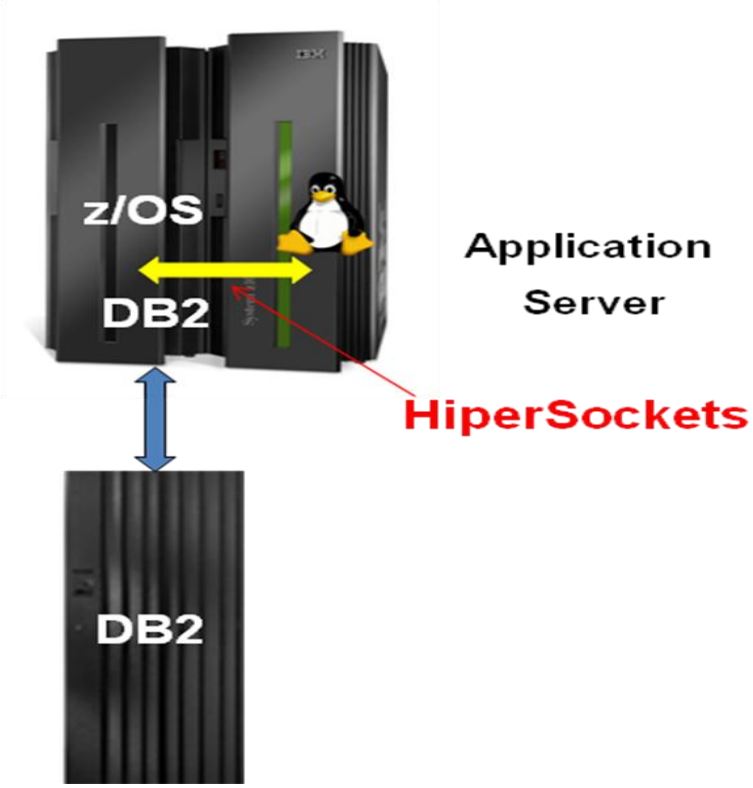
White Paper

SAP ERP on System z – state-of-the-art business resilience with the highest level of security



July 2009
Josh Krischer

2009 © Josh Krischer & Associates GmbH. All rights reserved. Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Josh Krischer & Associates GmbH disclaims all warranties as to the accuracy, completeness or adequacy of such information. Josh Krischer & Associates GmbH shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice. All product names used and mentioned herein are the trademarks of their respective owners.

White Paper

SAP ERP on System z – state-of-the-art business resilience with the highest level of security

© Josh Krischer & Associates GmbH. All rights reserved.

SAP ERP on System z – state-of-the-art business resilience with the highest level of security

Josh Krischer

Josh Krischer is an expert IT advisor with 39 years of experience in high-end computing, storage, disaster recovery, and data center consolidation. Currently working as an independent analyst at Josh Krischer & Associates GmbH, he was formerly a Research Vice President at Gartner, covering mainframes, enterprise servers and storage from 1998 until 2007. During his career at Gartner he was responsible for high-end storage-subsystems and disaster recovery techniques. He spoke on these topics and others at a multitude of worldwide IT events, including Gartner conferences and symposia, industry and educational conferences, as well as major vendor events.

According to a report by Gartner Inc., SAP's Enterprise Resource Planning (ERP) packages lead by market share in 2007, capturing 27.5 percent of the ERP market - roughly double that of the second-ranked competitor (13.9 percent). More than 82,000 customers worldwide run SAP applications. For most of these customers, this application is crucial to run their business, and hence, requires more than just IT infrastructure availability. Rather, a robust business resilience infrastructure should include:

- **Business Continuity** ensures continuity of service and support for its customers, employees, and business partners. Deploying a high-availability, robust IT infrastructure with disaster recovery capabilities is an essential part of business continuity.
- **Security, privacy and data protection** guards against internal and external threats.
- **Regulatory compliance** ensures adherence to government rules and regulations.
- **Flexibility** to quickly implement changes and easy migrations.
- **Performance** to deliver a constant response time, regardless of number of users, and smooth scalability.
- **Sites and facilities** need to be well-designed and protected.

SAP ERP on System z answers all these requirements, and, in addition, delivers solutions at lower energy costs, lower carbon-dioxide emission, and lower facility costs, but with more effective management and less man-power.

SAP ERP platforms and architecture

SAP ERP applications are based on a three-tier architecture: database server, application servers, and the presentation clients connected via the Internet or Intranet. The different

© Josh Krischer & Associates GmbH. All rights reserved.

servers are System z mainframes, Unix (and increasingly Linux), and Windows. The vast majority of the large-scale customer installations, however, run mainframe or Unix platforms. By December 2008, there were more than 1,000 installations on System z worldwide.

Mainframe as database server

SAP R/2 was an ERP application designed to run on IBM or compatible mainframes, whereas R/3 was designed for Unix and Windows. In 1996 IBM and SAP kicked off the mainframe platform project after porting R/3's database server to DB2 on mainframe while using AIX-based Unix or Windows as the application server (see Figure 1). So far, this has been the most popular deployment of SAP on mainframes; however, a recent trend is to use the Integrated Facility for Linux (IFLs) Linux capability of a mainframe as the application server. The communication between the database server and external application server works via TCP/IP using external teleprocessing controllers or internal Open Systems Adapters (OSA) in a mainframe. Application servers running on IFL can benefit from using internal HiperSockets[1] for improved performance.

Figure 1: System z as DB2 database server, AIX as application server

Using DB2 on the mainframe allows for large database scalability, performance, I/O sharing, very high availability, and advanced disaster recovery techniques. An SAP ERP can span multiple servers in a Parallel Sysplex cluster with real parallel read/write data sharing capabilities. Mainframe internal hardware compression on all paths may save up to 70% of disk space and dramatically reduce data transfer times. In addition, part of DB2 execution can

[1] HiperSockets, unique to the System z series, provide lower-cost, fast, low-latency TCP/IP emulation within System z memory instead of TCP/IP communication via external devices. For example, this feature may reduce communication overhead and significantly increase performance of connecting DB2 running under z/OS with an application server in a Linux partition on IFL.

© Josh Krischer & Associates GmbH. All rights reserved.

be offloaded to special zIIP engines, which are priced significantly lower than z/OS processors[2].
The major reasons to select System z as a database server for SAP applications are:

- High availability and manageability of large databases without the need for database splitting, which may result in losing a single view of the enterprise data.
- Automated Service Levels (SLAs) management by the Workload manager (WLM)[3] . An effective usage of WLM allows users to purchase fewer MIPS and channels to effectively handle peaks in demand and increase the efficiency of computing resources.
- Online database reorganization and DB2 release upgrade.
- Effective data sharing between systems in a Parallel Sysplex cluster.
- Ability of a single mainframe to handle multiple SAP database servers and databases.
- Synergy between SAP and DB2 on System z - IBM has implemented more than 100 feature requests over different DB2 for z/OS versions.

Today the majority of SAP Business Suite applications, as well as R/3 and SAP NetWeaver components, are supported on the mainframe database server.
IBM Global Technology Services (GTS) can perform migrations to DB2. With the DB2 Fastloader for SAP, databases can be usually migrated to DB2 within a day or weekend.

Mainframe as application server

z/Linux on System z as the application server platform (see Figure 2) benefits from the increased recognition of Linux as an enterprise-ripe operating system. This option was initially announced in March 2002 for 32 and 64 bit mode to run in IFLs. Very fast communication between the database server and the application server is achieved by HiperSockets (see [1] above). I/O operations on Linux on System z are executed by the System z Dynamic Channel

[2]The System z offload engines: z Integrated Information Processor (zIIP) is used to offload DB2; z Application Assist Processor (zAAP) supports Java code execution; Integrated Facility for Linux (IFL) runs Linux on the mainframe; Internal Coupling Facility (ICF) provides support for Parallel Sysplex clustering.
All of these offload engines are priced significantly lower than the usual z/OS engines. The computing power (MSUs) of these engines is excluded from software charges. Users who skilfully employ these engines can off-load their z/OS MIPS, stem z/OS growth requirements, and thus, lower TCO.

[3] The System z Workload Manager is the industry's most effective load-balancing tool. WLM is capable of dynamically distributing and adjusting computing resources according to pre-set business goals and policies. This dynamic resource management goes across clustered Logical Partitions (LPARs), allowing management of processor capacity, prioritization of I/Os, and activation of newly-installed resources.

© Josh Krischer & Associates GmbH. All rights reserved.

Subsystem, which off-loads almost all I/O overhead from the instruction processor and improves performance. In general, using Linux on System z as the application server platform yields the following dis-/advantages:

Linux as application server pros

- "Special engine" pricing for hardware, no z/OS charges for IFL engines,
- Better performance, particularly for I/O operations,
- Fast connectivity to DB2 for z/OS'
- Ability to use z/VM to configure additional servers in a matter of minutes,
- Consolidation of several central instances, applications, as well as development and test environments,
- Cost reduction due to:
  - Fewer nodes, lower software charges,
  - Lower energy costs, lower carbon-dioxide emissions,
  - Lower facility costs,
  - More effective management, less man-power required,
- Better disaster recovery than with discrete servers
- Utilization of System z platform's powerful I/O capabilities (Dynamic Channel Subsystem)
- Present and future wide availability of skilled staff.

Linux as application server cons

- Linux clustering vs. Parallel Sysplex,
- Higher hardware costs in comparison to discrete servers

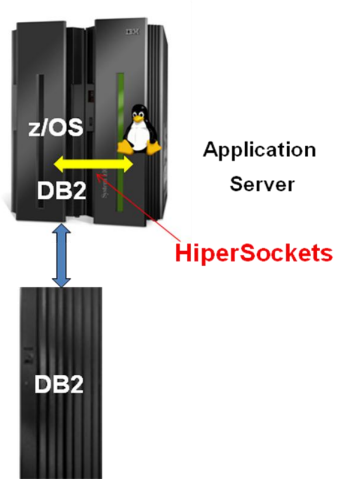


Figure 2: System z as DB2 database server, Linux on IFL as application server

© Josh Krischer & Associates GmbH. All rights reserved.

For an optimzed availability of the SAP solution, the SAP Standalone Central Services can be run under z/OS, namely in mainframe partitions under Unix Software Services (USS).

Case Study: Baldor Electric

Baldor Electric is a leading global designer and manufacturer of industrial electric motors, power transmission products, drives, and generators. The company with its global headquarters in Fort Smith, Arkansas, can look back at a history of 88 years and is well established in more than 20 countries. In 2007 Baldor employed 3,800 full-time employees with revenues reaching USD 1.8 Billion. Baldor Electric was an early adopter of SAP solutions on the IBM mainframe - one of the first U.S. companies to run SAP R/3 on the mainframe in the late 1990s. The company decided to port SAP's ERP application to the IBM System z mainframe in order to achieve better performance and higher reliability and availability. Tangible benefits of running SAP DB2 database server on the mainframe led in 2005 to further consolidation of distributed Unix and Windows servers on IBM's System z platform, employing SUSE Linux Enterprise Server running in IFL partitions. The migration of 15 UNIX and 20 Windows servers to 24 Linux partitions was completed in mid 2006. The SAP Business Suite (HR/Payroll, FICO, MMPP, S&D), portals, and business intelligence applications are crucial for managing a company's entire operation including sales and distribution, manufacturing, payroll, and finance. In addition, Baldor uses Linux on System z for some Web applications such as Apache and Lotus Domino. The new infrastructure permitted Baldor to build portal technology that allows customers and distributors to order products and schedule deliveries based on live manufacturing data. Currently, 4300 users generate daily averages of a million transactions with response times in the sub-second range. In addition, 1,350 scheduled batch jobs for SAP and other System z applications are executed daily. The 2 TByte DB2 for z/OS uses two data sharing images. The current number of Linux partitions running on 16 IFLs is more than 60; two native Linux partition and the rest under z/VM.

"The migration of our SAP application servers to Linux on the System z produced an immediate increase in performance, and has made it easier to manage and maintain our systems," said Mark Shackleford, Vice President, Information Services Officer, Baldor Electric."

"The migration of our SAP application servers to Linux on the System z produced an immediate increase in performance, and has made it easier to manage and maintain our systems," said Mark Shackleford, Vice President, Information Services Officer, Baldor Electric. "*This consolidation project made it possible for us to take on innovative initiatives like the ShopFloor Display portal. It has also significantly trimmed the total cost of IT and reduced the administrative workload on our department -- requiring less than 40 technology professionals to run our global operation."*

"*Customers will be able to see right into our production systems, including time-to-delivery, using the SAP Portal technology over the Web. This reduces paperwork and costs, and enables Baldor to offer a faster service for customers who simply cannot wait for an overseas*

© Josh Krischer & Associates GmbH. All rights reserved.

delivery. The IBM and SAP solution is truly a key part of our competitive strategy" Mark Shackelford comments.

One of the benefits of the server consolidation was the ability to conduct a consolidated backup instead of having to manage a backup on each individual server. Baldor deployed Innovation Data Processing's FDR/UPSTREAM to backup the z/Linux partition and some Windows servers (which were not consolidated) to a tape library employing a single solution. The Linux mainframe's data is transferred via its HiperSockets to the FDR/UPSTREAM (run under z/OS) and then sent through FICON channels to the enterprise tape library. Using HiperSockets and FICON channels instead of IP over 1Gbps Ethernet resulted in significant performance improvements and shorter backup window requirements.

To summarize, Baldor Electric's gained the following benefits from porting SAP onto System z (database and application servers):

- Improved reliability and availability,
- Better performance,
- Simplified infrastructure,
- Simplified management resulting in manpower reduction,
- Ability to create "test" and "development" partitions in matter of minutes,
- Reduced software charges,
- Reduced maintenance charges,
- Reduced energy requirements (costs) and carbon-dioxide emission by more than 60%
- Reduced floor space by 70%
- Consolidated backup on enterprise tapes.

All these benefits allowed Baldor Electric to concentrate on its business processes instead of focusing on the IT infrastructure, resulting in a better alignment of its IT with its business requirements. Despite a huge increase in sales revenue, IT costs as a percentage of sales have dropped every year since 2003, with cost savings attributed to its SAP ERP on System z consolidation estimated at around 42 percent.

Business continuity of SAP on System z

One of the strongest arguments in favor of deploying SAP ERP on System z is the highest standard of hardware and software availability and advanced disaster recovery capabilities of this platform. High-availability systems are designed to have no single points of failure (SPOF) and no single points of repair (SPOR) through the use of redundant components and architectures. Non-disruptive upgrades and micro-code updates also play a crucial role in achieving high availability. Some examples of internal availability features in System z hardware include:

- redundant and hot-swappable power supplies, blowers, logic cards,
- Error Correction Codes (ECC) for memory,
- spare processors,

© Josh Krischer & Associates GmbH. All rights reserved.

- memory fencing,
- alternate channels and network paths.

Consider System z memory ECC, for example. IBM developed *Chipkill* (or Advanced ECC memory technology) specifically for the NASA pathfinder mission to Mars. Standard ECC is able to detect and correct single-bit memory errors, which make up the vast majority of memory errors. However, Chipkill memory also has the ability to correct multi-bit memory errors by deploying techniques similar to those used by RAID disk storage subsystems.

Another high-availability feature available on IBM mainframes is that upon encountering a hardware failure, it can automatically activate a spare processor to replace a failing processor and perform a software retry. Software recovery on System z is very powerful, with several layers of retries.

System z supports Parallel Sysplex as a local or remote cluster. Up to 32 local or remote mainframes can participate in a single cluster. System z Parallel Sysplex also works in conjunction with IBM's disaster recovery software called Geographically Dispersed Parallel Sysplex (GDPS). GDPS enables automated complete site fail-over with no or minimum loss of data.

One of the most disruptive tasks can be the installation of a new storage subsystem and the migration of the data. It is usually time-consuming and sometimes risky. Data migrations are also required during tuning activities or for building tiered storage infrastructures. System z supports migration using DFSMS or non-disruptive data set level migration with IBM Softek zDMF.

Geographical Dispersed Parallel Sysplex (GDPS)

Multiple sites and remote data mirroring are only one part of a well-structured disaster recovery infrastructure. To ensure very-high availability and automation, software support is required. This software controls the fail-over and provides end–to-end application availability in case of a planned outage or an unplanned disaster. IBM's GDPS for System z is a multi-site application availability solution, with fast recovery time and highly-automated control. It manages application availability in and across sites for both planned maintenance and unplanned situations, such as a site failure or full-blown disaster. GDPS was initially designed for mainframe z/OS systems, but, with continuous development, was later enhanced to support selected other system platforms as well. GDPS can now manage other System z production operating systems such as Linux for System z, z/VM, and z/VSE, which means it can provide coordinated disaster recovery to customers with distributed hybrid applications that span z/OS and Linux for System z, such as SAP.
GDPS is a licensable product that a customer deploys through IBM Global Technology Services. Once the installation and testing are complete, the customer is self-sufficient in operation, modifications, configuration changes, updates etc.

© Josh Krischer & Associates GmbH. All rights reserved.

HyperSwap function

The unique HyperSwap function is probably the most important business continuity and availability improvement for IBM mainframes. While disasters rarely occur in reality, disk subsystem failures are far more likely to happen. In current integrated and complex application environments - assuming a highly-available data-sharing Parallel Sysplex environment - disk becomes a single point of failure for the entire Sysplex. The HyperSwap function, which is used by multiple GDPS solutions, is controlled by GDPS automation. Use of HyperSwap can eliminate an outage caused by planned maintenance or disk failure by reducing the time needed to switch disks between sites to a matter of seconds and allowing the primary site to use the secondary site's disk storage subsystems.
Basic HyperSwap between two remote or locally installed storage subsystems in order to provide automated fail-over for planned or un-planned outages can be deployed with z/OS alone, without requiring multi-site GDPS. Similarly to GDPS, there is no equivalent functionality on any other platform besides System z.

Capacity Back-UP (CBU)

A best practice in disaster recovery planning is to purchase a provision of additional processors which can be activated in an emergency to compensate for lost capacity without any additional charges. This option enables business-critical applications to run with appropriate service levels without up-front investment for spare capacity. GDPS can automatically activate the CBUs in case of a disaster. CBUs can be provisioned for z/OS and for any special engine such as IFL. CBU provisioning in a disaster recovery plan saves on CapEx and OpeEx.

IBM Business Continuity and Resiliency Services (BCRS)

Availability and business continuity products are available for businesses of all sizes. However, the main challenge for these organizations is the lack of available experienced IT staff to plan the corporate-wide recovery plan, deploy the appropriate BC/DR recovery products, and then test the overall plan. IBM Business Continuity and Resiliency Services (BCRS) from IBM Global Technology Services can be employed to design, manage and deploy a customized, integrated, end-to-end continuity program. The solutions are designed to be integrated into the existing corporate organization and meet relevant government compliance and industry regulations.
BCRS supports hundreds of third-party hardware and software components in addition to IBM products. BCRS can be employed to perform a risk analysis and work with the organization's users to perform a Business Impact Analysis (BIA). The BIA will identify critical business processes, components, platforms and applications, and analyze individual recovery requirements. It can also provide alternate recovery services in the event of a major disaster, including hot site provisioning, mobile data centers, and staff.

© Josh Krischer & Associates GmbH. All rights reserved.

Case study: Postbank's improved business continuity

Postbank Systems AG is the IT service provider for Postbank, one of the largest retail banks in Germany. Postbank has more than 14 million clients, total assets of €240 billion, and approximately 20,000 employees.

Challenge and requirements: The bank's new banking system, developed in conjunction with SAP AG, is based on SAP ERP. To ensure high service levels with continuous 24/7 operation, the bank needed a platform offering both high availability and rapid recovery capabilities from unscheduled downtime or disaster.

Solution: To answer these requirements, the bank initially deployed four IBM eServer zSeries 990 servers (later upgraded to System z10) and storage, divided between two data centers and linked using IBM GDPS. The database server employed is DB2 for z/OS.

Result: Postbank Systems AG built a robust, integrated solution with high performance and high resiliency for its SAP ERP infrastructure. The architecture yields greatly reduced outage times for both planned and unplanned maintenance.

System z security

Security issues top the priority lists of any responsible IT organization. Every industry corporation understands the need to protect itself from industry espionage and it is obvious for every financial institute to prevent frauds, however not every institution took precautions to prevent personal data breaches. The number of cybercrime cases has been growing steadily from year to year. *"Businesses, governments and universities reported a record number of data breaches in the first half of this year, a 69 percent increase over the same period in 2007 driven by a spike in data thefts attributed to employees and contractors, according to an analysis by identity theft experts"* - Brian Krebs on Computer Security, Washington Post, June 2008. Every few days, media reports about new cases of stolen identity, privacy breaches, and loss of personal data[4] emerge. These incidents, on top of high direct financial cost (compensation, notification of exposed personal data, etc.) and administration work, also cause heavy damage to the affected companies' reputation, in particular for financial institutions. According to a Cyber Security Industry Alliance survey of consumers in 2007, 33% of consumers notified of a security breach would terminate their relationship with the company they perceived as responsible. The larger the organization, the bigger is the potential damage, and the bigger is the attracted news media coverage and resulting loss of reputation.

A Ponemon Institute benchmark study in 2008 examined the costs incurred by 35 organizations after experiencing a data breach. The study estimated the costs for activities resulting from actual data loss incidents, with the following key findings:

- The total average cost of a data breach was $197 per record.

[4] Since January 2005 the Privacy Rights Clearinghouse has identified more than 215 million records of U.S. residents that have been exposed due to security breaches.

© Josh Krischer & Associates GmbH. All rights reserved.

- The average total cost per reporting company was more than $6.3 million per breach (up from $4.8 million the previous year) and ranged from $225,000 to almost $35 million.
- The cost of lost business averaged $4.1 million or $128 per record compromised, which accounts for 65 percent of data breach costs.

Regulations in more than 35 U.S. states and many countries require that individuals (customers, employees, citizens, students, alumni, etc.) be notified if their confidential or personal data has been lost, stolen, or compromised. Examples include the California Database Protection Act of 2003[5], §19a (1) and Federal Data Protection Act in Germany. Furthermore, legislation such as the Gramm-Leach-Bliley Act[6], the Health Insurance Portability and Accountability Act (HIPAA)[7], and various other privacy protection rules in many countries impose strict security requirements on enterprises. When a regulatory breach happens, the responsible organizations must notify all affected individuals and attempt to minimize possible damages.

Security is not a piece of hardware or software package that can be purchased and installed. It requires establishing an information security plan for a data center and a business. It should cover the complete IT Infrastructure: from application to network (end-to-end encryption), storage media, and people. It requires continuous management, change management, attention to detail, and a healthy dose of paranoia. The various building blocks of good a security plan cover:

- **Authentication** - validation of users, security administrators, and system administrators.
- **Access control** - limits what data portion can be seen by a user; assigning of appropriate privileges for a specific job responsibility.
- **Integrity -** ensures that data is consistent and correct and has not changed as result of transfer, malfunction, or malicious attack.
- **Data encryption** - protects, beyond access control, content from unauthorized access, in particular on storage media or during data transmission.

[5] California law requires any person, agency, or company doing business in California to disclose any security breaches to each affected California customer whose personal information has been compromised.

[6] The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions.

[7] The final rule adopting HIPAA standards for security was published in the Federal Register on February 20, 2003. This final rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information. The standards are delineated into either required or addressable implementation specifications.

© Josh Krischer & Associates GmbH. All rights reserved.

- **Secure key management** - ensures that data can be accessed when required; losing a key is equivalent to data shredding.
- **Non-repudiation of data** (safe digital signature) - acknowledgements or receipts to verify that the sender/receiver did send/receive the message.
- **Auditing capability** – logging of all accesses and administrative changes for later analysis.

"System z has provided robust hardware and software solutions to answer cryptographic security needs for almost two decades. For more than a decade, IBM mainframes have been certified at the highest security level."

System z cryptographic solutions

System z has provided robust hardware and software solutions to answer cryptographic security needs for almost two decades. For more than a decade, IBM mainframes have been certified at the highest security level[8]. The follow-on generations of cryptographic-coprocessor features have received similar certification for secure-key processing.
The Common Criteria Security Certification is an internationally recognized ISO security standard used by governments and other organizations. In this standard, there are seven stages of Evaluation Assurance Level (EALs), EAL-1 to EAL-7; in the United States, evaluation to EALs 5-7 for the U.S. Government must be performed by the National Security Agency (NSA). On March 2003, IBM's eServer System z 900 was the first server to be awarded EAL5 security certification (the highest commercial level). The subsequent mainframe generations were awarded the same level. z/OS V1R7 and 8 were certified at EAL-4+ and the same level was achieved by SUSE LINUX Enterprise Server 9. The EAL-5 certification of System z includes logical partitioning (LPARs), which ensures organizations' ability to run multiple z/OS, z/VM, and Linux-based applications such as payroll, human resources, e-commerce, etc. on a single System z mainframe without jeopardizing confidentiality requirements[9].

The cryptographic hardware (optional feature) of System z consists of special processors that are customized to perform selected cryptographic algorithms. There are two options:

1. **Hardware Security Module** (HSM) is designed to withstand most physical attacks. Upon tampering detection, HSM erases any sensitive information such as encryption master keys.

[8] In 1997 IBM's PCI Cryptographic Coprocessor (PCICC) and S/390* Cryptographic Coprocessor Facility (CCF) were certified at Federal Information Processing Standard (FIPS) 140-1 Level 4, the highest certification for commercial security awarded by the U.S. and Canadian governments.

[9] These certifications levels are recognized by many countries' authorities, e.g., Germany's IT security agency Bundesamt für Sicherheit in der Informationstechnik (BSI).

© Josh Krischer & Associates GmbH. All rights reserved.

2. **Cryptographic accelerators** are specialized processors that are designed to support a cryptographic algorithm's specific computing requirements. For example, the DES or SHA accelerator is specifically designed to sift through lots of data; the RSA accelerator is effective at exponential and modulus mathematics. The accelerators off-load cryptographic tasks from the System z general purpose processors, reducing encryption overhead and the impact on performance.

Both these solutions are supported by the System z operating systems used by SAP ERP (z/OS, Linux on System z, and z/VM).
IBMs Integrated Cryptographic Service Facility (ICSF) provides methodologies to help protect and manage keys with a single point of control for all z/OS key-management processes. ICSF frees applications from having to perform encryption; nor do applications need to know whether or what hardware encryption facilities are available, which ensures future compatibility. Furthermore, ICSF provides load-balancing and intelligent routing capabilities on the available encryption hardware.

IBM z/OS Security Server

IBM's z/OS Security Server is a set of features in z/OS to control the access (user ID and passwords) and restrict the actions an authorized user can perform on data files and programs. The best-known part of the Security Server is the Resource Access Control Facility (RACF), the backbone of mainframe security, which controls access to all protected z/OS resources. Additional security components include a DCE Security Server, Lightweight Directory Access Protocol (LDAP) Server[10], z/OS Firewall Technologies, and more. The firewall allows the mainframe to be connected directly to the Internet (if required) without any intervening hardware and can provide the required levels of security to protect vital company data. It supports VPN technology to establish securely-encrypted tunnels through the Internet from a client to the mainframe.
RACF, as mentioned above, provides the tools to help the installation manage access to its critical resources and is the main component of the Security Server. RACF retains information about users, resources, and access authorizations in special structures called *profiles* in its database, and it refers to these profiles when deciding which users should be permitted access to protected system resources. Comparable products offered by third parties include Computer Associates' ACF2 and Top Secret solutions. RACF employs a user ID and a system-encrypted password to perform its user identification and verification. The user ID identifies the person to the system as an RACF user; the password verifies the user's identity. In addition to users' identification and authentication, RACF logs and reports various attempts of unauthorized access to a protected resource, which aids in investigating security breaches. Digital signatures to ensure non-repudiation of data are delivered by RACF as a standard feature. It is

[10] An LDAP directory provides an easy way to maintain directory information in a central location for storage, update, retrieval, and exchange.

© Josh Krischer & Associates GmbH. All rights reserved.

mandatory for a financial institution or e-commerce organization to confirm that a transaction has genuinely been sent by whom it considers the sender and that it has been received by the expected recipient.

Tivoli security products for z/OS

The z/OS Communications Server includes firewall filtering as well as components to encrypt TCP/IP network traffic for Virtual Private Network (VPN) and Transport Layer Security (TLS) capabilities.

Tivoli's zSecure Suite contains several modules allowing user-friendly RACF administration (such as a Microsoft Windows–based GUI for RACF administration), e.g., compliance and auditing, detection (and reporting) of security exposures, and intrusion monitoring. Another product is Tivoli Compliance Insight Manager, which provides compliance reporting across applications, databases, and operating systems. IBM Tivoli Identity Manager for z/OS provides a secure, automated, and policy-based solution that helps effectively manage user accounts, permissions and passwords across heterogeneous IT resources.

In early 2007 IBM acquired Consul Risk Management Inc, a privately held company headquartered in Delft, Netherlands with a principal office in Herndon, VA. Consul has developed several solutions to manage security on z/OS systems with RACF, improve security and compliance reporting, and add mitigation measures.

"SAP on mainframe is a robust and reliable SAP deployment, especially for large-scale or SAP Business Suite projects. The System z platform ensures the highest availability and security for SAP ERP and other applications, building on experience of more than 40 years."

Consul's products, such as zAdmin, zVisual, and zToolkit (Consul's zSecure Suite), offer a friendly RACF administration and reporting interface for users. The products allow options to delegate, or decentralize, part of the security administration to non-technical staff allowing business units some (limited) security administration. Consul's products have been added to the Tivoli brand as part of IBM's Service Management solutions.

Total Cost of Ownership

IBM is flexible when negotiating hardware and software charges for new applications; SAP ERP falls under the category of NALC (New Application License Charge), which means that z/OS hardware MIPS and software charges are significantly lower than the charges for legacy applications such as CICS or IMS. The IFL and the zIIP engines cost a fraction of non-NALC z/OS engines. One customer in Denmark running SAP on System z manages to offload ca. 1700 MIPS to 5 zIIPs at peak time, resulting in substantial savings on hardware and software. z/VM is priced using a flat price, regardless of the number of engines or partitions.

Major TCO savings can be achieved through the reduction of processors and man-power. For example, Oracle software charges are based on the number of processors and one mainframe

© Josh Krischer & Associates GmbH. All rights reserved.

engine can replace several RISC or x86 processors[11]. Of the several users I have interviewed, all emphasized the reduction in man-power requirements after consolidation from Unix or Windows to mainframe. Additional savings can be achieved as the result of lower energy and floor space requirements. With skillful negotiations, SAP ERP on System z may cost 20-30% more than comparable deployments on Unix; however, because of the large potential savings, the return on investment (ROI) can be reached in a relatively short time.

Summary and conclusions

SAP on mainframe is a robust and reliable SAP deployment, especially for large-scale or SAP Business Suite projects. The System z platform ensures the highest availability and security for SAP ERP and other applications, building on experience of more than 40 years. GDPS and HyperSwap provide a unique solution to reach the highest level of business continuity and availability. Skillful negotiations can price these solutions at an acceptable level without compromising on business and compliance requirements. A holistic security design protects the system from external and internal threats, with Tivoli tools providing a user-friendly interface to manage the security features. IBM's Global Technology Services provide migrations and deployment services, and IBM Finance can finance the deployments, the software, and the hardware (including third-party components).

[11] IBM Global Technology Services is certified by SAP to deploy Oracle to DB2 migration projects.

© Josh Krischer & Associates GmbH. All rights reserved.