allows them to monitor the use of SQLXPress, and be able to answer questions like:

- Who accessed or changed data?
- When was it changed?
- From which PC was it changed?
- Who tried to perform an unauthorized command?

Audit data is also useful for troubleshooting and problem determination. To facilitate the exchange of helpful diagnostic information to other departments, like operations, the Security Administrator can grant audit report access to other users on an individual, audited basis.



Every HPE NonStop server is delivered with XYGATE Merged Audit [XMA] software. Additionally, XYPRO has developed an audit plugin which integrates the collection of SQLXPress audit data directly into the XMA database. This enables sophisticated audit reporting and alerting capabilities for all NonStop SQL activity, along with the ability to deliver this audit data to your enterprise SIEM devices.

Name	Value
Action	UPDATE
Activity Outcome	Pass
Activity Subtype	Not Available
Activity Time	2016-04-27 10:33:40
Activity Type	UPDATE
Blacklisted	N
Online	Y
PC BIOS Serial Number	VMware-56 4d 22 f2 14 09 53 b0-b1 ba 92 93 9c 6a 39 c6
PC MAC Address	00-0C-29-6A-39-C6
PC Name	WIN-6BQF16L4FR1
PC TCP/IP Address	192.168.129.15
PC Volume Serial Number	F668 - CFE2
SQL Database Type	SQLMX
SQL Defaults	JDFCAT.T
SQL Object	JDFCAT.T.CUSTOMER
SQL Operation	UNIQUE_UPDATE
SQL Param P1	12 Alvira Close.
SQL Param P2	1
SQL Statement	UPDATE JDFCAT.T.CUSTOMER SET STREET = ?P1 WHERE (CUSTNUM) = (CAST(?P2 AS NUMERIC(4) UNSIGNED))
Server CPU	1
Server Creator Access ID	255,255(SUPER.SUPER)
Server Home Terminal	/MIZZEN.\$ZHOME
Server Login ID	CLIDER CLIDER

Figure 1: Example audit details for a user action

Access Control

NonStop SQL supports access control “out of the box”. SQLXPress augments these standard access control features by providing a more granular level of control over the actions users are permitted to perform, and the SQL objects they are permitted to access from within SQLXPress.

Role-based Access Control

Like all XYGATE software, SQLXPress now supports a role-based access control model:

- Roles are granted permissions to perform activities
- Users are assigned to roles
- Users acquire the permissions that have been granted to their roles
- Roles may be restricted to an “environment” (an environment is a collection of specific SQL objects)
- When a user attempts to perform an activity, an authorization check is performed

A key advantage of the role-based approach is that once the access control rules have been initially set up, on-going maintenance involves simply adding or removing users from Role Groups.

Access control configuration is easily customized to suit the needs of the organization.

Separation of Duties

SQLXPress supports the principle that the Security Administrator is responsible for the configuration and management of the SQLXPress security subsystem, including audit and access control.

There is a special Security Manager Windows client program for use only by the Security Administrator. The typical SQLXPress user is not granted access to most functions in the Security Manager client and the Security Administrator is not allowed to use the other SQLXPress client programs.

To really appreciate SQLXPress access control let’s take a look at some use cases:

Use Case 1: Command Lockdown

NonStop SQL permits the owner of an SQL object, like a table, or a view, to perform any DDL or utility operation on the object. SQLXPress access control refines this so that restrictions can be applied to individual operations.

Many commands, like Update Statistics, or Split Partition, are performed as part of the routine duties of a DBA. The DBA should have permission to perform them on an ongoing basis.

However, there are some operations like Purge Data, Drop Table, or Disable Trigger, that are not required for the normal operation of the database, and can have disastrous consequences if performed inadvertently.

SQLXPress access control allows these potentially dangerous commands to be “locked down” during normal use. When the DBA needs to perform a locked down command, the Security Administrator temporarily grants permission for the command. When the command has been completed, the security administrator revokes the permission.

Use Case 2: Data Access Restrictions

NonStop SQL permits the owner of a table to view and change the data stored in the table. SQLXPress access control can be used to limit the owner’s access to data while still permitting the owner to manage the table.

SQLXPress security controls means the owner can be prevented from changing data and can even be prevented from viewing data at all.

Use Case 3: Database Visibility Restrictions

SQL metadata is a rich source of information about the databases on the system. It includes details on table names, column names, security settings, data validation rules, and much more. Most organizations will want to limit access to SQL metadata to authorized users only.

However, with NonStop SQL/MX, SQL metadata is secured for public read access. This means that any SQL/MX user can view information about all the databases on the system. In SQL/MP, metadata is secured per catalog.

To enable database visibility restrictions, the SQLXPress access control feature allows the Security Administrator to define one or more “environments” on a system.

An environment provides a restricted view of the SQL objects on a system. Only objects that have been registered in an environment are made visible to the user.

The Security Administrator can restrict the SQL objects that are made visible to a user by assigning him a role for an environment. The user must open an environment in order to use SQLXPress, and can only work with the SQL objects that are registered in that environment.

Furthermore, a user can be granted roles for more than one environment, and even granted a different role in each of those environments. For example, user DEV.JOHN can be granted the role Senior DBA in the DEV_ATM environment, and the role Guest in the QA_ATM environment.

Session Encryption

SQLXPress supports the use of Transport Layer Security (TLS)--also frequently referred to as SSL (Secure Sockets Layer)--to protect the data exchanged between the SQLXPress client and server components. The use of TLS provides both privacy and data integrity.

The data exchanged between the SQLXPress client and server remains private because it is encrypted using symmetric cryptography where the encryption keys are generated uniquely for each session.

The identity of the server can be authenticated using public key cryptography and data integrity is ensured because each message is protected by a message authentication code.

TLS support is available either by linking to an external DLL, or by using a proxy process.

Code Integrity

SQLXPress is available for download over the Internet and the setup programs are digitally signed. This digital signature confirms that Merlon is the publisher of the setup program, and that it has not been tampered with since it was published.

In addition, the various SQLXPress client programs are also digitally signed so that the code cannot be tampered with after it has been installed.

SQL Injection Protection

SQL Injection is a type of cyber attack in which malicious SQL statements are injected into the entry fields of data-driven applications.

Secure NonStop SQL Database Management



To protect against SQL Injection attacks, SQLXPress uses SQL statement templates for most of its client-generated SQL code. These templates are stored as resources in the Windows client .exe files. Since the .exe files are digitally signed, the templates are protected from tampering.

Data values entered by the user are validated, not used “as-is” to construct SQL statements. In addition, SQLXPress uses parameterized SQL statements so that user-entered data does not form part of the SQL statement text.

Additionally, SQL statements entered directly by the user are parsed in the client code and access control restrictions are applied to the SQL statement, and the objects it references.

Summary

With the most comprehensive set of features and full support of both NonStop SQL/MX and SQL/MP, Merlon SQLXPress is the leading solution for managing NonStop SQL databases. SQLXPress users describe it as “indispensable” for database administrators, software developers, technical support personnel and any other users who work with NonStop SQL databases.

However, HPE NonStop SQL databases typically store highly sensitive and private information, and, in an increasingly security-conscious world, customers also expect their database engines and database management tools to provide comprehensive security--and Merlon SQLXPress delivers.

As of March 2017, Merlon became a wholly-owned division of XYPRO, the leading provider of security solutions for the HPE NonStop platform. So it is no surprise that not only is SQLXPress the most complete database management solution for NonStop SQL, it is also the most secure. [🔗](#)

For more information about the Merlon Products please visit: www.xypro.com/sdm or contact sales@xypro.com.

John Furlong is the development team leader for SQLXPress, and is responsible for the design of the Visual Query Tuner. John has over thirty years' experience working on the HPE NonStop platform. To get in contact with the author, please email: jfurlong@merlon.com.

OmniPayments

Financial Transaction Switch

- 10,000 TPS / 14,000 ATMs
- Proven in production - 1 billion transactions per month
- Managed services provider / 7 locations worldwide
- OmniPayments switch supports ATMs, POS, Web, and Mobile
- Built for Instant Payments / GDPR-compliant / Ready for PDS2
- Fraud Blocker seamlessly integrates with our switch and others
- OmniCloudX hosts OmniPayments instances on pay-for-use basis
- OmniWallet offers real-time, anywhere banking via mobile devices
- Loyalty Card Management System creates, manages, and operates loyalty programs

www.omnipayments.com

BackforMore

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

To even the most casual reader of what I publish, it would be hard to miss the many references that have been made to user, vendor and industry events that I have attended in the past couple of months. As a writer I need to be mingling with the crowds, so as to speak, in order to stay atop all that is happening within our industry. IT is changing and changing rapidly. No, this is not news to anyone in the NonStop community or even in IT, but to the world at large it is gaining a lot more attention and barely a major headline is generated today without some references being made to technology. However, it is the emergence of software as the defining element of even the most staid of computer vendors that is perhaps the most obvious example of change and the increased rate of change that we see occurring even as we attempt to stay on top of just that software that interests us most.

To these same casual readers of all that I publish, it would be hard to miss how at heart, I am a car guy. I read car magazines and subscribe to car forums. This month it was a column by Aaron Robinson in Car And Driver magazine that caught my attention. "Our world is changing; the machinery matters less than the software. Mazda R&D chief, Kiyoshi Fujiwara told me at the Detroit auto show this year that in the age of electric vehicles, the powertrain, that core technology that is so important to the identity of a car brand, will become just another purchased component. It is the software, the brains that the company must own to call itself an automaker."


Robinson also quoted Stanford University artificial intelligence expert and Honda consultant, Edward Feigenbaum, explaining to Automotive News that Honda's "current R&D leadership saw the need to move beyond the mechanical engineering of the past toward a digital future dominated by software, not mechanism." There really shouldn't be any surprises here for the NonStop community who, for the past two years, has been subject to numerous messages by HPE NonStop managers to pay more attention to the software. Perhaps we may have missed it but it was a couple of years ago when we were all informed of how NonStop was the best software platform on the planet. But what does this really mean? Stated as simply as I can, HPE, the computer company, will be recognized by the software it runs. And this will direct the spotlight squarely onto NonStop!

This issue of The Connection has, as its theme, the protection of your NonStop enterprise. With so much focus now being given to software, protecting the solutions your enterprise depends upon has taken on a sense of urgency. Headlines continue to remind us of just how critical it has become to erect fences around our data and apps and to defend them at all costs. The images of castles,

moats and even archers have become icons and are regularly featured in advertising for vendors providing security products. In a world that is talking up the value of software defined everything there will likely be even more pressing issues to address – if it is all in software, then it becomes a case of can my software detect and eliminate your software?

In the coming months, we are going to see our networks evolve to better support the "intelligent Edge." The Internet of Things (IoT) is beginning to be more important for the enterprise as detecting changes in behavior matters and the consequences of missing out on opportunities as they present themselves can be detrimental to an enterprises' ability to remain in business. But there will be so many devices generating events that it will be difficult to screen them all for potential outsiders and broadening our defenses sufficiently to ensure the enterprise remains protected will likely be as challenging as anything we dealt with in the past. I have always been a firm believer in thin clients with the only code on the client being what I provided but with IoT interacting with Edge products that may in turn be comprised of multiple tiers, the moat surrounding our castle may no longer be good enough. We need to add more walls, more fences and push out our archers to the very first touch point a potential enemy may encounter.

NonStop occupies a unique niche in that it is a platform few enemies have tried to attack. That isn't to encourage attempts by anyone so much as it's a reflection on the internal architecture of the NonStop kernel. Traditional methods of overlaying code downloaded from a hostile source by outsiders simply won't cut it! But it's more than that as NonStop, as a software platform, forms a strong foundation for running multilayered security programs. Consider the opportunities that look likely to appear with Virtualized NonStop – when it comes to powering the intelligent edge, as HPE promotes today, wouldn't it be highly valued by the enterprise to have a NonStop security workload running fully virtualized on an x86-powered edge product? We aren't quite there yet but I see the opportunity to pursue this by a nonstop vendor as one likely outcome from HPE's push to power the intelligent edge.

It is becoming very true, as it is in many other industries, that the identity of a computer brand will be recognized by the software it runs – and for HPE, the presence of NonStop among its offerings will differentiate its place in the market. Stated another way, NonStop protecting your enterprise, will go a long way to strengthen the brand that is HPE. Very soon, NonStop may not just be the best software platform on the planet but the most secure software on a planet and beyond. 



Security Solutions for your HPE NonStop Environment



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

Learn more at
www.xypro.com

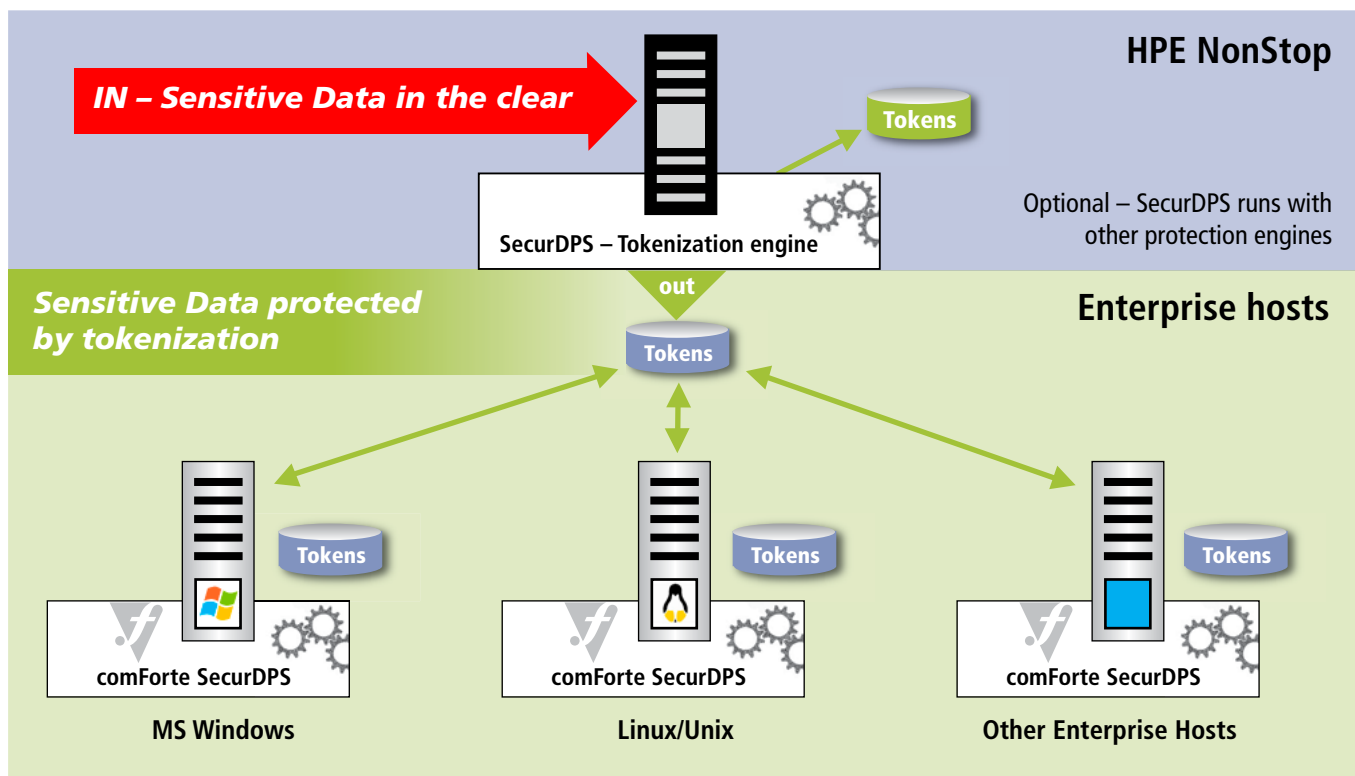
SecurDPS Enterprise Data Protection

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



Learn more at comforte.com/SecurDPS

comforte
better always on