



Information Management

DB2 on z/OS and z/Series Hardware - Secure Solutions for an Un-secure World

Ernie Mancill

Executive IT Specialist

DB2 for z/OS Tools

IBM Software Group



ON DEMAND BUSINESS™

Agenda

Introduction:

- **z9 and ICSF Overview**
- **DB2 V8 Column Level Encryption**
- **IBM Encryption Tool for DB2 and IMS Databases**
- **IBM z/OS Encryption Facility and IBM Encryption Roadmap**

Security:

- **DB2 V8 Row Level Security**
- **DB2 Audit Trace**

Compliance:

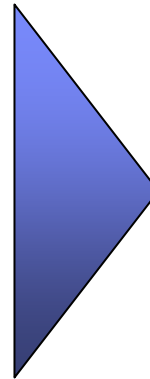
- **DB2 Audit Management Expert**
- **DB2 Data Archive Expert**
- **DB2 Test Database Generator**



The Bottom Line – Improving Internal Control

Regulators have multiple goals. . .

- ✓ Security of the national and international services infrastructure
- ✓ Improved risk management across the enterprise
- ✓ Integrity of financial reporting processes and related business practices
- ✓ Customer information security



. . . which drive investment in several areas

- People: Professionals with regulatory experience will be hired to enable firms to meet and anticipate new regulatory requirements
- Process: More robust processes and procedures will enable top management to monitor and enhance regulatory compliance
- Technology: Significant investment will be made to do the following:
 - ▶ **Encrypt sensitive data**
 - ▶ **Protect sensitive production data**
 - ▶ **Save data for future audits and to comply with retention rules**
 - ▶ **Auditiability - discover who did what, where and when**
 - **Real time**
 - **Historically**
 - ▶ **Engage in real-time monitoring of operations**





Information Management

z9 and Security Overview

IBM Software Group



ON DEMAND BUSINESS™

Protect sensitive information on line and off line

System z provides security without sacrificing responsiveness

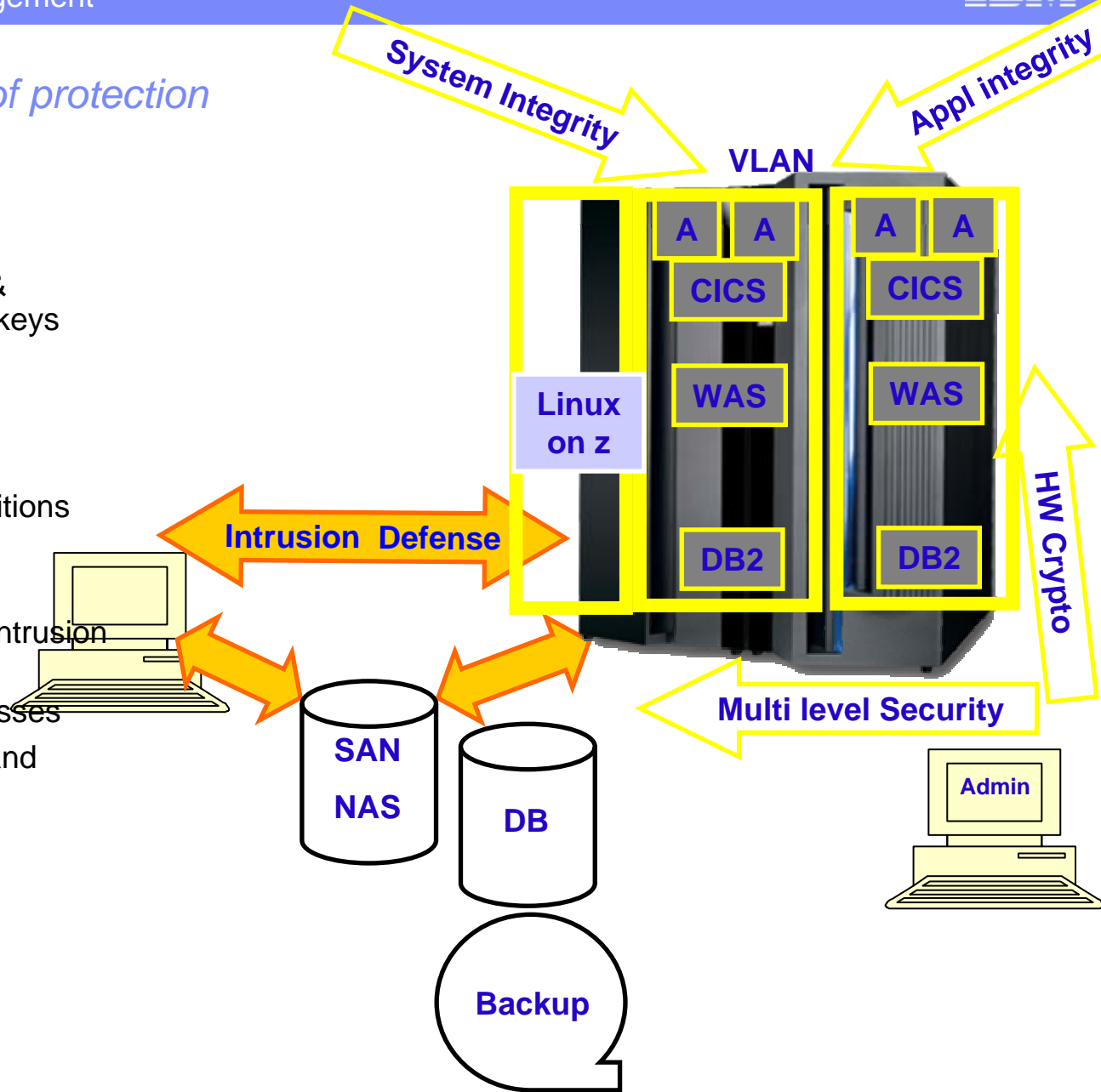
- Protect the data
 - ▶ **End-to-end protection that helps keep data uncorrupted and uncompromised**
 - ▶ **Multiple Level Security for different levels of “need to know”**
- **Encrypt sensitive data**
- Prevent unauthorized access
 - ▶ **IBM Resource Access Control Facility – 25 years strong**
 - ▶ **Support for a variety of encryption algorithms**
 - ▶ **EAL5 and other security certifications**
- Secure and speed the transaction
 - ▶ **Specialized Cryptographic co-processor hardware**
- Monitor, manage, and control
 - ▶ **Centralized access and control helps lower security costs, meet compliance guidelines, and simplify audit trail.**
- Compliance with privacy/security legislation
 - ▶ **Auditability**
 - ▶ **Control**
 - ▶ **Recoverability**
- Solutions available
 - ▶ **DM tools from IBM**
 - ▶ **Tivoli Consul InSight**



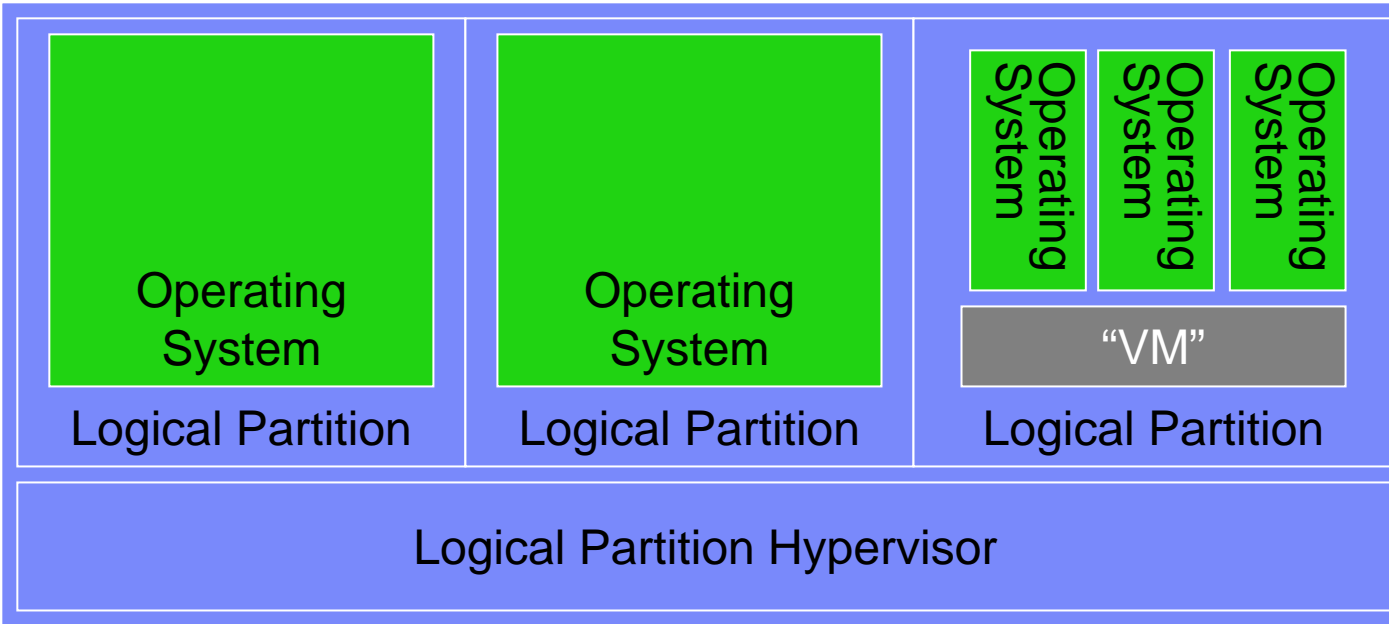
zSeries Architecture value

40 year heritage of protection

- System & Application Integrity
 - ▶ z/OS integrity statement
 - ▶ Inhibits trojan horses, worms & viruses via storage protection keys
 - ▶ Business Process Integration
 - ▶ Business Resilience
- Compartmentalization of work
 - ▶ Common Criteria certified partitions and guest isolation
 - ▶ Workload management
 - ▶ Virtual LANs reduce Security intrusion points
 - ▶ Middleware deployment processes
 - ▶ Row based security for DB2 and multi level security
- Data Confidentiality
 - ▶ Hardware encryption services
 - ▶ Encryption Key Management



IBM Trusted Server Compartmentalization

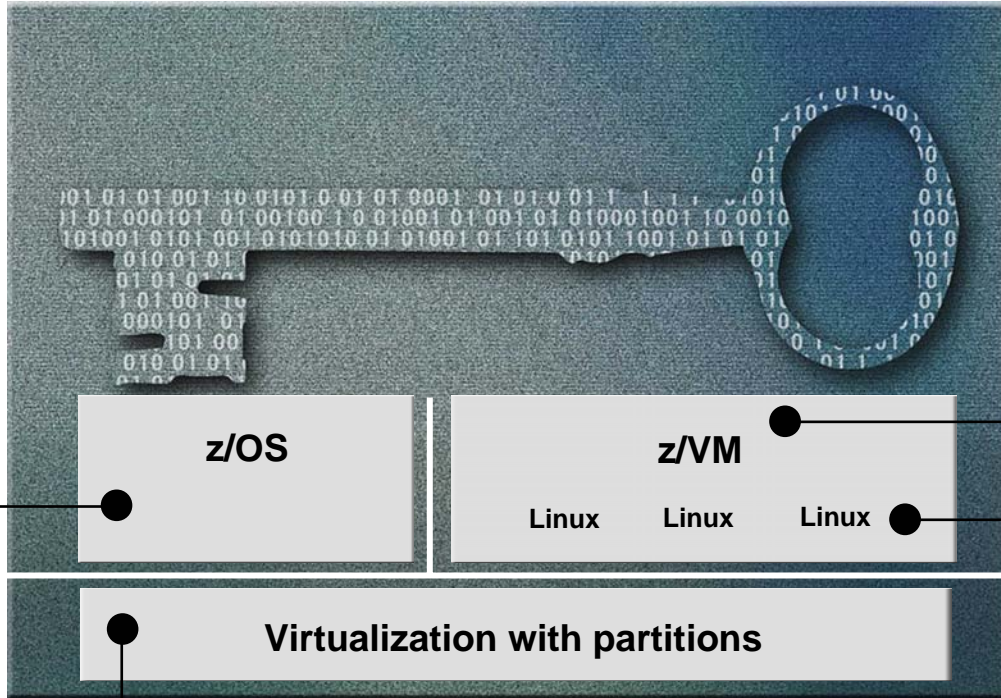


Server	Partition Manager	Linux	Other OS	"VM"	Database	Many other middleware
zSeries	EAL5+	CAPP EAL4 LSPP EAL4	z/OS CAPP/LSPP EAL4 Avail	zVM CAPP/LSPP EAL3 Avail	DB2 for z/OS CAPP/LSPP In Eval EAL3	z/OS & Linux



Certifications on System z

The Common Criteria program developed by NIST and NSA establishes an organizational and technical framework to evaluate the trustworthiness of IT Products and protection profiles



z/OS

- **Common Criteria** EAL4+ with CAPP and LSPP
 - z/OS 1.7 + RACF
- **IdenTrust™** certification for z/OS PKI Services

z/VM

- **Common Criteria** EAL3+ with CAPP and LSPP
 - **z/VM 5.1 + RACF**

Linux on System z

- **Common Criteria** EAL4+ with CAPP and LSPP
 - **SUSE LES9** certified
- **Common Criteria** EAL3+ with CAPP and LSPP
 - **Red Hat EL3** certified at EAL3+
 - **Red Hat EL4** EAL4+ in progress

System z EC and other System z servers

- **Common Criteria** EAL5 with specific Target of Evaluation
 - **Logical partitions**
- **FIPS 140-2 level 4**
 - **Crypto Express 2**

See: www.ibm.com/security/standards/st_evaluations.shtml





Information Management

IBM z Series Encryption Support

Encrypt sensitive data

IBM Software Group



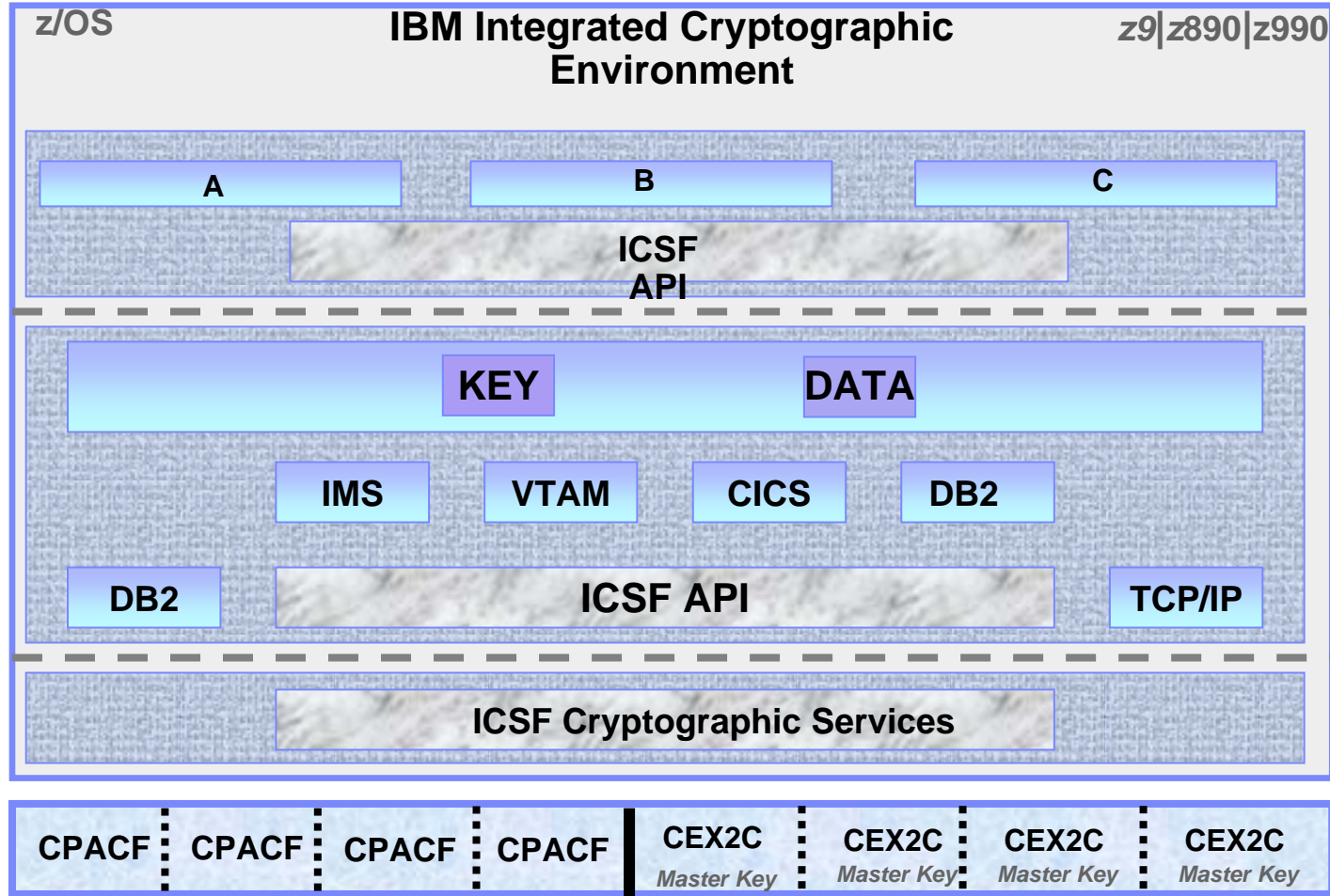
ON DEMAND BUSINESS™

Integrated Cryptographic Service Facility (ICSF)

z/OS Integrated Software Support for Data Encryption

- **Enhanced Key Management (Cryptographic Key Data Set (CKDS) Key Repository)**
 - ❖ **Key Creation and Distribution**
 - Public and Private Keys
 - Secure and Clear Keys
 - Master Keys
 - ❖ Unique **Key Label** (Key Alias) Indexes each Key stored in the CKDS
- **Access Control for CKDS via Security Access Facility (SAF)**
 - ❖ Control access to ICSF Callable Services
 - ❖ Control access to **Key Labels** (Key Alias) stored in the CKDS
- **ICSF Software Implementation of AES (z9 CPACF)**
- **Operating System S/W API Interface to Cryptographic Hardware**
- **Procedures for creating Installation-Defined Callable Services (UDX)**

IBM Encryption Flow



Key Label

CKDS
Clear and Enciphered User Keys
Master Key Verification Pattern

Cryptographic Key Data Set

CP Assist for Cryptographic Functions

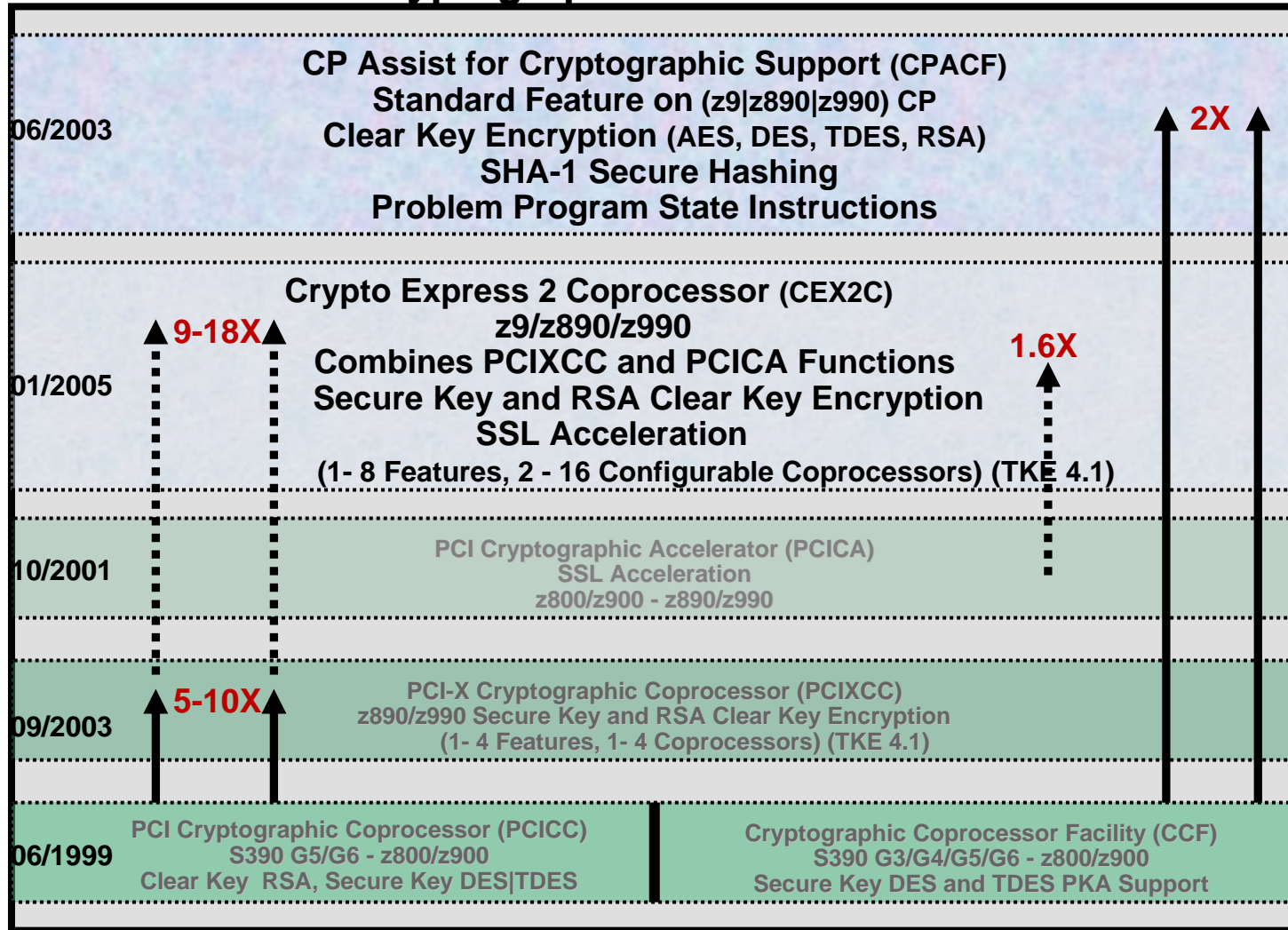
Crypto Express 2 Coprocessor

- Problem State Instructions
- Clear Keys Only
- DES/TDES Encryption
- AES (128 Bit)
- SHA-1 (256 on z9)

- ICSF Access Only (Key 0)
- Master Key Stored Within Boundary of Crypto Express 2 Feature
- Secure Key DES/TDES Encryption
- SSL Accelerator
- Tamper Resistant

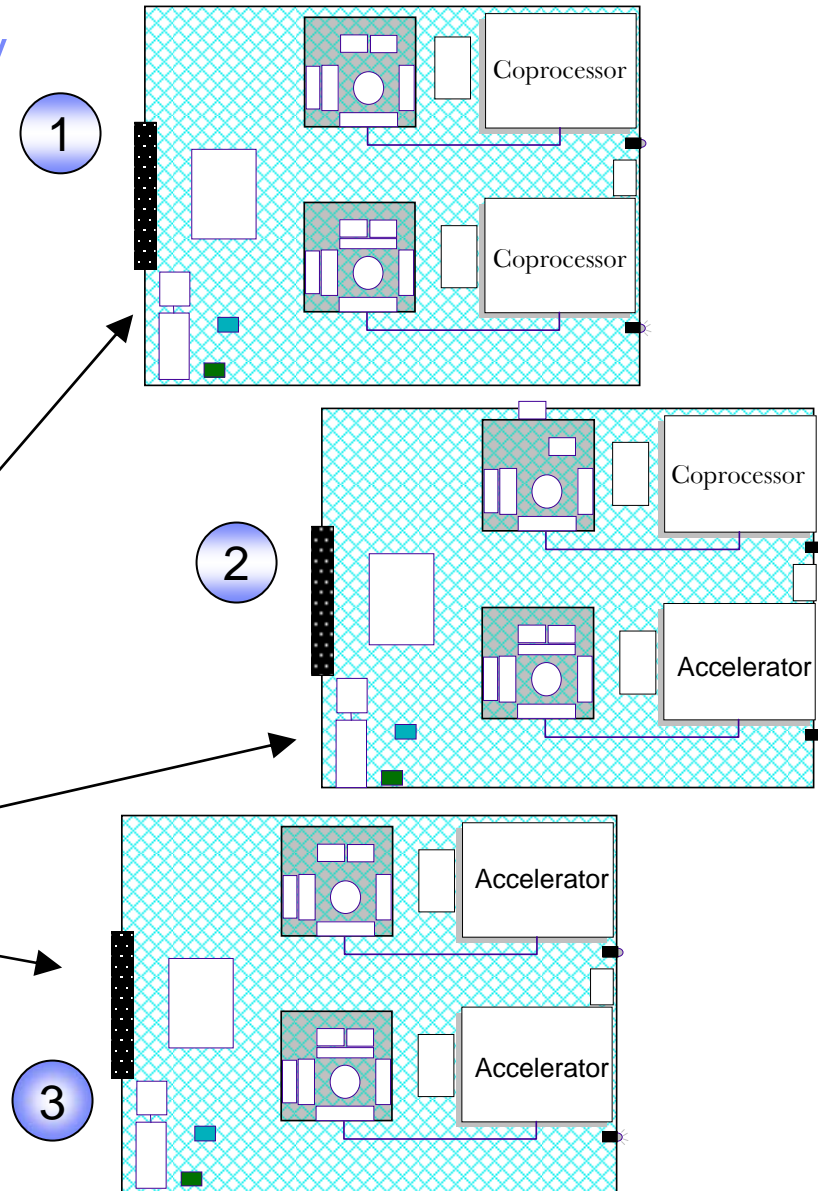
zSeries H/W Support for Data Encryption

zSeries Cryptographic Functional Evolution

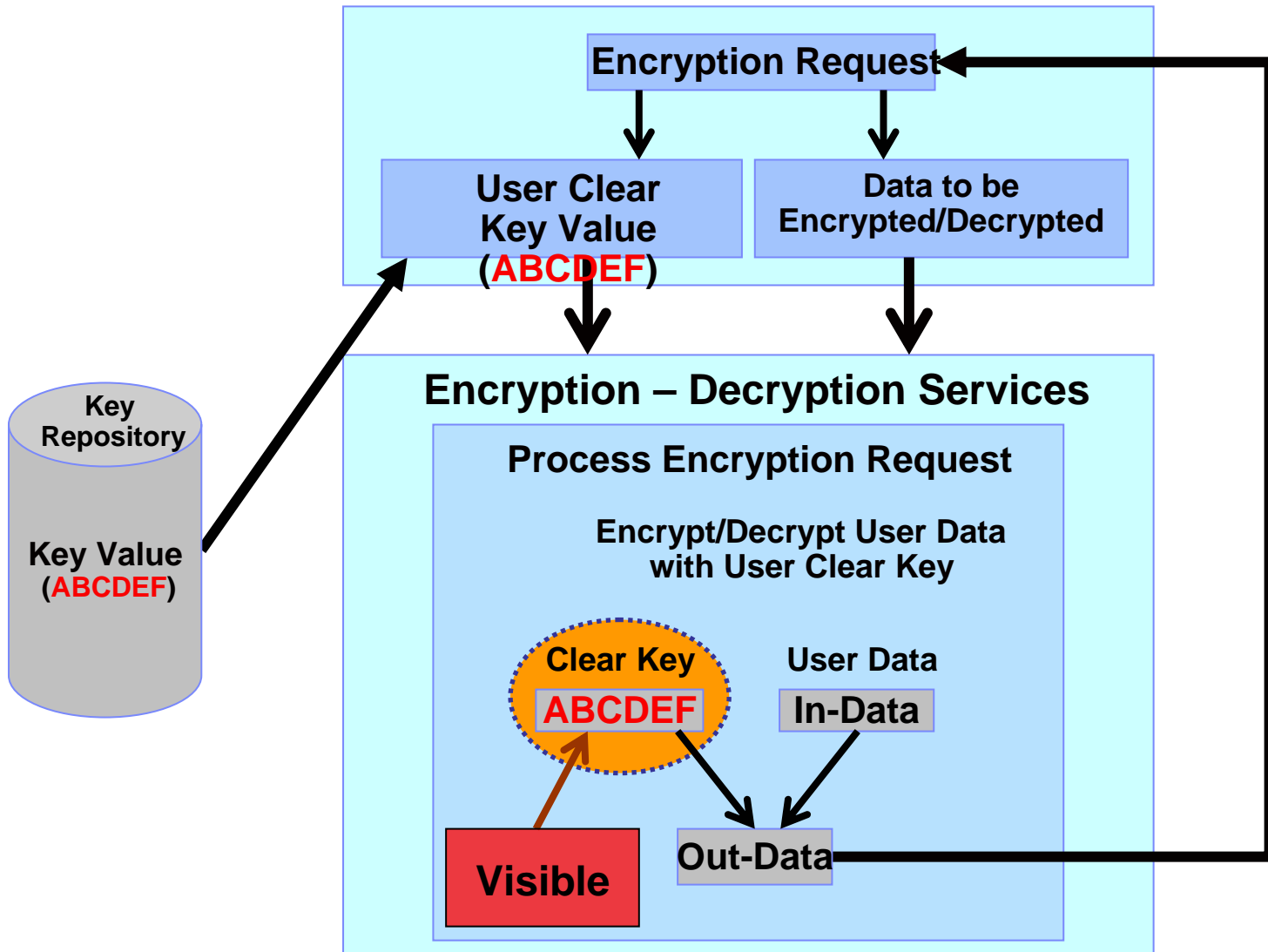


System z9 Cryptographic Support Summary

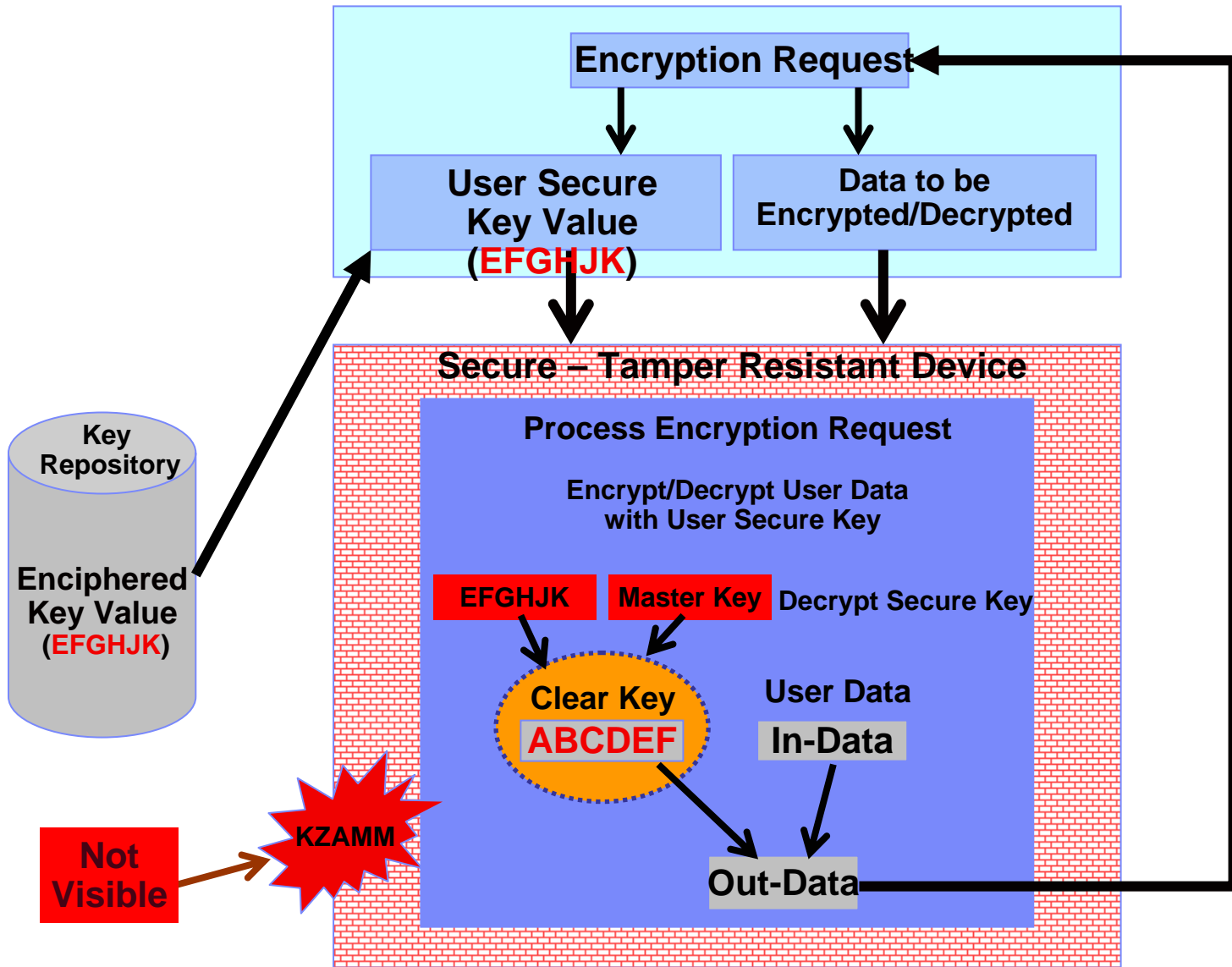
- CP Assist for Cryptographic Function (CPACF)
 - ▶ **Standard on every CP and IFL**
 - ▶ **Supports DES, TDES and SHA-1**
 - ▶ **New to System z9**
 - **Advanced Encryption Standard (AES)**
 - **Secure Hash Algorithm – 256 (SHA-256)**
 - **Pseudo Random Number Generation (PRNG)**
- Crypto Express2
 - ▶ **Two configuration modes**
 - **Coprocessor (default)**
 - **Federal Information Processing Standard (FIPS) 140-2 Level 4 certified**
 - **Accelerator (configured from the HMC)**
 - ▶ **Three configuration options**
 - **Default set to Coprocessor**
- TKE workstation with 5.0 level of LIC
 - ▶ **Supports configurable Crypto Express2 feature**
 - ▶ **New Graphical User Interface (GUI)**
 - ▶ **Smart Card Reader**



Visual Representation of Clear Key Processing



Visual Representation of Secure Key Processing





Information Management

DB2 V8 Row Level Encryption

IBM Software Group



ON DEMAND BUSINESS™

V8 Built-in Functions Supporting Data Encryption

- SET ENCRYPTION PASSWORD – used to provide a password as a key to encryption
- ENCRYPT (or ENCRYPT_TDES) – used to encrypt column during INSERT or UPDATE
- To retrieve (decrypt) encrypted data
 - ▶ DECRYPT_BIN
 - ▶ DECRYPT_CHAR
- GETHINT – Provide access to a previously stored password hint to the application requestor

DB2 V8 Encryption and retrieval Example

- Create the EMP table with the EMPNO column. The EMPNO column must be defined with the VARCHAR data type, must be defined FOR BIT DATA, and must be long enough to hold the encrypted data. The following statement creates the EMP table:
 - ▶ CREATE TABLE EMP (EMPNO VARCHAR(32) FOR BIT DATA);
- Set the encryption password. The following statement sets the encryption password to the host variable :hv_pass:
 - ▶ SET ENCRYPTION PASSWORD = :hv_pass;
- Use the ENCRYPT keyword to insert encrypted data into the EMP table by issuing the following statements:
 - ▶ INSERT INTO EMP (EMPNO) VALUES(ENCRYPT('47138'));
 - ▶ INSERT INTO EMP (EMPNO) VALUES(ENCRYPT('99514'));
 - ▶ INSERT INTO EMP (EMPNO) VALUES(ENCRYPT('67391'));



DB2 V8 Encryption and retrieval

Example II

- Select the employee ID numbers in decrypted format:
 - ▶ `SELECT DECRYPT_CHAR(EMPNO, :hv_pass) FROM EMP;`
- If you provide the correct password, DB2 returns the employee ID numbers in decrypted format
- Notice the above example provides the password in a host variable, this can also be declared using the special register `SET ENCRYPTION PASSWORD` which is the recommended approach for performance



DB2 V8 Encryption Restrictions and Considerations

- CHAR and VARCHAR are directly supported. Numeric and Timestamp data are only indirectly supported using casting.
- If a predicate requires decryption, the predicate is a stage 2 predicate, which can degrade performance.
- Because encrypted data is binary data, range checking of encrypted data requires table space scans. Range checking requires all the row values for a column to be decrypted.
- Avoid joins of encryption columns where possible to reduce decryption overhead



DB2 V8 Encryption – Additional Considerations

- All encrypted columns must be declared “for bit data”. So, unchanged read-applications see data in encrypted form.
- LOAD and UNLOAD utilities do not support DB2 encryption
- SQL based programs such as DSNTIAUL do support encryption.
- Indexes are also encrypted, so predicates that depend on the collating sequence of encrypted columns, (for example range predicates), may produce wrong results (unless modified to use built-in functions correctly).





Information Management

IBM Encryption Tool for DB2 and IMS Databases

IBM Software Group



ON DEMAND BUSINESS™

IBM Data Encryption for IMS and DB2 Databases (5799-GWD)

Standard DB2 EDITPROC for Accessing Cryptographic Functions

- All Supported DB2 Versions
- Member of IBM IMS | DB2 Tools Family of Products
- Pre-coded EDITPROC for encryption of DB2® Data
- Encryption/Decryption occurs at the DB2 Row Level
- Unique EDITPROC can be defined for each DB2 Table
- Exploits z/OS Integrated Cryptographic Service Facility (ICSF)
- Exploits zSeries CPACF Cryptographic Hardware Directly
- Requires no changes to your applications
- Fast implementation

Edit Procedures (EDITPROC) are Programs That:

- Transform Data on INSERT | UPDATE | LOAD
- Restore Data to Original Format on SELECT
- Transformations on Entire ROW
- Supported by Utilities
- Implemented via Create Table specification
- Requires unload/load of data



Restrictions and Considerations

- A DB2 table can only specify one EDITPROC exit. If your DB2 table already has an EDITPROC exit specified and you wish to implement this product, then you must code an alternative solution for your existing EDITPROC exit.
- Indexes cannot be encrypted (the EDITPROC function doesn't support encryption of indexes).
- Tables with ROWIDs, Identity Columns or LOBs cannot be encrypted (again a restriction of EDITPROC).
- In DB2, there can only be one encryption key label per table
- You can define different encryption key labels for as many tables as you wish. (Encryption key labels are set up by your security analyst.) A separate exit must be built for each encryption key label that you define.
- In DB2, you can both encrypt and compress data using DB2's hardware compression. However, compression takes place after encryption, which greatly compromises the effectiveness of the compression.

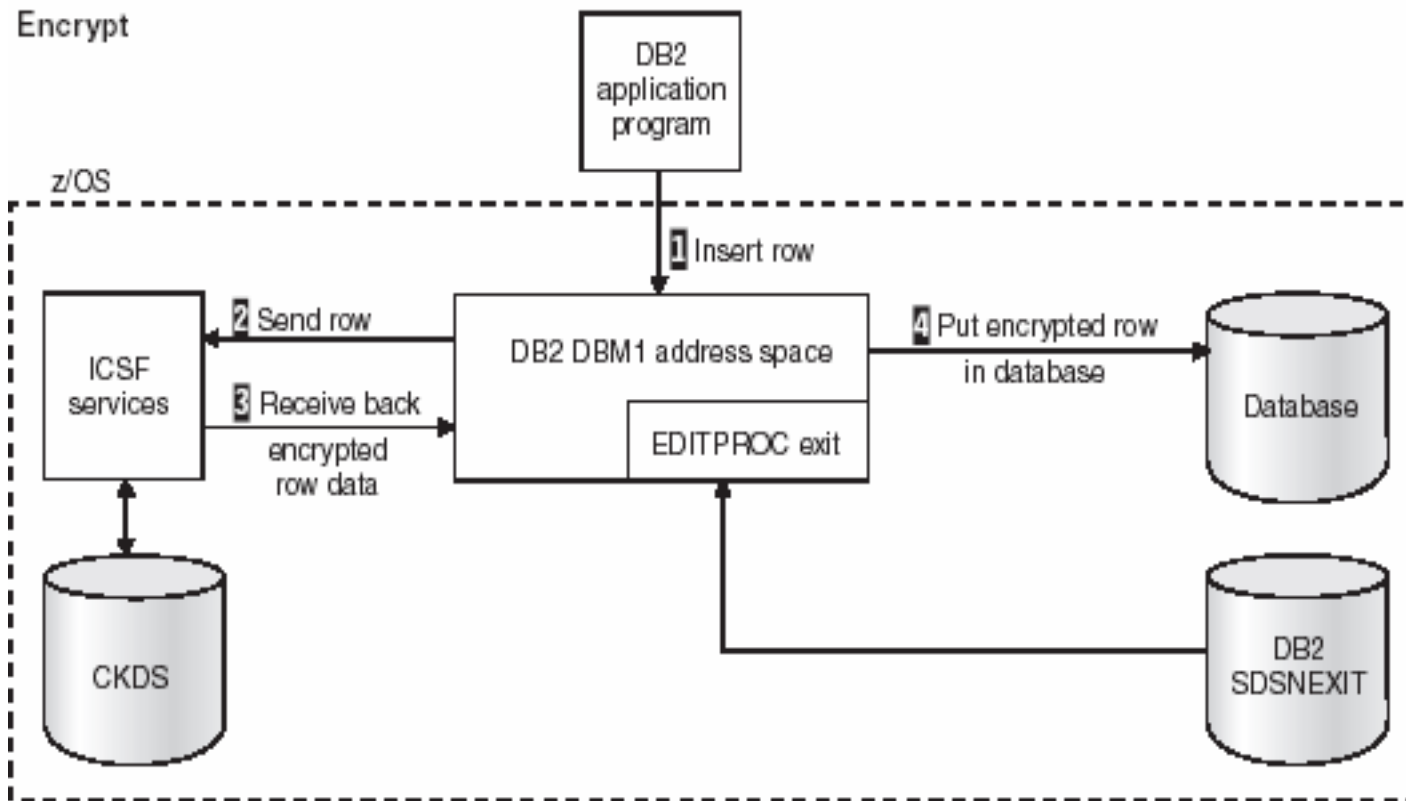


IBM Data Encryption for IMS and DB2 Databases Summary

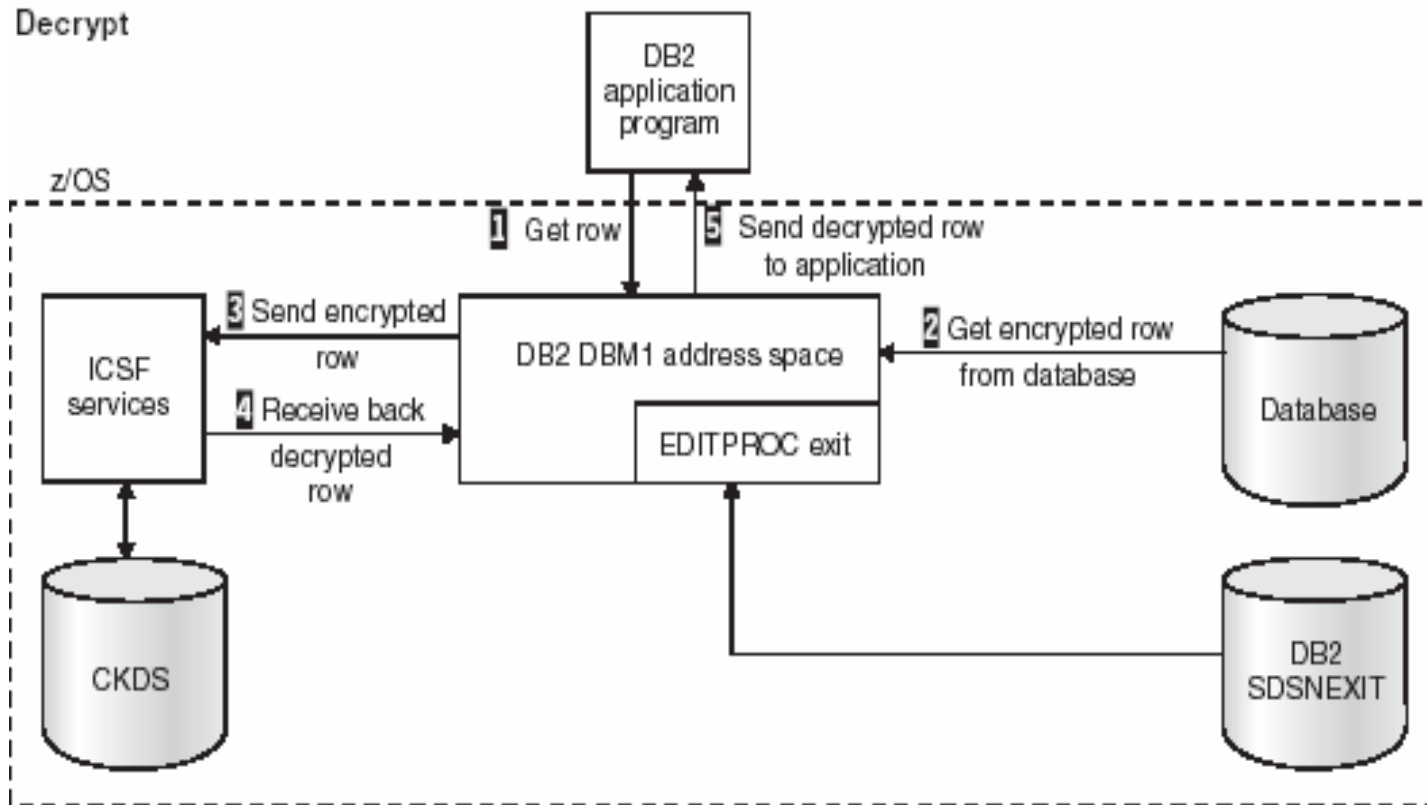
- **Configure the Integrated Cryptographic Service Facility (ICSF)**
- **Enable CP Assist for Cryptographic Functions (CPACF) (z890/z990)**
(This Feature subject to US Export Restrictions)
- **Generate and store in the Cryptographic Key Data Set (CKDS) Key Labels**
- **Build the IMS User Exit or DB2 EDITPROC**
 - ❖ For IMS use the Sample JCL Provided or the ISPF Panels
 - ❖ For DB2 use the ISPF Panels
 - ❖ For IMS Custom Built Exits follow Instructions outlined in:
 - ICSF Application Programmers Guide (SA22-7522)
 - IMS Customization guide (SC18-7817)
 - IMS Utilities Reference System (SC18-7834)
- **Back - Up and Unload Databases**
- **Create Exits for IMS or EDITPROCS for DB2**
- **Reload the Databases: Data Bases will be Encrypted**
- **Validate your Output**



IBM Data Encryption Tool for DB2 and IMS Databases - Encryption



IBM Data Encryption Tool for DB2 and IMS Databases - Decryption



Tape encryption with System z in the enterprise

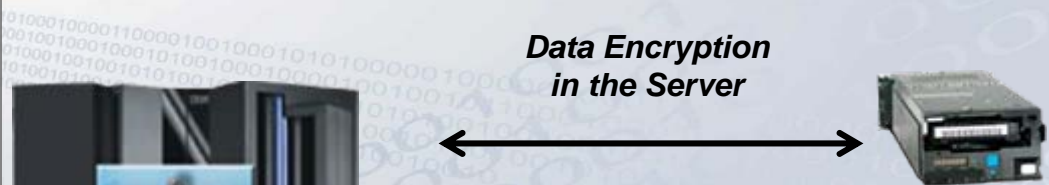


Help secure data from theft or compromise

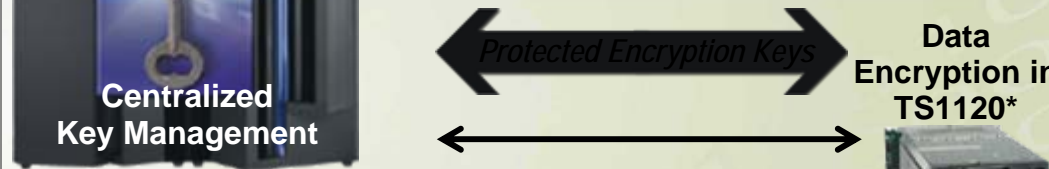
Why z/OS centralized key management?

- Can help to protect and manage keys
 - Highly secure and available key data store
 - Long term key management
 - Disaster recovery capabilities
- Single point of control
- Over a decade of production use

Encryption Facility for z/OS, V1.1



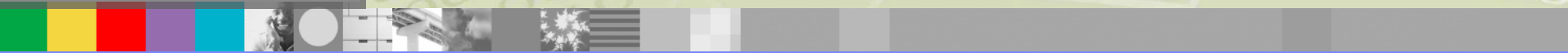
- Flexible options for business partner exchange
- Partners can encrypt and decrypt using no-charge JAVA client
- Supports public key or password based exchange



Plans for encryption in IBM System Storage 2H2006*



- Highly secure tape library
- High performance archive encryption
- Transparent to existing processes and applications
- Can help provide audit compliance



IBM Encryption Facility for z/OS, 1.1

Licensed Program Product
MSU-based pricing*

Runs on the following servers: System z9 109 (z9-109), or equivalent
zSeries z900 or z990, or equivalent
zSeries z800 or z890, or equivalent

Requires: z/OS V1.4 or higher z/OS.e V1.4 or higher

Feature: *Encryption Services*

Optional Priced Feature*
Planned availability:
Oct. 28, 2005

Feature: *DFSMSdss Encryption*

Optional Priced Feature*
Planned availability:
December 02, 2005

Encryption Facility Client

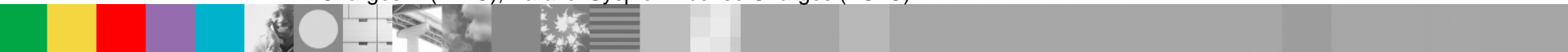
Web download
Planned availability:
October 28, 2005

- Supports encrypting and decrypting of data at rest (tapes, disk)
- Supports either Public Key/Private keys or passwords to create highly-secure exchange between partners

- Java technology-based code that allows client systems to decrypt and encrypts data for exchange with z/OS systems

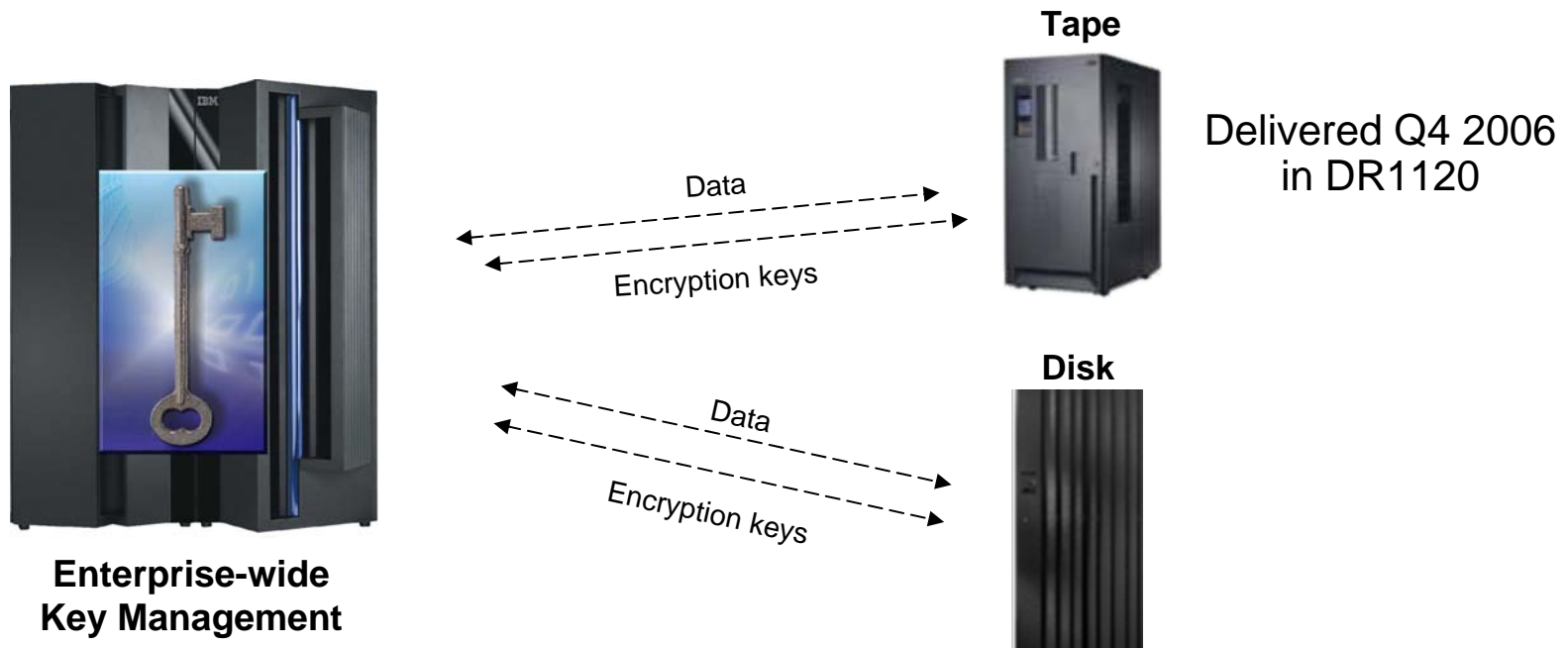
- Allows encryption and compression of DUMP data sets created by DFSMSdss
- Supports decryption and decompression during RESTORE

* Variable Workload License Charges (VWLC), Entry Workload License Charges (EWLC), zSeries Entry License Charges™ (zELC), Parallel Sysplex License Charges (PSLC)



Future Directions – Extending Encryption to IBM TotalStorage

- Statement of Direction:
 - ▶ To address customers' growing concern with data security, IBM is announcing a statement of direction for the development, enhancement and support of encryption capabilities within storage environments such that the capability does not require the use of host server resources.
 - ▶ This includes the intent to offer, among other things, capabilities for products within the IBM TotalStorage portfolio to support outboard encryption and to leverage the centralized key management functions planned for z/OS ICSF.



Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only



Information Management

DB2 V8 on z/OS : Multi-row Security

Access for “need to know” only

IBM Software Group



ON DEMAND BUSINESS™



Provide access to data based on need to know

Multilevel Security

REQUIREMENT:

Data shared between people/organizations with different "need to know"

System z solution:

- Highly secure access to DB2 databases
- Security labeling at the row-level of DB2
- With RACF as single security manager for both z/OS and DB2

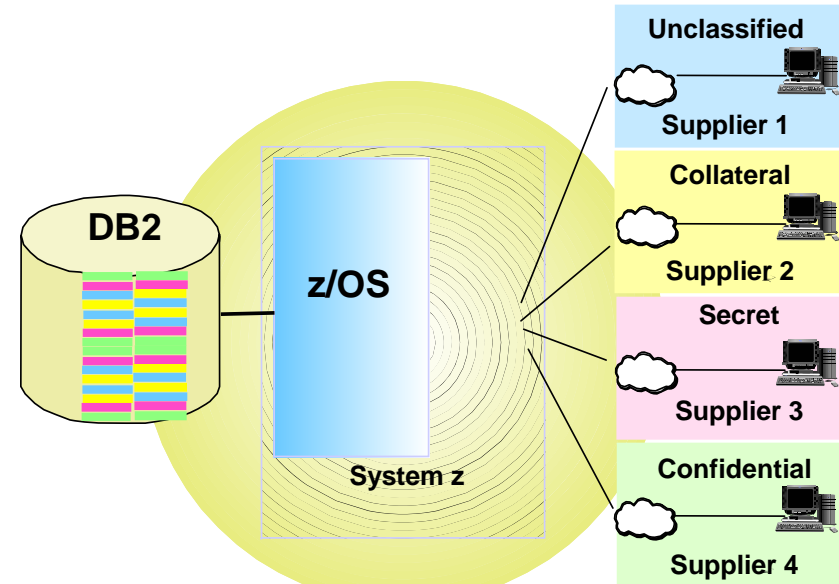
Public Sector: Hierarchical security

Commercial opportunities:

- ▶ Hosting similar applications
- ▶ Single database

hosting subsidiaries

hosting partners



MLS on System z

Imagine the possibilities!



DB2 MLS

- Rows in a DB2 table have a security label associated with them by means of a special column of the table that contains only the 8-character security label that defines the security classification of each row in that table.
- new attribute 'AS SECURITY LABEL'
 - ▶ The traditional response to these sorts of requirements for DB2 applications has been to use views
 - ▶ some DB2 customers have adopted is to use exits, using fieldprocs or editprocs.





Multilevel Security by Row

Sally 
 SECLABEL='RAINBOW'

Joe 
 SECLABEL='PASTEL'

Sam 
 SECLABEL='SUNSET'

DB2_SECURITY_LABEL_EXT	COL1	COL2	COL2
RAINBOW	56	7	76
RAINBOW	24	56	65
RAINBOW	42	6	45
BLUE	3	456	7
INDIGO	113	456	56
VIOLET	3	456	4
BLUE	4	4556	7
RED	4	76	567
ORANGE	33	7	567
RED	5455	76	567
YELLOW	999	65	45



Row Granularity Multilevel Security



Table has column defined AS SECURITY LABEL

Each row value has a specific security label

Get security labels from RACF

Save in rows for INSERT, UPDATE, LOAD, ...

Check for each new seclabel value accessed

If access is allowed, then normal access

If access is not allowed, data not returned

Runtime user to data checking

Seclabel values are cached to minimize cpu

Requires z/OS V1R5 and Security Server (RACF)



Implement Security Labels in DB2

- In order to implement MLS for DB2, it is first necessary to implement MLS on your MVS system.

- identify all of the SECLABELs to be used in the system.
 - ▶ 1. Identify which users and groups require what access to which rows of which tables.
 - ▶ 2. Design a set of security labels for users and table rows that reflects the result of step 1.
 - ▶ 3. Get the RACF administrators to define that set in RACF, and then activate the RACF SECLABEL class.
 - ▶ 4. Add a security label column to each table requiring row-level security. This process assigns an initial default value to every row.
 - ▶ 5. Update the security labels of the rows to appropriate values.

Users & Objects

- relationship between DB2 users and DB2 objects is important
- a user is any entity that requires access to system resources. The term user includes not only human users, but can also be stored procedures or batch jobs.
- an object is any system resource to which access must be controlled
 - ▶ Data sets
 - ▶ Tables
 - ▶ Rows
 - ▶ Commands



Its not all or nothing

- You do not have to enable the DB2 RACF exit DSNX@XAC in order to use SECLABELS for row-level security. You may continue to use native DB2 GRANTS and REVOKEs to control all other DB2 access, but you will not have SECLABELS for object-level security.
- To run in a DB2 row-level security environment, it is sufficient to have:
 - ▶ the RACF SECLABEL class active
 - ▶ SECLABELS for users
 - ▶ SECLABELS on DB2 table rows
 - ▶ With this setup, *all* DB2 users are equivalent to having write-down authority.

Securing DB2 and Implementing MLS on z/OS - SG24-6480





Information Management

DB2 V9 on z/OS :Trusted Context and Roles

Access for “as long as needed” only

IBM Software Group



ON DEMAND BUSINESS™

Trusted context functional overview

- Trusted context addresses the problem of establishing a trusted relationship between DB2 and an external entity, such as a middleware server.
- A series of trust attributes are evaluated at connect time to determine if a specific connection is to be trusted.
- The relationship between a connection and a trusted context is established when a connection to the server is first created



Trusted context functional overview

- Users must be allowed to use a trusted context.
- Can restrict trusted connections to a specific server
- Trusted connection can be established for a local or remote application



Trusted context functional overview

- Once established, a trusted connection provides the ability to:
 - ▶ Use the trusted connection for a different user without authentication.
 - ▶ Acquire special set of privileges by an authorization ID, that are not available to it outside the trusted context. **This is accomplished by associating a role with the trusted context.**
 - ▶ Allow a role to own objects, if objects are created in a trusted context with role defined as the owner.
- Trusted context provides:
 - ▶ User accountability
 - ▶ Improved Security and Manageability
 - ▶ **Ability of DBADM to perform DDL on behalf of others**



Database role functional overview

- DB2 extends trusted context concept to optionally assign a role to a user of the context
- Entity that groups together one or more privileges and can be assigned to users via a trusted context
- Virtual authorization id assigned via a trusted context and not available outside of context
- Privileges can be granted /revoked from a role
- Privileges are additional to those available via primary and secondary authid
- Can be assigned/removed from individuals via the trusted context as needed.

Database role functional overview

- Can optionally be the owner of DB2 objects. A ROLE can be dropped if it owns no objects
- Removing a person's ROLE does not cause the objects to be cascade deleted
- Role is independent of it's creator. Allows a DBA to have privileges to create objects and manage them for a time, even though ownership is to be another id.
- Without roles, transferring onwership implies drop/recreate
- Implement on weekend, privileges no longer available on Monday morning
- Roles are a way to allow multiple DBA authids to have ownership of an object at the same time or at different times





Information Management

DB2 V8 on z/OS : Audit Class Tracing

IBM Software Group



ON DEMAND BUSINESS™

Audit class Events that are traced

1. Access attempts that DB2 denies because of inadequate authorization. This class is the default.
2. Explicit GRANT and REVOKE statements and their results. This class does not trace implicit grants and revokes.
3. CREATE, ALTER, and DROP statements that affect audited tables, and the results of these statements. This class traces the dropping of a table that is caused by DROP TABLESPACE or DROP DATABASE and the creation of a table with AUDIT CHANGES or AUDIT ALL. ALTER TABLE statements are audited only when they change the AUDIT option for the table.
4. Changes to audited tables. Only the first attempt to change a table, within a unit of recovery, is recorded. (If the agent or the transaction issues more than one COMMIT statement, the number of audit records increases accordingly.) The changed data is not recorded, only the attempt to make a change is recorded. If the change is not successful and is rolled back, the audit record remains; it is not deleted. This class includes access by the LOAD utility.

Accesses to a dependent table that are caused by attempted deletions from a parent table are also audited. The audit record is written even if the delete rule is RESTRICT, which prevents the deletion from the parent table. The audit record is also written when the rule is CASCADE or SET NULL, which can result in deletions that cascade to the dependent table.

5. All read accesses to tables that are identified with the AUDIT ALL clause. As in class 4, only the first access within a DB2 unit of recovery is recorded. References to a parent table are also audited.
6. The bind of static and dynamic SQL statements of the following types:
 - INSERT, UPDATE, DELETE, CREATE VIEW, and LOCK TABLE statements for audited tables. Except for the values of host variables, the audit record contains the entire SQL statement.
 - SELECT statements on tables that are identified with the AUDIT ALL clause. Except for the values of host variables, the audit record contains the entire SQL statement.
7. Assignment or change of an authorization ID because of the following reasons:
 - Changes through an exit routine (default or user-written)
 - Changes through a SET CURRENT SQLID statement
 - An outbound or inbound authorization ID translation
 - An ID that is being mapped to a RACF ID from a Kerberos security ticket
8. The start of a utility job, and the end of each phase of the utility.
9. Various types of records that are written to IFCID 0146 by the IFI WRITE function.



V9 Trace Extensions – START TRACE

- Qualifications by:

- ▶ LOC

- Location-Name
- LUName
- IPAddress

- ▶ PLAN

- ▶ PACKAGE

- PKGLOC
- PKGCOL
- PKGPROG

- ▶ Workstation Identifiers

- USERID
- APPLNAME
- WRKSTN

- ▶ Miscellaneous

- CORRID
- CONNID
- ROLE

- Exclude by:

- ▶ LOC

- XLOC

- ▶ PLAN

- XPLAN

- ▶ PACKAGE

- XPKGLOC
- XPKGCOL
- XPKGPROG

- ▶ Workstation Identifiers

- XUSERID
- XAPPLID
- XWRKSTN

- ▶ Miscellaneous

- XCORRID
- XCONNID
- XROLE

V9 Trace Extensions - Wildcards

- Tracing threads using the * wildcard:
 - ▶ You can use the wildcard suffix, "*" to filter threads. For example, if you specify "-START TRACE PLAN (A,B,C*)", DB2 will trace, and then return A, B, CDE, CDEFG, CDEFGH, and so on. It will trace threads "A", "B" and all threads starting with "C".
- Tracing threads using the positional, (_) wildcard:
 - ▶ You can utilize the positional wildcard, which is represented by the, "_" character, to trace threads when you want the wildcard in the middle, or when you want to trace threads of a specific length. For example, if you specify "-START TRACE PLAN (A_C)", all threads will be traced that are three characters that have "A" as the first character, and "C" as the third.
- Tracing multiple threads at once using wildcards:
 - ▶ You also have the option of tracing multiple threads based on multiple trace qualifications. For example, you can specify, "-START TRACE PLAN (A*, B*, C*)" to simultaneously trace ALL threads for plan that start with "A", "B", and "C". The wildcard character, "*" will trace all threads.
 - ▶ You have the ability to filter multiple threads at the same time, setting specific criteria for the trace: For example, you can specify "-START TRACE PLAN (A) USERID (B)". This will trace the threads where the plan thread is A, and the user ID is B.

V9 Trace Extensions – Some Restrictions

- When tracing threads, you can only specify more than one thread criteria for one filter per “-START TRACE” command.
 - ▶ For example, you can specify “-START TRACE PLAN (A,B) USERID (B) WRKSTN (E),” but you cannot specify “-START TRACE PLAN (A, B) USERID (A, B) WRKSTN (E).”
- If you use one or no values for PLAN, AUTHID, or LOCATION, the START TRACE command starts a single trace. If you use multiple values for PLAN, AUTHID, or LOCATION, the command starts a trace for each plan, authorization ID, or location. There can be up to 32 traces going at one time.
- You must use a privilege set of the process that includes one of the following privileges or authorities:
 - ▶ TRACE privilege
 - ▶ SYSOPR authority
 - ▶ SYSCTRL authority
 - ▶ SYSADM authority



Limitations of the audit trace

- The audit trace does not record everything, as the following list of limitations indicates:
 - ▶ The auditing that is described in this information takes place only when the audit trace is on.
 - ▶ The trace does not record old data after it is changed because the log records old data.
 - ▶ If an agent or transaction accesses a table more than once in a single unit of recovery, the audit trace records only the first access.
 - ▶ The audit trace does not record accesses if you do not start the audit trace for the appropriate class of events.
 - ▶ The audit trace does not audit some utilities. The trace audits the first access of a table with the LOAD utility, but it does not audit access by the COPY, RECOVER, and REPAIR utilities. The audit trace does not audit access by stand-alone utilities, such as DSN1CHKR and DSN1PRNT. (And some 3rd party utilities)
 - ▶ The trace audits only the tables that you specifically choose to audit.
 - ▶ You cannot audit access to auxiliary tables.
 - ▶ You cannot audit the catalog tables because you cannot create or alter catalog tables.
- This auditing coverage is consistent with the goal of providing a moderate volume of audit data with a low impact on performance. However, when you choose classes of events to audit, consider that you might ask for more data than you are willing to process.



Audit Trace

- Those wanting to audit by authid, specific table accesses, and other DB2 events will find the audit trace invaluable. Eight categories of audit information are provided:
 - All instances in which an authorization failure occurs for which user has not been granted the appropriate authority
 - All executions of the GRANT and REVOKE statements
 - Every DDL statement issued for specific tables created by specifying AUDIT CHANGES or AUDIT ALL
 - The first DELETE, INSERT, or UPDATE for an audited table
 - The first SELECT for only the tables created specifying AUDIT ALL
 - DML statements encountered by DB2 when binding
 - All authid changes resulting from SET CURRENT SQLID statement
 - All execution of DB2 utilities
- Estimated overhead: Approximately 5 – 7 percent CPU overhead per transaction is added when all audit trace classes are started.



Audit Trace Overhead v8 admin

- The performance impact of auditing is directly dependent on the amount of audit data produced. When the audit trace is active, the more tables that are audited and the more transactions that access them, the greater the performance impact. The overhead of audit trace is typically less than 5%.
- When estimating the performance impact of the audit trace, consider the frequency of certain events. For example, security violations are not as frequent as table accesses. The frequency of utility runs is likely to be measured in executions per day. Alternatively, authorization changes can be numerous in a transaction environment.
- Following is the summary of results of the DB2 V8 Audit trace measurements :

The measurements were done with Audit trace class(*) on, similar to the tool. All the tables in the workload were enabled for 'Audit All'.

For OLTP measurement with distributed IRWW SQL CLI workload with 9 Tables, 3 PI, 8 NPI and 7 transactions running at 493 transactions per second, the DB2 Class 2 CPU increase was +7.2%.

For Utility measurements with LOAD, Rebuild Index, Reorg Table, Reorg Index utilities using 1 Table, 10 partitions, 1 PI and 5 NPI, there was no measurable CPU increase.



What to Audit

- **Closed Application Environment**
 - ▶ **Traditional Application controls well defined**
 - **CICS and IMS – Signon and Transaction Access secured via RACF**
 - **Production Batch – Controlled via program pathing / Job Scheduling**
- Data mining – no risk of update but access audit might be needed
- Adhoc environment – QMF, SPUFI, etc. Constitutes exposure
 - ▶ SPUFI Plan can be restricted but ALL use should be audited
 - ▶ Privileged ID's (DBA) should be audited
 - ▶ SYSADMIN are difficult to audit
- Distributed Application Environment
 - ▶ Use of SQLESETI can provide granularity with ID
- “Offline” Utilities and certain tools are used outside of DB2
 - ▶ RACF dataset access defined controls
- Use of DSN1COPY should be restricted
- Data may not be as granular as you think
 - ▶ Depending on how you configured your connections into DB2 – CICS attach, SAP, or CICS users with unique id's, and distributed transactions. May get all audit data but may not be meaningful because of attach environments. Group versus AUTHID.



What to Audit?- Continued

- Some items that should always be audited
 - ▶ DB2 commands
 - ▶ DDL
 - ▶ Class 1 – attempts
 - ▶ Class 2
 - ▶ Class 3
 - ▶ Class 7 – set current SQL ID (exclude OMPE and authorized users)
 - ▶ Class 8 – utilities
 - ▶ Class 4 and 5 only run for SYSADM users
- Audit classes 1, 2, and 7 add no additional overhead. Because most transactions do not result in authorization failures or issue GRANTS, REVOKEs, or utilities, running these trace classes is cost-effective.

Database Security

- Database security is no longer something that *should* be implemented,
 - ▶ but something that every serious company *must* have, to bring a certain level of reassurance to their clients.
 - ▶ and it is the LAW.
- Any business should know who is reading or changing their valuable information stored in their databases.
 - ▶ Companies should have a log of actions performed inside the DB2 database, for later tracking and problem solving.
 - ▶ The DB2 audit trace record is a unique source of information
 - can be retroactively queried if fraud is suspected
 - if individuals wish to know how their information was used



For the DBA

- Management said we have to audit access to tables with sensitive data, so get with the auditors and take care of it!
 - ▶ Which Audit Trace classes do we start?
 - What audit information do we want?
 - To what destination?
 - ▶ Which tables need 'AUDIT ALL' ?
 - ▶ How many audit trace records will we produce?
 - ▶ Do we run the Audit Trace all the time?
 - ▶ What is the overhead?
 - ▶ How do we get reports from the Audit Trace data?
 - ▶ What other sources of audit information is there?
 - ▶ How do I set up enough reports to keep the Auditors busy?
 - ▶ How do we get the Auditors to do it?
 - How much of my time will I have to spend with the Auditors?



At A Glance

- Audit Management Expert
 - ▶ Centralized auditing tools that can bring together information from different sources into a correlated, coherent view of the system
 - ▶ Enable auditors to collect, view, analyze, and report on data via the audit repository
 - ▶ Enable administrators to define customized filters for the collection of audit data
 - By data of interest – not by audit trace classes
 - ▶ Provides an administration UI
 - allows product administrators to easily define
 - users and groups, assign privileges, define data collection policies
 - ▶ Provides an auditor-friendly reporting UI
 - Many user friendly options for examining data in the repository
 - Allows detailed analysis and visualization of data collected by the DB2 auditing tool
 - Auditors can export audit data into other applications such as Excel®.
 - ▶ Product provides Batch reporting
 - ▶ Can perform Log Analysis to view changed data values



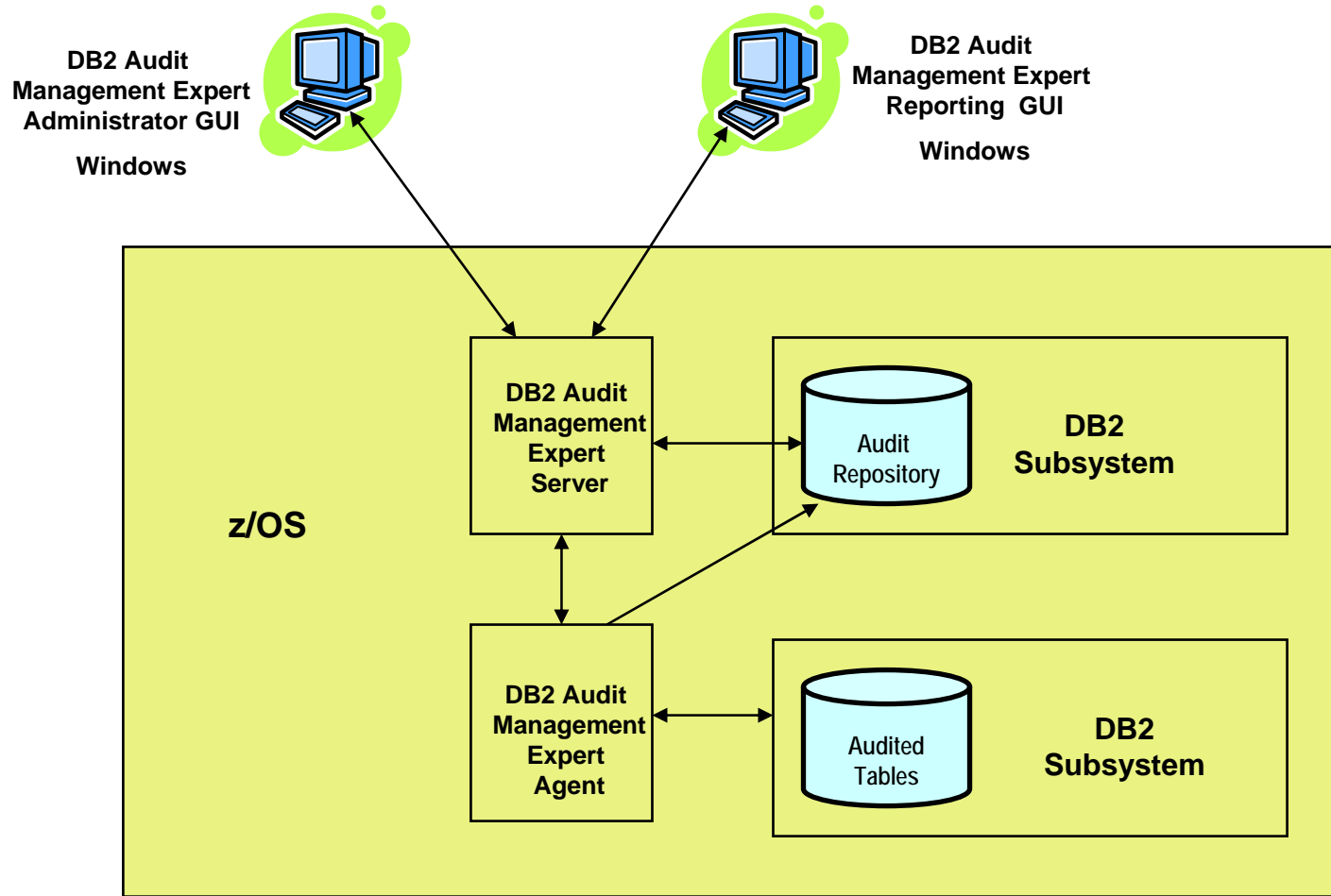
Audit Management Expert Overview

- Collects and correlates information from DB2 resources.
 - ▶ Audit Trace Data, Log Analysis data
- Provides a central resource for auditors to produce a coherent view of DB2 access information.
- Auditors will be able to Access:
 - ▶ SELECT, INSERT, UPDATE, and DELETE activity by user or by object.
 - ▶ CREATE, ALTER, and DROP operations against an audited object
 - ▶ Utility access to an audited object
 - ▶ DB2 commands entered
 - ▶ Assignment or modification of an authorization ID
- **Provides auditors with flexible options for examining the data in the audit repository.**

Security

- **Supporting internal and external auditors in collection and reporting of DB2 audit data**
- Does not require auditors to be DB2 defined users within the monitored DB2 system(s)
- Does not require the auditors to log on to the operating system where the monitored system is running
- Does not require extensive interaction between the auditor and the system support personnel (DBA/Sys admin)
- Auditor will not be able to directly manipulate any DB2 resources
- **Provide complete visibility of all auditable objects to an administrator level user**
- **Provide controls for limiting visibility to auditors of auditable objects**

DB2 Audit Management Expert Architecture



Audit Management Expert

File Edit Settings Help

Users Groups Agents Collection Profiles Collections Authorizations Repository

Username	Description	Connect to ...	Create Users	Create Grou...	Create Profil...	Edit Profiles	Assign Per...	Assign Con...	A
adhadmin	Audit Expert ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
adhlimited	Audit Expert ...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
SLUser1	Susan Super...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
linux	bahvalov	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
pddavi	Barry Davis ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

◀ ▶

Add Edit Clone Delete Refresh

Collection Profile Editor

Left sidebar: _profile2, Source, Rule 1, Schedule, General, **Targets**, Events, Identity, Plans, Summary

Tab: Tables

Target Filter

Schema: %
Name: %
Refresh

Audited targets

Type	Schema	Name
	PDWDBX4	TABLE1
	PDWDBX4	TABLE2
	PDWDBX4	TABLE3
	PDWDBX4	TABLE4

Known targets

Type	Schema	Name	Status
	ABPGG99	ABPOBJ...	Unaudited
	ABPTST...	TST01TB1	Unaudited
	ABPTST...	TST01TB2	Unaudited
	ADB	ADBCH...	Unaudited
	ADB	ADBPART	Unaudited
	ADHSCH1	ADH1T1	Audited
	ADHSCH1	ADH1T2	Audited
	ADHSCH1	ADH1T3	Audited
	ADHSCH1	ART_EM...	Audited
	ADHSCH2	ADH1T1	Unaudited

Buttons: Add, Remove, Remove All

Other targets

Type	Schema	Name

Add Other

Bottom buttons: New Rule, Delete Rule, OK, Cancel

Collection Profile Editor

AuthID | WSName | WSTran

Known authids

Included authids

Excluded authids

Other authids

Included
 Excluded

Add
 Remove
 Remove All
 Add Other

_profile2
 - Source
 - Rule 1
 - Schedule
 - General
 - Targets
 - Events
 - Identity
 - Plans
 - Summary

ABPSTC
 ADB
 ADHSPSRV
 APPCUSER
 CDKRAY
 CDKRAYA
 CSBAHA
 CSBANK
 CSBANKA
 CSBELK
 CSBELKA
 CSBICE
 CSBICEA
 CSBILL
 CSBILLA
 CSBOHNA
 CSBOWL
 CSBOWLA
 CSBOWLA

CSIVAN

New Rule Delete Rule OK Cancel

Report Options:

Date Range:

From: Calendar >
 Mon, Jul 17, 2006 Hour: 0

To: Calendar >
 Fri, Jul 21, 2006 Hour: 23

Last Summary Table Update: 07-21-2006 11:56

Selected Users:

> All Users Edit...

Activity Type:
 All

Set time period to check for Threshold:

Every Hour
 Every Day
 Every Week
 Every Month

Refresh

Edit Thresholds...

Collection History

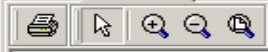
- | | | |
|---------------------------|---------------------------------|---|
| a. Access Attempts | b. First Read of Audited Object | c. First Change of Audited Object |
| d. CREATE, ALTER and DROP | e. GRANT and REVOKE | f. Assignment or change of authorization ID |
| g. IBM Utility Access | h. DB2 Commands | i. Other Authorization Failures |

Critical	Warning	Normal

Subsystem: RS23:D81B

a.	b.	c.
d.	e.	f.
g.	h.	i.

> Available Dates: 2006-7-13 to 2006-7-21



Report Options:

Date Range:

From: [Calendar >](#)

Hour:

Mon, Jul 17, 2006

0

To: [Calendar >](#)

Hour:

Fri, Jul 21, 2006

23

> Available Dates: 2006-7-13 to 2006-7-21

Subsystem:

> All Subsystems

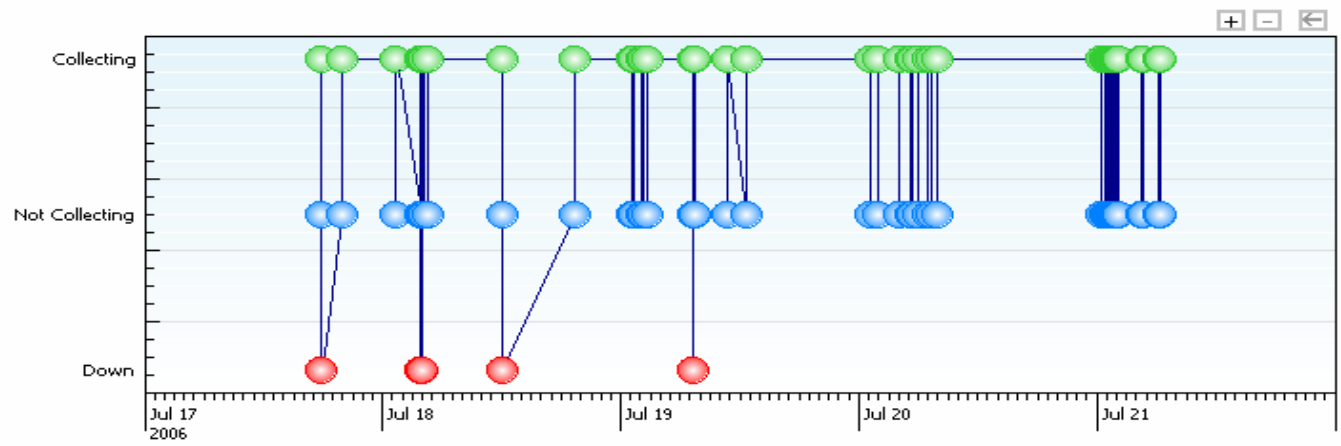
RS23:DB1B

Refresh

Display Colors...

Close

Collection Status Timeline for: > All Subsystems



Report Options:

Date Range:

From: Calendar >
 Mon, Jun 5, 2006 Hour: 0 Minute: 0

To: Calendar >
 Thu, Jun 8, 2006 Hour: 23 Minute: 59

> Available Dates: 2006-6-1 to 2006-6-9

Subsystem:
 RS23:D81A

Activity Result:
 All

Show Top Number:
 5

Drill Down Options:

- Retrieve data for selected item only
- Retrieve all currently displayed data

Time Chart Options:

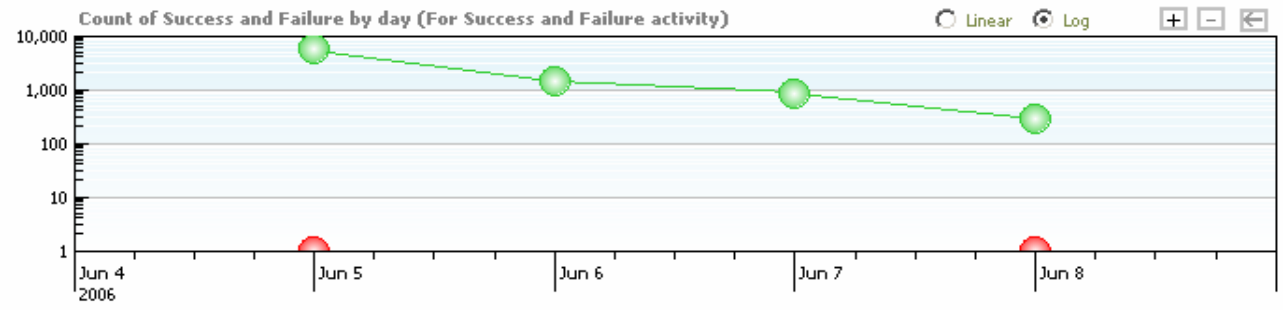
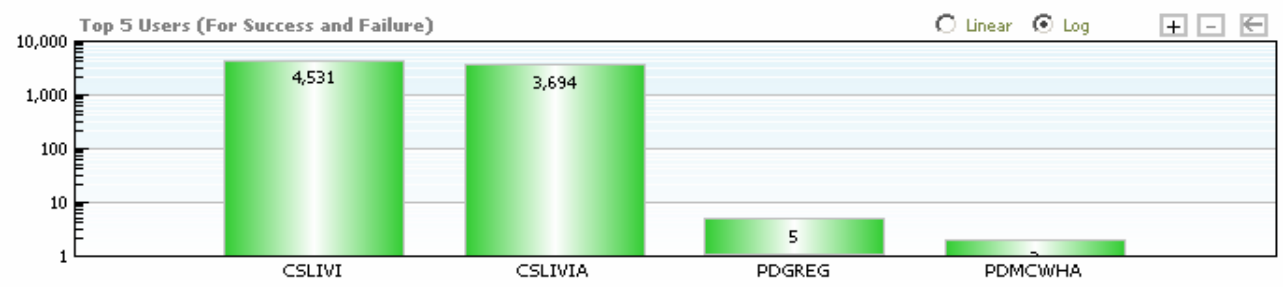
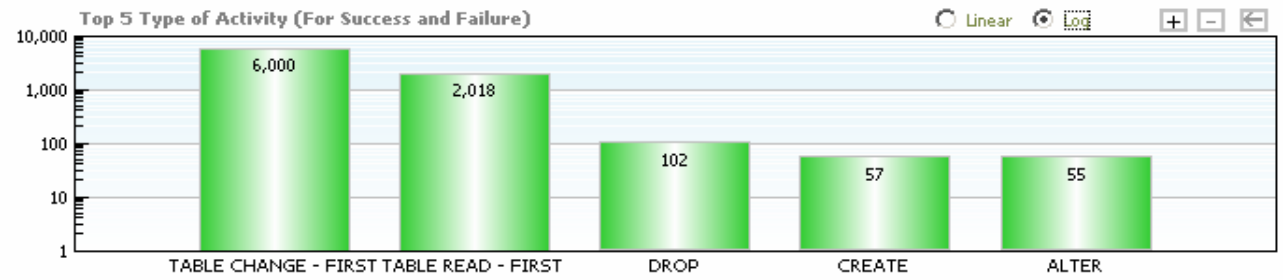
- Group Activity By Minutes
- Group Activity By Hours
- Group Activity By Days

Refresh

Filter Options... Display Colors...

Summary of Objects in subsystem: RS23:D81A

■ Success ■ Failure



DB2 Audit Management Expert Reporter

File Reports Settings Help

Log in Reporting Log Analysis



DB2 SYSTEMS
OBJECTS
DB2 AUDIT MANAGEMENT EXPERT
Welcome adhadmin

> Summary of Objects
Help
< Back

Audit Management Expert Data

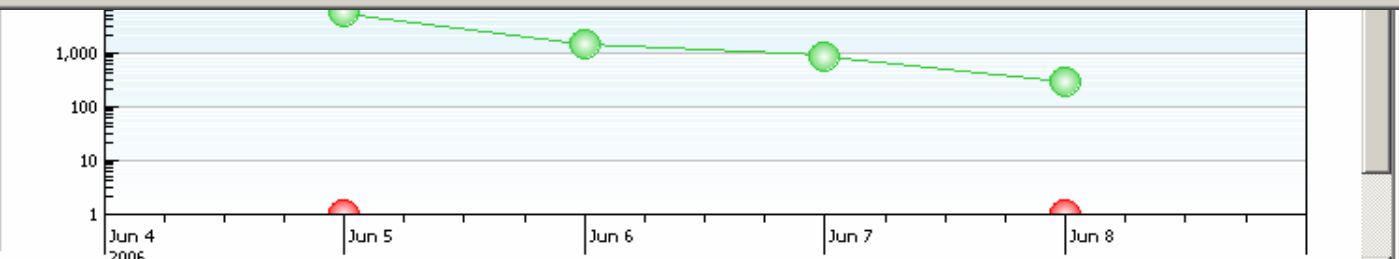
Option

Record Count: 55

TIME	RESULT	RETURNED	SCHEMA	NAME	IFICODE	CORRELATI...	CONTEXT_T...	CONTAINER	TYPE	STATEMENT_TXT
2006-06-05 11...	0	SUCCESS	CSLIVI	ART_ACT1	00142	385804688	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUC
2006-06-05 11...	0	SUCCESS	CSLIVI	ART_ACT1	00142	385799496	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUC
2006-06-05 11...	0	SUCCESS	CSLIVI	ART_ACT1	00142	385805632	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUC
2006-06-05 11...	0	SUCCESS	CSLIVI	ART_ACT1	00142	385805632	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUC
2006-06-05 11...	0	SUCCESS	CSLIVI	ART_ACT1	00142	385805632	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUC
2006-06-05 11...	0	SUCCESS	CSLIVI	ART_ACT1	00142	385796664	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUC
2006-06-05 11...	0	SUCCESS	CSLIVI	ART_ACT1	00142	385805632	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUC
2006-06-05 17...	0	SUCCESS	CSLIVI	ART_ACT1	00142	302392176	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUC
2006-06-05 17...	0	SUCCESS	CSLIVI	ART_ACT1	00142	302392176	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUC
2006-06-05 17...	0	SUCCESS	CSLIVI	ART_ACT1	00142	302394064	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUC
2006-06-05 17...	0	SUCCESS	CSLIVI	ART_ACT1	00142	302394064	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUC
2006-06-05 18...	0	SUCCESS	ADHSC830	ART_EMP	00142	302396896	ALTER	ADHTS1	TABLE/VIEW	ALTER TABLE ADHSC830.ART_EMP A

Copy Export Cancel Close

Group Activity By Minutes
 Group Activity By Hours
 Group Activity By Days



Users_Object

DB2 Audit Management Expert Reporter

File Log Analysis Settings Help

Log in Reporting Log Analysis

Welcome

Subsystem

Table

Filter

Run

Output

Save

Log Range:

From: Jul 17, 2006 00:00:00 To: Jul 21, 2006 23:59:00

Audit Management Expert typically uses the SYSLGRNX directory table to optimize which log files must be read. You can choose not to use the SYSLGRNX if errors occur when trying to use it, or if the overhead of using it will likely outweigh the savings it provides.

Use SYSLGRNX

Statement Type:

Include inserts

Include updates

Include deletes

ignore catalog tables

Report Output Options:

Optionally choose to generate a Detailed Activity Report:

Summary report

Detailed Activity Report

< Back Next >

Connected to D81B Log Analysis Filter