

The Connection

A Journal for the Hewlett Packard Enterprise Business Technology Community

**Bank Chooses “Sizzling-Hot-Takeover”
Data Replication for its BASE24™
Business Continuity Solution**

**The real estate
of infrastructure:**

*Architecting multi-tenancy
for disaster avoidance*

**How to Survive the
zombie
Apocalypse**

**(and Other Disasters) with
Business Continuity
and Security Planning**

XYGATE® Data Protection

All the benefits of HPE SecureData™
No application changes

Simplicity

Secure Stateless Tokenization
Format Preserving Encryption
Page Integrated Encryption
Standards Based AES
Stateless Key Management



Now available from



Hewlett Packard
Enterprise

Protect your Data
at rest and in transit

Learn more at
xypro.com/XDP

 **XYPRO**
Mission Critical Security

©2016 XYPRO Technology Corporation. All rights reserved.
Brands mentioned are trademarks of their respective companies

Get In-Depth Monitoring of NonStop Systems.

At Some of The Industry's Most Intelligent, No-Sweat Prices.



ALTERNATIVE THINKING ABOUT SYSTEMS MONITORING:

Alternative thinking isn't just about constantly monitoring your applications and systems.

It's about alerting you to issues and even fixing them – automatically – based on your specific business goals.

HP's NonStop Availability, Stats and Performances product (known worldwide as HP ASAP) provides automatic monitoring of your system and application objects, keeping you aware of the status of your processing environment at all times.

With HP ASAP, you can set goals that alert you if problems occur. You can also link goals to corrective actions such as initiating repairs or restarting failed components – automatically.

While many monitoring solutions track a few dozen system attributes, HP ASAP lets you monitor thousands simultaneously. What's more, ASAP consumes very few CPU cycles.

Now, you'll know instantly when CPUs are too busy, when disks switch paths, when applications are not performing well, or when there are a myriad of other problems that NonStop ASAP can isolate and resolve.

HP ASAP. For 10 years, the smart, affordable way to keep NonStop servers running non-stop.

Technology for better business outcomes.

HP NONSTOP ASAP

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

Contact your HP representative or partner for a FREE 60-day trial.
Visit www.hp.com/go/nonstop/ASAP





Hewlett Packard
Enterprise

Discover 2016

Accelerating next

Las Vegas June 7–9

Looking forward to seeing you



Table of Contents



14 Cyber Crime Report has Important Insights for NonStop Users

Ken Scudder

16 Machiavellian Software Engineering

Luther Martin

18 Local, remote, and centrally unified key management

Nathan Turajski

23 TIC & NuWave: A Legacy of NonStop Modernization

Gabriella Guerrero, Phil Ly

27 Bank Chooses "Sizzling-Hot-Takeover" Data Replication for its BASE24™ Business Continuity Solution

William G. Holenstein, Keith Evans



30 Data Integration hooking the big fish

Richard Buckle

32 Integrating data protection into legacy systems Methods and Practices

Jason Paul Kazarian

35 The real estate of infrastructure: Architecting multi-tenancy for disaster avoidance

Matt Reisz, Peter Schvarcz, Rebecca Howey

NonStop Technical Library

See [Tips for Locating NonStop Manuals on the HPSC](#) for helpful information. The most recently updated manuals will appear first on these collection pages. Click **Title** to sort the manuals alphabetically.

[HP Integrity NonStop L-Series](#)

[HP Integrity NonStop J-Series](#)

[HP Integrity NonStop H-Series](#)

[HP Integrity NonStop G-Series](#)

[HP Integrity NonStop Release and Migration](#)

[HP Integrity NonStop Safety and Compliance](#)

[HP Integrity NonStop Service Information](#)

38

38 Native Tables in NonStop SQL/MX Part 1

Frans Jongma

42 How to Survive the Zombie Apocalypse (and Other Disasters) with Business Continuity and Security Planning

Steve Tcherchian

Columns...

05 A Note from Connect Leadership

Rob Lesan

06 ADVOCACY The HPE Helion Private Cloud and Cloud Broker Services

Dr. Bill Highleyman

10 NonStop Innovations Deep Dive ETI-NET's Recent Buyout and Acquisition of Insider Technologies

Gabrielle Guerrero

44 Back for More...

Richard Buckle

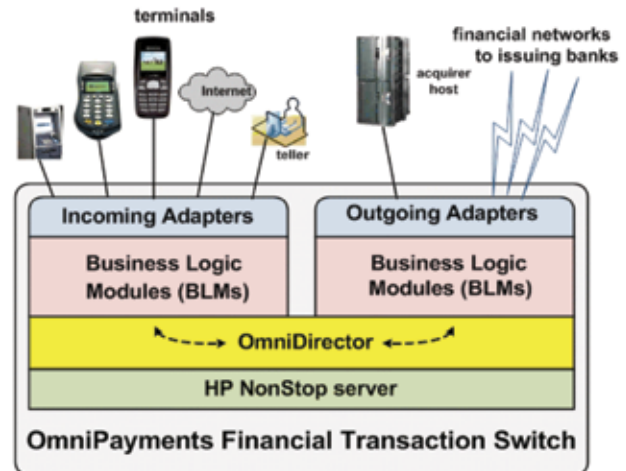
Migrate to OmniPayments

Pain-Free Transition, No Disruption to Customer Service

We're not just talking "in theory." Several large customers already count on the OmniPayments Financial Transaction Switch to support their debit/credit card authorization systems. They migrated from BASE24 to OmniPayments with ease and with no negative impacts on their clients. In some cases, the migration averaged only four months.

How does OmniPayments do it?

- Our team of 100+ programmers is skilled at rapid project turnarounds, meeting deadlines, and enhancing OmniPayments to address each customer's specific requirements.
- The OmniPayments organization is flat. As such, issues requiring attention are addressed quickly.
- Our staff is based in time zones around the world. We work 24 hours a day.
- OmniPayments' modular design permits gradual implementation for smooth migration from existing payments infrastructures.



The OmniPayments pricing model for its standalone system is based on a one-time software license instead of on transaction volume. OmniPayments guarantees that customers will save at least 50% off their current transaction processing costs.

OmniPayments also distributes OmniCloudX on NonStop X. OmniCloudX hosts numerous OmniPayments instances at a pay-for-use price so attractive that mid-size retailers and financial organizations now can enjoy the benefits of having their own high-capacity transaction switches. Starts at only \$5000 USD per month.

The OmniPayments Preauthorization Engine is used by financial institutions in conjunction with the OmniPayments Financial Transaction Switch or as a seamless interface to other providers' switches via a custom support module (CSM). We call it the Fraud Blocker!

OmniPayments systems in production today process 700 million transactions per month, generated by point-of-sales terminals and over 14,000 ATMs. A single OmniPayments system supports up to 10,000 transactions per second. Multiple OmniPayments systems can cooperate to provide any capacity required by an application. From our seven worldwide locations, we serve as a 24x7 managed services provider for remote production monitoring.

OmniPayments Inc.

1566 La Pradera Drive
Campbell, CA 95008 USA
PHONE: +1 408 364 9915
sales@omnipayments.com
www.omnipayments.com

About OmniPayments

OmniPayments is a switching solution for the financial and retail industries. It is deployed on NonStop for the highest availability and offers all the requisite functionality to manage credit/debit-card transactions. It manages multiple devices, hosts application interfaces, and interoperates with third-party products or other systems if required. OmniPayments easily expands to provide additional functionality when needed and supplies complete security functions for every financial transaction handled. Available 24x7, OmniPayments will survive any single fault, requires no downtime for maintenance or upgrades, and supports a range of disaster recovery solutions. Now available on NonStop X and OmniCloudX. Call us today!

* Paid Advertisement



A Note from Connect Leadership

What is a disaster and how do you prepare for one? Everyone's idea on this will vary greatly, but my answer to this is: A disaster is any event that has the ability to interrupt business. The severity of the disaster can be measured many ways. Financial impact to the enterprise seems to be the most logical choice, but I suppose there are as many measures as there are people impacted by such events.

This month's issue focuses on ways to minimize the impact of a disaster. Something we should all understand and be prepared for.


Every enterprise that entrusts HP NonStop Servers with their most critical data clearly understands the three pillars that are the NonStop architecture: Availability, scalability and data integrity. Sometimes I worry that they put almost too much faith in the capabilities of these systems.

Day-to-day disasters occur in every enterprise. Most are small enough that they don't even register on the radar of senior management. A single disk failure, severed communication line, broken index or a corrupted table wouldn't distract most teams. But we don't work on "most teams," do we? The loss of even a single data element to us is cause for alarm. A broken index put us in panic mode and even the thought of losing an entire table is enough to cause me to break into a sweat. Fortunately we have a myriad of tools at our disposal to minimize the impact of these rare, yet possible, database events that would cripple most platforms.

Whether or not disaster recovery and business continuity is your primary function, I recommend you at least keep it in the back of your mind. Treat it as a thought experiment or a game. There are many correct answers and the more you consider, the better you will get.

As always, the devil is in the details. Work with your enterprise team members and your vendors to ensure you understand absolutely every detail about how your operation operates. BC/DR exercises can really show you how much you know about your operation and uncover shortcomings you never realized existed!

Now get out there and exercise your disaster plan. Nothing highlights the cracks in a plan like executing it. If you do it before disaster strikes, you can shore up any issues before an actual disaster strikes.

Good luck and happy testing! 

Thanks.

Rob Lesan

Rob Lesan
XYPRO

2016 Connect Board of Directors



PRESIDENT
Rob Lesan
XYPRO



VICE PRESIDENT
Michael Scroggins
Washington St. Community College



PAST PRESIDENT
Henk Pomper
Plusine ICT



DIRECTOR
Jamil Rashdi
wasl Asset Management Group



DIRECTOR
Trevor Jackson
SOCAN



CHIEF EXECUTIVE OFFICER
Kristi Elizondo
Connect Worldwide



HPE LIAISON
Janice Zdankus
Enterprise Group, HPE

The Connection

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

Kristi Elizondo.....CEO
Stacie Neall.....Managing Editor
Kelly Luna.....Event Marketing Mgr.
Keith McLemore.....Membership Director
Janice Reeder-Higleyman.....Editor at Large
Dr. Bill Higleyman.....Technical Review Board
Karen Copeland
Thomas Burg
Bill Honaker
Justin Simonds

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

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

We accept advertisements in *The Connection*. For rate and size information contact:
E-mail: info@connect-community.org

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

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

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

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

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

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

The HPE Helion Private Cloud and Cloud Broker Services

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

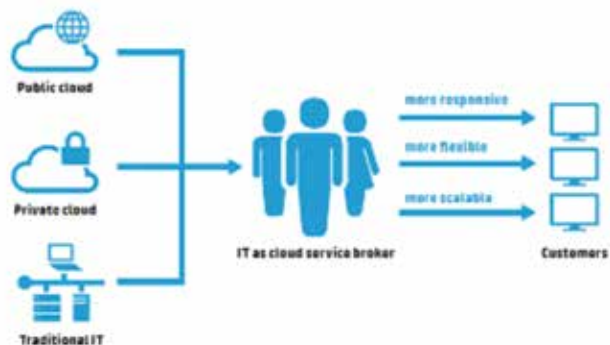
First – A Reminder

Don't forget the HP-UX Boot Camp, which will be held in Chicago from April 24th through April 26th. Check out the Connect website for details.



HPE Helion

HPE Helion is a complete portfolio of cloud products and services that offers enterprise security, scalability, and performance. Helion enables customers to deploy open and secure hybrid cloud solutions that integrate private cloud services, public cloud services, and existing IT assets to allow IT departments to respond to fast changing market conditions and to get applications to market faster. HPE Helion is based on the open-source OpenStack cloud technology.



How a Hybrid Cloud Delivery Model Transforms IT
(from "Become a cloud service broker" HPE white paper)

The Helion portfolio includes the Helion CloudSystem, which is a private cloud; the Helion Development Program, which offers IT developers a platform to build, deploy, and manage cloud applications quickly and easily; and the Helion Managed Cloud Broker, which helps customers to deploy hybrid clouds in which applications span private and public clouds.

In its initial release, HPE intended to create a public cloud with Helion. However, it has since decided not to compete with Amazon AWS and Microsoft Azure in the public-cloud space. It has withdrawn support for a public Helion cloud as of January 31, 2016.

The Announcement of HP Helion

HP announced Helion in May 2014 as a portfolio of cloud products and services that would enable organizations to build, manage, and run applications in hybrid IT environments. Helion is based on the open-source OpenStack cloud. HP was quite familiar with the OpenStack cloud services. It had been running OpenStack in enterprise environments for over three years. HP was a founding member of the OpenStack Foundation and a leader in the OpenStack and Cloud Foundry communities.

HP's announcement of Helion included several initiatives:

- It planned to provide OpenStack public cloud services in twenty of its existing eighty data centers worldwide.
- It offered a free version of the HP Helion OpenStack Community edition, supported by HP, for use by organizations for proofs of concept, pilots, and basic production workloads.
- The HP Helion Development Program based on Cloud Foundry offered IT developers an open platform to build, deploy, and manage OpenStack cloud applications quickly and easily.
- HP Helion OpenStack Professional Services assisted customers with cloud planning, implementation, and operation.

These new HP Helion cloud products and services joined the company's existing portfolio of hybrid cloud computing offerings, including the HP Helion CloudSystem, a private cloud solution.

What Is HPE Helion?

HPE Helion is a collection of products and services that comprises HPE's Cloud Services.

- Helion is based on OpenStack, a large-scale, open-source cloud project and community established to drive industry cloud standards. OpenStack is currently supported by over 150 companies. It allows service providers, enterprises, and government agencies to build massively scalable public, private, and hybrid clouds using freely available Apache-licensed software.
- The Helion Development Environment is based on Cloud Foundry, an open-source project that supports the full lifecycle of cloud developments from initial development through all testing stages to final deployment.

- The Helion CloudSystem (described in more detail later) is a cloud solution for a hybrid world. It is a fully integrated, end-to-end, private cloud solution built for traditional and cloud native workloads and delivers automation, orchestration, and control across multiple clouds.
- Helion Cloud Solutions provide tested custom cloud solutions for customers. The solutions have been validated by HPE cloud experts and are based on OpenStack running on HP ProLiant servers.

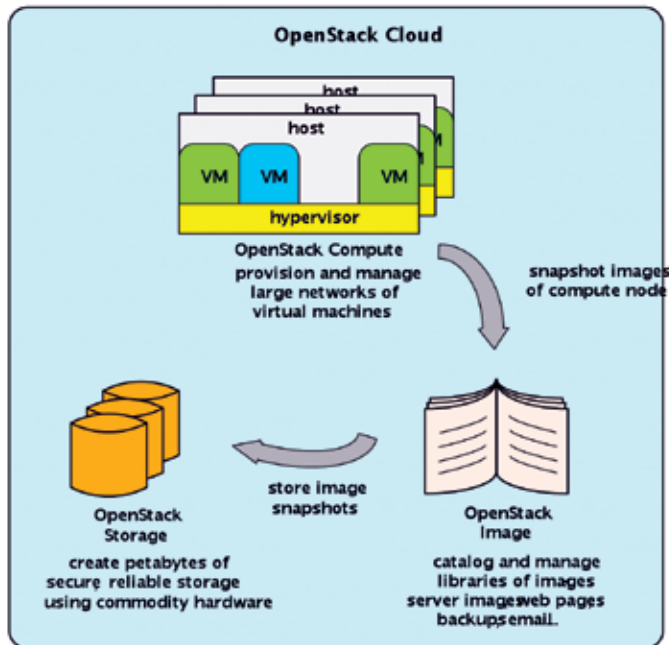
OpenStack – The Open Cloud

OpenStack has three major components:

- OpenStack Compute - provisions and manages large networks of virtual machines.
- OpenStack Storage - creates massive, secure, and reliable storage using standard hardware.
- OpenStack Image - catalogs and manages libraries of server images stored on OpenStack Storage.

OpenStack Compute

OpenStack Compute provides all of the facilities necessary to support the life cycle of instances in the OpenStack cloud. It creates a redundant and scalable computing platform comprising large networks of virtual machines. It provides the software, control panels, and APIs necessary for orchestrating a cloud, including running instances, managing networks, and controlling access to the cloud.



OpenStack Storage

OpenStack Storage is modeled after Amazon's EBS (Elastic Block Store) mass store. It provides redundant, scalable data storage using clusters of inexpensive commodity servers and hard drives to store massive amounts of data. It is not a file system or a database system. Rather, it is intended for long-term storage of large amounts of data (blobs). Its use of a distributed architecture with no central point of control provides great scalability, redundancy, and permanence.

OpenStack Image Service

OpenStack Image Service is a retrieval system for virtual-machine images. It provides registration, discovery, and delivery services for these images. It can use OpenStack Storage or Amazon S3 (Simple Storage System) for storage of virtual-machine images and their associated metadata. It provides a standard web RESTful interface for querying information about stored virtual images.

The Demise of the Helion Public Cloud

After announcing its public cloud, HP realized that it could not compete with the giants of the industry, Amazon AWS and Microsoft Azure, in the public-cloud space. Therefore, HP (now HPE) sunsetted its Helion public cloud program in January, 2016.

However, HPE continues to promote its private and hybrid clouds by helping customers build cloud-based applications based on HPE Helion OpenStack and the HPE Helion Development Platform. It provides interoperability and cloud bursting with Amazon AWS and Microsoft Azure.

HPE has been practical in terminating its public cloud program by the purchase of Eucalyptus to provide ease of integration with Amazon AWS. Investment in the development of the open-source OpenStack model is protected and remains a robust and solid approach for the building, testing, and deployment of cloud solutions. The result is protection of existing investment and a clear path to the future for the continued and increasing use of the OpenStack model.

Furthermore, HPE supports customers who want to run HPE's Cloud Foundry platform for development in their own private clouds or in large-scale public clouds such as AWS or Azure.

The Helion Private Cloud – The HPE Helion CloudSystem

Building a custom private cloud to support an organization's native cloud applications can be a complex project that takes months to complete. This is too long a time if immediate needs must be addressed. The Helion CloudSystem reduces deployment time to days and avoids the high cost of building a proprietary private cloud system.

The HPE Helion CloudSystem was announced in March 2015. It is a secure private cloud delivered as a preconfigured and integrated infrastructure. The infrastructure, called the HPE Helion Rack, is an OpenStack private-cloud computing system ready for deployment and management. It comprises a minimum of eight HP ProLiant physical servers to provide performance and availability. The servers run a hardened version of Linux, hLinux, optimized to support Helion. Additional servers can be added as bare-metal servers or as virtual servers running on the KVM hypervisor.

The Helion CloudSystem is fully integrated with the HP Helion Development Platform. Since the Helion CloudSystem is based on the open-source OpenStack cloud, there is no vendor lock-in.

HP's white paper, "HP Helion Rack solution architecture,"¹ is an excellent guide to the Helion CloudSystem.

Helion Cloud Broker Services

HPE extends the private cloud services offered by the Helion CloudSystem by providing hybrid cloud management with its Helion Managed Cloud Broker. This service is designed to solve the

¹ HP Helion Rack solution architecture, HP White Paper; 2015. <http://www8.hp.com/h20195/V2/getpdf.aspx/4AA5-7655ENW.pdf?ver=1.0>

You wouldn't jump out of an airplane unless you knew your parachute worked – would you?



No, of course you wouldn't. But that's effectively what many companies do when they rely on active/passive or tape-based business continuity solutions. Many companies never complete a practice failover exercise because these solutions are difficult to test. They later find out the hard way that their recovery plan doesn't work when they really need it.

HPE Shadowbase data replication software supports advanced business continuity architectures that overcome the uncertainties of active/passive or tape-based solutions. You wouldn't jump out of an airplane without a working parachute, so don't rely on inadequate recovery solutions to maintain critical IT services when the time comes.

With HPE Shadowbase software, you'll know your parachute will open – every time.

Find out how **HPE Shadowbase** can help you be ready for anything.
Visit www.shadowbasesoftware.com and www.hp.com/go/nonstopcontinuity.



Business Partner

Hewlett Packard
Enterprise

problems of managing cloud and IT services from in-house and external providers. It brokers public-cloud platforms for customers who wish to distribute workloads both on-premises with a Helion CloudSystem private cloud and off-premises using other public-cloud platforms such as Amazon AWS and Microsoft Azure. It also supports virtualized environments using VMware.

The Helion Managed Cloud Broker supports the entire Helion portfolio. It is a universal system for both on-premises private clouds and off-premises public clouds. It offers customers a self-service portal, monitoring dashboards, and management services for security, performance, budgets, and application life-cycle.

HPE also will help organizations become their own cloud brokers. Via its Helion Managed Cloud Services, it provides the following guidance to customers:


- **Advise** – Advise services deliver insight and education on possible uses for cloud technologies in the organization.
- **Transform** – A hybrid cloud system is developed to meet the organization's specific needs.
- **Manage** – Experts monitor and manage day-to-day

operations to ensure secure, consistent delivery and responsive, reliable service.

Summary

The HPE Helion Cloud offering includes the following services:

- The Helion CloudSystem, a private cloud based on the open-source OpenStack cloud.
- The HP Helion Development Program based on Cloud Foundry, an open platform for developers to build, deploy, and manage cloud applications quickly and easily.
- The Helion Managed Cloud Broker, a service designed to solve the problems of managing cloud and IT services from in-house and external providers.
- The Helion Managed Cloud Services, a service that helps organizations become their own cloud brokers.

Two excellent HP white papers describing Helion are “Designing private clouds for cloud native apps”² and “Become a cloud service broker.”³ 

² Designing private clouds for cloud native apps, HPE White Paper; 2015. <http://www8.hp.com/h20195/v2/GetPDF.aspx/4AA5-8470ENN.pdf>

³ Become a cloud service broker, HPE White Paper; 2015. <http://www8.hp.com/h20195/v2/GetPDF.aspx/4AA5-8470ENN.pdf>

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.

SPEAK NOW. BE HEARD.



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



connect

**Support Our
Future Leaders in Technology
TODAY!**

The Connect Future Leaders in Technology (FLUT) is a non-profit organization dedicated to fostering and supporting the next generation of IT leaders. Established in 2010, Connect FLUT is a separate US 501 (c)(3) corporation and all donations go directly to scholarship awards.

ETI-NET's Recent Buyout and Acquisition of Insider Technologies

Gabrielle Guerrero >> NuWave Technologies

I had the opportunity to chat with ETI-NET President Andrew Hall, Chief of Staff Said Hini, and investor Dan Charron to discuss the company's recent acquisition of UK-based Insider Technologies and ETI's growth strategy in the NonStop space and beyond.

Gabrielle Guerrero: Could you give a brief history of ETI-NET?



Andrew Hall: ETI-NET is among the oldest partners in the NonStop space. The company was founded in the mid-80s, and we partnered with Tandem

by 1987. We partnered with Tandem on early projects, where Tandem machines were installed in data centers next to IBM machines. So, the company dates back several decades.

I joined the business in 1990. I had been with Tandem for 10 years, but in 1990 when I joined the Silicon Valley branch, the goal was to transform us from a Canadian-based company to a US-based company. We went through various efforts to accomplish that, but by the time we were ready to start moving staff into the US, the existence of the internet made it cheaper and easier to continue to operate with what I guess you would now call with a more virtual footprint. So we stayed in Canada.

We always specialized in the NonStop space, and in the early 90s we branched into a secondary business, in partnership with Tandem, going after state- and country-level lotteries. It was an interesting campaign because it really takes the idea of an ATM system, where you have a wide network of terminals that come in to a central computer and a central application. Lotteries are not dissimilar from ATMs in this way, except with ATMs the money goes out, and with lottery systems the money comes in. That part of the business was sold in 2000 to a group of investors, but the core business of working in the NonStop space and working with intersystem products, we have been doing now for 30 years.

Gabrielle: Why was there a goal to move from Canada to the US?

Andrew: Well, I think because of the long-range view that if you were going to take the company public it was a better idea. I think also the orientation of tech companies was better served being in the US than in Canada. But it ended up making more sense, strategically and financially at the time, to just stay in Canada.

Gabrielle: What led to the recent sale of ETI-NET to a Canadian investor?

Andrew: Probably the most interesting or the trigger event that led to the sale of the company surrounds the selection by HP to use our BackBox product (a virtual tape system) as their second-generation offering to the customers. By 2012, we had been so successful with the system that we had engineered to

compete against HP, that when it came time for them to refresh their virtual tape system (VTS), we were selected to be the product of choice. That put us in conversations with HP to get the contracts built, and the lawyers who were representing us were in fact the conduit by which the buyer became aware of us. That's Dan. We weren't actively seeking the sale of the company, but like a lot of the NonStop-based businesses, the founders were ready to retire, and they didn't have an exit strategy. In our case, it was easy because the founder hadn't been active in the business for 15 years.

Dan: We are a private equity firm that's looking to invest in software companies, and we believe in the future of NonStop. We acquired ETI in January 2015 and then made the acquisition of Insider Technologies in October 2015. So we acquired two companies that are heavily involved in the NonStop space, and we are looking to make additional acquisitions as well. We're working to create an enterprise that is better organized, with synergies between companies. All of this is part of broader strategy to build a company within the NonStop space and beyond that is able to leverage the strengths of all of the subsidiaries and create better products for the customer in the process.

Gabrielle: What's Dan's background and how did he get into business investments? What made ETI an attractive acquisition?

Andy: Principally, his group investments are in real estate, IT and pharmaceutical, but he's a marketing guy, so what I like about working with him is his perspective is that of a customer-facing sales guy. His attraction to ETI is really due to the caliber of our customers, and this applies to all of NonStop. We're supplying the largest companies in the world.

Dan: We're always looking for companies with enterprise software that cater to the needs of major corporations--Fortune 500 corporations, especially in the financial sector. That's primarily our acquisition strategy. When we look for software companies, we're not interested in the hardware part of the business. We're interested in the software. These companies, like ETI and Insider Technologies, fit well into that strategy of acquiring mission-critical enterprise software.

Gabrielle: Can you tell me a little about Insider Technologies and how that company complements what you do?

Dan: Insider was an interesting target for us because they have a long history of stable customer relationships with major banks and government organizations. Some of Insider's customers include two of the largest armies in Europe, several government branches, The Bank of England, and other major banks across Europe. So the customer profile is very stable, and it also allowed us to expand beyond the traditional customer

base with government agencies and defense departments.

Insider is a very solid company with great software and great development personnel. Also, when we looked into the company, we thought that there was a lot of intellectual property (IP) that they had that would greatly reduce our time to go to market on the new products that ETI was developing. Their UK team has a lot of brain power and talent. ETI has been working for a while now on new products, so the acquisition of Insider has brought in a lot of IP that has helped us speed up the launch of these products and improve them as well. That's the synergy from a product perspective.



From a staffing perspective, incorporating both companies into one organization has helped with sharing information and increasing cooperation between the staff members. Finally, the acquisition of a company in the UK provided us with better support coverage in Europe and worldwide. By buying Insider and having a presence in Europe, the US, and Canada, we were in a better position to service our customers around the world.

Andy: Insider Technologies was formed by a first-generation Tandem sales guy. It had basically grown with customers in the UK market. So what you have is an older partner with a select group of customers, but almost no exposure outside of their local geography. The company had gone through a buyout about three years ago, and when we found the business, it had accomplished a lot in the sense of building product both within and outside of the NonStop market, directed at payments processors. So the overlap there is that, like many NonStop vendors, about 80% of ETI's customers are in the payments space. That's Insider's expertise, and Insider's code (the IP) was built using the same tool set, programming language, databases, and so on. So one of the things you look at in an acquisition is whether the people there are using the same vocabulary and tools that the employees of the parent company are using, and that was the case. That made it really attractive for us.

The piece that we've gone through rethinking and are working hard on now is simplifying the product's basic features so that we can more readily deploy it. Since the Insider product depends upon Windows servers, one of the other attractions for us was that our BackBox product, which is a Windows server, is already on the floors of most of the large data centers that are running NonStop systems. So we have the footprint already in the data center that will allow us in future releases

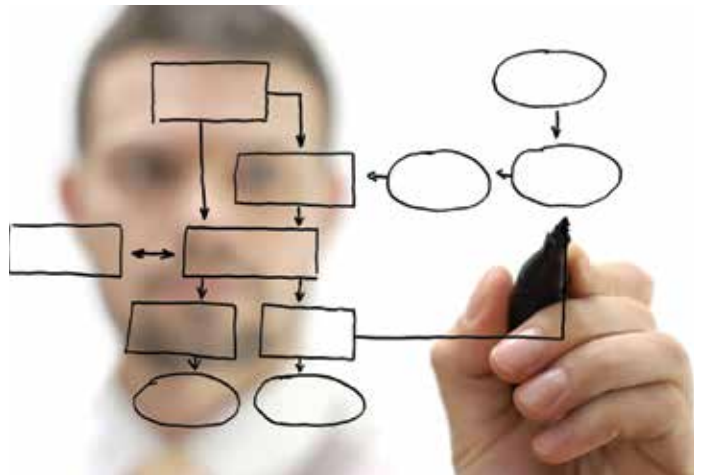
of our products to embed the Insider IP and offer expanded functionality and additional licensing opportunities.

The point here is that the investment profile, or the growth profile, is certainly not limited to the NonStop space. We are more interested in taking advantage of the access we have to the customers in the payments space.

Dan: We are taking the best of both worlds and merging them together: the strength, talents, and brainpower of the people in both organizations and the IP in both organizations has been brought together in one healthy tree, which means that the "roots" of the parent company must be strong and well planted. We're able to leverage some of the strengths that complement our organization and vice versa.

Gabrielle: Have you guys been experiencing any growing pains while you're merging the two company cultures and the different skills of your resources?

Said: One of the biggest challenges we had to tackle when we merged two companies was to have everyone, as Dan said, under the same healthy tree. What that means is to have everyone use the same system to communicate with each other, and to encourage two different groups of people, who never knew each other, to work together. So this was the challenge with communication, but it was made possible by modernizing the infrastructure and putting in place support software so that both groups can work together, as well as project management software, so we can share resources and information.



Andy: Yeah I would say that it's been interesting. One of the things we acquired from Insider was Agile, which as many people know is a very well-organized and well-implemented development methodology. It was a well-known term among ETI's developers, but it includes some principles and practices that we hadn't used before. So we have incorporated that into ETI's development methodology, while keeping our original development methodology alive. Certainly we are dealing with additional time zone issues. We have Canadian operations as well as labs in San Jose, California, so we have always had a three-hour time difference, but Insider is five hours east of us, and we actually have some people who are over in Asia as well, so we're learning to "follow the sun" in a sense.

The other difference is that there is a certain pace that we've gotten used to in the NonStop space, and Dan has energized us

Everyone is lining up to get LightWave Server



Don't get left behind.

LightWave Server™ uses JSON and REST technology to send data to modern clients like mobile apps and browser-based applications that run on virtually any platform.



Learn more at
www.nuwavetech.com/lwsconnection

NuWave
TECHNOLOGIES

to a different intensity level, so he's really brought some new expectations. There's always some adjustments that have to be made when a company changes hands and the buyer is looking to not only keep running it, but grow it.

Dan: And these things all put us in a better position to make additional acquisitions in the future. We've been able to merge the two companies by modernizing infrastructure to improve communication and cooperation, and now we're in a position to make additional acquisitions.

Gabrielle: Andy, it's great he's pushing you guys. That's what you want.


Andy: Yes, it is! But the reality of the Insider transaction is, as with most acquisitions, that we had to say goodbye to a fair amount of staff. I had the hard duty of going in, saying, "Hi, we bought the company," and then a week later, a number of the departments had become redundant. I'm pleased to say that we did all the right things in terms of providing placement services, references, and so on, so to my knowledge everyone who was impacted by the acquisition is now gainfully and happily employed. And this was all just in October.

Gabrielle: You mention that you're going to be acquiring a couple of companies this year that are larger than ETI.

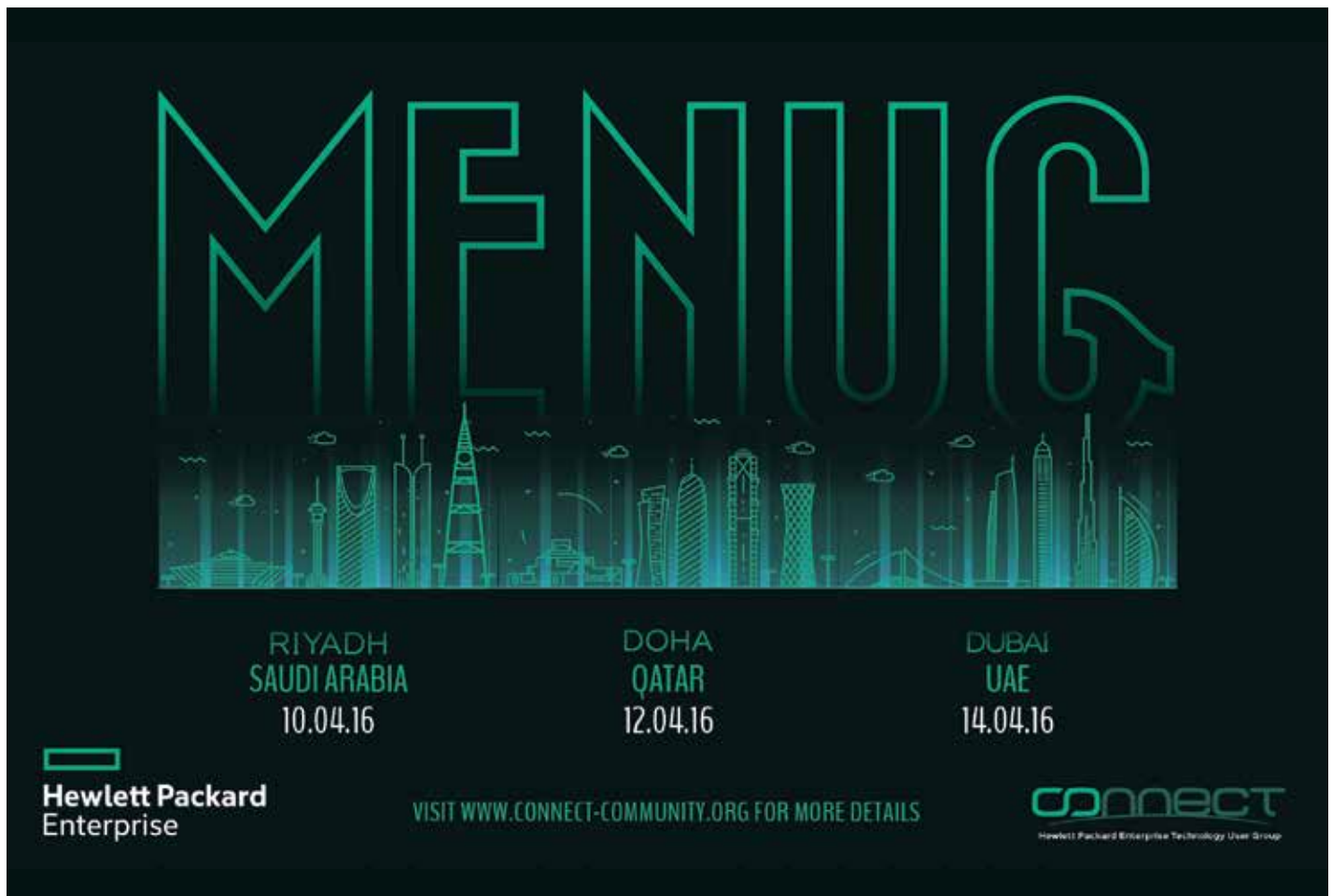
Do you see any challenges down the road with acquiring companies larger than your own?

Andy: I would say right now the challenge in the market we are looking in is finding candidate projects where there's an appetite to be acquired. I am attending some events in the IBM space because, in my own opinion, you also find companies that have a long history with solid customers and owners at retirement age or older.

Dan: We don't see any challenges with acquiring large companies because our business processes are very well-streamlined and organized. We wouldn't look to buy a company that was larger that was in a difficult position. We wouldn't want to buy a distressed company larger than us, for example. That's a path and an adventure we don't want to embark on. But to acquire a company that is larger than us and doing well wouldn't be a problem. We have a very strong management team, strong processes, and tremendous resources. So as long as the company we are acquiring is in pretty good shape, it's not really a problem at all.

We look forward to future acquisitions in the NonStop space and beyond, in order to further our technology and better serve our customers. 

Gabrielle Guerrero is the director of business development for NuWave Technologies, an HPE NonStop middleware (integration) and consulting company. She is also the co-author of the NonStop Innovations blog (www.nuwavetech.com/hp-nonstop-innovations), which takes an unbiased look at the latest innovations and announcements in the NonStop space.



The graphic features the word "MENU" in large, stylized, teal-outlined letters at the top. Below the letters is a teal-colored skyline of various city buildings. At the bottom, there are three event listings in teal text:

Location	Date
RIYADH SAUDI ARABIA	10.04.16
DOHA QATAR	12.04.16
DUBAI UAE	14.04.16

In the bottom left corner is the Hewlett Packard Enterprise logo. In the bottom center is the text "VISIT WWW.CONNECT-COMMUNITY.ORG FOR MORE DETAILS". In the bottom right corner is the "CONNECT" logo with the text "Hewlett Packard Enterprise Technology User Group" underneath it.



Cyber Crime Report has Important Insights for NonStop Users

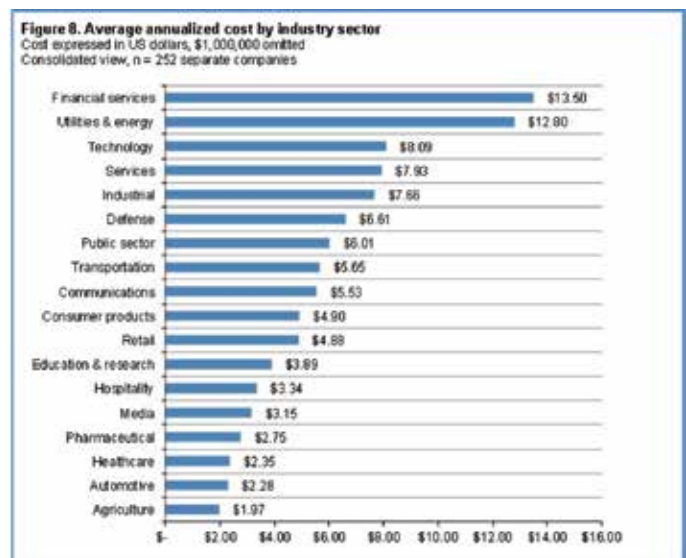
Ken Scudder >> Sr. Director, Business Development and Strategic Alliances >> XYPRO Technology

The latest reports on IT security all seem to point to a similar trend—both the frequency and costs of cyber crime are increasing. While that may not be too surprising, the underlying details and sub-trends can sometimes be unexpected and informative. The Ponemon Institute’s recent report, “[2015 Cost of Cyber Crime Study: Global](#)”, sponsored by Hewlett Packard Enterprise, definitely provides some noteworthy findings which may be useful for NonStop users.

Here are a few key findings of that Ponemon study which I found insightful:

- **Cyber crime cost is highest in industry verticals that also rely heavily on NonStop systems**

The report finds that cost of cyber crime is highest, by far, in the Financial Services and Utilities & Energy sectors, with average annualized costs of \$13.5 million and \$12.8 million, respectively. As we know, these two verticals are greatly dependent on NonStop. Other verticals with high average cyber crime costs that are also major users of NonStop systems include Industrial, Transportation, Communications and Retail industries. So, while we’ve not seen the NonStop platform in the news for security breaches, it’s clear that NonStop systems operate in industries frequently targeted by cyber criminals and which suffer high costs of cyber crime—which means NonStop systems should be protected accordingly.



Source: Ponemon Institute “2015 Cost of Cyber Crime Study: Global”

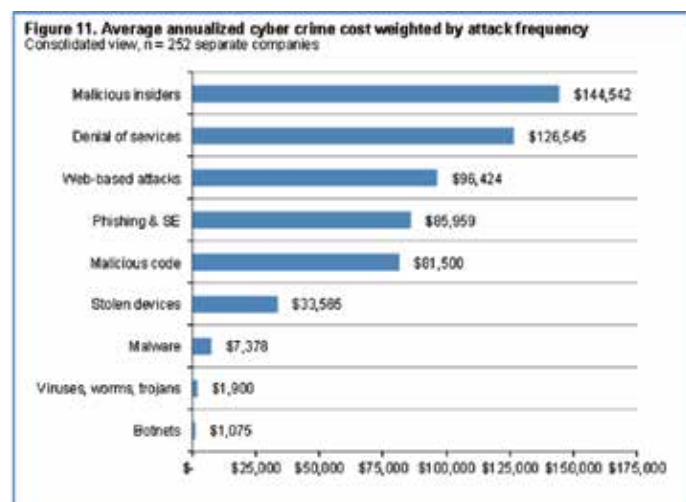
- **Business disruption and information loss are the most expensive consequences of cyber crime**

Among the participants in the study, business disruption and

information loss represented the two most expensive sources of external costs: 39% and 35% of costs, respectively. Given the types of mission-critical business applications that often run on the NonStop platform, these sources of cyber crime cost should be of high interest to NonStop users and need to be protected against (for example, protecting against data breaches with a NonStop tokenization or encryption solution).

- **Malicious insider threat is most expensive and difficult to resolve per incident**

The report found that 98-99% of the companies experienced attacks from viruses, worms, Trojans and malware. However, while those types of attacks were most widespread, they had the lowest cost impact with an average cost of \$1,900 (weighted by attack frequency). Alternatively, while the study found that “only” 35% of companies had had malicious insider attacks, those attacks took the longest to detect and resolve (on average, over 54 days!). And with an average cost per incident of \$144,542, malicious insider attacks were far more expensive than other cyber crime types. Malicious insiders typically have the most knowledge when it comes to deployed security measures, which allows them to knowingly circumvent them and hide their activities. As a first step, locking your system down and properly securing access based on NonStop best practices and corporate policy will ensure users only have access to the resources needed to do their jobs. A second and critical step is to actively monitor for suspicious behavior and deviation from normal established processes—which can ensure suspicious activity is detected and alerted on before it culminates in an expensive breach.



Source: Ponemon Institute “2015 Cost of Cyber Crime Study: Global”

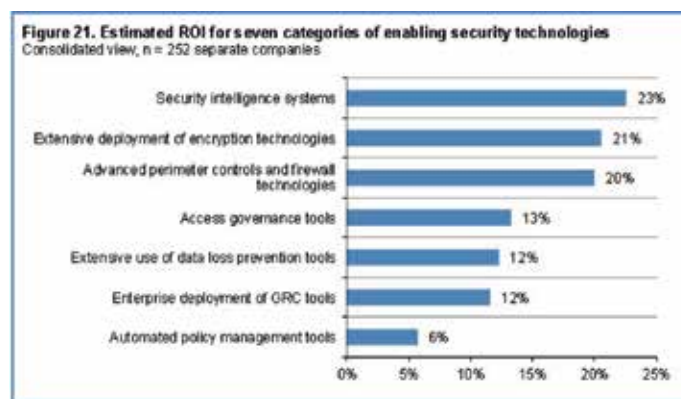
- **Basic security is often lacking**

Perhaps the most surprising aspect of the study, to me at least, was that so few of the companies had common security solutions deployed. Only 50% of companies in the study had implemented access governance tools and fewer than 45% had deployed security

intelligence systems or data protection solutions (including data-in-motion protection and encryption or tokenization). From a NonStop perspective, this highlights the critical importance of basic security principles, such as: strong user authentication, policies of minimum required access and least privileges, no shared super-user accounts, activity and event logging and auditing, and integration of the NonStop system with an enterprise SIEM (like HPE ArcSight). It's very important to note that HPE includes XYGATE User Authentication (XUA), XYGATE Merged Audit (XMA), NonStop SSL/TLS and NonStop SSH in the NonStop Security Bundle, so most NonStop customers already have much of this capability. Hopefully, the NonStop community is more security conscious than the participants in this study—but we can't be sure and it's worth reviewing whether security fundamentals are adequately implemented.

- **Security solutions have strong ROI**

While it's dismaying to see that so few companies had deployed important security solutions, there is good news in that the report shows that implementation of those solutions can have a strong ROI. For example, the study found that security intelligence systems had a 23% ROI and encryption technologies had a 21% ROI. Access governance had a 13% ROI. So while these security solutions aren't as widely deployed as they should be, there is a good business case for putting them in place.



Source: Ponemon Institute “2015 Cost of Cyber Crime Study: Global”

Those are just a few takeaways from an excellent study; there are many additional interesting points made in the report and it's worth a full read. The good news is that today there are many great security products available to help you manage security on your NonStop systems—including products sold by HPE, as well as products offered by NonStop partners such as XYPRO, comForte and Computer Security Products.

As always, if you have questions about NonStop security, please feel free to contact me (email: kenneth.scudder@xypro.com) or your XYPRO sales representative.

Statistics and Information in this article are based on the Ponemon Institute “2015 Cost of Cyber Crime Study: Global” sponsored by Hewlett Packard Enterprise (<http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/>)

Ken Scudder, Senior Director, Business Development and Strategic Alliances – Ken joined XYPRO in 2012, with more than a decade of enterprise software experience in product management, sales and business development. Ken is PCI-ISA certified and his previous experience includes positions at ACI Worldwide, CA Technologies, Peregrine Systems (now part of HPE) and Arthur Andersen Business Consulting. A former navy officer and U.S. diplomat, Ken holds an MBA from the University of Southern California and a Bachelor of Science degree from Rensselaer Polytechnic Institute.



Machiavellian Software Engineering

Luther Martin >> HPE Security – Data Security Distinguished Technologist

We may be able to learn a useful thing or two about software engineering from the Italian Renaissance writer Niccolò Machiavelli. In particular, it might be interesting to ask what Machiavelli might think about some of the established standards for software engineering.

The term “Machiavellian” has come to mean behavior that combines diabolical cunning with a ruthless disregard for morality, but this may be due to the fact that the Machiavelli’s irony was missed by many readers of his now-famous book *The Prince*.

Supporters of this interpretation note that all of Machiavelli’s other writings supported a more republican view of politics, the fact that he had been imprisoned and tortured on the rack by the Medici family to whom he dedicated *The Prince*, and that Casare Borgia, whom Machiavelli cited as a role model in this book, was widely known as a fool and a failure. If this interpretation is correct, *The Prince* may be one of the most widely misunderstood books ever written, probably coming in right behind the textbooks used in freshman calculus and physics classes.

From our point of view, over 500 years after Machiavelli wrote *The Prince*, it’s impossible to know for sure whether or not he meant this book to be taken literally, but the fact that many people interpret it as a serious guide to politics shows that if he meant the book to be a satire, he was much too subtle. This shouldn’t be too surprising, for even less subtle arguments can be misunderstood, and the origins of what’s now known as the “waterfall model” of software development provides a good example of this.

In the waterfall model, software development proceeds in an orderly, structured way through a set of steps that take you from defining requirements through to a finished product. Proponents of this model argue that the big, up-front costs that ensure that the requirements and design are correct pay for themselves in terms of greatly reduced time and effort to fix any bugs that may occur. They note that a bug found at design time can be up to 200 times cheaper to fix than the same bug found after software is in use by customers.

An alternative are agile methods. Instead of making a single pass through a carefully-considered set of steps, these techniques require more than one iteration through a set of much smaller

steps. Agile methods assume that you cannot get requirements and design correct the first time because the requirements will always change over time, and that the development process for software should reflect this reality. Smaller steps let you adjust to changing requirements after each step, while a strict implementation of the waterfall model will unerringly move towards the same requirements that it started with, even if they are later proven to be inadequate.

Winston Royce summarized the lessons that he had learned in large government software projects in his 1970 paper “Managing the Development of Large Software Systems.” This paper is often cited as the basis for the waterfall model, but Royce’s discussion of software development in this paper certainly doesn’t suggest that the waterfall model is a good one. Although Royce did describe what came to be known as the “waterfall model,” he also noted that it is “risky and invites failure.” He also suggested that a more iterative process would be better, a process much like what we call agile methods today.

Thus Royce was even less subtle than Machiavelli - he was fairly clear in expressing his disapproval of what came to be known as the “waterfall model.” So we might wonder why the model that Royce described as being bad was widely adopted while the agile models, which Royce described as being good, were largely ignored for many years. And although cynics might be tempted to note a possible similarity between Machiavelli being tortured by the Medicis and Royce’s work on large government contracts, it’s unlikely that Royce’s paper was ever interpreted as satire. So we need to find another reason to explain the adoption of the waterfall model.

One reason that the waterfall model was adopted soon after Royce wrote his famous paper may have been that it’s much easier to understand and define than agile methods. It’s relatively easy to write standards that define the use of waterfall-like methods, but doing the same for agile methods is very difficult. As early as 1974, for example, the US Navy had already used the waterfall model as the basis for their MIL-STD-1679 standard, “Weapon System Software Development.” By 1995, this had evolved into the ISO/IEC 12207 standard “Software Life Cycle Processes,” keeping a strong bias towards the waterfall model as it did.

But while the more rigid waterfall process has found its way into several standards, the more complicated agile methods have yet to find the same level of acceptance by standards bodies. This may be because agile methods are more difficult to understand and define than more rigid models are. It may even be the case that even though we can easily list general principles that they may follow, we still don't exactly know how to define agile methods, and this makes creating standards for them extremely difficult.

Many of the early discussions of software development models were based on the experiences in large government projects, where rigid, hierarchical structures tend to be preferred, and this probably led to a bias that favored such structures in managing software projects. Software project managers may also have just supported what they believed to be feasible, in the large government software projects, with which they were familiar, instead of promoting what they really thought was the best way to manage their projects. Even if they believed that agile models were better, it may have been the case that it wasn't practical to use these within the constraints of their projects, so that they may have accepted an alternative that was practical for them to use, hoping that it would at least reduce some of the problems that they faced.

The adoption of the waterfall model may also have been a reaction to the more chaotic processes that were common in the early days of software engineering. When these processes were seen not to be working well, a natural reaction may have been

to try to impose a more rigid structure, and the waterfall model provided an easy way to formalize this additional structure. So the eventual return to agile models that we see today may have been caused by the realization that rigid structures also had shortcomings. Because agile models are also not perfect, we shouldn't be too surprised if the pendulum swings back towards more structured approaches in the future. If the past is an accurate guide to this, we might expect this to start in the next 10 years or so.

So it may have been the case that software project managers didn't misinterpret Royce's first discussion of the waterfall model as satire. Instead, they may have adopted the waterfall model because it was relatively easy, fit within the constraints they were accustomed to and seemed to be an adequate solution to some of the problems that they faced at the time. The fact that Royce first described it in a less-than-positive way may have been ignored because of these perceived advantages. So early software engineers didn't develop the waterfall model from Royce's work - they probably developed it in spite of it.

Machiavelli's reaction to this would probably depend on his intent when he wrote *The Prince*. If he meant it to be taken literally, he would probably admire the audacity that early software engineers showed when they pointed to Royce's paper as the first description of the waterfall model. But if he meant *The Prince* to be interpreted as satire, he might be surprised by how writing that was even less subtle than his could be misinterpreted by its readers. [CS](#)

Luther Martin is a Hewlett Packard Enterprise Distinguished Technologist. You can reach him at luther.martin@hpe.com.

Get Connected!

Sign up today! It's easy and FREE for HPE customers and HPE employees.

Tell a friend!

www.ow.ly/ZbdCc

CONNECT
Hewlett Packard Enterprise Technology User Group

Local, remote, and centrally unified key management

HPE Enterprise Secure Key Manager solutions

Nathan Turajski >> Senior Product Manager >> Hewlett Packard Enterprise

Key management for encryption applications creates manageability risks when security controls and operational concerns are not fully realized. Various approaches to managing keys are discussed with the impact toward supporting enterprise policy.

Overview

When deploying encryption applications, the long-term maintenance and protection of the encryption keys need to be a critical consideration. Cryptography is a well-proven method for protecting data and, as such, is often mandated in regulatory compliance rules as reliable controls over sensitive data, using well-established algorithms and methods.

However too often, not as much attention is placed on the social engineering and safeguarding of maintaining reliable access to keys. If you lose access to keys, you by extension lose access to the data that can no longer be decrypted. With this in mind, it's important to consider various approaches when deploying encryption with secure key management that ensure an appropriate level of assurance for long-term key access and recovery that is reliable and effective, throughout the information lifecycle of use.

Key management deployment architectures

Whether through manual procedures or automated, a complete encryption and secure key management system includes the encryption endpoints (devices, applications, etc.), key generation and archiving system, key backup, policy-based controls, logging and audit facilities, and best-practice procedures for reliable operations. Based on this scope required for maintaining reliable ongoing operations, key management deployments need to match the organizational structure, security assurance levels for risk tolerance, and operational ease that impacts ongoing time and cost.

Local key management

Key management that is distributed in an organization where keys coexist within an individual encryption application or device is a local-level solution. When highly dispersed organizations are responsible for only a few keys and applications, and no system-wide policy needs to be enforced, this can be a simple approach. Typically, local users are responsible for their own ad hoc key management procedures, where other administrators or auditors across an organization do not need access to controls or activity logging.

Managing a key lifecycle locally will typically include manual operations to generate keys, distribute or import them to applications, and archive or vault keys for long-term recovery—and

as necessary, delete those keys. All of these operations tend to take place at a specific data center where no outside support is required or expected. This creates higher risk, if local teams do not maintain ongoing expertise or systematic procedures for managing controls over time. When local keys are managed ad hoc, reliable key protection and recovery become a greater risk.

Although local key management can have advantages in its perceived simplicity, without the need for central operational overhead, it is weak on dependability. In the event that access to a local key is lost or mishandled, no central backup or audit trail can assist in the recovery process.

“Organizations must develop a business-led data-centric security strategy that will lead to the appropriate selection of either multiple siloed KM solutions or a single Enterprise Key Manager (EKM). As EKM products continue to mature and improve, clients will be better-able to implement a consistent, enterprise-class strategy—thereby protecting data, and achieving legal and regulatory compliance, while limiting risk in a demonstrable way, and reducing operational and capital costs.”

– Hype Cycle for Data Security, Gartner, 2015



Figure 1: Local key management over a local network where keys are stored with the encrypted storage.

Fundamentally risky if no redundancy or automation exist

Local key management has potential to improve security if there are no needs for control and audit of keys as part of broader enterprise security policy management. That is, it avoids wide access exposure that, through negligence or malicious intent, could compromise keys or logs that are administered locally. Essentially, maintaining a local key management practice can minimize external risks to undermine local encryption and key management lifecycle operations.

However, deploying the entire key management system in one location without benefit of geographically dispersed backup or centralized controls can add higher risk to operational continuity. For example, placing the encrypted data, the key archive, and a key backup in the same proximity is risky in the event a site is attacked or disaster hits. Moreover, encrypted data is easier to attack when keys are co-located with the targeted applications—the analogy being locking your front door, but placing keys under a doormat, or leaving keys in the car ignition instead of your pocket.



Figure 2: When keys are co-located along with the encrypted data, easy access creates more risk.

While local key management could potentially be easier to implement over centralized approaches, economies of scale will be limited as applications expand, as each local key management solution requires its own resources and procedures to maintain reliably within unique silos. As local approaches tend to require manual administration, the keys are at higher risk of abuse or loss as organizations evolve over time, especially when administrators change roles, compared with maintenance by a centralized team of security experts.

As local-level encryption and secure key management applications begin to scale over time, organizations will find the cost and management simplicity originally assumed now becoming more complex, making audit and consistent controls unreliable. Organizations with limited IT resources that are oversubscribed will need to solve new operational risks.

Pros

- May improve security through obscurity and isolation from a broader organization that could add access control risks
- Can be cost effective if kept simple with a limited number of applications that are easy to manage with only a few keys

Cons

- Co-located keys with the encrypted data provides easier access if systems are stolen or compromised
- Often implemented via manual procedures over key lifecycles—prone to error, neglect, and misuse
- Places “all eggs in a basket” for key archives and data without benefit of remote backups or audit logs
- May lack local security skills, creates higher risk as IT teams are multitasked or leave the organization
- Less reliable audits with unclear user privileges and a lack of central log consolidation, driving up audit costs and

remediation expenses, long-term

- Data mobility hurdles—media moved between locations requires key management to be moved also
- Does not benefit from a single, central policy-enforced, auditing efficiencies or unified controls for achieving economies and scalability

Remote key management

Key management where application encryption takes place in one physical location, while keys are managed and protected in another, allows for remote operations, which can help lower risks. As illustrated in the local approach, there is vulnerability from co-locating keys with encrypted data if a site is compromised, due to attack, misuse, or disaster.

Remote administration enables encryption keys to be controlled without management being co-located with the application, such as a console UI via secure IP networks. This is ideal for dark data centers or hosted services that are not easily accessible and/or widely distributed locations where applications need to deploy across a regionally dispersed environment .



Figure 3: Remote key management separates encryption key management from the encrypted data.

Provides higher assurance security by separating keys from the encrypted data

While remote management doesn't necessarily introduce automation, it does address local attack threat vectors and key availability risks through remote key protection, backups, and logging flexibility. The ability to manage controls remotely can improve response time during manual key administration, in the event encrypted devices are compromised in high-risk locations. For example, a stolen storage device that requests a key at boot-up could have the key remotely located and destroyed, along with audit log verification, to demonstrate compliance with data privacy regulations for revoking access to data. Maintaining remote controls can also enable a quicker path to safe harbor, where a breach won't require reporting if proof of access control can be demonstrated.

As a current high-profile example of remote and secure key management success, the concept of “bring your own encryption key” is being employed with cloud service providers, enabling tenants to take advantage of co-located encryption applications, without worry of keys being compromised within a shared environment. Cloud users maintain control of their keys and can revoke them for application use at any time, while also being free to migrate applications between various data centers. In this way, the economies of cloud flexibility and scalability are enabled at a lower risk.

While application keys are no longer co-located with data locally, encryption controls are still managed in silos, without the need to co-locate all enterprise keys centrally. Although economies of scale are not improved, this approach can have similar simplicity as local methods, while also suffering from a similar dependence on manual procedures.

Pros

- Provides the lowered-risk advantage of not co-locating keys, backups, and encrypted data in the same location, which makes the system more vulnerable to compromise
- Similar to local key management, remote management may improve security through isolation if keys are still managed in discrete application silos
- Cost effective when kept simple—similar to local approaches, but managed over secured networks from virtually any location where security expertise is maintained
- Easier to control and audit without having to physically attend to each distributed system or applications, which can be time consuming and costly
- Improves data mobility—if encryption devices move, key management systems can remain in their same place, operationally

Cons

- Manual procedures don't improve security, if still not part of a systematic key management approach
- No economies of scale if keys and logs continue to be managed only within a silo for individual encryption applications

Centralized key management

The idea of a centralized, unified—or commonly, an enterprise secure key management—system is often a misunderstood definition. Not every administrative aspect needs to occur in a single, centralized location; rather, the term refers to an ability to centrally coordinate operations across an entire key lifecycle by maintaining a single pane of glass for controls. Coordinating encrypted applications in a systematic approach creates a more reliable set of procedures to ensure what authorized devices can access keys and who can administer key lifecycle policies, comprehensively.

A centralized approach reduces the risk of keys being compromised locally along with encrypted data by relying on higher-assurance, automated management systems. As a best practice, a hardware-based tamper-evident key vault and policy/logging tools are deployed in clusters, redundantly for high availability, spread across multiple geographic locations, to create replicated backups for keys, policies, and configuration data.



Figure 4: Central key management over wide area networks enables a single set of reliable controls and auditing over keys.

Higher assurance key protection combined with reliable security automation

As mentioned with local and remote key management, a higher risk is assumed if relying upon manual procedures to manage keys. Whereas, a centralized solution runs the risk of creating toxic combinations of access controls if users are over-privileged to manage enterprise keys, or applications are not properly authorized to store and retrieve keys.

Realizing these critical concerns, centralized and secure key management systems are designed to coordinate enterprise-wide environments of encryption applications, keys, and administrative users, using automated controls that follow security best practices. Unlike distributed key management systems that may operate locally, centralized key management can achieve better economies with the high-assurance security of hardened appliances that enforce policies with reliability, while ensuring that activity logging is tracked consistently for auditing purposes, and alerts and reporting are more efficiently distributed and escalated when necessary.

Pros

- Similar to remote administration, economies of scale achieved by enforcing controls across large estates of mixed applications from any location, with the added benefit of centralized management economies
- Coordinated partitioning of applications, keys, and users to improve on the benefit of local management
- Automation and consistency of key lifecycle procedures universally enforced to remove the risk of manual administration practices and errors
- Typically managed over secured networks from any location to serve global encryption deployments
- Easier to control and audit with a “single pane of glass” view to enforce controls and accelerate auditing
- Improves data mobility—key management system remains centrally coordinated with high availability
- Economies of scale and reusability as more applications take advantage of a single, universal system

Cons

- Key management appliances carry higher upfront costs for a single application, but do enable future reusability to improve total cost of ownership (TCO)/return on investment (ROI) over time with consistent policy and removing redundancies.
- If access controls are not managed properly, toxic combinations of users are over-privileged to compromise the system—best practices can minimize risks.

Best practices—adopting a flexible strategic approach

In real world practice, local, remote, and centralized key management can coexist within larger enterprise environments driven by the needs of diverse applications deployed across multiple data centers. While a centralized solution may apply globally, there may also be scenarios where localized solutions require isolation for mandated reasons (e.g., government regulations or weak geographic connectivity); application sensitivity level; or organizational structure where resources, operations, and expertise are best to remain in a center of excellence.

In an enterprise-class, centralized and secure key management solution, a cluster of key management servers may be distributed globally while synchronizing keys and configuration data for failover. Administrators can connect to appliances from anywhere globally to enforce policies with a single set of controls to manage and a single point for auditing security and performance of the distributed system.



Figure 5: Clustering key management enables endpoints to connect to local key servers, a primary data center, and/or disaster recovery locations, depending on high availability needs and global distribution of encryption applications.

Considerations for deploying a centralized enterprise key management system

Enterprise secure key management solutions that offer the flexibility of local, remote, and centralized controls over keys will include a number of defining characteristics. It's important to consider the aspects that will help match the right solution to an application environment for best long-term reusability and ROI—relative to cost, administrative flexibility, and security assurance levels provided:

- **Hardware or software assurance:** Key management servers deployed as appliances, virtual appliances, or software will protect keys to varying degrees of reliability. FIPS 140-2 is the standard to measure security assurance levels. A hardened hardware-based appliance solution will be validated to level 2 or above for tamper evidence and response capabilities.
- **Standards-based or proprietary:** The OASIS Key Management Interoperability Protocol (KMIP) standard allows servers and encrypted applications to communicate for key operations. Ideally, key managers can fully support current KMIP specifications to enable the widest application range, increasing ROI under a single system.
- **Policy model:** Key lifecycle controls should follow NIST SP800-57 recommendations as a best practice. This includes key management systems enforcing user and application access policies depending on the state in a lifecycle of a particular key or set of keys, along with a complete, tamper-proof audit trail for control attestation.
- **Partitioning and user separation:** To avoid applications and users having over-privileged access to keys or controls, centralized key management systems need to be able to group applications according to enterprise policy, and to offer flexibility when defining user roles to specific responsibilities.
- **High availability:** For business continuity, key managers need to offer clustering and backup capabilities for key vaults, and configurations for failover and disaster recovery. At a minimum, two key management servers replicating data over a geographically dispersed network, and/or a server with automated backups, are required.

- **Scalability:** As applications scale and new applications are enrolled to a central key management system, keys, application connectivity, and administrators need to scale with the system. An enterprise-class key manager can elegantly handle thousands of endpoint applications and millions of keys for greater economies.
- **Logging:** Auditors require a single pane of glass view into operations, and IT needs to monitor performance and availability. Activity logging with a single view helps accelerate audits across a globally distributed environment. Integration with enterprise systems via SNMP, syslog, email alerts, and similar methods help ensure IT visibility.
- **Enterprise integration:** As key management is one part of a wider security strategy, a balance is needed between maintaining secure controls and wider exposure to enterprise IT systems for ease of use. External authentication and authorization such as Lightweight

Directory Access Protocol (LDAP), or security information and event management (SIEM) for monitoring, helps coordinate with enterprise policy and procedures.

Conclusions

As enterprises mature in complexity by adopting encryption across a greater portion of their critical IT infrastructure, the need to move beyond local key management towards an enterprise strategy becomes more apparent. Achieving economies of scale with a single-pane-of-glass view into controls and auditing can help accelerate policy enforcement and control attestation.

Centralized and secure key management enables enterprises to locate keys and their administration within a security center of excellence, while not compromising the integrity of a distributed application environment. The best of all worlds can be achieved with an enterprise strategy that coordinates applications, keys, and users with a reliable set of controls.

As more applications start to embed encryption capabilities natively, and connectivity standards such as KMIP become more widely adopted, enterprises will benefit from an enterprise secure key management system that automates security best practices and achieves greater ROI as additional applications are enrolled into a unified key management system.

HPE Data Security Technologies

HPE Enterprise Secure Key Manager

Our HPE enterprise data protection vision includes protecting sensitive data wherever it lives and moves in the enterprise, from servers to storage and cloud services. It includes HPE

Enterprise Secure Key Manager (ESKM), a complete solution for generating and managing keys by unifying and automating encryption controls. With it, you can securely serve, control, and audit access to encryption keys while enjoying enterprise-class security, scalability, reliability, and high availability that maintains business continuity.

Standard HPE ESKM capabilities include high availability clustering and failover, identity and access management for administrators and encryption devices, secure backup and recovery, a local certificate authority, and a secure audit logging facility for

policy compliance validation.

Together with HPE Secure Encryption for protecting data-at-rest, ESKM will help you meet the highest government and industry standards for security, interoperability, and auditability.

Reliable security across the global enterprise

ESKM scales easily to support large enterprise deployment of HPE Secure Encryption across multiple geographically distributed data centers, tens of thousands of encryption clients, and millions of keys.

The HPE data encryption and key management portfolio uses ESKM to manage encryption for servers and storage including:

- HPE Smart Array Controllers for HPE ProLiant servers
- HPE NonStop Volume Level Encryption (VLE) for disk, virtual tape, and tape storage
- HPE Storage solutions including all StoreEver encrypting tape libraries, the HPE XP7 Storage Array, and HPE 3PAR

With certified compliance and support for the OASIS KMIP standard, ESKM also supports non- HPE storage, server, and partner solutions that comply with the KMIP standard. This allows you to access the broad HPE data security portfolio, while supporting heterogeneous infrastructure and avoiding vendor lock-in.


Benefits beyond security

When you encrypt data and adopt the HPE ESKM unified key

management approach with strong access controls that deliver reliable security, you ensure continuous and appropriate availability to keys while supporting audit and compliance requirements. You reduce administrative costs, human error, exposure to policy compliance failures, and the risk of data breaches and business interruptions. And you can also minimize dependence on costly media sanitization and destruction services.

Don't wait another minute to take full advantage of the encryption capabilities of your servers and storage. Contact your authorized HPE sales representative or visit our website to find out more about our complete line of data security solutions.

About HPE Security—Data Security

HPE Security - Data Security drives leadership in data-centric security and encryption solutions. With over 80 patents and 51 years of expertise, we protect the world's largest brands and neutralize breach impact by securing sensitive data-at-rest, in-use, and in-motion. Our solutions provide advanced encryption, tokenization, and key management that protect sensitive data across enterprise applications, data processing infrastructure, cloud, payments ecosystems, mission-critical transactions, storage, and Big Data platforms. HPE Security - Data Security solves one of the industry's biggest challenges: simplifying the protection of sensitive data in even the most complex use cases. 

Learn more at: hpe.com/software/ESKM

Nathan Turajski is a Senior Product Manager for Hewlett Packard Enterprise - Data Security (Atalla), responsible for enterprise key management solutions that support HPE storage and server products, and technology partner encryption applications based on interoperability standards. Prior to joining HP, Nathan's background includes over 15 years launching Silicon Valley data security start-ups in product management and marketing roles including Securant Technologies (acquired by RSA Security), Postini (acquired by Google), and NextLabs. More recently, he has also lead security product lines at Trend Micro and Thales e-Security.

Do you have your Library Card?

Get your Card from HP Education Services and start checking out the Security User Awareness Training Library

HP offers computer-based training (CBT) that has advantages like:

- The ability to scale the training across your organization.
- Users can take training as per their schedule.
- It ensures that your program communicates a standardized message.
- It is easier to track who took the training, which is often required for compliance purposes.

Free 21 Day Trial Available Now
Library Card Available January 2015

Get your Card...Get Secure.

Learn more at
hp.com/learn/securityawareness

Why choose HP Security User Awareness training?

- More than 40 engaging modules.
- Available in 28 languages.¹
- Sharable Content Object Reference Model (SCORM) compliant.
- U.S. Federal 508 compliant for compliance with the Americans with Disabilities Act.
- Regularly reviewed and updated.
- Global content for global enterprises.


Hewlett Packard
Enterprise

TIC & NuWave: A Legacy of Nonstop Modernization

Gabrielle Guerrero >> NuWave Technologies Phil Ly >> President >> TIC Software

Integrating NonStop systems with other platforms is a niche market focused on by NonStop modernization experts. These specialists help corporations capitalize on their investments in NonStop by allowing their servers to function like modern, open platforms. Two of these modernization companies, TIC Software and NuWave Technologies, partnered together a long time ago to offer their NonStop clients the products and services they need to address their IT challenges today, and to keep overcoming them in the future.



Transaction Innovation Corporation (TIC) Software

After working in IT from the mid-70s to the mid-80s, including four years at Tandem Computers, Phil Ly founded TIC Software. When he started the company in 1983, his goal was to keep customers' NonStop (then Tandem) systems up-to-date by using modernization technology

and in-depth consulting services; and it remains his priority today. Phil is a force in the NonStop world. He works tirelessly both to educate users on the benefits of modernization, and to help them achieve the best results. He also has the expertise and experience to make project recommendations and implement software developments.

While TIC began as a specialized consulting group, it has grown and evolved into a full-service firm with a comprehensive range of NonStop modernization solutions, many of which are offered through value-added reseller (VAR) agreements with companies like NuWave. Other TIC products are the result of their clients looking to address particular needs and challenges. By tackling these requests and creating new products, TIC has been able to help customers integrate and adapt their NonStop systems seamlessly.



Today, TIC provides customers with tools to integrate their NonStop servers with email, SOAP and JSON Web services, content management systems, and other modern technologies.

These tools include NuWave middleware solutions, which connect NonStop servers to other platforms; but TIC also offers many other modernization products to extend system lifecycles and integrate the latest technology into NonStop servers. These include products such as data flow offerings designed to integrate legacy data with other platforms through format conversion and data delivery, and gateway development products to allow NonStop applications to interoperate with other platforms and technologies, including Windows, .NET, XML, and Web services, among others.

NuWave Technologies



Like many people in the NonStop community, Ernie Guerrero worked with Tandem systems all through the 80s; holding positions in development, sales, and management at familiar names like Logica (now CGI) and Cornerstone Software. In 1999, though, he decided to go rogue and start his

own consulting firm. When he founded NuWave, the company was a small firm focused on providing IT services and project managers to large corporations and government organizations, including NonStop users.

While NuWave is still known for helping companies develop, modernize, and migrate NonStop applications, the company now receives the most recognition for its high-quality, affordable NonStop middleware, mainly thanks to flagship products SOAPam Server (then SOAP/AM® Server) and SOAPam Client (then SOAP/AM® Web Service Client). SOAPam Server allows you to expose your existing Guardian or Pathway servers as industry-standard Web services. Customers, partners, or coworkers can then access these Web services from SOAP clients running on virtually any computing platform. The product does this while maintaining the security, reliability and scalability of your HP NonStop server and applications. SOAPam Client does the reverse by allowing HP NonStop applications to access Web services that are on any platform, anywhere in the world. It hides the complexity of TCP/IP, HTTP, SSL/TLS, and SOAP required to participate in Web services.

Since these user-friendly solutions went to market in the early 2000s, NuWave has become famous for connecting NonStop to other platforms, applications, and Web services (PAWS). The firm's latest solution, LightWave Server™, is also generating a lot of buzz in the space. This product uses newer technology like JSON Web services and RESTful APIs to send NonStop data to modern clients such as mobile applications and desktop browsers.

The Perfect Partnership for NonStop Modernization

TIC and NuWave have been partners since the early 2000s—shortly after NuWave released SOAPam Server and SOAPam Client. The middleware products were complementary additions to TIC's portfolio of modernization solutions; and TIC's experience and relationships in the NonStop space helped NuWave to increase its market share. For these nearly fifteen years, NuWave and TIC have enjoyed a symbiotic relationship: by working together to help NonStop users modernize their applications, both companies have been able to gain recognition in the NonStop community. NonStop customers get the best of both

worlds by leveraging the expertise of not just one, but two companies dedicated to modernizing NonStop systems.

The two companies share many of the same values, including a commitment to improve the customer's overall experience and to increase the functionality of HPE NonStop hardware and software. "We have a very strong and successful partnership with NuWave. There is great synergy between our teams, and together we have been able to come up with creative solutions and excellent support to help our customers. That's why we have such happy and loyal customers who always come to us for solutions," says Phil. According to Ernie, "It's a great match because NuWave provides best-in-class connectivity products and TIC is a reliable VAR that not only sells our products, but also provides IT integration, software implementation services, and first-level support to our shared customers."

Shared Customers Reap the Benefits

One mutual customer of TIC's and NuWave's, a large US-based department store company, is using NonStop to process point-of-sale (POS) transactions. They purchased NuWave SOAPam Client from TIC so they would be able to access their key management system, which is located on a disparate platform, from NonStop using SOAP Web services. This provides a seamless integration between their NonStop applications and the key management system.

Another shared customer, a leading heavy equipment supplier, has had a long and happy relationship with TIC. They use NuWave SOAPam Server to access NonStop COBOL servers from their customer portal and internal web applications, and they are using NuWave SOAPam Client to access the Cybersource Web service for credit card authorization. The SOAPam products enable the customer to build a powerful and yet flexible service-oriented architecture that hides the underlying entities from the applications. This helps set the standard for their NonStop modernization strategy.

One other mutual customer, a large financial services corporation, is using NonStop to interface to their point-of-sale (POS) devices and authorize transactions. They had also been using ACI Webgate (now called Web Access Services) to send messages to BASE24, but they were able to replace Webgate with a customized version of NuWave SOAPam Server, which they purchased through TIC. Phil was able to recognize the customer's major pain point as cost-driven, and he understood that their unique requirements would allow them to drop in a replacement, granted that NuWave's developers would be able to make some adjustments to the product. The development team at NuWave customized SOAPam Server so it would look inside the SOAP envelope and then send the message through an XML parser. With this customized version of the product, the financial services company has been able to replace Webgate completely, and in the process has saved over \$300,000 in less than five years. Over time, they will continue to save even more money, and they could not be happier with SOAPam Server and TIC's product support.

Customer Spotlight: Cass Information Systems

Cass is the leading provider of expense management services for transportation, utility, telecom and waste-related business intelligence providers. Cass leverages the latest technologies to ensure that these complex bills are paid accurately and on time, and the company also provides critical reporting to help their clients better manage expenses in target areas.

The corporation initially sought out TIC for its TeleMail

solution, but when their business needs evolved in 2012, the firm approached TIC once again—this time to send and receive data to and from their NonStop systems. TIC recommended NuWave SOAPam Server and SOAPam Client to transform the functionality of the Cass payment-scheduling engine. The goals of the project included the following:

1. Modify all Web services to include a user-friendly narrative explaining the entire process that was followed to arrive at the answer to the request. This would form the basis of a dynamic documentation system that would track and report upon itself at each decision point.
2. Build a tool that would allow users to click on an invoice and access the details of the scheduling system and billing process; including the bill's timeline, methods of payment, and funding.

Shortly after TIC completed the software implementation and the project, Tom Schaper, Project Lead in Cass' internal programming department, commented on the ongoing use of the SOAPam solutions. "We use SOAP/AM and SOA to automate just about everything in the process." Cass' software users would frequently send requests to accelerate payments on a given set of bills, and before installing SOAPam, developers would have to write a custom program each time in order to extract and modify the set of bills. With SOAPam Server and SOAPam Client, they were able to build a browser interface that would communicate directly with programs running on their NonStop server. Tom and his team were relieved once users were able to access to the tools they needed to perform these tasks quickly and efficiently.

Decades ago, one of the most exciting developments in IT was the service-oriented architecture (SOA) concept. As you probably know, SOA is a way for corporations to deliver services throughout their enterprise, which in turn enhances business agility while protecting the existing IT investment. One of the great things about the Integrity NonStop platform is that it was specifically designed for the implementation of a service-oriented architecture. Existing NonStop server applications can be readily exposed as services, thereby modernizing the applications and increasing their value to the enterprise, without the need to rewrite them.

At Cass, services would come into play in many areas; for example, they were used to match images of bills with associated electronic data. All of the business logic would be included in a Web service, then the interface (in this case, either a browser or a desktop client) would simply send a request to the Web service to receive decisions on security, bills that were available for processing, and so on. The web or desktop client would be able to deal only with the presentation, not the business-level decisions.

Like most SOAPam customers, Cass did a comparison before choosing the products. "Using the other solution would have required us to purchase, install, and learn several packages," Tom recalled. "Each package involved an investment in time, and a pretty steep learning curve. Once we had a short demo of SOAP/AM, we were able to use it within a half hour. It made the purchase decision very easy."

Part of what makes it so quick and easy to install NuWave products is that the process is similar to that of Windows® applications. What's even better, though, is the ease of use of the products. "Using the SOAP/AM browser interface is very intuitive," Tom explained. By using this interface, the process of setting up a new Web service is as simple as answering a series of questions, and the software guides you through the process. "It literally takes less than five minutes to set up and test a new Web service," Tom continued. "All of this requires no

change to the NonStop application or its configuration, allowing us to leverage our legacy applications in new ways.”

Cass’ NonStop developers claimed that the products not only performed as advertised, but they also delivered some pleasant surprises. Like most NonStop customers; Cass uses the Guardian operating system; which has unique file structures, utilities, and commands; and the SOAPam products allow Cass’ users who are not familiar with Guardian to work with those files. The software simply presents the files in the familiar Windows Explorer format. In fact, once the solutions have been set up, all interaction with the products happens using the browser interface, which delivers security, functionality, and sophistication without the need to memorize commands or settings.

“We purchased SOAP/AM Server and SOAP/AM Web Service Client because we were confident they could help blend our Windows and NonStop environments, protect our IT investment, and enhance the efficiency of our operations,” said Jim Crowley, who was the manager of Cass’ internal programming department at the time. “They have met our expectations, and then some.”


Cass strongly recommends SOAPam products to other NonStop users who are on the cusp of implementing a SOA strategy. “You want an easy way in, and this is the easiest and most cost-effective way,” Tom claims. “The learning curve is so minimal with SOAP/AM that you can be up and running quickly. You don’t have that long investment in time and energy trying to get another solution to work. The products work right out of the box, and everything is designed for ease of use.”

Jim’s overall impression of the software was also overwhelmingly

positive: “It’s easy to use and requires very little training. We basically have two platforms: Windows and NonStop; this product allows us to blend the functionality contained in both of those platforms and make it one. It’s been great—I really can’t say enough about it.”

The Legacy Continues

In order to be successful, NuWave and TIC have to constantly evaluate modern technology and decide whether to incorporate it into new products that can keep NonStop systems current and connected. So, while they have the experience and talent to help NonStop corporations keep up with evolving technology, they have also both planned ahead: they are not only NonStop X-ready, but they are also ready for the next generation of NonStop modernization solutions. The firms recently started selling LightWave Server, which utilizes JSON and REST technology to send data to modern clients like tablets. In the near future, they plan to release LightWave Client™, which will use the same modern technology to receive data on NonStop from other platforms and Web services. Both companies also have plans to develop other innovative solutions that will help NonStop companies address their latest business needs. As corporations continue to rely on NonStop to keep their businesses running smoothly, NuWave and TIC will overcome these organizations’ technological challenges, now and into the future.

For more information about these companies and how they can help you get the most out of your NonStop systems, visit www.ticsoftware.com and www.nuwavetech.com. 

Phil Ly is the president and founder of TIC Software. His original vision was to provide a broad range of solutions, including design and development consulting services, for NonStop server mission-critical applications, all with the goal of legacy application modernization.

Gabrielle Guerrero is the director of business development at NuWave Technologies, a NonStop middleware company founded and managed by her father, Ernie Guerrero. She has a BS in business administration from Boston University and is an MBA candidate at Babson College.



NEW BENEFIT

Annual travel insurance exclusively for Connect members through Nationwide Insurance

- ✓ Starting at \$39 annually
- ✓ Travel as many times you want in any given year, and be protected
- ✓ Remember, most personal medical plans are not valid outside the country.
- ✓ Great trip cancellation protection for entrepreneurs who pay their own travel expenses.
- ✓ Comprehensive coverage
- ✓ Travel worry free
- ✓ The plan is extended to friends and family.

[Read More](#)

Protect your most sensitive data from damaging breaches

Make your most sensitive data useless to hackers. Encrypt and tokenize it—at the moment it's created and throughout its lifecycle. HPE SecureData protects your data at rest, in motion, and in use. On-site, in the cloud, on mobile endpoints, and in big data platforms. Our continuous data-centric security keeps your business out of the headlines. It helps enable PCI compliance and audit scope reduction, and de-identifies data to protect personally identifiable information, protected health information, and intellectual property. HPE Security—Data Security format-preserving encryption, stateless key management and tokenization solutions keep you ahead of hackers.

Learn more at:

voltage.com

hpe.com/go/DataSecurity

Visit us at Booth #114



Bank Chooses “Sizzling-Hot-Takeover” Data Replication for its BASE24™ Business Continuity Solution

William G. Holenstein >> Senior Manager of Product Delivery >> Shadowbase Products Group
Keith Evans >> Shadowbase Product Manager >> Gravic, Inc.

Introduction

For the past eight years, a tier 1 regional bank serving a major resort island was using an ACI BASE24 Classic financial transaction switch to manage its network ATMs and POS terminals. For business continuity, its BASE24 system was running in an active/passive mode on a pair of HPE NonStop S-Series servers. Early in 2015, the bank found that it needed to upgrade these servers, which along with the operating system and application software, were nearing their end-of-support life. The bank made the decision to migrate its BASE24 system to a pair of NonStop NS-Series servers, again running as an active/passive pair.

The bank also decided to replace its current data replication product with HPE Shadowbase solutions, due to cost issues and to optimize its business continuity failover time for system outages, whether scheduled or unscheduled. Furthermore, this replacement positioned the bank to take advantage of the Shadowbase *sizzling-hot-takeover* (SZT) facility, which can typically reduce failover time to a few seconds.

The Bank's Original BASE24 System

The original configuration employed by the bank running its BASE24 system is shown in Figure 1. It comprised a production system (\S78PRD) and a backup system (\S78BKP), each running on a NonStop S-Series server. The production system ran the BASE24 application, which managed the bank's ATMs and POS terminals, and it communicated with other hosts in the financial transaction network to forward ATM and POS transactions for authorization.

The BASE24 files were initially all unaudited Enscribe files. The source system could not run audited files (via HPE NonStop's TMF facility using AutoTMF), because the customer used \$DSMSCM and \$SYSTEM for application data volumes. (TMF auditing is not recommended/should not be used on these special disk packs.)

The source Enscribe files were replicated to the backup system by a replication product that intercepted changes to the production databases via an intercept attached to the source application and created extract files of the database changes. The extract files were then sent to the backup system via an Expand communication link to update the backup databases with the source application database changes.

The log files held all of the transactions processed by the BASE24 application during the day. The data in these files was processed daily through a batch settlement process, and an extract

file was built of the business transactions. The extracts were then sent to the card issuing organizations for reconciliation, and the accounts of the corresponding acquiring banks and merchants were credited and debited with the appropriate transaction values.

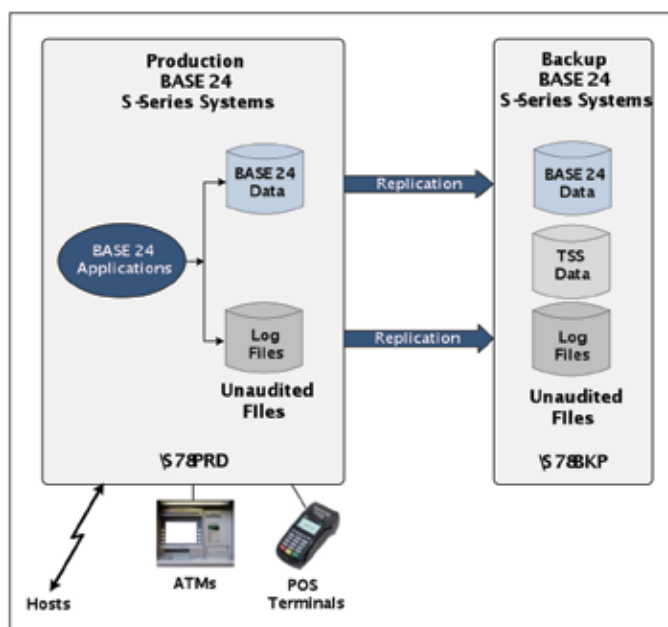


Figure 1 – The Original BASE24 System

The Bank's New BASE24 System

As shown in Figure 2, the bank's new production system (\NSPROD) and backup system (\NSBKUP) are both NonStop NS-Series servers. The backup system is kept synchronized with the production system by using the HPE Shadowbase data replication engine.

The latest BASE24 Classic application is installed on both systems. Since the backup system has the BASE24 application already installed and tested, it serves as a hot backup and can take over processing from the production system in just a few minutes in the SZT configuration.

The Shadowbase replication engine is configured to be bi-directional, meaning it can simultaneously replicate in either direction. This configuration supports failover to the backup system, which must then act as the production system and replicate changes back to the old production system once that system is restored to service, to bring the systems back into synchronization.

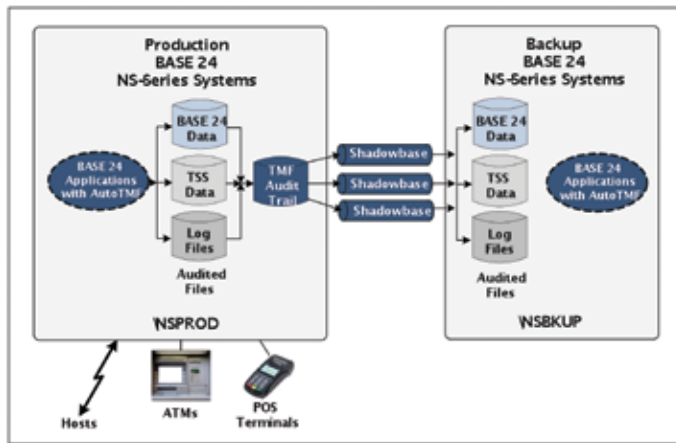


Figure 2 - The New BASE24 System

The Phased Migration

The bank faced several challenges as it planned its upgrade. The primary problem was the existing BASE24 version possessed some data inconsistencies with the new BASE24 version running on the NS-Series servers. Therefore, data transformation was required in migrating the production data to the new BASE24 release. These transformations were handled by customized User Exits implemented in the Shadowbase software.

The bank also decided, in part, to move from the original product that replicated data between the production and backup systems, to HPE Shadowbase software, which requires TMF audited files. All of the files in the BASE24 system were unaudited, so the upgraded BASE24 system was further modified to support audited files using the HPE NonStop AutoTMF product.¹

This was accomplished by installing a replay facility on the old Backup server to convert the unaudited database changes into audited database changes. These new audited database files were then used as the data source for HPE Shadowbase replication, as shown in Figure 3.

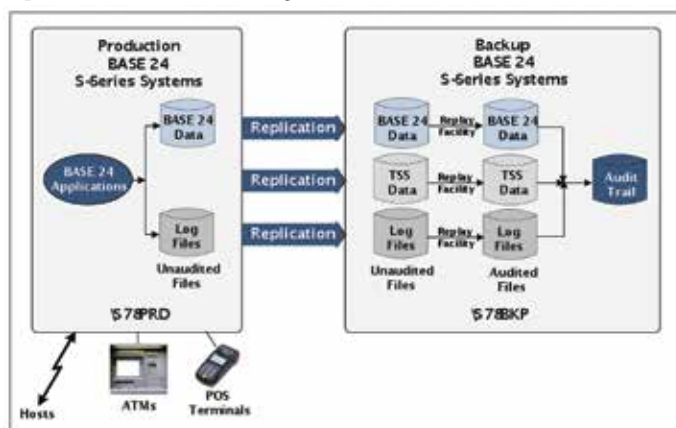


Figure 3 - Configuring the Backup Server as a Shadowbase Source Database

To address these issues and perform the migration, the bank enlisted the aid of a professional services (PS) team assembled by HPE. This team utilized the following resources:

- HPE for hardware, operating system and software installation and support
- PayX, an industry leading provider of consulting services and support in the payments industry for BASE24 Classic and BASE24-eps, among other payments products
- Gravic Shadowbase personnel, for the replication engine work

Since the bank felt it was imperative that switchover to the new system be seamless and with no impact on its customers, the project was organized into steps. Each step accomplished only one task and involved only the necessary project partners, with the results thoroughly tested before the next step began. The multiple steps were carried out from June through October 2015, when the new system was put into production. The basic steps of the project consisted of the following tasks (see Figure 4):

- Install new NonStop NS-Series systems (production and backup)
- Install current BASE24 Classic on new systems
- Implement AutoTMF to automatically create audited BASE24 files
- Install and configure HPE Shadowbase software to replicate BASE24 data from old systems to new systems, without interrupting service and keeping all systems synchronized with current production data
- Test new system independently (including failover/failback testing)
- Cut over from the old system to the new system with minimal service interruption using Shadowbase Zero Downtime Migration (ZDM)
- Shut down old systems

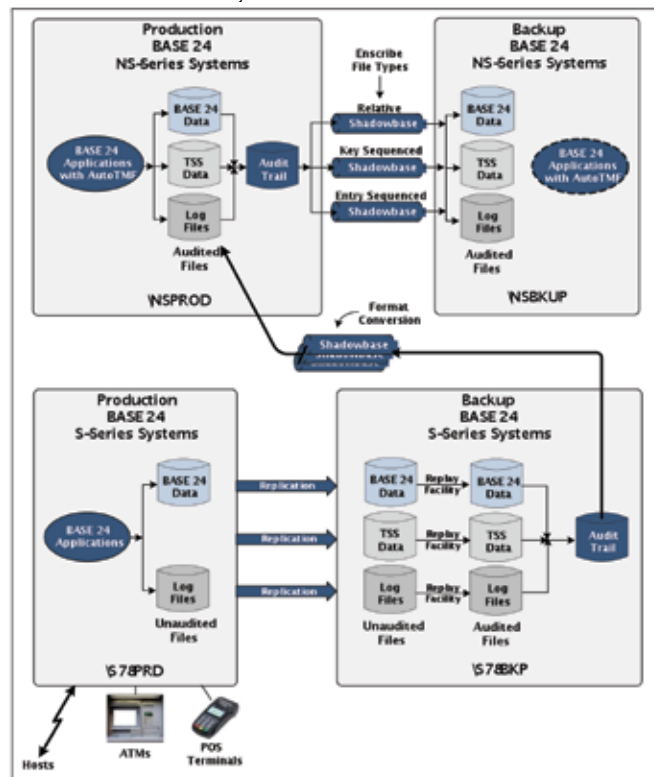


Figure 4 - Shadowbase Configuration for a Zero Downtime Migration

¹ Using AutoTMF to audit database file updates is a non-invasive process, and does not require any changes to the application itself.

There are many implementations of AutoTMF for BASE24 customers.

Mission Accomplished

The first transactions were actively processed on the new production system just 15 minutes after the cut over began, and the new BASE24 system was fully operational and in production after 45 minutes. During this entire migration process, the old production system remained in service to act as a fall back in case anything went wrong. As expected, it wasn't needed. The bank now conducts regular failover testing, with complete tests that bring the backup system into full service.

The bank is now positioned to move from its active/backup configuration to a Shadowbase SZT architecture. With the BASE24 application up and running on both production and backup nodes, if an outage of the production system occurs, all that is needed is to re-route users to the backup system (which is known-working and ready to process transactions), resulting in failover times that can be measured in seconds.

Summary

The bank took a very stale, aged BASE24 system and upgraded both the hardware platform and BASE24 software with no outages except for a brief time during the final cutover. At the same time, the bank replaced a costly data replication product with HPE Shadowbase software. The cutover application service outage could, in fact, have been completely avoided if the bank had elected to use the Shadowbase ZDM features that were installed and tested (an abundance of caution). Choosing a team whose members had specific expertise to support the project was another major factor in the success of the upgrade. This team included HPE for the NS-Series system upgrade, PayX for its BASE24 expertise, and Gravic for the configuration of HPE Shadowbase software. In addition, the bank implemented reliable failover procedures that reduced its downtime due to a production failure from two hours to under four minutes. The bank is now positioned to reduce its outage time to just seconds when it moves to a full SZT configuration. [CO](#)

William G. Holenstein manages the Product Delivery department for the Shadowbase product line, which includes Support, QA, and Training/Documentation. He joined our organization as a software developer in the late 1980's. During his time with the company, Mr. Holenstein worked at many professional services sites, performing a wide array of software tasks ranging from data acquisition, heterogeneous connectivity and high level application software on a variety of platforms. He regularly participates in Shadowbase customer installations and software projects as either a team leader or project manager. He received his undergraduate degree from the College of Liberal Arts and Sciences at Villanova University, and has taken masters classes in international business and new business ventures at Penn State University's Great Valley Campus.

Keith B. Evans works on Shadowbase business development and product management for Shadowbase synchronous replication products, a significant and unique differentiating technology. Asynchronous data replication suffers from certain limitations such as data loss when outages occur, and data collisions in an active/active architecture. Synchronous replication removes these limitations, resulting in zero data loss when outages occur, and no possibility of data collisions in an active/active environment. Shadowbase synchronous replication can therefore be used for the most demanding of mission-critical applications, where the costs associated with any amount of downtime or lost data cannot be tolerated. For more information contact us at sbproductmanagement@gravic.com

YOUR NONSTOP AUDIENCE JUST GOT BIGGER!

Read The Digital Version of The Connection Now



For Real-Time Advertising Results Contact sales@connect-community.org

A photograph of a fisherman in a river, wearing a cap and waders, casting a line. The background shows a river flowing through a valley with mountains in the distance.

Data Integration hooking the big fish!

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

Ask any fisherman active in the mountain streams that flow from the Colorado Rockies how to catch the fish feeding in the streams and the answers are as numerous as there are fishermen. Each has his own ideas about where to stand, how to cast and what flies to attach to the line – and all enjoy about the same level of success. If it was easy, as it's commonly reported, everyone would be doing it. However, as the volume of water flowing down these streams begins to attract anglers that, at certain times of the year can be seen standing almost shoulder to shoulder up and down the rivers. Yes, the streams are passing by at a rapid clip but the fish you are looking for can prove elusive.

Whenever HPE executives involved with NonStop talk about strategy and goals for NonStop they are quick to point out that NonStop isn't in need of a new strategy. Instead, discussion turns to topics in support of the mainstreaming of NonStop, where it is acknowledged that to mainstream software today it all revolves around four things – Linux, Virtualization, Open Source and Cloud. What's missing? While it's possible to wrap into any discussion about Cloud or even Open Source everything to do with Big Data, its absence from the above list tells its own story – few within HPE are placing any priority on having NonStop support Big Data frameworks. The world of HADOOP, Cloudera, Hortonworks, etc. are not for NonStop, and yet, with the vision of HPE for the Idea Economy and the Transformation to a Hybrid Infrastructure, the door is open for NonStop to participate as both a source of data destined for Big Data as well as the recipient of analytics being performed on that data.

I have been involved in the data replication / data integration business for more than a decade, beginning with my time at Insession Technologies, which was the distributor

of GoldenGate. The value that can be derived from timely replication is hard to ignore. As the industry moved from simply having backup systems set aside in a warehouse for those “just in case” moments to where these very same systems were integrated passively into the data center operations as a whole with data being backed up in near real time to where, for many NonStop users, utilizing network load balancing and other schemes, these systems were integrated actively into the data center operations. In other words, no system was left idle no matter what the circumstances. Every system was active 24 X 7 and was capable of near real time take over should a crisis ever arise.

I will leave it to the vendors of data replication and data integration products to document the merits of their offerings elsewhere in this issue of The Connection and I am sure there will be plenty of information provided. Certainly, with a choice between ShadowBase, DRNET, and GoldenGate for data replication and not forgetting too products like DataExpress for file transfer, getting data out of a NonStop system could be done in many ways and every systems manager knew there are various options. And having all of these options is important. According to a January 7, 2016, report from Rackspace, Getting data into your Big Data cluster “After you have successfully created a new Cloud Big Data cluster, you need to get your data into the cluster.” Most important of all is to know where your data is located and according to Rackspace, “the current location of your data” can be residing in Cloud files, on a HTTP or FTP server, on a local computer (data base) and even another cluster.

One of the strengths of the NonStop vendor community is that there are numerous products to choose from and NonStop systems have been well served by these products for decades. However, whether it's a simple file transfer or the

most sophisticated replication product all are coming under scrutiny when it comes to possible contribution to Big Data. After all, where do the data lakes get their data – from data streams and yes, NonStop systems provide one of the most important data streams of all. The stream generated by mission critical transaction processing. Transactions generate data, changes to the database are logged and these in turn can be read. Transactions may also generate tables or files that in turn end up on HTTP and FTP servers. No matter, they all represent legitimate sources of data that external data analytics products need to access.

I am often asked whether Big Data is relevant to NonStop and if so, in what areas? Likewise, these same parties will query me about the likely impact on NonStop solutions should they embrace the outcome from analytics being performed near real time? My response is always the same – whether you embrace it today or tomorrow, integration between transaction processing and data analytics is going to happen. As HPE acknowledges at the highest level, there's a new style of business powered by IT and without data analytics playing a role, failing to leverage data analytics, business will essentially be flying blind. Those data streams that pass by on their way to the data lake hold some really tasty fish, are you missing out?

In the post of December 2, 2015, to the blog on the Striim web site, The Tipping Point – Data Stream Analytics Meets NonStop Transaction Processing in Real Time you will read of how the intersection between data stream analytics and transaction processing has indeed arrived and it does represent a sizable course change that all those in the data center are coming to appreciate. Even the most hardened of NonStop system managers is aware of the need to integrate the data being generated by the execution of adjacent applications. Are databases truly in synch? Do networks and firewalls really functioning for all users? Are the processes running actually conform to the SLAs in place? And yes, it's exactly with this in mind that Striim has won its first business with NonStop customers.

But I am expecting NonStop vendors to be even more involved as they look to add value to their products. Attending the ATM Industry Association (ATMIA) US Conference held in New Orleans at the end of February, there was no mistaking the message coming from the various panels discussing the future of ATMs. It wasn't good enough to simply look at reports and summary screens to see what had happened. More important was to gain valuable business insight as to what was likely to come with many of the Financial Institutions present at the event being very vocal about their desire to see greater adoption of Big Data and Data Stream Analytics by solution vendors.

This is a topic I have been pursuing all month and those parties in the NonStop vendor community I have reached out to share similar sentiments. It's no surprise then that DataExpress, who have cut their teeth moving files, is considering adding features to ensure files on the very HTTP and FTP servers they already read from can become a source that it taps to move data into Big Data frameworks. Likewise, it's hard to escape the language of IR as it describes the mission for Prognosis moving beyond simply visualizing data as Prognosis reports on events and alarms to where Prognosis predicts what is likely to happen

even as it looks to take steps to correct potential faults before they happen.

In the post of August 28, 2015, to the blog on the IR web site, For NonStop users the projected upward path of Prognosis heralds good news you will read of what the addition of prediction and prescription and then a little further out, the addition of self-healing models, heralds a transition to where technologies such as big data and artificial intelligence lend a hand. Yes, the transaction processing world, so important to users, is going to re-tune to embrace data analytics and do so rapidly. As HPE continues to emphasize, IT strategy and business strategy are no longer separate – every business is a technology business. To which I can safely predict, no application runs in isolation; to be effective and provide value to the business, it must leverage the data in the streams that pass by.

It's not just about Striim and it's not just about DataExpress or even ShadowBase or even Prognosis. As I walk the exhibition halls at recent conferences there's simply no escaping the impact Big Data is making on every aspect of technology. Security? It's important to detect patterns and trends, of course as you build a depth of defense. Even as we see the transformation to a hybrid infrastructure under way, where the interconnect fabric is becoming so fast as to be almost transparent, what may have been barriers to integrating the worlds of transaction processing with stream analytics are beginning to crumble. Having said that no application runs in isolation we can now add that no vendor provides viable solutions without awareness of Big Data and data stream analytics.

As the fisherman gather around the streams flowing down from the Colorado Rockies and talk turns to the best flies to use to catch the biggest fish, it's inevitable to draw comparisons with the world of Big Data. As so often is the case, actually hooking a fish is still very difficult and takes skill and when it comes to finding pertinent data with the potential to impact transactions in flight, without the tools it's every bit as difficult. With roots in data integration and data replication, what we are now seeing from all vendors in the data and file movement marketplace suggests that Big Data has become a focus area for them all and so all in the NonStop user community will be better equipped to hook those big fish in a timely manner!

.....
Richard Buckle is the founder and CEO of Pyalla Technologies, LLC. He has enjoyed a long association with the IT industry as a user, vendor, and more recently, as an industry commentator. Richard has over 25 years of research experience with HP's NonStop platform, including eight years working at Tandem Computers, followed by just as many years at InSession Inc. and ACI Worldwide.

Well known to the user communities of HP and IBM, Richard served as a Director of ITUG (2000- 2006), as its Chairman (2004-2005), and as the Director of Marketing of the IBM user group, SHARE, (2007-2008). Richard provides industry commentary and opinions through his community blog and you can follow him at www.itug-connection.blogspot.com, as well as through his industry association and vendor blogs, web publications and eNewsletters.

The quotes come from some of Richard's clients including HP, Integrated Research, comForte, DataExpress, WebAction, Inc., InfraSoft, and OmniPayments, Inc.

Integrating data protection into legacy systems Methods and Practices

Jason Paul Kazarian >> Senior Architect >> Hewlett Packard Enterprise

Legacy systems remain critical to the continued operation of many global enterprises. Recent cyber-attacks suggest legacy systems remain under protected, especially considering the asset values at stake. Development of risk mitigations as point solutions has been minimally successful at best, completely ineffective at worst.

The NIST FFX data protection standard provides publically auditable data protection algorithms that reflect an application's underlying data structure and storage semantics. Using data protection at the application level allows operations to continue after a data breach while simultaneously reducing the breach's consequences.

This paper will explore the application of data protection in a typical legacy system architecture. Best practices are identified and presented.

Legacy systems defined

Traditionally, legacy systems are complex information systems initially developed well in the past that remain critical to the business in which these systems operate in spite of being more difficult or expensive to maintain than modern systems.¹ Industry consensus suggests that legacy systems remain in production use as long as the total replacement cost exceeds the operational and maintenance cost over some long but finite period of time.

We can classify legacy systems as supported or unsupported. We consider a legacy system as supported when operating system publisher provides security patches on a regular, open-market basis. For example, IBM z/OS is a supported legacy system: IBM continues to publish security and other updates for this operating system, even though the initial release was fifteen years ago.²

We consider a legacy system as unsupported when the publisher no longer provides regular security updates. For example, Microsoft Windows XP and Windows Server 2003 are unsupported legacy systems even though the US Navy obtains security patches for a nine million dollar annual fee,³ as such patches are not offered to commercial XP or Server 2003 owners.

Unsupported legacy systems present additional security risks: as vulnerabilities are discovered and documented in more modern systems, attackers use these unpatched vulnerabilities to exploit an unsupported system. Continuing this example, Microsoft has published 110 security bulletins for Windows 7 since the retirement of XP in April, 2014.⁴ This presents dozens of opportunities for hackers to exploit organizations still running XP.

Security threats against legacy systems

In June 2010, Roel Schouwenberg of anti-virus software firm Kaspersky Labs discovered and publishing the inner workings of the Stuxnet computer virus.⁵ Since then, organized and state-sponsored

hackers have profited from this cookbook for stealing data. We can validate the impact of such well-orchestrated breaches on legacy systems by performing an analysis on security breach statistics publically published by Health and Human Services (HHS).⁶

Even though the number of health care security breach incidents between 2010 and 2015 has remained constant, bounded by $O(1)$, the number of records exposed has increased at $O(2n)$ as illustrated by the following diagram:¹

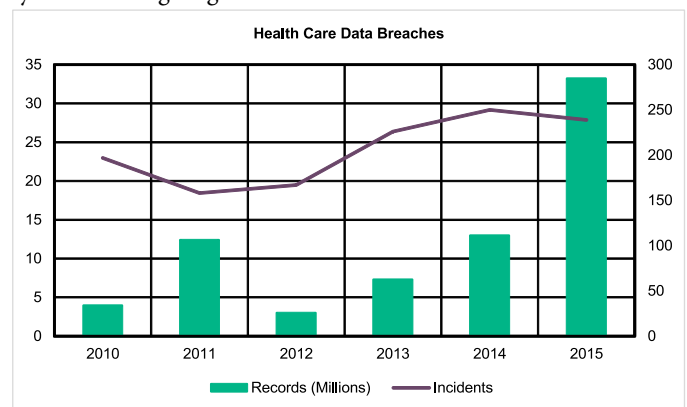


Figure 1 - Health Care Data Breaches.

Analysis of the data breach types shows that 31% are caused by either an outside attack or inside abuse, split approximately 2:3 between these two types. Further, 24% of softcopy breach sources were from shared resources such as emails, electronic medical records, and network servers. Thus legacy systems involved with electronic records need both access and data security to reduce the impact of security breaches.

Legacy system challenges

Applying data security to legacy systems presents a series of interesting challenges. Without developing a specific taxonomy, we can categorize these challenges in no particular order as follows:

- **System complexity:** Legacy system evolve over time and slowly adapt to handle increasingly complex business operations. The more complex a system, the more difficulty protecting that system from new security threats.
- **Lack of knowledge:** The original designers and implementers of a legacy system may no longer be available to perform modifications.⁷ Also critical system elements developed in-house may be undocumented, meaning current employees may not have the knowledge necessary to perform modifications. In other cases, software source code may have not survived a storage device failure, requiring assembly level patching to modify a critical system function.

¹ This analysis excludes the Anthem, Inc. breach reported on March 13, 2015, as it alone is two times larger than the sum of all other breaches reported in 2015.

- **Legal limitations:** Legacy systems participating in regulated activities or subject to auditing and compliance policies may require non-engineering resources or permissions before modifying the system. For example, a payment system may be considered evidence in a lawsuit, preventing modification until the suit is settled.
- **Subsystem incompatibility:** Legacy system components may not be compatible with modern day hardware, integration, software, or other practices and technologies. Organizations may be responsible for providing their own development and maintenance environments without vendor support.
- **Hardware limitations:** Legacy systems may have adequate compute, communication, and storage resources for accomplishing originally intended tasks, but not sufficient reserve to accommodate increased computational and storage responsibilities. For example, decrypting data prior to each and every use may be too performance intensive for existing legacy system configurations.

These challenges intensify if the legacy system in question is unsupported. One key obstacle is vendors no longer provide resources for further development. For example, Apple Computer routinely stops updating systems after seven years.⁸ It may become cost-prohibitive to modify a system if the manufacturer does provide any assistance. Yet sensitive data stored on legacy systems must be protected as the data's lifetime is usually much longer than any manufacturer's support period.

Data protection model

Modeling data protection methods as layers in a stack similar to how network engineers characterize interactions between hardware and software via the Open Systems Interconnect seven layer network model is a familiar concept.⁹ In the data protection stack, each layer represents a discrete protectionⁱⁱ responsibility while the boundaries between layers designate potential exploits. Traditionally we define the following four discrete protection layers, sorted in order of most general to most specific: storage, object, database, and data.¹⁰

At each layer, it's important to apply some form of protection. Users obtain permission from multiple sources, for example both the local operating system and a remote authorization server, to revert a protected item back to its original form. We can briefly describe these four layers as follows and as illustrated by the following diagram:

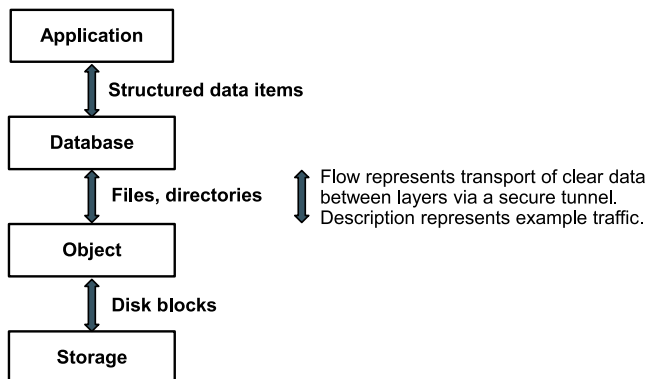


Figure 2 - Data Protection Stack.

ⁱⁱ We use the term “protection” as a generic algorithm transform data from the original or plain-text form to an encoded or cipher-text form. We use more specific terms, such as encryption and tokenization, when identification of the actual algorithm is necessary.

ⁱⁱⁱ American Express uses a 15 digits while Discover, Master Card, and Visa use 16 instead. Some store issued credit cards, for example the Target Red Card, use fewer digits, but these are padded with leading zeroes to a full 16 digits.

- **Storage:** protects data on a device at the block level before the application of a file system. Each block is transformed using a reversible protection algorithm. When the storage is in use, an intermediary device driver reverts these blocks to their original state before passing them to the operating system.
- **Object:** protects items such as files and folders within a file system. Objects are returned to their original form before being opened by, for example, an image viewer or word processor.
- **Database:** protects sensitive columns within a table. Users with general schema access rights may browse columns, but only in their encrypted or tokenized form. Designated users with role-based access may re-identify the data items to browse the original sensitive items.
- **Application:** protects sensitive data items prior to storage in a container, for example a database or application server. If an appropriate algorithm is employed, protected data items will be equivalent to unprotected data items, meaning having the same attributes, format, and size (but not the same value).

Once protection is bypassed at a particular layer, attackers can use the same exploits as if the layer did not exist at all. For example, after a device driver mounts protected storage and translates blocks back to their original state, operating system exploits are just as successful as if there was no storage protection. As another example, when an authorized user loads a protected document object, that user may copy and paste the data to an unprotected storage location. Since HHS statistics show 20% of breaches occur from unauthorized disclosure, relying solely on storage or object protection is a serious security risk.

A-priori data protection

When adding data protection to a legacy system, we will obtain better integration at lower cost by minimizing legacy system changes. One method for doing so is to add protection *a priori* on incoming data (and remove such protection on outgoing data) in such a manner that the legacy system itself sees no change. The NIST FFX format-preserving encryption (FPE) algorithms allow adding such protection.¹¹

As an exercise, let's consider “wrapping” a legacy system with a new web interface¹² that collects payment data from customers. As the system collects more and more payment records, the system also collects more and more attention from private and state-sponsored hackers wishing to make illicit use of this data.

Adding data protection at the storage, object, and database layers may be fiscally or technically (or both) challenging. But what if the payment data itself was protected at ingress into the legacy system?

Now let's consider applying an FPE algorithm to a credit card number. The input to this algorithm is a digit string, typically 15 or 16 digits.ⁱⁱⁱ The output of this algorithm is another digit string that is:

- **Equivalent:** besides the digit values, all other characteristics of the output, such as the character set and length, are identical to the input.
- **Referential:** an input credit card number always produces exactly the same output. This output never collides with

another credit card number. Thus if a column of credit card numbers is protected via FPE, the primary and foreign key relations among linked tables remain the same.

- **Reversible:** the original, input credit card number can be obtained using an inverse FPE algorithm.

Now as we collect more and more customer records, we no longer increase the “black market” opportunity. If a hacker were to successfully breach our legacy credit card database, that hacker would obtain row upon row of protected credit card numbers, none of which could be used by the hacker to conduct a payment transaction. Instead the payment interface, having exclusive access to the inverse FPE algorithm, would be the only node able to charge a transaction.

FPE affords the ability to protect data at ingress into an underlying system and reverse that protection at egress. Even if the data protection stack is breached below the application layer, protected data remains anonymized and safe.

Benefits of sharing protected data

One obvious benefit of implementing a priori data protection at the application level is the elimination or reduction of risk from an unanticipated data breach. Such breaches harm both businesses, costing up to \$240 per breached healthcare record,¹³ and their customers, costing consumers billions of dollars annually.¹⁴ As the volume of data breached increases rapidly, not just in financial markets but also in health care, organizations are under pressure to add data protection to legacy systems.


A less obvious benefit of application level data protection is the creation of new benefits from data sharing: data protected with a referential algorithm allows sharing the relations among data sets without exposing personally identifiable information (PII), personal healthcare information (PHI), or payment card industry (PCI) data. This allows an organization to obtain cost reduction and efficiency gains by performing third-party analytics on anonymized data.

Let us consider two examples of data sharing benefits: one from retail operations and one from healthcare. Both examples are case studies showing how anonymizing data via an algorithm having equivalent, referential, and reversible properties enables performing analytics on large data sets outside of an organization's direct control.

For our retail operations example, a telecommunications carrier currently anonymizes retail operations data (including “brick and mortar” as well as on-line stores) using the FPE algorithm, passing the protected data sets to an independent analytics firm. This allows the carrier to perform “360° view” analytics for optimizing sales efficiency.¹⁵ Without anonymizing this data prior to delivery to a third party, the carrier would risk exposing sensitive information to competitors in the event of a data breach.

For our clinical studies example, a Chief Health Information Officer states clinic visit data may be analyzed to identify which patients should be asked to contact their physicians for further screening, finding the five percent most at risk for acquiring a serious chronic condition.¹⁶ De-identifying this data with FPE allows sharing patient data across a regional hospital system or even nationally. Without such protection, care providers risk fines from the government¹⁷ and chargebacks from insurance companies¹⁸ if live data is breached.

Summary

Legacy systems present challenges when applying storage, object, and database layer security. Security is simplified by applying NIST FFX standard FPE algorithms at the application layer for equivalent, referential, and reversible data protection with minimal change to the underlying legacy system. Breaches that occur subsequently expose only anonymized data. Organizations may still perform both functions originally intended as well as new functions enabled by sharing anonymized data. 

- ¹ Ransom, J., Somerville, I., & Warren, I. (1998, March). A method for assessing legacy systems for evolution. In Software Maintenance and Reengineering, 1998. Proceedings of the Second Euromicro Conference on (pp. 128-134). IEEE.
- ² IBM Corporation. “z/OS announcements, statements of direction, and notable changes.” IBM, Armonk, NY, US, 11 Apr 2012. Web. 19 Jan 2016.
- ³ Cullen, Drew. “Beyond the Grave: US Navy Pays Peanuts for Windows XP Support.” The Register. London, GB, UK, 25 June 2015. Web. 8 Oct. 2015.
- ⁴ Microsoft Corporation. “Microsoft Security Bulletin.” Security TechCenter. Microsoft TechNet, 8 Sept. 2015. Web. 8 Oct. 2015.
- ⁵ Kushner, David. “The Real Story of Stuxnet.” Spectrum. Institute of Electrical and Electronic Engineers, 26 Feb. 2013. Web. 02 Nov. 2015.
- ⁶ US Department of Health & Human Services. Office of Civil Rights. Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. Comp. HHS Secretary. Washington, DC, USA: US HHS, 2015. Breach Portal. Web. 3 Nov. 2015.
- ⁷ Comella-Dorda, S., Wallnau, K., Seacord, R. C., & Robert, J. (2000). A survey of legacy system modernization approaches (No. CMU/SEI-2000-TN-003). Carnegie-Mellon University, Pittsburgh, PA. Software Engineering Institute.
- ⁸ Apple Computer, Inc. “Vintage and Obsolete Products.” Apple Support. Cupertino, CA, US, 09 Oct. 2015. Web.
- ⁹ Wikipedia, “OSI Model,” Wikimedia Foundation, San Francisco, CA, US. Web. 19 Jan 2016.
- ¹⁰ Martin, Luther. “Protecting Your Data: It's Not Your Father's Encryption.” Information Systems Security. Auerbach, 14 Aug. 2009. Web. 08 Oct. 2015.
- ¹¹ Bellare, M., Rogaway, P., & Spies, T. The FFX mode of operation for format-preserving encryption (Draft 1.1). February, 2010. Manuscript (standards proposal) submitted to NIST.
- ¹² Sneed, H. M. (2000). Encapsulation of legacy software: A technique for reusing legacy software components. Annals of Software Engineering, 9(1-2), 293-313.
- ¹³ Gross, Art. “A Look at the Cost of Healthcare Data Breaches.” HIPAA Secure Now. Morristown, NJ, USA, 30 Mar. 2012. Web. 02 Nov. 2015.
- ¹⁴ “Data Breaches Cost Consumers Billions of Dollars.” TODAY Money. NBC News, 5 June 2013. Web. 09 Oct. 2015.
- ¹⁵ Barton, D., & Court, D. (2012). Making advanced analytics work for you. Harvard business review, 90(10), 78-83.
- ¹⁶ Showalter, John, MD. “Big Health Data & Analytics.” Healthtech Council Summit. Gettysburg, PA, USA. 30 June 2015. Speech.
- ¹⁷ McCann, Erin. “Hospitals Fined \$4.8M for HIPAA Violation.” Government Health IT. HIMSS Media, 9 May 2014. Web. 15 Oct. 2015.
- ¹⁸ Nicols, Shaun. “Insurer Tells Hospitals: You Let Hackers In, We're Not Bailing You out.” The Register. London, GB, UK, 28 May 2015. Web. 15 Oct. 2015.

Jason Paul Kazarian is a Senior Architect for Hewlett Packard Enterprise and specializes in integrating data security products with third-party subsystems. He has thirty years of industry experience in the aerospace, database, security, and telecommunications domains. He has an MS in Computer Science from the University of Texas at Dallas and a BS in Computer Science from California State University, Dominguez Hills. He may be reached at jason.kazarian@hpe.com

The real estate of infrastructure:

Architecting multi-tenancy for disaster avoidance

Matt Riesz >> Master Architect >> HPE Business Critical Systems – NonStop

Peter Schvarcz >> Master Solution Architect >> HPE Business Critical Systems – Nonstop

Rebecca Howey >> Release Manager >> HPE Communication & Media Solutions (CMS ACI SDM)



“Location, location, location!” Real estate experts cite these as the first three principles of successful investment in land or buildings. Solution architects rely on similar guidelines when considering where to house applications and instances of applications. And, like their realtor counterparts, solution architects must consider not just the fit of budget and size but the purposes for which the investment is being made. Likewise, just as homeowners might consider taking in roomers to save cash, IT customers often contemplate co-locating one or more applications on a physical system with similar hopes for economy.

While the overall objective when sharing a system must be to prevent applications from interfering with each other, solution architects – and their customers – must also consider initial cost, on-going TCO and ROI before deciding to co-locate applications. Security and risk participate in each of these calculations, primarily business continuity and contention among “roommates” when quarters are shared. Sharing might include multiple applications running on the same system or the co-location of development, QA, production or DR instances of a one or more applications. This “sharing” might seem at first glance to be a money-saver but can prove to be quite expensive when the concomitant operational and other costs are considered. Sadly, a good neighbor does not always make a good roommate.

The remainder of this article summarizes a recent exchange among HPE NonStop solution architects about best practices regarding multiple environments on a single system. Although some comments are specific to this platform, the concepts are universal.



No one likes to share... Hardware

CPU scheme: Applications, like some children, often play best together when they each have their own room. Segregating

applications to their own set of CPUs helps them co-exist without contention, although care must be taken to include system processes in this scheme. For example, TMF, a crucial subsystem of the operating system, runs in CPUs 0/1, rendering this duo ill-suited to hosting roommates. However, even the best laid plan of CPU sharing can be trumped by a utility that enables free range use of system resources. Stuff happens, especially when multiple teams play in the same arena.

CPUs and Low PINs: Applications vary in their need for Low PINs. When multiple applications run on a system, their Low PIN requirements, collectively and individually, must be mapped to the available CPUs as part of the CPU sharing scheme. Sometimes a set of applications simply will not fit the number of existing or planned CPUs for a system. Adding CPUs to that system might not be the optimal choice, given the complexities (and costs) that come with co-locating applications.

Network CLIMs: But, if you do share a system, segregate applications to their own pairs of network CLIMs, if possible. ... Or buy more.



No one likes to share... System software

Operating system upgrades: “All for one and one for all” – that about sums up the OS deal when applications share a single system.

- **TCFs:** Any problem that produces a TCF (time critical fix) that must be applied for one of the applications will affect all of the applications sharing the system.
- **Testing:** All of the applications must be tested against a new OS version before any of them can live on the upgraded system...no matter how long this testing takes. Or you can cross your fingers and go for it.

- **Installation:** All of the applications sharing the system must be willing to take an outage, however brief, at the same time.

Doing system software upgrades will be complex if you decide to co-locate applications, and you need to be prepared. You will need to prepare for a successful implementation of the OS upgrade, and you will need to be prepared for a successful rollback should misadventures occur.

Or maybe you decide just not to do this upgrade or the next one...until somewhere down the line you have a different and bigger problem, commonly known as “a crisis.”

Or you could decide not to co-locate unlike things.

Middleware and OS subsystems: Sometimes sharing middleware is unavoidable, as in the case of TMF and SQL/MX, which are limited to a single instance per system. Otherwise, where multiple instances are allowed, sharing is entirely optional.

- **TMF:** TMF (Transaction Management Facility) makes HPE NonStop Servers non-stop: fault- and disaster-tolerant. Because a single instance exists per system, contention for TMF resources may easily occur when applications coexist. This can be minimized by a TMF configuration that ensures the applications share only the master audit trail. Specifically:
 - o Separate applications by disk volume: don't share volumes between applications.
 - o Assign each application's volumes to their own set of auxiliary audit trails.
 - o Don't make any volume's usage “master.” Assign them all to auxiliaries.
- **SQL/MX:** The current release of SQL/MX also supports only one instance per system, which likewise creates opportunities for contention. Logical and physical database design techniques can mitigate this. Additionally:
 - o Use separate ODBC/JDBC datasources for each application. In addition to pleasing your auditors, creating separate datasources positions you to take advantage of the forthcoming ability to restrict ESPs to specific sets of CPUs.
- **Pathway and other middleware:** This category represents cases where sharing the resources of a single instance is entirely optional. Think long and hard before sharing middleware between applications. Doing so can introduce intractable operational, licensing and auditing issues – unnecessarily.



To mix or not to mix... DR, Dev, QA and/or Production instances

A decision to co-locate application instances requires determining which of the four kinds of environments – DR, Development, QA and Production – might be suitable roommates. A good neighbor can make a disastrous roommate, and sometimes that's predictable.

DR plus <anything> = Disaster In addition to the previous

points, consider this:

► The purpose of a DR system is to act as a production system in the event of a disaster. ◀

Natural events, including human events like fat-fingers and spilled coffee, are just that: events. Whether or not an event becomes a disaster depends on the preparations we have made to deal with it. Although we rarely know the timing of potentially disastrous events, like earthquakes, fires or spilled coffee, we know that these events can, do and will occur, *even to us*.

DR plans that intentionally build in the complexities and risks inherent with development and QA applications are misnamed, because the “recovery” part is suspect from the get-go. We should probably stop pretending this is an option.

DR plus DR = Disaster Let's also stop pretending we are smart enough to figure out which applications can “share” disasters and that we are energetic enough to test failovers to multiple DR sites or to shared DR sites. ALL applications have to coordinate failover at the same time, but this can become cumbersome to plan and implement, leading to partial testing in preparation and then to full-scale disasters in real-life.

Production plus <anything> = Disaster Likewise, mixing a production environment with any other environment type is a recipe for disaster.

- o **Development – No-ooo!:** Development, by its nature, can cause problems with faults and performance. Additionally, developers often require (and have) higher system permissions than is appropriate for a secure production environment; your auditors won't like it.
- o **QA:** See above. This combination also raises the question of where to test a new OS version safely.
- o **DR** Seriously? We already talked about this: DR plus <anything> equals Disaster. The possible exception is two systems that each host half of a single application and that act as each other's DR node – sometimes called reciprocal DR. But mix this with multiple applications, and you're asking for trouble.

QA plus Development Combining QA and Development makes more sense than the other combinations, despite the challenges listed above. However, QA performance testing requires the cessation of all development activity to ensure consistent behavior and reliable results. Clearly this escalates the level of “contention” to the entire system and two or more work groups, at the same time that upgrades of the OS and core software versions raise the level of challenge for everyone. This option might make sense in some situations, but conditions change, so make sure your considerations include both present and likely future conditions.



Adding it all up and making your move

Obviously applications and instances can coexist on the same system. It's possible, and many organizations have done it. In fact, all of the preceding observations and advice result from real life experiences at real customer sites.

But the consensus of the NonStop solution architects is this:


Bottom-line, don't do it, but if you want to share [physical] environments, limit it to QA and Development and make sure you have good plans – with separate disk volumes, separate sets of users and good Safeguard ACLs to control disk, file and object access - and consider using partner products for additional security, monitoring and control.

All of that requires considerable planning, testing and work but still doesn't completely eliminate a fair degree of risk and adverse side effects. This may very well negate any savings anticipated for using the same physical system. There are many ways to bust a budget, and being penny-wise can be pound-foolish.

Need more convincing? Big solution vendors like SAP

also advise their customers to have four separate physical environments: Production, Backup, Reference/QA and Test. (The latter two can be relatively small.)

Decoupling applications on several smaller systems is not only easier and safer, but the current range of options for physical systems, from the NS2300 to the NS7X, and the current NED software licensing practices (per CPU, not per system) allow this recommendation to fit neatly with most customers' budgetary concerns.

In the words of one of this article's contributors, "One of my customers has been sharing a single system among three production applications for several years, and we've learned quite a bit about it. I think if they had the decision to make again today they would NOT do this again." 

Matt has worked with NonStop systems for more than 30 years: for Tandem, Compaq, HP, and HPE. He specializes in NonStop system and application architecture and performance. His recent work with customers who chose to host multiple applications on a single system led to first-hand experience with some of the successes and drawbacks of this approach. Contact information: matt.riesz@hpe.com

Peter joined Tandem in 1984, working primarily with NonStop systems. He participated in the Regionally Designated Specialist (RDS) program in the areas of Performance and Capacity Planning and Security. He is currently responsible for a number of customers with multi-site split-load, as well as shared systems. His experience, along with his experience with external storage systems, enable him to identify the risks associated with shared systems and insufficient DR practices. Contact information: peter.schvarcz@hpe.com

Rebecca Howey, formerly with NED ATC-SDI, currently works as a Release/Project Manager in a global HPE Communication & Media Solutions (CMS) group that develops subscriber data management (SDM) software for mobile network and IoT companies.



**SAVE THE
DATE**

NonStop Technical Boot Camp

**November 13-16, 2016
Fairmont San Jose Hotel
San Jose, CA**

#NonStopTBC

>> Native Tables

>> in NonStop SQL/MX Part 1

Frans Jongma >> Master Technologist >> NonStop Advanced Technology Center

Introduction

HPE NonStop SQL/MX is the relational database management system (RDBMS) that is based on ANSI SQL:1999 with extensions from ANSI SQL:2003. The product can be seen as a SQL engine and a SQL file system. The engine can be used to access the tables of previous RDBMS called NonStop SQL/MP as well as the SQL/MX native tables.

Many customers of NonStop SQL/MP are using the SQL/MX engine to access the data that is stored in SQL/MP tables. They enjoy the features of ANSI DML and use the JDBC drivers in Java programs and ODBC drivers for off-platform applications written in other languages.

Long-time NonStop customers may recall some of the SQL/MX features, such as the support for Referential Integrity (RI), and GRANT/REVOKE for access control to the data. However, in the last few years, many new features have been added to the SQL/MX file system and customers that have been using the engine only may not be aware of the complete feature set that the newer file system might bring them. In this article, the features are grouped into the following categories:

- Security and data integrity: For example, GRANT/REVOKE, Referential Integrity, triggers.
- File characteristics: Hash partitioning, support for large (upto 32KB) rows and large keys.
- Extended data type support: For example, big numbers.
- Other features: Meta data, tools and utilities.

It is assumed that the reader is familiar already with the HPE Nonstop SQL/MX Comparison Guide for SQL/MP Users manual. References to additional documentation are provided in the sections where they apply. The NonStop SQL/MX manuals can be found in the NonStop Technical Library at: www.hpe.com/info/nonstop-docs. From this page, select the appropriate server model, L-series, J-Series or H-Series. This document refers to the manual titles as they appear in the Technical Library without the release number. The current release of SQL/MX is 3.3.

Security and Data Integrity features

The security and data integrity features of the NonStop SQL/MX file system enhance the quality of the data by enforcing the ANSI model of access control to the data in addition to the integrity checks prior to deleting or adding a row to the database. These checks include removal of dependent rows if a parent row is deleted in a cascaded delete operation. Database triggers may be used to

create more complex validation rules.

ANSI user access control

Access to SQL/MX objects is granted to PUBLIC, the set of user IDs known to the system, or to specific users of the system by their Guardian user ID. SQL/MX allows the creation of a Security Administrator group. This group contains the users that are allowed to GRANT and REVOKE object-privileges to other users without having access to the objects themselves. This feature is also referred to as “Separation of Duties” and was introduced in Release 3.1. In older releases, the Super-ID, or an operator-ID was used to create and own the objects, but this owner was also allowed to access the data.

Users are added to the Security Administrators by granting them security administrator (SECURITY_ADMIN) rights.

The list of security administrators can be obtained by the following command in mxci.

```
>>get all security_admins;
--- SQL operation complete.
>>
```

If no Security Administrator group exists, the Super-ID has the privilege to maintain metadata, such as granting other users to create catalogs, grant users to create schemas in a catalog that is not owned by these users and to revoke permissions. If a Security Administrator group exists, only the members of this group have this privilege, and the Super-ID only has the privilege if it has been added to this group also.

Referential Integrity constraints

Referential Integrity (RI) constraints define relations between tables and may restrict addition or delete operations on one table based on the existence of data in another table. The typical example is a constraint on an employee table that only allows adding an employee if the department number exists in the department table. And, optionally, the restriction to delete a department row if there is still an employee row referencing it. Without the DBMS enforcing these rules, program code must be written to do the same. Using RI constraints can therefore simplify the application development, especially where the effect of an update or delete requires cascading to other tables. But more importantly, without these RI constraints, one should not allow end-user tools to access the database in update mode.

Triggers

A trigger is a mechanism to perform certain actions automatically in response to specified database events such as INSERT, UPDATE and DELETE. These actions can be performed before or after the event. There are many uses for triggers, not only in relation to security and data integrity.

Triggers may call Stored Procedures to perform more complex code than the trigger definition allows, which can be useful when porting code from other DBMSes.

References

SQL/MX reference manual: Chapter 1, Security.

File characteristics

SQL/MX native tables are key-sequenced, TMF-audited tables that are defined in SQL/MX catalogs and schemas. SQL Access to these tables can only happen using their three-part ANSI name (catalog.schema.table_name). The physical locations of these tables are in Guardian subvolumes that have 8 character names starting with ZSD. SQL/MX tables are represented by two files: one holding the data, the other containing system information. The latter file is also referred to as the resource fork. A DBA can assign a 6 character Guardian name to the table; however, in most cases these names are system-generated. The last two position of the file name denotes whether it is the data fork (value 00), or the resource fork (value 01).

Increased block, row and key sizes

SQL rows are stored by the Disk Access Manager (DAM) in blocks of either 4K or 32K bytes. The DBA can define the block size when the table is created. The system default is defined by the DEFAULT_BLOCKSIZE Control Query Default (CQD) and is 4096 bytes.

SQL/MX tables can have 4K block and 32K block sizes if the row size is less than 4036 bytes. The maximum row size available to users is 32708 bytes. Row definitions that exceed 4K bytes, can only be stored in blocks of 32K (32768) bytes. It may be beneficial to store small rows in 32K blocks, because the blocks are used to store the index structures of the keys. Larger blocks can hold more index entries resulting in a lower number of index levels.

The maximum primary key size of a SQL/MX native table is 2048 bytes when no triggers are defined. With triggers defined, the maximum size is 2032 bytes. Tables with 4K blocks support a maximum clustering key size of 2010 bytes.

Indexes are subject to the same restrictions as the base tables. The sum of the columns that form the key of the index may not exceed 2048 bytes when the index is stored in 32K blocks. Note that the length of the key of an index is the sum of the lengths of the columns that form the key plus the sum of the length of the clustering key of the base table if the index is non-unique.

Multiple partitions per volume

All SQL objects of a schema reside in the same Guardian subvolume, but multiple partitions of a table or index may be present on the same volume. This is different from SQL/MP partitioned tables where every disk can only have one partition of a table or index because all partitions have the same guardian file name. This feature allows a development system do have the same number of partitions as a production system but on a smaller

amount of physical disks.

Decoupling of clustering and partitioning keys

SQL/MX allows more freedom in ordering and partitioning the data compared to SQL/MP tables. In SQL/MP, the order of the columns in the primary key determines the order of the rows placed on disk as well as the way the data can be partitioned. In a table or index definition, SQL/MX recognizes three key types: the primary key, the clustering or storage key, and the partitioning key.

Storage or Clustering key

The storage or clustering key determines the order of the rows in each partition of the table. All SQL/MX tables are key-sequenced and the index blocks within the base table contain the index records in the order of the storage key. The set of columns that make up the clustering key must guarantee uniqueness. If necessary, SQL/MX will add an additional column to the clustering key to create uniqueness, the SYSKEY column.

The example shows the creation of a table without a primary key, but with a storage key specified. The order of the rows within the table is based on region. Even without a primary key, partitioning is possible: the table is partitioned on the REGION column.

```
>>CREATE TABLE ORDER_EXAMPLE
+>(ORDERNUM NUMERIC (6) UNSIGNED NO DEFAULT NOT NULL,
+>PARTNUM NUMERIC (4) UNSIGNED NO DEFAULT NOT NULL,
+>REGION CHARACTER(10) NO DEFAULT NOT NULL,
+>UNIT_PRICE NUMERIC (8,2) NO DEFAULT NOT NULL,
+>QTY_ORDERED NUMERIC (5) UNSIGNED NO DEFAULT NOT NULL )
+>STORE BY (REGION)
+>LOCATION $DATA01 NAME PARTITION_01
+>RANGE PARTITION BY (REGION)
+>( ADD FIRST KEY 'REG_01' LOCATION $DATA01 NAME
PARTITION_02,
+> ADD FIRST KEY 'REG_50' LOCATION $DATA02 NAME
PARTITION_03
+>);

--- SQL operation complete.
>>
```

When no storage key is defined and no primary key constraint is present, the storage key will be the SYSKEY column. Partitioning of such a table is not possible, just like in SQL/MP.

The example shows the use of a partition name. SQL/MX tables have partition names that can be used for a better identification of the partition. For example, a sequence number can be assigned such as is done in this CREATE TABLE statement. The default partition name is the full file system name (node_volume_subvolume_filename). When tables are restored to another location using Backup-Restore2, the partition name will still refer to the original location of the object.

Partitioning key

The partitioning key is defined by the RANGE or HASH PARTITION BY clause when a table or index is created. The partitioning key consists of one or more columns of the storage or clustering key. The order of the partitioning columns may differ from that of the storage key. In this example, the ORDER_EXAMPLE table has the rows stored in order of order number, part number and region.

The table is partitioned by region. This means that only within a partition, the rows are ordered by ordernum, partnum and region.

```
>>CREATE TABLE ORDER_EXAMPLE
+>(ORDERNUM NUMERIC (6) UNSIGNED NO DEFAULT NOT NULL,
+>PARTNUM NUMERIC (4) UNSIGNED NO DEFAULT NOT NULL,
+>REGION CHARACTER(10) NO DEFAULT NOT NULL,
+>UNIT_PRICE NUMERIC (8,2) NO DEFAULT NOT NULL,
+>QTY_ORDERED NUMERIC (5) UNSIGNED NO DEFAULT NOT NULL )
+>STORE BY (ORDERNUM, PARTNUM, REGION)
+>LOCATION $DATA01 NAME PARTITION_01
+>RANGE PARTITION BY (REGION)
+>( ADD FIRST KEY 'REG_01' LOCATION $DATA01 NAME
PARTITION_02,
+> ADD FIRST KEY 'REG_50' LOCATION $DATA02 NAME
PARTITION_03
+>);
--- SQL operation complete.
>>
```

Primary key

The primary key is really a constraint that enforces uniqueness of the row in the table. SQL/MX uses the primary key (when it is not droppable) as the base table index. In fact, it then becomes the storage key.

The example shows the three columns defined as the primary key. The STORE BY clause is optional and mainly used for documentation purposes. If the STORE BY clause is specified, it must be the same as or a prefix of the primary key.

```
>>CREATE TABLE ORDER_EXAMPLE
+>(ORDERNUM NUMERIC (6) UNSIGNED NO DEFAULT NOT NULL,
+>PARTNUM NUMERIC (4) UNSIGNED NO DEFAULT NOT NULL,
+>REGION CHARACTER(10) NO DEFAULT NOT NULL,
+>UNIT_PRICE NUMERIC (8,2) NO DEFAULT NOT NULL,
+>QTY_ORDERED NUMERIC (5) UNSIGNED NO DEFAULT NOT NULL
+>, PRIMARY KEY (ORDERNUM, PARTNUM, REGION) )
+>STORE BY PRIMARY KEY
+>LOCATION $DATA01 NAME PARTITION_01
+>RANGE PARTITION BY (REGION)
+>( ADD FIRST KEY 'REG_01' LOCATION $DATA01 NAME
PARTITION_02,
+> ADD FIRST KEY 'REG_50' LOCATION $DATA02 NAME
PARTITION_03
+>);
--- SQL operation complete.
>>
```

Droppable Primary Key constraints

SQL/MX tables support the droppable primary key constraint. To enforce the constraint, a unique index on the primary key columns will be created by the system. Note however, that this automatically created index is not automatically partitioned. The base table requires a clustering key definition which defines the structure of the base table index.

```
>>CREATE TABLE ORDER_HASH_EXAMPLE_DROPPABLE
+>(ORDERNUM NUMERIC (6) UNSIGNED NO DEFAULT NOT NULL,
+>PARTNUM NUMERIC (4) UNSIGNED NO DEFAULT NOT NULL,
```

```
+>REGION CHARACTER(10) NO DEFAULT NOT NULL,
+>UNIT_PRICE NUMERIC (8,2) NO DEFAULT NOT NULL,
+>QTY_ORDERED NUMERIC (5) UNSIGNED NO DEFAULT NOT NULL
+>, PRIMARY KEY (ORDERNUM, PARTNUM, REGION) DROPPABLE )
+>STORE BY (REGION)
+>LOCATION $DATA01 NAME PARTITION_01
+>HASH PARTITION BY (REGION)
+>( ADD LOCATION $DATA01 NAME PARTITION_02 ,
+> ADD LOCATION $DATA02 NAME PARTITION_03
+>);
--- SQL operation complete.
>>
```

Updating the primary key value

With the release of SQL/MX 3.2, updates on the primary keys are allowed. Note however, that this update is implemented as a delete of the row(s) followed by and an insert. The reason is simple: as a result of the update of the primary key the row may have to move from one partition (one volume) to another.

Hash partitioned tables

NonStop SQL/MX supports range partitioning and hash partitioning for tables and indexes. With range partitioning, one uses a FIRST KEY clause to define key ranges for each partition. Each record is assigned to the partition whose range includes the value of its partitioning key.

With hash partitioning, NonStop SQL uses a hash function on the values of the partitioning key (which can be just a part of the clustering key) and each record is assigned to a partition based on the result.

```
>>CREATE TABLE ORDER_HASH_EXAMPLE
+>(ORDERNUM NUMERIC (6) UNSIGNED NO DEFAULT NOT NULL,
+>PARTNUM NUMERIC (4) UNSIGNED NO DEFAULT NOT NULL,
+>REGION CHARACTER(10) NO DEFAULT NOT NULL,
+>UNIT_PRICE NUMERIC (8,2) NO DEFAULT NOT NULL,
+>QTY_ORDERED NUMERIC (5) UNSIGNED NO DEFAULT NOT NULL
+>, PRIMARY KEY (ORDERNUM, PARTNUM, REGION) )
+>STORE BY PRIMARY KEY
+>LOCATION $DATA01 NAME PARTITION_01
+>HASH PARTITION BY (REGION)
+>( ADD LOCATION $DATA01 NAME PARTITION_02,
+> ADD LOCATION $DATA02 NAME PARTITION_03
+>);
--- SQL operation complete.
```

Sequence Generators

Sequence generators (SG) are used to create unique numerical values.

NonStop SQL/MX supports two types of sequence generators, Internal Sequence Generators, which are used by columns defined as IDENTITY, and Sequences or External SGs.

Internal Sequence Generator

An Internal Sequence Generator is implicitly created when an IDENTITY column is defined in a CREATE TABLE statement. The SG is a separate table with only one row associated only with that IDENTITY column. The example shows how the ORDERNUM

column is defined as an IDENTITY column. The GENERATED ALWAYS AS IDENTITY clause tells the system to assign a unique value for each inserted row. A GENERATED BY DEFAULT AS IDENTITY clause allows the application to supply a value when inserting a row, but it can also let the system determine the value.

```
>>CREATE TABLE ORDER_SG_EXAMPLE
+>(ORDERNUM LARGEINT GENERATED ALWAYS AS IDENTITY
+>  (START WITH 1 INCREMENT BY 1 MINVALUE 1 NO CYCLE),
+>PARTNUM NUMERIC (4) UNSIGNED NO DEFAULT NOT NULL,
+>REGION CHARACTER(10) NO DEFAULT NOT NULL,
+>UNIT_PRICE NUMERIC (8,2) NO DEFAULT NOT NULL,
+>QTY_ORDERED NUMERIC (5) UNSIGNED NO DEFAULT NOT NULL
+>, PRIMARY KEY (ORDERNUM, PARTNUM, REGION ) )
+>STORE BY PRIMARY KEY
+>LOCATION $DATA01 NAME PARTITION_01
+>HASH PARTITION BY (REGION)
+>( ADD LOCATION $DATA01 NAME PARTITION_02 ,
+> ADD LOCATION $DATA02 NAME PARTITION_03
+>);

--- SQL operation complete.
>>prepare x1 from insert into order_sg_example
(partnum, region, unit_price, qty_ordered) values (
?, ?, ?, ?);

--- SQL command prepared.
>>prepare x2 from insert into order_sg_example values
(DEFAULT, ?, ?, ?, ?);

--- SQL command prepared.
```

The two prepare statements demonstrate how an application can supply parameterized values. When no column names are provided as in statement x2, the keyword DEFAULT can be used as a value for the IDENTITY column.

Sequences

An external sequence generator is explicitly created using the CREATE SEQUENCE statement. The external sequence generator is a schema level database object that the application uses to generate values for a numeric column. The values generated by the external sequence generator are unique for that sequence generator and can

be used to create unique values across a set of tables in a schema.

The next example shows simple usage of a sequence. It is created as a SQL object; in the example all the defaults are used. To get the next value of the sequence, one uses a SQL SELECT statement to select the pseudo column NEXTVAL. The DUAL view¹ is used to return only one value, and since this is the first call to select NEXTVAL SQL/MX returns 1. This value remains the current value until another call to select nextval is issued.

```
>>create sequence myseq;

--- SQL operation complete.
>>select myseq.nextval from dual;

NEXTVAL
-----
1

--- 1 row(s) selected.
>>select myseq.currval from dual;

CURRVAL
-----
1

--- 1 row(s) selected.
>>select myseq.nextval from dual;

NEXTVAL
-----
2

--- 1 row(s) selected.
>>
```

References

SQL/MX reference manual: Chapter 2, CREATE TABLE Statement.
SQL/MX reference manual: Chapter 2, IDENTITY Columns and internal Sequence Generators.
SQL/MX reference manual: Chapter 6, Language Elements: KEYS. [SD](#)

¹ The DUAL view is a view that has the same purpose as the DUAL pseudo table in other DBMSes. It returns one row. The DUAL view and metadata views for SQL/MX are described in the paper called Concepts of NonStop SQL/MX, Introduction to SQL/MX Metadata (part three in the series).

.....

Frans Jongma is a Master Technologist for the NonStop Advanced Technology Center (ATC) and is based in Europe in The Netherlands. Frans has worked in several consulting positions for the NonStop Enterprise Division since 1989. His main areas of expertise are: NonStop SQL (MP as well as MX), application design, performance analysis and high-availability. Prior to joining Tandem, Frans has worked on the design and implementation of database management systems and developer productivity tools for UNIX and proprietary systems. Over the years he has been advocating the use of new technologies that operate in the HPE Open Systems Services (OSS) environment, such as NonStop Server for Java and NonStop SQL/MX software.

How to Survive the Zombie Apocalypse

(and Other Disasters) with Business Continuity and Security Planning

Steve Tcherchian >> CISO & Product Manager, XYGATE SecurityOne >> XYPRO Technology

Years ago, I was one of three people in a startup company providing design and development services for web hosting and online message boards. We started the company on a dining room table. As we expanded into the living room, we quickly realized that it was getting too cramped and we needed more space to let our creative juices flow, plus we needed to find a way to stop being at each other's throats. We decided to pack up our laptops and move into a co-working space in Venice, California. We were one of four other companies using the space and sharing the rent. It was quite a nice setup and we were enjoying the digs. We were eager to get to work in the morning and wouldn't leave sometimes till very late in the evening.

One Thursday morning as we pulled up to the office to start the day, we noticed the door wide open. Someone had broken into the office in the middle of the night and stolen all of our equipment, laptops, computers etc... This was before the time of cloud computing, so data backup at that time was mainly burning CDs, which often times we would forget to do or just not do it because "we were just too busy". After the theft, we figured we would purchase new laptops and recover from the latest available backups. As we tried to restore our data, none of the processes were going as planned. Either the data was corrupted, or the CD was completely blank or too old to be of any value. Within a couple of months, we bit the bullet and had no choice but to close up shop.

BY THE NUMBERS

Business interruptions come in all shapes and sizes. From natural disasters, cyber security incidents, system failures, human error, operational activities, theft, power outages... the list goes on and on. In today's landscape, the lack of business continuity planning not only puts companies at a competitive disadvantage, but can spell doom for the company as a whole. Studies show that a single hour of downtime can cost a small business upwards of \$8,000. For large enterprises, that number skyrockets to millions. That's 6 zeros, folks! Compound that by the fact that 50% of system outages can last 24 hours or longer, and we're talking about scarily large figures.

The impact of not having a business continuity plan doesn't stop there. As if those numbers weren't staggering enough,

a study done by the AXA insurance group showed 80% of businesses that suffered a major outage filed for bankruptcy within 18 months, with 40 percent of them out of business in the first year. Needless to say, business continuity planning (BCP) and disaster recovery (DR) are critical components, and lack of planning in these areas can pose a serious risk to any modern organization.

We can talk numbers all day long about why BCP and DR are needed, but the bottom line is – THEY ARE NEEDED. Frameworks such as NIST Special Publication 800-53 Rev.4, 800-34 and ISO 22301 define an organization's "capability to continue to deliver its products and services at acceptable predefined levels after disruptive incidents have occurred". They provide much needed guidance on the types of activities to consider when formulating a BCP. They can assist organizations in ensuring business continuity and disaster recovery systems will be there, available and uncompromised when required.



DISASTER RECOVERY – DON'T LOSE SIGHT OF SECURITY & RISK

Once established, business continuity and disaster recovery strategies carry their own layer of complexities that need to be properly addressed. A successful implementation of any disaster recovery plan is contingent upon the effectiveness of its design. The company needs access to the data and applications required to keep the company running, but unauthorized access must be prevented.

Security and privacy considerations must be included in any disaster recovery planning.

Security and risk are top priority at every organization, yet traditional disaster recovery procedures focus on recovery from an administrative perspective — what to do to ensure critical business systems and applications are kept online. This includes infrastructure, staff, connectivity, logistics and data restoration. Oftentimes, security is overlooked and infrastructure items designated as disaster recovery are looked at and treated as secondary infrastructure, and as such, the need to properly secure (and budget) for them is also treated as secondary to the production systems. Companies invest heavily in resources, security hardware, software, tools and other solutions to protect their production systems. Typically, only a subset of those security solutions is deployed, if at all, to their disaster recovery systems.

The type of DR security that's right for an organization is based on need and risk. Identifying and understanding what the real risks are can help focus efforts and close gaps. A lot of people simply look at the perimeter and the highly visible systems. Meanwhile, they've got other systems and back doors where they're exposed, potentially leaking data and wide open for attack.

In a recent article, Barry Forbes, XYPRO's VP of Sales and Marketing, discusses how senior executives at a top five US Bank indicated that they would prefer experiencing downtime rather than dealing with a breach (<http://bit.ly/1mFNpRL>) The last thing you want to deal with during disaster recovery is being hit with the double whammy of a security breach. Not having equivalent security solutions and active monitoring for disaster recovery systems puts your entire continuity plan and disaster recovery in jeopardy. This opens up a large, exploitable gap for a savvy attacker or malicious insider. Attackers know all the security eyes are focused on production systems and data, yet the DR systems whose purpose is to become production systems in case of disaster are taking a back seat and ripe for the picking.

Not surprisingly, the industry is seeing an increasing number of breaches on backup and disaster recovery systems. Compromising an unpatched or an improperly secured system is much easier through a DR site. Attackers know that part of any good business continuity plan is to execute the plan on a consistent basis. This typically includes restoring live data onto backup or DR systems and ensuring applications continue to run and the business continues to operate. But if the disaster recovery system was not monitored or secured similar to the live system using similar controls and security solutions, the integrity of the system the data was just restored to is in question. That data may very well have been restored to a compromised system that was lying in wait. No one wants to issue outage notifications coupled with a breach notification.

The security considerations don't end there. Once the DR test has checked out and the compliance box ticked for a working DR system and a successfully executed plan, attackers and malicious insiders know that the data restored to a DR system can be much easier to gain access to and difficult to detect activity on. Therefore, identical security controls and inclusion of DR systems into active monitoring is not just a 'nice to have', but an absolutely necessity.

COMPLIANCE AND DISASTER RECOVERY




Organizations working in highly regulated industries need to be aware that security mandates aren't waived in times of disaster. Compliance requirements are still very much applicable during an earthquake, hurricane or data loss.

In fact, the HIPAA Security Rule specifically calls out the need for maintaining security in an outage situation. Section 164.308(a)(7)(ii)(C) requires the implementation, as needed, of procedures to enable continuation of processes for "protection of the security of electronic protected health information while operating in emergency mode."

The SOX Act is just as stringent, laying out a set of fines and other punishment for failure to comply with requirements, even at times of disaster. Section 404 of SOX discusses establishing and maintaining adequate internal control structures. Disaster recovery situations are not excluded.

It's also difficult to imagine the PCI Data Security Standards Committee relaxing its requirements on cardholder data protection for the duration when a card processing application is running on a disaster recovery system. It's just not going to happen.

CONCLUSION

Neglecting to implement proper and thorough security into disaster recovery planning can make an already critical situation spiral out of control. Careful consideration of disaster recovery planning in the areas of host configuration, defense, authentication and proactive monitoring will ensure the integrity of your DR systems and effectively prepare for recovery operations while keeping security at the forefront and keeping your business running. Most importantly, ensure your disaster recovery systems are secured at the same level and have the same solutions and controls as your production systems. 

.....

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

Back for More...

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

Perhaps the best value from being part of the NonStop community is the people – you meet a variety of very skilled community members that all have the same enthusiasm for NonStop as you do. It's not always aligned with where your interests lie, but all the same, it is the people that contribute to the value proposition of NonStop. Today, when we consider the key attributes of NonStop, they remain as important for all enterprises as they were at any time in the past. The capabilities of NonStop on the other hand go way beyond what NonStop provided when carrying the Tandem Computers logo and it is this story of NonStop that so often ignites the passions of all who are associated with NonStop today – HPE, vendors and consultants, but most of all users.

I was reminded of this just recently as I spent time at numerous industry and association events. While my observations have worked their way into numerous blog posts and commentaries, what really stands out for me is just how far we have come and how high we have climbed in the eyes of senior HPE executives. Unlike the outcome of other systems where the future is anything but stellar, for whatever reason, NonStop is being funded and the investments being made continue to be impressive. A reputed \$250 Million investment in the deep port to the Intel x86 architecture, not to mention the support for InfiniBand as a viable hybrid interconnect vehicle as part of the Yuma project, but many more millions of dollars in support of NonStop as Software capable of running in virtual machines.

As I wrapped up last month's Back for more ... column I wrote that the NonStop community consider this (column) a teaser for what is to come from me in future columns, musings, commentaries and posts. Look too for webinars sponsored by clients where I will go much deeper into what I see coming from HPE, a multi-part series of webinars I only just concluded early in March. But there will be more, of course. However, what I wanted the NonStop community to consider as a teaser were the remarks by Martin Fink, EVP and CTO of HPE, on the topic of ContainerOS where I asked whether this was going to be HPE's solution to virtualization? Quite probably, I concluded but in the past few weeks, a lot more has been revealed by HPE at events around the world.


If you missed it, I published a post on February 8, 2016, to the IR blog, Can you Visualize NonStop in a Virtual World? As is my custom, I then started several discussions on the content of this post to numerous LinkedIn groups and very quickly, comments started appearing on the discussion on two separate LinkedIn groups – Real Time View and Tandem User Group. Among the comments was a promotion by HPE about an upcoming event in Barcelona, Spain – the Mobile World Congress 2016, which one comment by a HPE NonStop Master technologist suggested “will be interesting.” What he was referring to was a HPE presentation, “Transfer to a hybrid infrastructure” where the audience was encouraged to, “Visit this demo to learn about the future of highly available and massively scalable infrastructure for your core network. This is a live demonstration

featuring a potential HPE virtual NonStop environment with x86 COTS (Commercial Off The Shelf) hardware. Touch and see virtual network core functions of HPE I-HSS and INS.”

Obviously, with a conference on Mobile, there would be references by HPE to applications in support of mobile devices and this is one market segment where NonStop continues to enjoy success. Furthermore, since the November, 2015, NonStop Technical Boot Camp in San Jose, we have all read of how the investments in NonStop continue and it's not just the Yuma project or the work to make NonStop independent of infrastructure, but equally as important, NonStop was going to be running on virtual machines just as it does today on real machines.

It's now a matter of public record that in the discussion on the LinkedIn group, Tandem User Group, this same topic attracted additional commentary from Andy Bergholz, Director of Engineering, HPE, who wrote of how, “The really cool thing is because all this software was already ported to NonStop X, it just worked in the virtual NonStop environment.” Furthermore, when it comes to the reason for pursuing NonStop running with a virtual machine, Bergholz noted, “Regarding the value proposition, virtual NonStop would enable customers to fully utilize their IaaS, run NonStop VM's and Linux VM's in the same physical server, connected via YUMA (RDMA over RoCE – RDMA over Converged Ethernet).”

But there's even more on this topic being published on the LinkedIn group, Tandem User Group. “New availability options may be brought forth in the future as well,” Bergholz suggests. “I see mention of just firing up another NonStop VM if a physical server fails, rapidly bringing the virtual CPU back up. Also, think about the possibility of doing hot patches / SPRs by firing up a second virtual NonStop system on the new SPRs running active/active, then downing the ‘old’ virtual NonStop system. This provides very little downtime (if any) to take a SPR (Software Product Revision) or even new RVU (Release Version Update).”

The people that belong to the NonStop community make all the difference and I am constantly being reminded that the value proposition for NonStop should never stray too far from the reality that NonStop continues to attract many of the best people in IT. Not for them are the catchy phrases from the “Gucci Marketers” as I call them, but rather, the more meaty conversations of those working with NonStop systems. The support for virtual machines can no longer be categorized as a teaser – it's real and is being demoed already – and I can only concur with Bergholz when he states, “I would expect customers that want the very best fabric latency performance to continue purchasing NonStop X converged systems on IB. The great thing is that we will offer our customers product choice points, and they can move forward with the right solution for their application!” And isn't it still all about having choice when it comes to how best we deploy NonStop in support of our applications? 

SQLXPress

Not just another pretty face

An integrated SQL Database Manager for HP NonStop.

Single solution providing database management, visual query planner, query advisor, SQL whiteboard, performance monitoring, MXCS management, execution plan management, data import and export, data browsing, and more...

With full support for both SQL/MP and SQL/MX



Learn more at
xypro.com/SQLXPress



The guiding light for your mission critical business Improve your NonStop'ness. Better always on!



Today's demands of mission critical businesses and customers are ever increasing. Unreliable and unavailable systems and applications are not an option. Minimizing downtime whilst maximizing security and operational efficiency is therefore paramount for the IT department. If your light is going out, your business and your customers can get in trouble. Systems and applications can't stop; they must be on, always!

comForte „better always on“ solutions help you gain ...

Better Infrastructure

Make the most of best in class communications and connectivity solutions by providing end users and system administrators with high performance, secure and reliable access to NonStop systems.

Better Security

Protect your mission critical data-in transit and at-rest. Improve your overall security posture on NonStop and achieve compliance with industry standards and regulations.

Better Applications

Modernize your legacy applications from the database layer, through better integration in the enterprise all the way to refreshing the application's Graphical User Interface.

Better always on with comForte's unparalleled solutions for HP NonStop.

www.comforte.com/better_always_on

com.forte®
better always on