Securing the IBM Mainframe

IBM Redbooks Solution Guide

Cybercrime is a sophisticated activity. It is no longer a playing field for “script-kiddies” trying to get access to systems and servers for fun, and it is not about quick hacks to get in and get out quickly. It is now about real commercial, political, or even military advantages. There have been reports in the press recently of large systems data breaches, and it is apparent that some of these are associated with attempts to access mainframe data.

The skills and knowledge that are required to manage and operate a sophisticated IBM System z mainframe are different from those that are used by professionals who use Linux, UNIX, or Windows servers for commercial organizations. The complexity of ways in which various organizations use System z over many years, means that there are now fewer people with the knowledge and skills to even attempt breaking into a mainframe system. However, as criminal organizations realize the benefits of gaining access to mainframe data, the efforts to achieve this increase. The requirement to secure mainframes and their valuable data exists within every organization, within a network of firewalls and network protection systems, access control hubs, DMZs, and application gateways, all of which can make up layers of defense. See Figure 1.

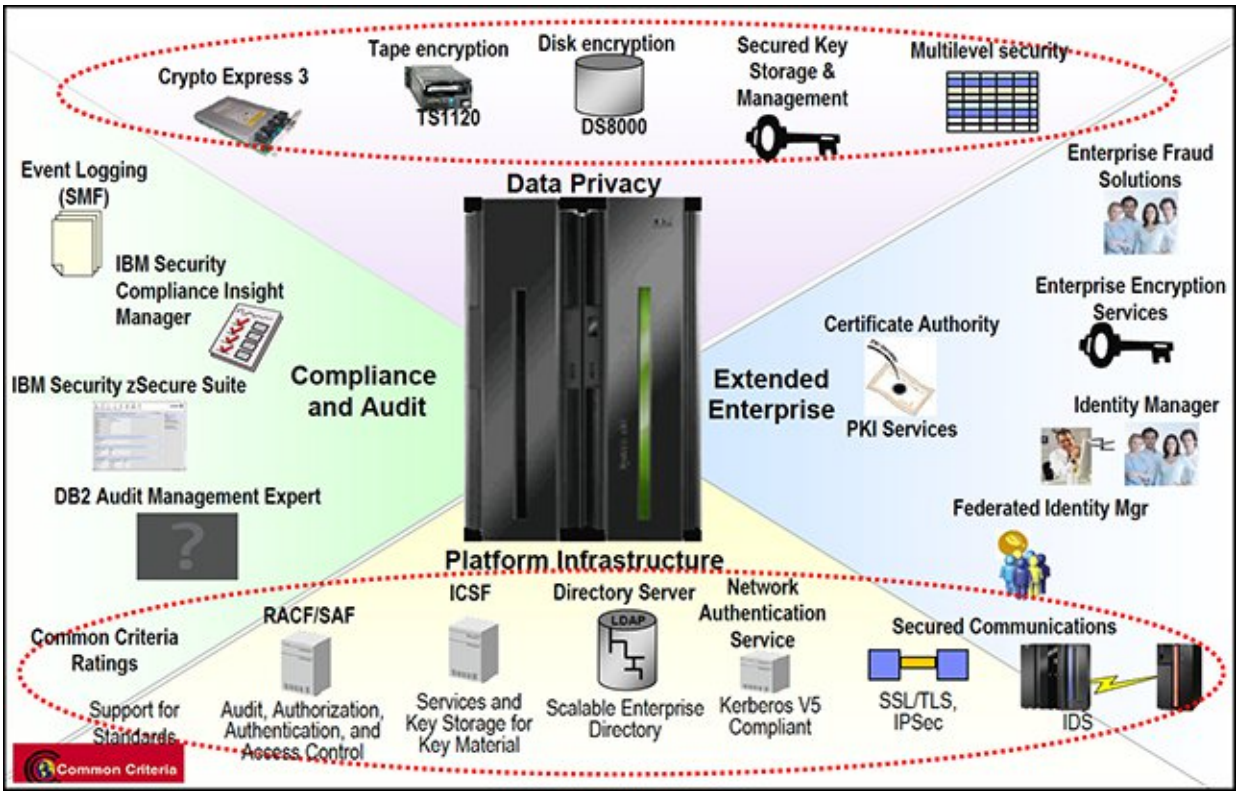

Figure 1. Elements of Enterprise Security

In consequence, it is of real value for us to consider the security capabilities of the mainframe. This time, however, we want to ensure that you know how to configure these machines so that they are highly resistant to attacks. If *resistance* is not possible or practical, you must understand where *detective controls* can be used. If detective controls are not possible, then you must understand what *forensic capabilities* are possible. This IBM Redbooks Solution Guide provides the security professional and the enterprise security architect with an understanding of best practices to secure the IBM mainframe in a holistic approach.

Did you know?

Very often you hear that IBM z/OS running on System z is the most secure commercial operating system available. We (the authors) beg to disagree. If configured properly, it is as secure as claimed. Many audits that are performed in System z environments are executed with a *light touch*. Some management teams are happy with this approach because they have a natural desire to pass audits. A passed audit typically signals that everything is working well and as designed. However, this approach can instill a false sense of security. While System z is inherently resistant to hacking and information theft because of the controls built into its hardware microcode to support process isolation and data integrity, it can also be configured and run in a *highly insecure manner*. So, we might more accurately claim that z/OS is *the most securable* commercial operating system available.

The 1973 MVS statement of integrity has formed the basis for more than three decades of the MVS successors' industry leadership in system security. The fact that IBM was able to make such emphatic claims so early in the life of the MVS family of operating systems, and has been able to maintain that claim for all the years since, speaks volumes for the stability and reliability of the hardware and software. The z/OS "System Integrity" is defined as the inability of any program that is not authorized by a mechanism under the installation's control to circumvent or disable store or fetch protection, access a resource that is protected by the z/OS Security Server (RACF), or obtain control in an authorized state. The current z/OS statement of integrity can be found at the following website:

http://www.ibm.com/systems/z/os/zos/features/racf/zos_integrity_statement.html

With the statement of integrity, IBM also commits to address and resolve any system integrity problem that is reported.

Business value

Hacking is only part of the process to gain access to enterprise data with malicious intent. If access to one part of an enterprise IT environment is gained, then this access can be used to extend access to another part. The initial breach of the security controls is used to create or obtain another breach. Usually, data is leaked carefully over a long period of time. Breaches are used and controlled by attackers so that detection is difficult. This level of activity is no longer associated only with distributed servers, which frequently run Linux, UNIX, or Windows based software. The goal in many of these attacks is to access the data that is held on the mainframe, also called the System of Record. Why would the mainframe be under attack? Well, many years ago, the infamous American bank robber John Dillinger was asked why he robbed banks. He replied, "Because that is where the money is." So, the answer to why the mainframe is now under attack is that this is the server where many organizations store and process their most valuable data.

The System z mainframe might be running z/VM to host Linux servers. There might be one or more z/OS LPARs in one sysplex, even with z/OS under z/VM for testing or software maintenance purposes. There are many aspects to the security of such an environment. To protect such an environment, you must consider the following subjects:

- Identity management
- Access management to data and other resources
- Log management and auditing
- Security intelligence and analytics
- Application security management (and its development)
- Process and procedure management
- Physical security management of the various servers and network components

These matters of business-driven enterprise security are encapsulated in a concept that is known as the IBM Security Framework (Figure 2). 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.

Figure 2. IBM Security Framework

The IBM Security Framework shows the four vertical security domains of People, Data, Applications, and Infrastructure, and the three horizontal security domains of Security Intelligence and Analytics, Advanced Fraud Protection, and Advanced Security and Threat Research. Those three horizontal domains apply to all four of the vertical domains. The underlying concepts of Governance, Risk, and Compliance drive and control all of the security domain activities within an organization. This framework tells you much about what security must be applied, and what types of questions you must ask about security matters.

Solution overview

Most organizations have a security policy in place that states the rules for controlling access to data. There also are statements for data ownership, and there are rules about granting the least access that is necessary for each role. However, there might be few instructions about the practical scenario of implementation. There might be little mention of any of the IT platforms that are involved. Thus, there might be little or no link between that policy and the security procedures that must exist. Organizations find a great benefit in having documentation that relates the policy to the platform, and to each software product that needs a security related configuration. It has to be possible to draw a line from policy to procedures, and to see that the policy is enforced in the implementation environment.

Over the years, IBM has introduced new security capabilities and controls. However, many organizations have decided to not implement many of these controls based on the assessment of the security threat level at a certain point in the past. Many regard the controls as too restrictive. Because a lot of the threat landscape has changed after some of those restrictive controls were introduced by IBM, it is a preferred practice to revisit these controls and see whether there is a justifiable reason to enable those controls. A secure infrastructure or secure applications do not just *happen*. Each one must be designed, and then implemented to that design. And, in any quality process, there is a need for continuous improvement. This applies to security management, which must be considered like any other process, as well.

Security controls differ in type. Some controls are designed to grant or prevent actions by individuals on objects, and other controls might monitor actions that occur and then record them. Some controls might produce an alert. Preventive controls prevent unauthorized access, where an enterprise security manager (ESM), such as RACF, denies access to a resource for a specific user. Monitoring controls keep a record of access that has been granted. ESMs, such as RACF, provide settings that can determine what levels of access need to be monitored. Whenever an unauthorized change is made by a user or a process, an alert can be raised by a detective control. Forensic controls refer to capabilities for analyzing security data *after* an event to determine the root cause. A mixture of all of these types of control is always advisable.

There are many security control standards for the various System z platform components. Some organizations maintain their own standards, and others use external standards. Having a standard to measure your own security controls is a good idea. It helps you to implement a measurement process to demonstrate that security is improving, or possibly getting worse. Without such a standard to measure against, it is not easy to determine whether improvements are happening.

The System z hardware and the z/OS operating system have excellent features to keep the IT environment secure. These controls depend on the system design and the required security policies as applicable to the business environment. A banking environment may have different requirements compared with a retail chain, or a healthcare system. In this Solution Guide we describe the common best practices that can be applied to the majority of the environment, but should be validated for their applicability to the design and accommodated in an appropriate way to keep the overall IT environment secure.

Lately, there are many solutions available that can contribute to the implementation of the IBM Security Framework and use the strengths of IBM System z. These products relate to components such as data security, security intelligence and analytics, policy and processes, audit and compliance, application security, access and privilege management, fraud detection and prevention, identity management, and network protection. These products either complement the mainframe built-in security services or they provide additional enterprise-wide security functions. Here is a list of these IBM security solutions:

- IBM InfoSphere Guardium for z/OS
- IBM Security QRadar
- IBM Security zSecure Suite
- IBM Security Key Lifecycle Manager
- IBM Enterprise Key Management Foundation

- IBM Encryption Facility for z/OS
- IBM Security AppScan
- IBM Security Access Manager
- IBM Security Trusteer
- IBM Security Identity Manager
- IBM Security Federated Identity Manager
- IBM Security Network Protection

Solution architecture

IBM chose to use a high-level service-oriented perspective for the Security Blueprint (Figure 3) based on the IBM service-oriented architecture (SOA) approach. Services use and refine other services (for example, policy and access control components affect almost every other infrastructure component).

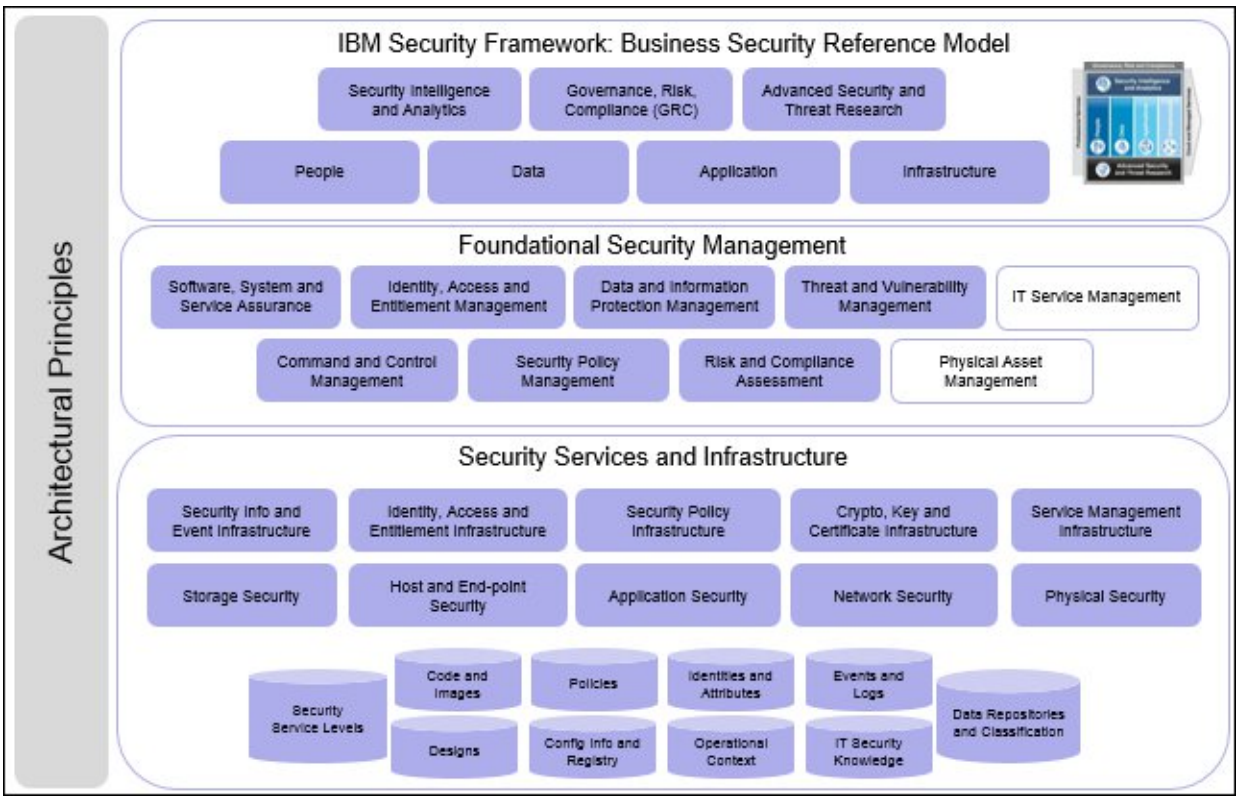

Figure 3. IBM Security Blueprint

The IBM Security Framework and the IBM Security Blueprint are tools to enable the security architect to understand the components and facilities that are needed to architect a secure solution. These tools are useful for all platforms and can be applied to systems hosted on System z and to applications that span multiple heterogeneous hardware and software platforms.

The security features on a mainframe are deeply integrated into the hardware, within every chip and the processor. These features also expand to the hypervisor, which uses the secure system design in the middleware layer. These features expand to the software layer to create a complete secure entity across multiple points of interception. This is where the process gains importance. The mainframe platform provides a model to secure an organization's data and environment, and it enables them to build simplified processes around its integrated security features.

System z is made up of hardware products, including a central processor (CP), software products, and an underlying OS, such as z/OS. Other types of software, such as the system application programs and the user applications, also run on the system. The CP is the functional hardware unit that interprets and processes program instructions. The CP and other system hardware, such as channels and storage, make up a server complex. The System z architecture and functional design provides a highly secure computing environment by preserving the integrity of its operations with a clear isolation of events.

z/OS provides concepts and functions such as dispatching, address spaces, SVCs, and address translation, to ensure that each instruction is run on the processor with great isolation and integrity in an efficient manner. Also, z/OS isolates the decision-making entities of security clearly from the resource managers that makes those security requests. This is achieved through functions such as SAF and External Security Managers (ESMs). z/OS also maintains an excellent record of all system events through its event recording mechanisms with functions, such as SMF. See Figure 4.

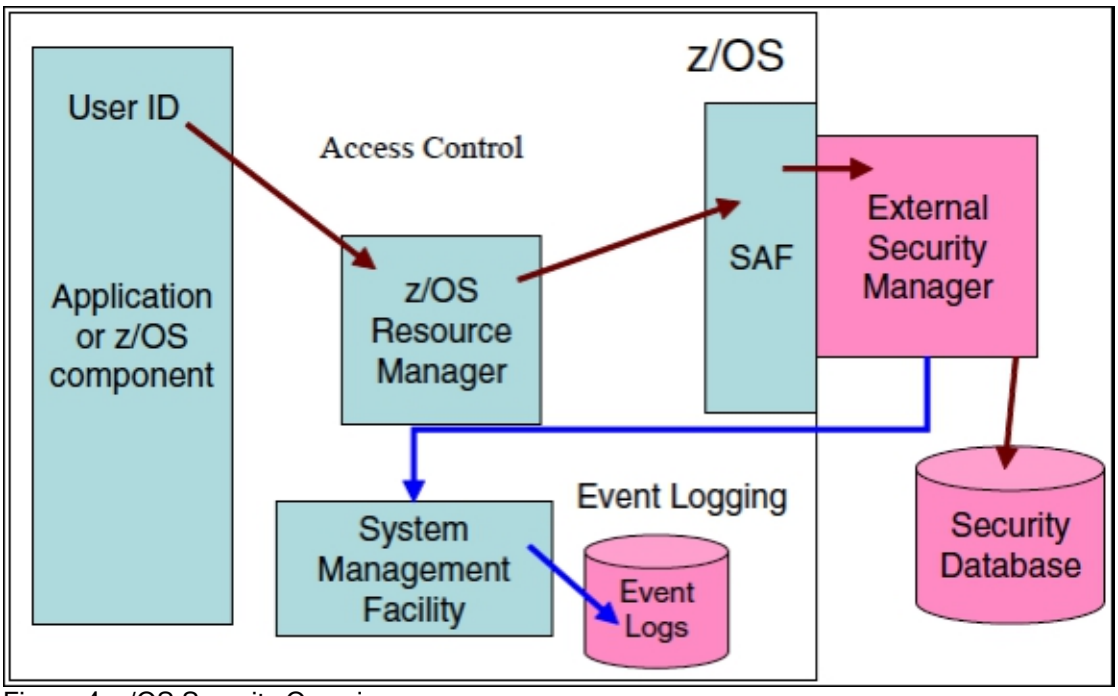

Figure 4. z/OS Security Overview

Similarly, the z/OS Security Server is the IBM security product which acts as the External Security Manager (ESM) for z/OS. The RACF product is a component of the z/OS Security Server, and it works together with the existing system features of z/OS to provide improved data security for an installation. RACF helps meet the need for security by providing the following functions:

- Flexible control of access to protected resources
- Protection of installation-defined resources
- Ability to store information for other products
- Choice of centralized or decentralized control of profiles
- Easy interfaces and transparency to users
- Customizable options to adopt to security policies

Usage scenarios

Securing the System z environment is not a straight-forward solution. While there are few common guidelines that may be applicable for the majority of the environments, there are also similar recommendations for the hardware configuration, operating system functions, security manager, encryption setup, and storage system features. Let us investigate each one of those and provide with a list of guidelines.

Common guidelines:

In this first section we look at the common guidelines.

- Revisit security controls regularly. If a control is available and a platform policy decision has been taken not to implement it, then this should be documented with the current justification, and revisited at regular intervals. These revisitations should examine the threats, and should be attended by technical staff who understand the nature of the control and the implications of enabling or disabling it.

- Institute a continuous improvement process for security management and security procedures. Make change an accepted part of the environment.

- If your organization has a System z audit that comes back with no exceptions and you know this is not correct, act to ensure that it is fixed.

- Make sure that you have the capability to detect changes to your operating systems, and security settings that are critical for your business. Enable logging with proper retention. Use security intelligence products and capabilities so that you are alerted when any potential breach occurs.

- Have a process for access recertification and continued business need verification. Institute a program for access reduction.

- Choose a standard for your System z security environment. After you choose a standard, the system should be carefully measured against the standard and a gap analysis should be performed. However, your goal should never be to simply meet the standard. Your goal is to meet your own security requirements with the restrictions that are set by your own business needs. Assume for the present that the agreed business needs require a higher standard of security than what is defined by the standard you measure against. You can now explore the “standards-plus” concept, which is based on the standard that you choose, but your set of controls are augmented by extra security controls to reduce the risk to the level that your business can stand.

- A dedicated security engineering department with cross-organization responsibility and authority is a good way to address such issues related to security in a large enterprise where business is complex and applications span across various platforms and domains. See Figure 5.

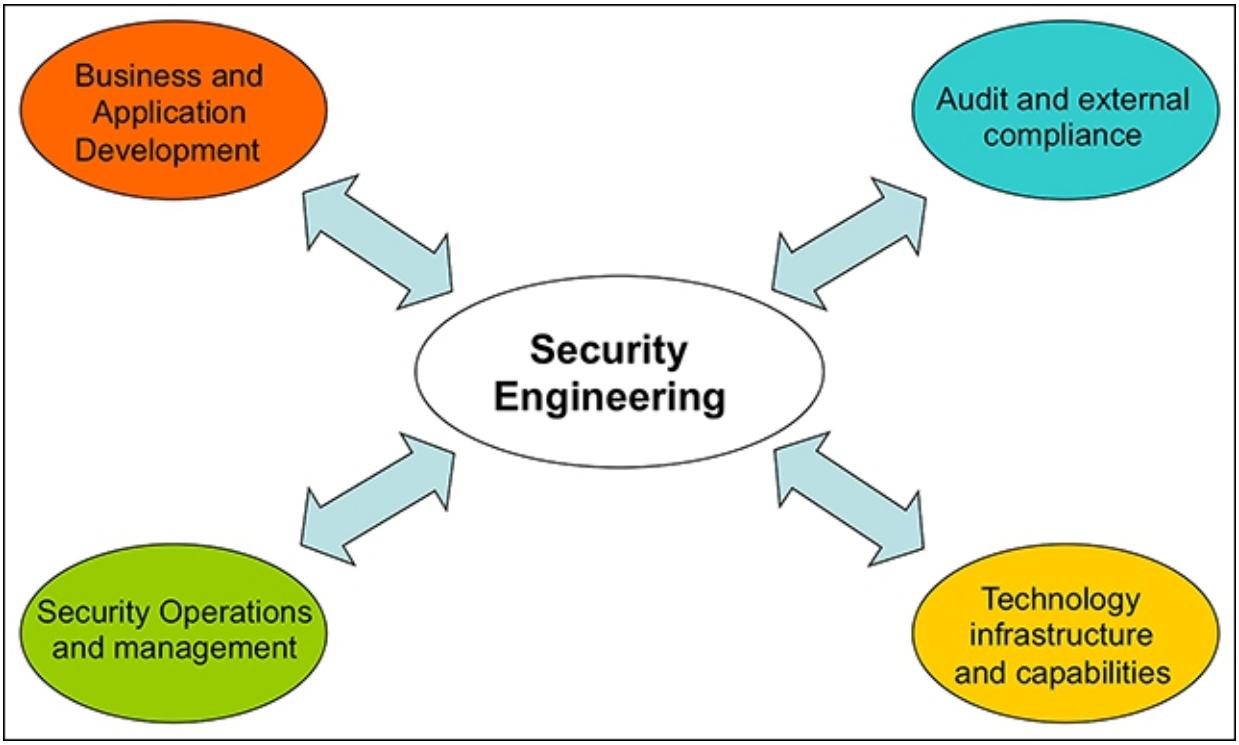

Figure 5. Security Engineering

- Ensure that security administrators are not given responsibilities for auditing and security management. There is a strong reason for separation of duties in security policies.
- Each security control needs some testing process before implementation. The tests that are used and the results of those tests should be retained so that they can be repeated in situations where a relevant change has taken place.
- Regular scanning for exposures or risks should take place.

Your aim here is for your system to be secure. Being compliant is good, but being secure is better.

System z hardware:

In this second section we look at the guidelines for the System z hardware.

- When you secure System z hardware, physical access protection is the first thing to be considered. It applies to all the hardware components of System z that are installed in a data center. Physical access is not limited to securing just the hardware, but also includes all remote devices or terminals that connect to System z and things such as the removable media that carries backup of mainframe data. Every connection to the mainframe must be secured becau7se any single vulnerability can lead to disruption of services on a large scale.
- As HMCs can perform disruptive tasks that might impact the availability of data, access to these HMCs is strictly restricted only to authorized engineers with a clear technical and business justification.

- Secure the access to IODF and IOCDS through all means of channels – from the SE/HMC and from z/OS.
- A defined housekeeping process for both physical and logical printers helps eliminating potential data theft. As JES also manages printers, it is necessary to implement effective controls over JES commands that operate printers.
- Proper care should be taken to ensure that the access to the enterprise storage systems or devices through SNMP is restricted only to those authorized devices that are used for monitoring them.
- The access controls of the logical data that is stored within the disks is managed by the ESM installed on z/OS. The encryption capabilities secure the data in physical form in the controller.
- Protect tape data both at the volume level and at the data set level. Use either ESM or a tape management product to secure data on tape.
- Ensure that the premises of the System z and the switch or router is restricted physically to authorized people and the cable is secure enough that it cannot be inadvertently removed from its designated port at both ends.
- Regularly audit HMC/SE logs, FFDC, EREP and SMF for any issues that can make the environment potentially insecure.
- If consoles are in open offices, then they should require a logon to use and should never be left unattended while logged on. Anyone outside of the day-to-day operators should be forced to use a logon when using a console.

z/OS:

In this next section we look at the guidelines for z/OS.

- Record types that are associated with creating, reading, modifying, renaming, and deleting of data sets should not be suppressed. All SMF records that are written by RACF should not be suppressed.
- Pay careful attention to the access levels that are required for access to each MVS command. These levels vary by command.
- As SMFDUMP may be used with all sorts of other data sets than SMF data, it can be used to overwrite almost any data set on the system if it is given the NOPASS property. Remove the NOPASS property from this copy of SMFDUMP.
- Security administrators need to work with systems programmers to ensure that the contents of APF/Linklist/LPA lists of program libraries are maintained correctly. Update access to these libraries to be defined for each library, independent of the RACF controls.
- Ensure that you know the provenance of all APF-authorized and system code that you install. If possible, get statements of assurance from the suppliers.
- Manage your APF lists with great care. Double-check entries. Do not leave dead entries in the list for simplicity or ease of use. Use a formal checker for the lists if possible.
- If your z/OS system contains SVCs that are 200 - 255 or user SVCs below 200, you should ensure that you understand the provenance of each of them. If you have SVCs that are modified or overlaid using software from non-IBM suppliers, you should understand what each one is doing.

- Badly coded exit points can cause integrity and security exposures.
- Do not grant READ access to any configuration libraries except to those users with a defined business need.
- Restrict the use of all-users access at UPDATE to profiles for CATALOG protection that really need it. Ensure data set naming standards isolate CATALOG names from other data sets.
- Never have an all-users access level for the master catalog that is UPDATE or higher. If it is feasible to run without any all-users access, then do so.
- Strictly follow the documented values for UACC values for system datasets.
- Page data sets should be protected from being viewed. They should have audit settings that show who accessed them, whether for READ access or anything else.
- System dump data sets should be protected from being viewed from almost all users. Those staff requiring access for system dump analysis should be the only users accessing these data sets. The data sets should have audit settings that show who accessed them, whether for READ access or anything else.
- System dump data sets are often archived. If this is done, then those archives also should be protected in a manner similar to the original system dump data sets.
- The LOGREC data set should be protected from being viewed from almost all users. Only those administrators that are associated with problem analysis should have READ access. It should have audit settings that show who accessed it, whether for READ access or anything else.
- Only those people that are concerned with auditing and those that are concerned with the management of SMF records should have access to them. Restrict all other access, both to the live SMF data sets and also to all archives of SMF material.
- Restrict READ access to the system linklist and LPA libraries to those who have a defined business need to read them.
- Keep started task procedures in a separate set from other cataloged procedures. Ensure that the order of libraries does not provide opportunities for Trojan horse JCL procedures.
- Always define the BPX.DAEMON and BPX.SERVER profiles in the FACILITY class. Restrict access to these profiles to those users with an absolute need. This is not expected to include human users, just user IDs for processes and daemons.
- Activate the UNIXPRIV class and define discrete resources for all of the privileges. Do not define a generic profile of the form BPX.**.
- Restrict access to the profiles BPX.FILEATTR.APF and BPX.FILEATTR.PROGCTL.
- Examine the STGADMIN profiles that are available at each new release of z/OS and carefully use them. Phase out all use of the OPERATIONS attribute and DASDVOL profiles.
- Restrict access to SYSLOG to those users who are performing tasks requiring it. Do not grant read access to SYSLOG to all users.
- Create a fallback generic profile for JES2 or JES3 commands names so that new commands are covered by that profile.

- Use surrogate job submission with great care. There is no control that is supplied over the nature of the JCL that is run under the execution-userid. So, anyone having that surrogate authority can do anything that the execution-userid can do.
- Keep the logon procedures for TSO users in a library separate from other procedures. This library should be carefully controlled and monitored for changes.
- Keep started task procedures in a separate set from other cataloged procedures. Ensure that the order of libraries does not provide opportunities for Trojan horse JCL procedures.

z/OS Security Server (RACF):

In this next section we look at the guidelines for the z/OS Security Server (RACF).

- Restrict all access to the RACF database to those who have an absolute need to know. Ensure that it has UACC=NONE and does not have an all-users entry in the access list. Apply these rules to all backup copies of the RACF database.
- Do not allow systems with separate RACF databases to share a DASD. Do not define paths that allow a DASD to be varied online from a system that has a different security database.
- Ensure that privileged users have the appropriate LOGON procedures for their role. These procedures should be designed so that it is not possible for Trojan horses to be introduced.
- Do not share UID values across multiple RACF user IDs.
- Ensure all access to the data sets comprising the RACF database is audited. Apply these rules to all backup copies of the RACF database.
- Ensure that INITSTATS is on.
- Ensure that SAUDIT is on.
- Ensure that users with the SPECIAL attribute do not own resources or profiles.
- Ensure that CMDVIOL is on.
- Ensure that OPERAUDIT is on.
- Ensure that all active classes are audited.
- Examine your GLOBAL settings carefully to ensure that they do not compromise security requirements. Ensure that you have good grounds for the use of GLOBAL, and that changes to the GAT are monitored and justified. Review GLOBAL profiles at regular intervals for continued applicability.
- Set EGN on if possible. Beware any routines that examine the output of RACF commands.
- Ensure that BATCHALLRACF is set on.
- Ensure PROTECTALL(FAILURES) is set.
- Storage administration should work with security administration to ensure that data placement does not alter the intended security of a data set.

- Protect tape data by using the same set of data classification as disk data. Ensure that BLP is secured. Use tape encryption if tapes are moved away from their working environment.
- Make strategic use of the erase on scratch capability for operating system sensitive data sets, and other data sets that are known to contain sensitive, unencrypted information.
- Ensure that a value is set on the INACTIVE interval.
- Enable dual-case passwords and encourage their use by using the RACF command SETROPTS PASSWORD(MIXEDCASE). Use password phrases wherever possible by using the PHRASE parameter with each ADDUSER command that is used to create a user ID.
- Set GENERICOWNER on.
- Avoid any use of UACC that is other than NONE. Use the all-users entry in access lists in preference to UACC. If there is a need for everyone to access a resource at a given level, then use a UACC of NONE and grant the all-users entry the access that is needed, which is READ in nearly all cases.
- Avoid any use of all-users access above NONE for data set profiles. Use all-users access of READ only for data sets that are needed by all users. For example, consider whether your CICS users need access to ISPF libraries.

z/VM:

In this next section we look at the guidelines for z/VM.

- Create new privilege classes that meet local security policy and the roles that are defined for guest workload.
- Remove SET PRIVCLASS command from Class C or disable the feature in z/VM.
- Use LOGONBY to ensure accountability of privileged operations in a shared environment. A VM with LOGONBY should have its password set to 'LBYONLY'. This function is extended in RACF/VM through the SURROGAT class of operations.
- Use COMMAND statement, instead of PROFILE EXEC to run privileged commands at the start of VM.
- Use MODIFY COMMAND or MODIFY DIAGNOSE commands remap CP commands and diagnose instructions from their default privilege classes to alternate ones. This allows the security administrator to remove potentially dangerous commands from use before a workload is deployed.
- Use OBSERVER authority to enable monitoring of VM in a secure manner for console operators.
- Use z/VM's ATTACH and SET RDEVICE commands to enable hardware encryption on the tape drive before the tape drive is dedicated to the server that is running the CMS application or licensed program.

Linux on z:

In this next section we look at the guidelines for Linux on System z.

- Secure the logical access to z/VM through the use of z/VM user passwords, privilege classes, and the network security features.
- Use RACF to control who can link to z/VM minidisks by using profiles in the VMMDISK resource class.
- Use the dm-crypt disk encrypt subsystem for flexibility and resilience.
- To strengthen an organization's security policies, implement the MAC method.
- To avoid having passwords traveling over communication lines, the use of either RSA or DSA key pairs might be considered as an alternative.
- Access to Linux guests can be facilitated with the use of SSH and the public key infrastructure (PKI).
- Define scope of job roles through security policies.
- Consolidate and manage all Linux user ids from a centralized repository

Integration

System z sets up an excellent platform to establish a secured application hosting environment. Although System z is an enterprise platform, an organization still hosts various other platforms in its technology architecture and hence demands an overall solution to secure its environment. Some of the security solutions that are described here caters specifically to System z or the z/OS. But, the intention is to provide an overview of all such solutions that present an enterprise view of managing security across all operating platforms. Thus, these products and solutions ensure to strengthen the security capabilities of System z as aligned with the IBM Security Framework.

IBM InfoSphere Guardium

The IBM InfoSphere Guardium solution offers a simple, powerful mean of securing critical data throughout the enterprise. It provides rapid, policy-based detection of anomalous activities that violate corporate policies, real-time responses, such as alerts, auditable workflow to ensure appropriate resolution of exceptions, and automated reporting capabilities, which simplify validation of compliance for mandates, such as SOX, PCI DSS, and data privacy regulations. See Figure 6.

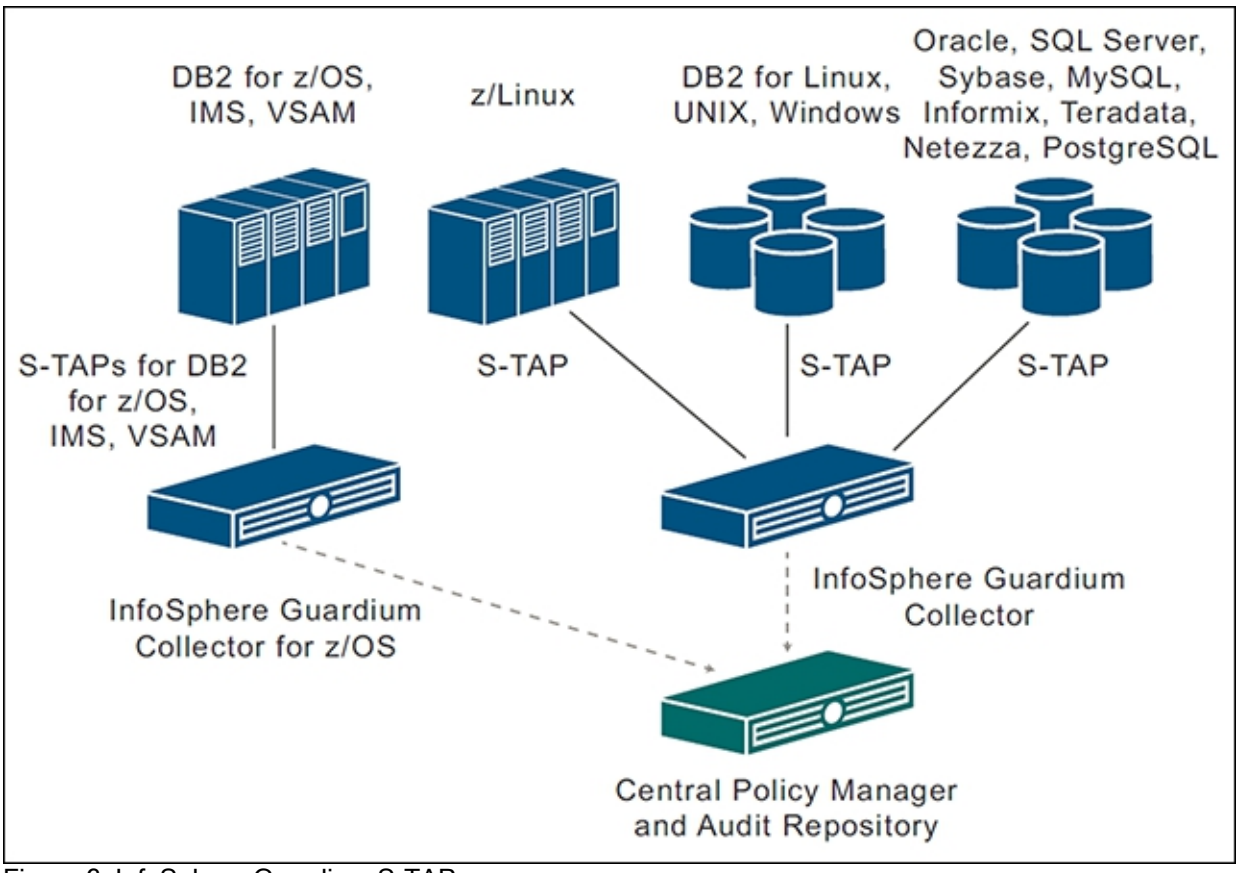

Figure 6. InfoSphere Guardium S-TAP

The InfoSphere Guardium for z/OS solution provides these capabilities for DB2, IMS, and VSAM on z/OS. The solution can be used independently for the mainframe environment only, or integrated with other InfoSphere Guardium database security and monitoring components throughout the enterprise to provide a secure, centralized audit repository and management point.

IBM Security zSecure Suite

The IBM Security zSecure Suite is a family of products that helps you enhance your mainframe administration, and provide a solution for audit and compliance reporting and management within your z/OS infrastructure. See Figure 7.

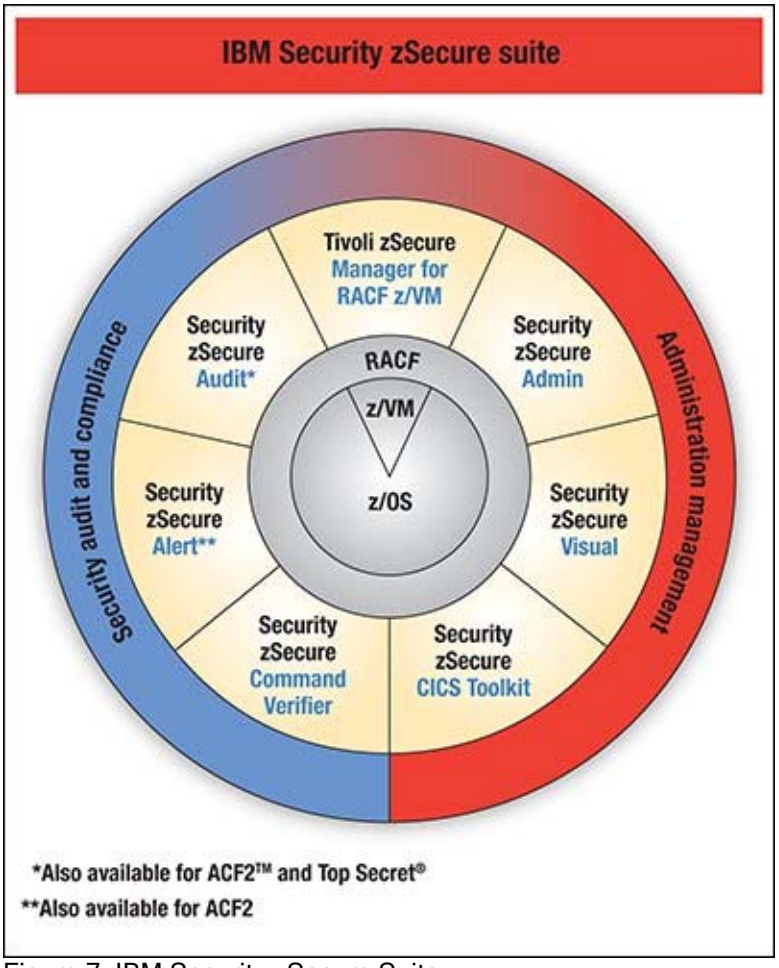

Figure 7. IBM Security zSecure Suite

The components of Security zSecure Suite are divided into two categories. The first category is administration management, to which Security zSecure Admin, Visual, Security zSecure for RACF on z/VM and the Security zSecure CICS Toolkit belong. The second category is defined as security audit and compliance. This category consists of Security zSecure Audit, Alert, and zSecure Command Verifier. Security zSecure Manager for RACF z/VM also includes the Audit component. Security zSecure Suite is built upon the special purpose Common Audit and Reporting Language (CARLa).

IBM Security QRadar

The over-arching value of the IBM Security QRadar is its ability to tie intelligence from the network to the broader set of data that is collected from the entire enterprise infrastructure. It provides collection, analysis, and correlation across a broad spectrum of systems, including networked solutions, security solutions, servers, hosts, operating systems, and applications. The result is security intelligence that provides a meaningful context for security professionals while radically reducing operational complexity across multiple systems. As with all IBM security intelligence solutions, IBM Security QRadar relies on a unified architecture for collecting, storing, analyzing, and querying log, threat, vulnerability, and risk-related data. See Figure 8.

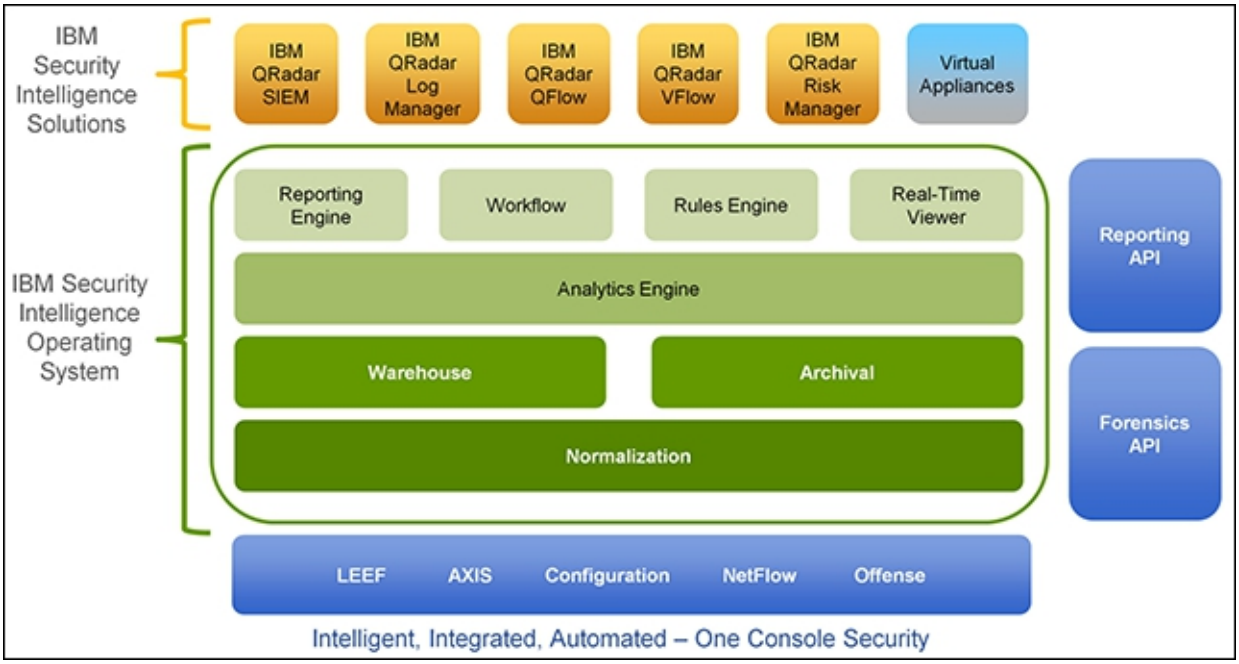

Figure 8. IBM Security intelligence product family that is built on a common foundation

The IBM Security QRadar security intelligence product family is based on a long-planned and carefully developed strategy to build an operating system approach to security intelligence. The IBM security intelligence operating system powers the IBM Security QRadar product family.

IBM Enterprise Key Management Foundation

The IBM Enterprise Key Management Foundation (EKMF) is a flexible and highly secure key management system for the enterprise. It provides centralized key management on IBM zEnterprise and distributed platforms for streamlined, efficient, and secure key and certificate management operations. The Enterprise Key Management Foundation is suitable for banks, payment card processors, and other businesses that must meet Europay, MasterCard, and Visa (EMV) and payment card industry (PCI) requirements. It includes crypto-analytic capabilities to identify compliance issues and help key officers understand who has access to key material. The Enterprise Key Management Foundation provides a foundation that can be tailored to address the needs of multiple industry segments to identify compliance issues and help key officers enforce enterprise key management policy requirements.

Encryption Facility for z/OS

Encryption Facility for z/OS provides this protection by offering encryption of data for exchange between different systems and platforms and for archiving purposes. It uses hardware compression and encryption and relies on a centralized key management that is based on the z/OS Integrated Cryptographic Service Facility (ICSF), which is highly secure and easy to use. Encryption Facility for z/OS can use ICSF to perform encryption and decryption and to manage cryptographic keys.

IBM Security AppScan

IBM Security AppScan is a suite of web application security testing products that are used to automate application scanning and vulnerability identification. The Security AppScan products scan and test for a wide range of web application vulnerabilities, including those identified by the Web Application Security Consortium (WASC) threat classification and the Open Web Application Security Project. The Security AppScan product line contains a wide variety of products, each of them adapted to the needs of a specific user.

IBM Security Access Manager

IBM Security Access Manager is an authentication and authorization solution for corporate web, client/server, and existing applications. Security Access Manager enables you to control user access to protected information and resources. By providing a centralized, flexible, and scalable access control solution, Security Access Manager enables you to build secure and easily managed network-based applications and e-business infrastructure. Security Access Manager supports authentication, authorization, audit and logging, data security, and resource management capabilities.

IBM Security Identity Manager

IBM Security Identity Manager enables organizations to drive effective identity management and governance across the enterprise. This solution helps strengthen regulatory compliance and security by reducing the risk of identity fraud. It automates the creation, modification, recertification, and termination of user privileges and supports policy-based password management throughout the user lifecycle. It features a redesigned business-friendly user interface and reporting tools to help managers make better governance decisions. As part of IBM Security Systems portfolio, IBM Security Identity Manager helps provide intelligent identity and access assurance.

IBM Security Federated Identity Manager

Federated identity management is based on the business agreements, technical agreements, and policy agreements that allow companies to interoperate based on shared identity management. This helps companies to lower their overall identity management costs and provide an improved user experience. It uses the concept of a portable identity to simplify the administration of users and to manage security and trust in a federated business relationship. The IBM Security Federated Identity Manager solution helps with this functionality for enterprise security.

Supported platforms

This Solution Guide focused on the following hardware and operating system platforms:

IBM System z
IBM z/OS
IBM z/VM
Linux on System z

Related information

For more information, see the following documents:

- IBM Redbooks: *Security on the IBM Mainframe: Volume 1- A Holistic Approach to Reduce Risk and Improve Security*, SG24-7803
  http://www.redbooks.ibm.com/abstracts/sg247803.html

- System z product page
  http://www.ibm.com/systems/z/

- System z Security solutions page
  http://www.ibm.com/systems/z/solutions/security.html

- z/OS product page
  http://www.ibm.com/systems/z/os/zos/

- z/VM product page
  http://www.vm.ibm.com/

- Linux on z product page
  http://www.ibm.com/systems/z/os/linux/

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.

This document was created or updated on March 26, 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/tips1295.html .

Trademarks