



Ultimate Security with the IBM z13

IBM Redbooks Solution Guide

Analytics, mobile, social, and cloud computing all have one thing in common: They need a platform that has a deeply integrated security stack. This is where IBM® z Systems™ excel. To help counter the many threats to your business in the current world, including hackers looking to penetrate your systems and government-backed attacks, z Systems offers a platform with layers of defense to protect your customer data, intellectual property, and your reputation.

You can no longer just wrap security around the system; you must build security into the system. The IBM z13™ is a new system that is designed for analytics, mobile, social, and cloud computing with built-in security.

Using the z13 cryptographic hardware, you gain security from using the Central Processor Assist for Cryptographic Functions (CPACF) and Crypto Express5S through in-kernel cryptography APIs and, for Linux on z Systems, the libica cryptographic functions library.

The benefits of using these features are:

- File system encryption
- Communication encryption (to the applications such as IBM HTTP Server)
- System security by providing advanced cryptographic functions

This IBM Solution Guide explains how the z13 can help your organization maintain the highest level of security that is possible, and achieve the goals that are shown in Figure 1.



Figure 1. Be ready. Be resilient. Be secure.

Did you know?

z Systems is the only commercial operating system that has achieved EAL 5+ certification. This certification means that although different workloads are running on the same hardware, they are protected when running in separate partitions; one logical partition (LPAR) cannot reach across boundaries into the next LPAR and compromise its security. The LPARs are allocated their own resources and are secure and separate environments.

Integrated cryptographic features provide leading cryptographic performance and functions. Reliability, availability, and serviceability (RAS) support for the Crypto Express5S is unmatched in the industry. IBM is in the process of gaining FIPS 140-2 Level 4 certification for the Crypto Express5S feature. With FIPS 140-2 Level 4 certified cryptographic hardware, IBM provides the most secure tamper-sensing and tamper-resistant security module that is available in the market.

Business value

The world is becoming more digitized and interconnected, which open the door to emerging threats, leaks and attacks. The average cost of a security breach is \$5.8 *million* US dollars (USD)! Analytics, mobile, social, and cloud computing all have one thing in common: They need a platform that has a deeply integrated security stack, as shown in Figure 2.

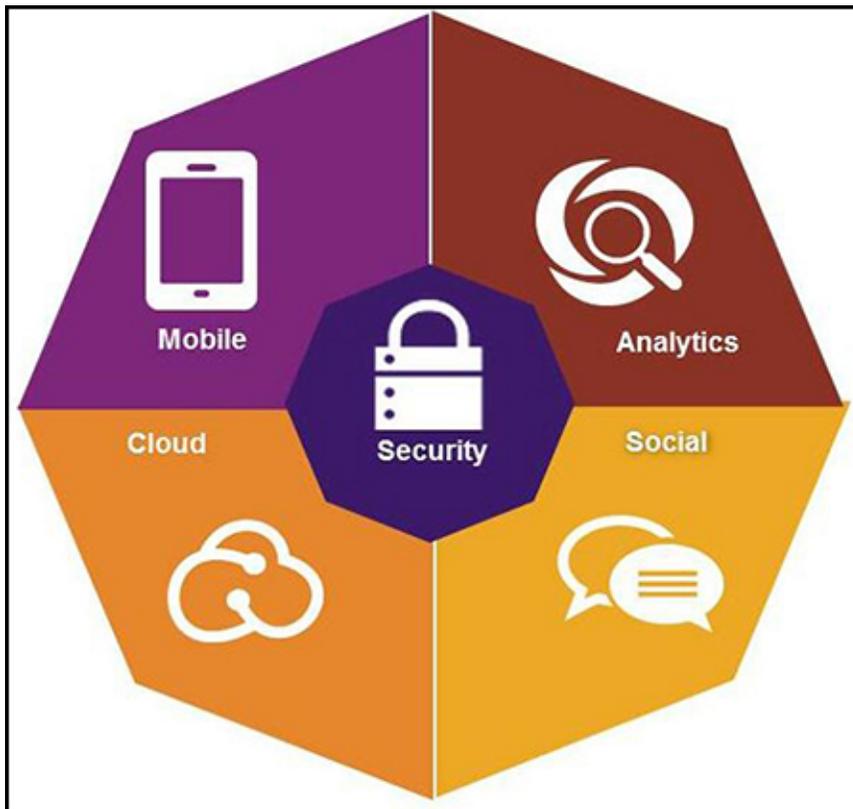


Figure 2. Analytics, mobile, social, and cloud computing require a deeply integrated security stack

This is where z Systems excel. To help counter the many threats to your business in the current world, including hackers looking to penetrate your systems and government-backed attacks, z Systems offers a platform with layers of defense to protect your customer data, intellectual property, and your reputation.

Business-driven enterprise security can be encapsulated by a concept that is known as the IBM Security Framework. The IBM Security Framework provides a business view of the security posture of an enterprise. It is a high-level view, but it incorporates all that is necessary for consideration.

The IBM Security Framework has the following features:

- Enables innovation through security-rich, end-to-end infrastructures and platforms.
- Reduces the number and complexity of required security controls.
- Reduces redundant security expenses.

- Improves organizational and operational agility and resiliency.
- Leverages industry expertise to help unify policy management.
- Delivers needed visibility, control, and automation.

There also is a physical layer of protection that is included with the z13 crypto cards. For example, if someone attempts to pull the cards out of the machine to access the keys, the cards automatically zeroize. They also zeroize if the temperature changes drastically, such as the case where someone attempted to freeze the cards and extract the crypto keys with a \$7 USD can of compressed air! These products have physical protection built-in.

Solution overview

To effectively detect and prevent security breaches, security intelligence and powerful analytics must be implemented. The solution to this is the IBM z13. New Common Cryptographic Architecture (CCA) enhancements that were recently announced include:

- VISA format preserving encryption (VFPE): The z13 offers VFPE for payment card account numbers. The z13 can help provide additional security by enabling legacy databases and applications to contain encrypted data of sensitive fields without having to undertake a restructuring of the database or applications. FPE is a valuable tool for payment card applications that helps maintain the character length between input clear text and resulting cipher text.
- Greater than 16 domain support: Greater than 16 domain support allows a cryptographic coprocessor to be shared across more than 16 domains, up to the maximum number of LPARs on the system. This support relies on enhanced firmware that is available with a minimum microcode level for the Crypto Express5S coprocessor. With the adjunct processor (AP) extended addressing (APXA) facility installed, the z Systems crypto architecture can support greater than 16 domains in an AP. Customers have the flexibility of mapping individual LPARs to unique crypto domains or continuing to share crypto domains across LPARs.

These enhancements use the following IBM z Systems features, which also are redesigned to provide even more security and performance:

- Cryptographic Functions (CPACF) and Crypto Express5S
CPACF is designed to improve performance for cryptographic functions. The optional Cryptographic Coprocessor adapter (Crypto Express5S) provides new virtualization capabilities and performance increases.
- SIMD allows the construction of richer, complex analytics models that use SIMD to provide better accuracy of insight:
 - Allows analytics workloads to be ported from IBM Power and x86 with ease, and can accelerate analytics to provide speedy business insight.
 - Increases programmer productivity of ISV and customer analytics workload development leading to rapid business insight generation for competitive advantage.
- SMT: Process more workloads (throughput for IFLs).

The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures that is intended to optimize the security of credit, debit, and cash card transactions, and protect cardholders against misuse of their personal information. It applies to all entities, including merchants and service providers that store, process, or transmit cardholder data, such as Personal Account Number (PAN) data. The PCI DSS was created jointly in 2004 by four major credit card companies: Visa, MasterCard, Discover, and American Express. The z13 solution can help you secure your data and IT infrastructure end to end and help you to exceed your PCI DSS goals.

Additionally, the following z Systems security software supports PCI-DSS compliance:

- IBM Resource Access Control Facility (IBM RACF®): The premier External Security Manager (ESM) for IBM z/OS® and IBM z/VM® environments.
- Integrated Cryptographic Service Facility (ICSF): The component of z/OS that provides cryptographic services interfaces (APIs).
- IBM Security Identity Manager: The IBM solution for Enterprise Identity Management
- Encryption Facility for z/OS: Encrypts (and optionally compresses) data at rest for media whose contents must be securely transported, that is, physically moved, for example, shipped in a truck, or electronically sent over non-secure links.
- IBM Security zSecure™ Suite: A comprehensive suite of products that enhance the management, auditing, reporting, and compliance of security in RACF, CA-ACF2, and CA-Top Secret environments (Figure 3). This suite includes the following products:
 - Security zSecure Admin
 - Security zSecure Audit
 - Security zSecure Alert
 - Security zSecure Command Verifier
- IBM InfoSphere® Guardium® Database Security: Provides the simplest, most robust solution for real-time database security, ensuring the privacy and integrity of trusted information in your data center.

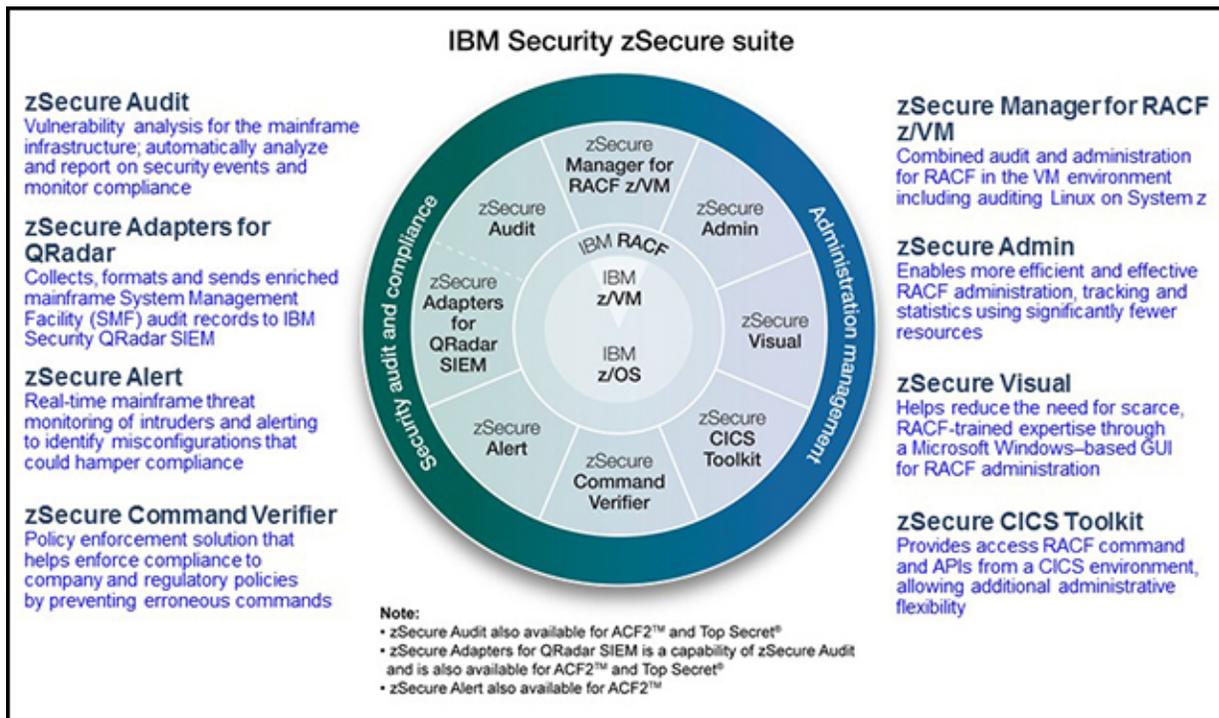


Figure 3. IBM Security zSecure suite

Solution architecture

To enable security intelligence and powerful analytics, a combination of z13 hardware and software products should be employed. Common Cryptographic Architecture (CCA) enhancements that have been announced that use the z13 enhancements and include CPACF and the Crypto Express5S are described in this section.

CPACF

The CP Assist For Cryptographic Functions (CPACF) delivers high-speed on-chip cryptography. CPACF was redesigned to allow handling higher volumes of transactions. CPACF has the following features:

- It is supported by z/OS, z/VM, IBM z/VSE®, z/TPF, and Linux on z Systems.
- It has protected key support for additional security of cryptographic keys (when using Common Cryptographic Architecture (CCA) mode; Crypto Express5S is required).
- It enhances the encryption/decryption performance of clear-key operations for SSL, VPN, and data storing applications.
- It provides a set of symmetric cryptographic functions and hashing functions for the following items:
 - Data privacy and confidentiality
 - Data integrity
 - Random Number generation
 - Message Authentication

Many users of the CPACF benefit from it, such as the following ones:

- IBM InfoSphere Guardium Data Encryption for DB2® and IBM IMS™ databases
- IBM DB2 built-in encryption
- z/OS Communication Server: IPsec/IKE/AT-TLS
- z/OS System SSL
- z/OS Network Authentication Service (Kerberos)
- IBM Encryption Facility for z/OS DFSMSdss encryption feature
- IBM Encryption Facility for z/OS
- z/OS Java SDK
- Linux on z Systems: Kernel, openssl, openCryptoki, and GSKIT

CPACF must be explicitly enabled by using a no-charge enablement feature (#3863). SHA algorithms are enabled with each server

Crypto Express5S

The Crypto Express5S is hardware-protected, secure-key cryptography. It provides the following features:

- High speed advanced cryptography, that is, intelligent encryption of sensitive data that runs off the processor, which saves on costs.
- PIN transactions, EMV transactions for integrated circuit-based credit cards (chip and pin), and general-purpose cryptographic applications that use symmetric key, hashing, and public key algorithms, and simplification of cryptographic key management to meet the needs of current banking, retail, and other applications.
- Designed for FIPS 140-2 Level 4 certification to meet regulations and compliance for PCI standards.
- Concurrent Segment 3 updates to meet the highest levels of availability.

- New features:
 - Hardware-based logic upgrades for Elliptic Curve Cryptography (ECC) for Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic curve Diffie-Hellman (ECDH) key agreement protocols
 - A new prime number generator
 - Firmware support for VFPE

Crypto Express5S PCIe adapter: A coprocessor or an accelerator

The PCIe adapter contains a tamper-resistant hardware security module. It can be configured in one of three ways by using the Hardware Management Console (HMC) panels:

1. IBM Common Cryptographic Architecture (CCA) coprocessor
2. IBM Enterprise PKCS #11 (EP11) coprocessor
3. Accelerator

When the PCIe adapter is configured as a CCA coprocessor, it supports the following features:

- Secure key transactions to protect your most sensitive information.
- It meets the requirements of national security applications with Federal Information Processing Standard (FIPS) 140-2 Security Level 4 certification.
- User-defined extension (UDX) services to implement custom cryptographic functions and algorithms.

When the PCIe adapter is configured as an IBM Enterprise PKCS #11 (EP11) coprocessor, it supports the following features:

- Provides open, industry-standard cryptographic services that follow the PKCS #11 specification v2.20.
- Simplifies porting PKCS#11 applications to z Systems.

When the PCIe adapter is configured as an accelerator, it is optimized for Secure Sockets Layer (SSL) acceleration and clear key RSA operations, which allows savings of processing time by offloading processor-intensive cryptographic algorithms.

Additionally, the z13 extends enhanced key public support for constrained digital environments that use Elliptic Curve Cryptography (ECC) by providing hardware-based ECC support through the CryptoExpress5S to improve performance. Here are some examples of the use of ECC:

- The US government uses ECC to protect internal communications,
- It is the mechanism that is used to prove ownership of bitcoins,
- It provides signatures in Apple's iMessage service,
- It is used to encrypt DNS information with DNSCurve,
- It is the preferred method for authentication for secure web browsing over SSL/TLS. Chrome and Firefox use it to establish secure connections.

IBM provides the Trusted Key Entry Workstation (TKE) as a means for ensuring secure creation and management of key material and for managing the crypto adapters on the host. Recent versions of the TKE have enhanced the management of those crypto adapters, including the ability to capture information from the current adapters, and then push that configuration to new adapters.

Here are some of the features of TKE:

- FIPS Certified Smart Card: A FIPS certified smart card, part number 00JA710, is now included in the smart card reader, and additional smart cards are optional features.
- Crypto coprocessors with more than 16 domains: In support of the z13 code's ability to allow more than 16 domains on the Crypto Express5S, TKE 8.0 allows the management of domains beyond the current limit of 16. This support is available only with the z13.
- Full-function migration wizard for EP11: The full-function migration wizard is designed to collect and apply quickly and accurately data to the Crypto Express features that are configured as EP11 coprocessors. This wizard previously supported CCA, but Crypto Module Groups are no longer supported on TKE 8.0, so the support has been removed.
- New master key management functions: TKE 8.0 allows support of three new master key management functions that are available when managing any type of master key:
 - The Generate a set of master key parts wizard-like feature allows you to create a key part for each of the different types of master keys.
 - The Load all new master keys wizard-like feature allows you to load a new key for each of the different types of master keys.
 - For the Smart Card Readers Available indicator, TKE 8.0 displays a window title with availability information about the smart card readers.
- Configure Displayed Hash Size: TKE 8.0 supports a configuration to allow the administrator to set the display length of certain hash values that are displayed on the TKE workstation. Hash types that can be affected by this function are MDC-4, SHA-1, AES-VP, and ENC-ZERO. The Configure Display Hash Size utility is available only when you have signed on with the Privileged Mode Access user ID of ADMIN.
- ECC Authority Signature Keys: TKE 8.0 allows a user to select a key strength of 320-bit ECC key when creating an Authority Signature Key that is assigned to an Authority Index on a Crypto Express5S coprocessor. This option is available only when you are creating an Authority Signature key from inside a Crypto Module notebook of a Crypto Express5S.
- Print Capability: TKE 8.0 has limited print support. The Configure Printers utility allows the administrator to add printers to the TKE. The only printers that are allowed to be added are printers that have device drivers on the TKE, including the GUTENPRINT and HPLIP device driver packages. You cannot load your own device drivers.
- New features in the Crypto Node Management (CNM) Utility: The TKE Workstation Setup utility allows you to load and save user roles and profiles. The CNM utility now has stand-alone launch points for these two tasks in the Access Control drop-down menu.
- ENC-Zero Verification Pattern for 24-byte DES Operational Keys: TKE 8.0 supports an ENC-Zero verification pattern that is computed and displayed with 24-byte DES operational keys.
- Usability enhancements: TKE 8.0 has many usability enhancements, including the ability for users to select a check box that allows them to change their passphrase on the logon screen for a passphrase profile. Additionally, users can now select multiple items in the Hosts container, Crypto Module Groups container, or Domain Groups container of the main window of the TKE application. If more than one item is selected, you can delete all of the definitions or close all of the hosts or groups at once.

Usage scenarios

Security intelligence solutions that use big data analytics can help organizations deal with a complex threat landscape. Industry experts recommend innovative thinking and a new approach to security.

IBM continues to leverage and enhance the leading security capabilities that are provided by the z/OS and z/VM operating systems to build the tightest IT Security Hub, and further enhance enterprise security in the authentication, authorization, encryption, and auditing areas through the new z13 technology.

The z13 and its latest enhancements to security, which are built into its hardware, and real-time big data analytics provide context to help detect threats faster, identify vulnerabilities, prioritize risk, and automate compliance activities.

For security threat management, the key challenge is to reduce millions of logs to actionable intelligence that identify key threats. Traditional first-generation security information and event management (SIEM) products achieved this goal by leveraging correlation, for example, five failed logins followed by a successful login, to identify suspected security incidents. Event correlation is an important tool, but it is not enough.

There are two problems:

- Consider a 100,000:1 reduction ratio of events to correlated incidents. On the surface, this sounds impressive, but for companies generating 2 billion events per day (and you do not need to be a massive company to do that), that means that the company's security team has 20,000 incidents per day to investigate. Traditional SIEM correlation cannot reduce the data enough, and log managers cannot get even a 10,000:1 reduction ratio.
- Exclusive reliance on event correlation assumes that the criminals that are intent on attacking your company do not figure out ways to disable or bypass logging infrastructure, but that is practically their entire focus, and you cannot correlate logs that are not there! This limitation results in missed threats or a poor understanding of the impact of a breach.

IBM Security QRadar® vastly expands the capabilities of traditional SIEMs by incorporating new analytics techniques and broader intelligence. Unlike any other SIEM in the market today, QRadar captures all activity in the network for assets, users, and attackers before, during, and after an exploit and analyzes all suspected incidents in this context. New analytical techniques such as behavioral analysis are applied. QRadar notifies analysts about "offenses", which are correlated sets of incidents with all of the essential, associated network, asset, vulnerability, and identity context. By adding business and historical context to suspected incidents and applying new analytic techniques, massive data reduction is realized, and threats that otherwise are missed are detected.

The z13 combined with IBM software products' real-time correlation and anomaly detection across a distributed and scalable repository of security information enables more accurate security monitoring and better visibility for any organization, small or large. As an example of the software products that can be monitored, see Figure 4.

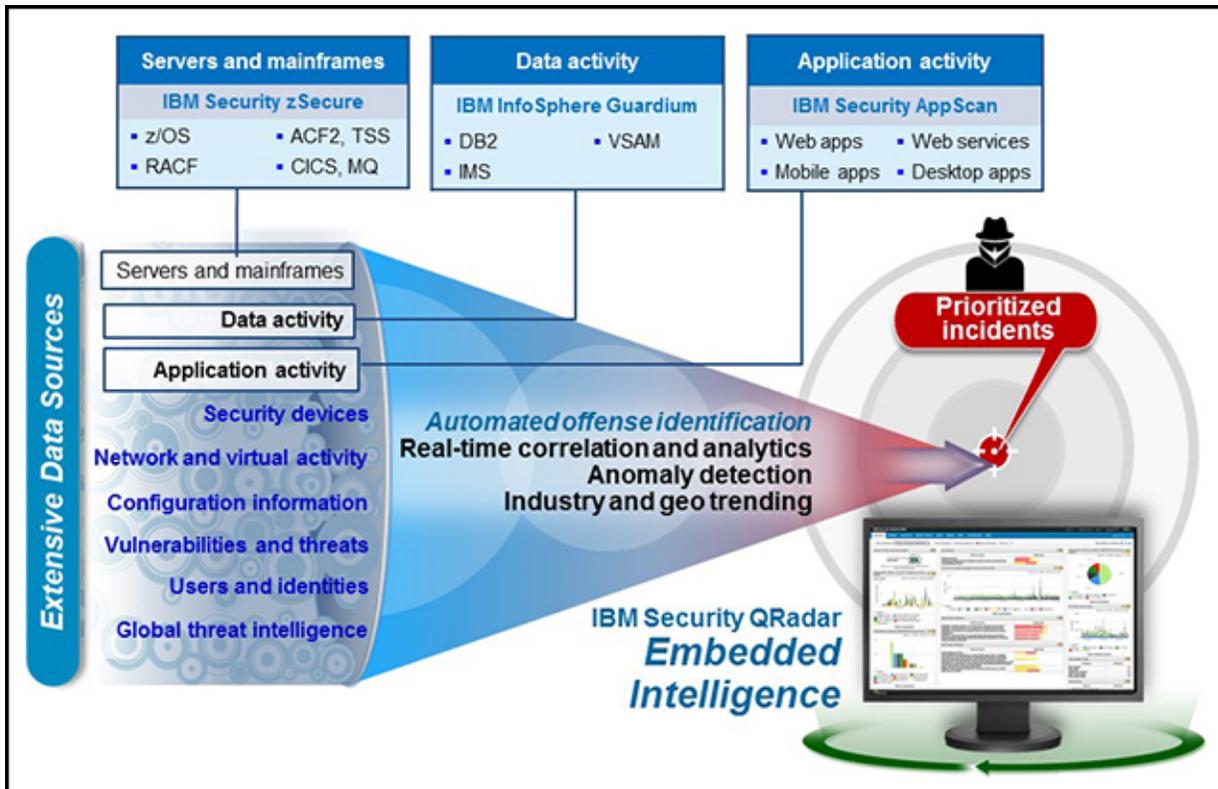


Figure 4. Real-time correlation and anomaly detection

Integration

The IBM z13 integrates with IBM technologies and transactional and information services and software products, such as the following ones:

- HTTP
- JSON
- IBM WebSphere® MQ
- MQTT
- SOA
- DB2 for z/OS
- IMS
- IBM CICS® through HTTP, JSON, and WebSphere MQ
- SAP
- IBM MobileFirst

Ordering information

For IBM z13 ordering information or for more information about security solutions, contact your IBM representative.

Related information

For more information, see the following documents:

- *IBM z13 Technical Introduction*, SG24-8250
<http://www.redbooks.ibm.com/abstracts/sg248250.html>
- The IBM z13 product page
<http://www.ibm.com/systems/z/hardware/z13.html>
- IBM Offering Information page (announcement letters and sales manuals):
<http://www.ibm.com/systems/z/announcement.html>

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you. This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk. IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

© Copyright International Business Machines Corporation 2015. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

This document was created or updated on February 12, 2015.

Send us your comments in one of the following ways:

- Use the online **Contact us** review form found at:
ibm.com/redbooks
- Send your comments in an e-mail to:
redbooks@us.ibm.com
- Mail your comments to:
IBM Corporation, International Technical Support Organization
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400 U.S.A.

This document is available online at <http://www.ibm.com/redbooks/abstracts/tips1257.html> .

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at <http://www.ibm.com/legal/copytrade.shtml>.

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

CICS®
DB2®
Guardium®
IBM®
IMS™
InfoSphere®
QRadar®
RACF®
Redbooks®
WebSphere®
z13™
z/OS®
z/VM®
z/VSE®
zSecure™
z Systems™

The following terms are trademarks of other companies:

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other company, product, or service names may be trademarks or service marks of others.