Greater data security and improved corporate accountability are required to meet new regulatory standards. Trusted contexts and Roles are introduced in DB2 9 for z/OS to help in the area of compliance by enforcing user accountability, end user identity at the data level, provide flexibility and simplify the management of authorization. Secure Socket Layer encryption improves security. Enterprise Identity Mapping enables products and applications to more securely and efficiently interoperate in a heterogeneous computing environment. This presentation will cover these enhancements in DB2.

Agenda

- Security objectives
- Trusted Contexts
- Roles
- Secure Socket Layer (SSL)
- Enterprise Identity Mapping (EIM)
- Improved Auditing

This presentation will review the security objectives and will go over the security enhancements in DB2 9 for z/OS.

Trusted Context and Role support will be covered with focus on usage in the area of audit and security compliance.

Trusted context provides a technique to work with other environments more easily and efficiently. Customers can use Trusted context to secure application servers and improve audit and accountability of the end user.

Role provides a more flexible technique than users and groups in assigning and controlling authorization. Customers who want to secure DBA activities with individual accountability and eliminate shared SYSADM or DBADM ids can do so using Roles in Trusted context.

Secure Socket Layer implementation provides encryption of data on the wire.

Enterprise Identity mapping provides a central place to store mappings between user IDs that are defined in different registries.

Improved audit provides the capability to see that security is functioning and also helps with compliance.

Security Objectives

- Better access control from application servers
- Provide flexibility by removing object dependency from users
- More controlled use of SYSADM
- More authority than existing privileges
- Manage objects from other user IDs
- Audit user with SYSADM / DBADM privileges
- End to end auditability of users

In a three-tier architecture model all interactions with the database server occur under middle-tier authorization ID. This results in loss of end-user identity, over granting of privileges to the middle-tier authorization ID, and weakened security. Hence, need better access control from application servers with end to end auditing of users.

When a user creates an object, the user becomes the owner. So, when the user leaves the company, in order to remove privileges from the user the object has to be dropped and recreated.

In some customer shops, a generic TSO id is created and granted SYSADM authority. This is done in order to avoid the cascading effect of revoking SYSADM when individual team members leave the organization. Unfortunately the use of the generic TSO user id does not provide the individual accountability that is now required for Sarbanes-Oxley (SOX) compliance. A function similar to shared DBADM/SYSADM is needed with auditing capability.

Also, DBADM can create view/alias for another ID, but has no DROP/ALTER privilege

Trusted Context

- Establishes trust between DB2 and an external entity such as
  - RRSAF (Resource Recovery Services Attachment Facility)
  - DSN Command Processor
  - Application Server
- Once established, a trusted connection provides the ability to
  - Efficiently switch user with optional authentication
  - Acquire special set of privileges using a Role
  - Acquire special RACF Security Label authority

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 context is to be trusted.

The relationship between a connection and a trusted context is established when a connection to the server is first created.

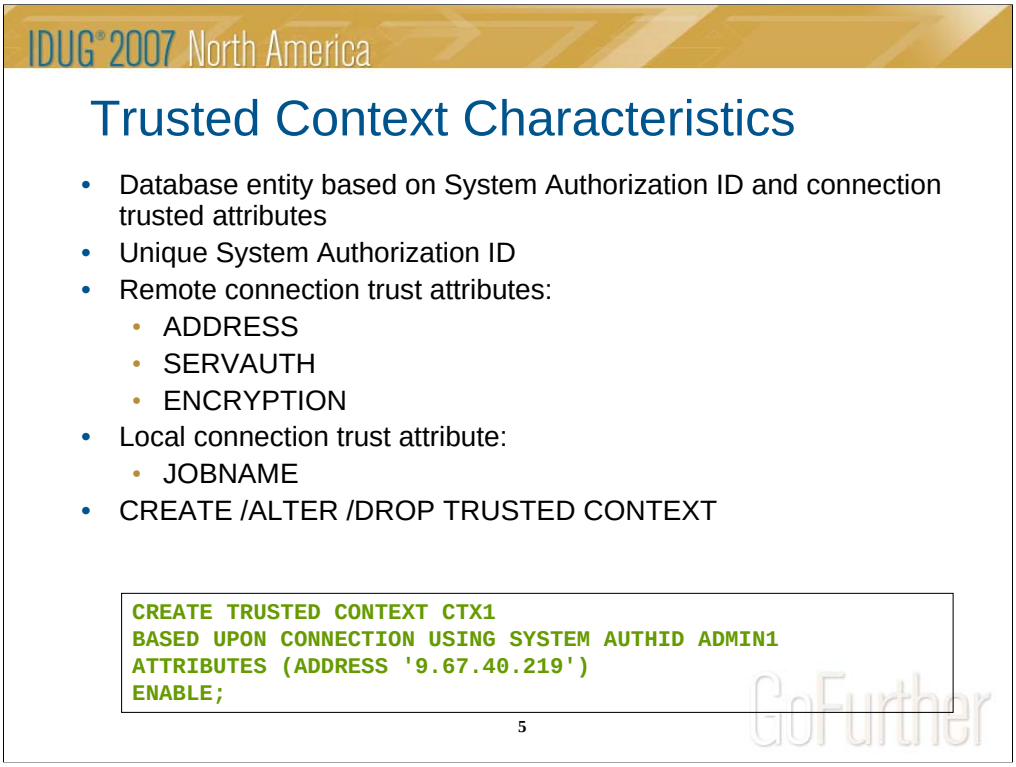
Once established, a trusted connection provides the ability to:

-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.

-Acquire security label (RACF SECLABEL) to be used for multi-level security verification. Multi-level security restricts access to an object or a row based on the security label of the object or row and the security label of the user.



To establish a remote trusted connection, SYSTEM AUTHID and attributes, ENCRYPTION and ADDRESS or SERVAUTH have to match.

The SYSTEM AUTHID is derived from the system user ID provided by e.g. a middleware server.

The attributes, ADDRESS is the client IP address or domain name [the protocol is restricted to TCP/IP only], SERVAUTH is a resource in the RACF SERVAUTH class, ENCRYPTION is the minimum level of encryption for the connection [None, Low, High].

To establish a local trusted connection, SYSTEM AUTHID and attribute, JOBNAME have to match.

SYSTEM AUTHID is typically derived from JOB statement USER or RACF USER for RRSAF applications, TSO logon ID for TSO sessions, and JOB statement USER for BATCH jobs.

The attribute JOBNAME is derived from JOB or started class name for RRSAF applications, TSO logon ID for TSO sessions, and JOB name for BATCH jobs.

Database Role

- Database entity with one or more privileges
- Established only through a trusted connection
- User assigned only one Role
  - Default Role or user specific Role
  - User specific Role takes precedence
- Auth privileges can be granted to a Role and revoked from a Role
- Can optionally be the OWNER of DB2 objects
- CREATE /DROP ROLE

```
CREATE ROLE CTXROLE;
GRANT DBADM … TO CTXROLE;

CREATE TRUSTED CONTEXT CTX1
BASED UPON CONNECTION USING SYSTEM AUTHID ADMIN1
DEFAULT ROLE CTXROLE
ATTRIBUTES (ADDRESS '9.67.40.219')
ENABLE;
```


6

Trusted context allows for the assignment of a default role to a trusted context and assignment of a role to the user of the context. Same role can be assigned in different trusted contexts.

In current DB2 security model, privileges assigned to an id is universally available. By assigning privileges to a role (for ex: SELECT) in a trusted context and allowing access to the user only when connected from certain location provides better control and flexibility on where and when and how DB2 privileges can be exercised

Roles can be assigned and removed from individuals via trusted context. This allows DBA to perform object maintenance during a change control window and then lose the role privilege when the window is shut. This is similar to shared SYSADM or DBADM user IDs, but avoids the audit compliance problems associated with shared user IDs.

Auditing trails of the work completed during the maintenance window

Drop role: Role should not own objects or part of trusted context definition or associated with the current thread.

Role Owner Of Objects

- Role owns objects
- Role must have all the privileges needed to create objects
- Users of the Role can grant/revoke for objects owned by that Role
- Statement prepared dynamically
  - Role associated with the process
- Statement embedded in a program
  - Owner (Role) of the plan or package

Since, role can own objects, revoking a person's access to a role does not cause the object to be cascade deleted.

For dynamic statements, SET CURRENT SQLID, if specified, is not considered for creating objects, when role as object owner is in effect.

Table, view, index qualifiers do not become the owner.

If the BIND OWNER option is not specified, the role associated with the binder becomes the owner. If the BIND OWNER option is specified, the role specified in the OWNER option becomes the owner.

Trusted context with a role associated, but ROLE AS OBJECT OWNER clause is not specified: Current rules for plan/package ownership apply

Trusted Context Auth ID Switching

- Allows trusted connection to be used by a different user
- Optional authentication requirement
- Specific ROLE and RACF Security Label authority for the user

```
CREATE TRUSTED CONTEXT CTX1
BASED UPON CONNECTION USING SYSTEM AUTHID ADMIN1
ATTRIBUTES (ADDRESS '9.67.40.219')
ENABLE
WITH USE FOR JOE ROLE JROLE SECURITY LABEL JLABEL;
```


The administrator must add specific users to the list of authorization IDs that can use the trusted context.

If PUBLIC is specified for the user, then it allows the trusted connection to be used by any authorization ID.

The administrator can specify if authentication is required by WITH AUTHENTICATION clause. Default: WITHOUT AUTHENTICATION.

The administrator can also specify different role and SECLABEL for the user, other than the default.

Switch Auth ID Characteristics

- Local connections
  - RRSAF SIGNON
  - DSN ASUSER
  - SQL CONNECT USER/USING
- Remote connections
  - For z/OS applications, users are switched automatically based on catalog definition in the Communications Database (CDB) tables
  - For JDBC and CLI applications, users are switched using the new APIs

DB2 determines if primary authorization ID is allowed to switch in the trusted context based on AUTHENTICATION parameter in the trusted context definition and SECURITY LABEL verification, if defined.

If primary authorization ID does not have access to the trusted context, then the connection request fails and returns to an unconnected state

SPUFI: DSN ASUSER

```
DSNEOP01                  DB2I DEFAULTS PANEL 1
COMMAND ===>

Change defaults as desired:

1 DB2 NAME .............  ===> DSN       (Subsystem identifier)
2 DB2 CONNECTION RETRIES  ===> 0         (How many retries for DB2
connection)
3 APPLICATION LANGUAGE    ===> IBMCOB    (ASM, C, CPP, IBMCOB, FORTRAN, PLI)
4 LINES/PAGE OF LISTING   ===> 60        (A number from 5 to 999)
5 MESSAGE LEVEL ........  ===> I         (Information, Warning, Error,
Severe)
6 SQL STRING DELIMITER    ===> DEFAULT   (DEFAULT, ' or ")
7 DECIMAL POINT ........  ===> .         (. or ,)
8 STOP IF RETURN CODE >=  ===> 8         (Lowest terminating return code)
9 NUMBER OF ROWS .......  ===> 20        (For ISPF Tables)
10 CHANGE HELP BOOK NAMES?===> NO        (YES to change HELP data set names)
11 AS USER                ===>           (Userid to associate with the
                                           trusted connection)
PRESS: ENTER to process END to cancel HELP for more information
```


A new option, ASUSER is added to the DSN command. The ASUSER option provides the capability to switch user on an established trusted connection without authentication information. This facilitates DBADM to perform view/alias maintenance on behalf of other users.

Secure Socket Layer (SSL)

- DB2 Server can listen on secondary secure port for SSL connections
- DB2 requester can be configured to use SSL connections to other servers
- Prerequisite:
  - Communication server implementation of AT-TLS (Application Transparent Transport Layer Security)
  - Policy defined in communication server
- Trusted context attribute ENCRYPTION 'HIGH' corresponds to SSL encryption validation.

Server:

Secure port is specified using DSNTIP5 installation panel or DSNJU003 BSDS DDF record

Requester:

SYSIBM.LOCATIONS new SECURE column should be set to 'Y'

PORT column should be the remote server's SECPORT. If not specified default port 448 is used.

Data sharing considerations:

Each DB2 member that needs SSL support must specify a secure port and should be the same as the secure port for other members in the group.

Location Alias consideration

At the requester CDB, define two rows in SYSIBM.LOCATIONS table. One specifying the location name to be used for non-secure communications and the other specifying different location name to be used for secure communications

At the server, define a location alias for DB2 requester to access the server using SSL.

Enterprise Identity Mapping (EIM)

- Needed when user registries are different and not shared between systems
- Exploits RACF Security Server user mapping plug-in service
  - Retrieves RACF user ID (DB2 primary authorization ID) from the client user ID
- Enhances the auditing of end user identities
  - Client user ID and DB2 auth ID are included in DB2 and RACF audit records

Identity mapping is a one-to-one mapping of a user identity between two servers, so that the proper authorization decisions are made by the downstream servers such as a DB2 z/OS server.

The default implementation of the z/OS Security Server RACF (SAF) user mapping plug-in makes use of EIM domain on z/OS. EIM is a LDAP server, which acts as a repository of mappings between an authenticated user registry name and a z/OS user ID.

For DB2 to use the SAF user mapping plug-in, you need to set up and configure an EIM domain with user registries and user ID mappings on the z/OS system

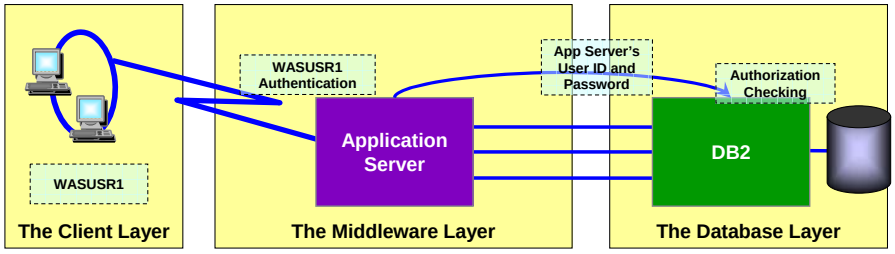
To enhance the auditing of user identities who authenticate themselves in a distributed security domain and then access resources on a z/OS system, DB2 provides the original end user identity and the authenticated source registry name (Identity Context) to be included in RACF audit records.

z/OS V1.8 or later is required for EIM.

More details about EIM can be found at:

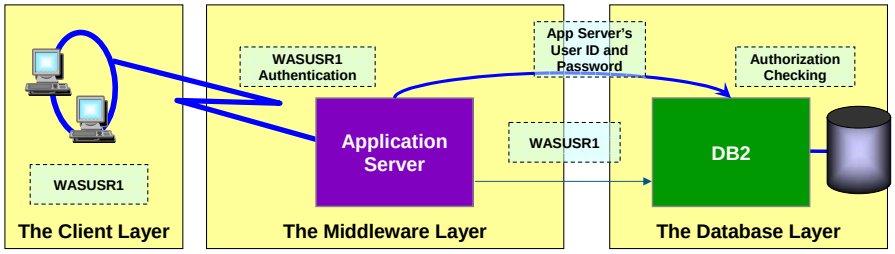
http://www-1.ibm.com/servers/eserver/security/eim/

Current Authentication in a Three-Tier Architecture



- In a typical three-tiered application model with DB2 as the database server, the middle layer
  - Authenticates users running client applications
  - Manages interactions with DB2
- The application server's user ID and password are used for authentication purposes
- The application server authorization ID's database privileges are checked for access on behalf of all end-users

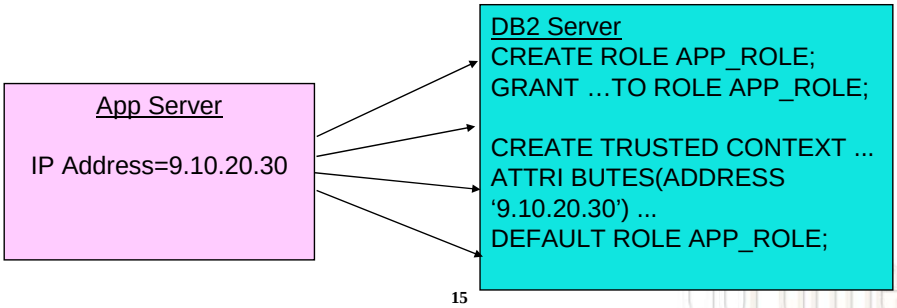
Trusted Authentication in a Three-tier Architecture



- The application server's user ID and password are used to establish the trusted connection.
- The user is switched in the trusted connection and client user ID is propagated to the server
- The client authorization ID's privileges are checked for database access

Usage 1: Securing an App Server

- App server system auth ID is granted the needed privileges for all the actions performed by end users
- Trusted context and role can be used to limit the exposure
  - Privileges can be granted to a role
  - Access can be restricted so that they are only valid when used by a valid app server IP address
- No change needed to the code in the application server

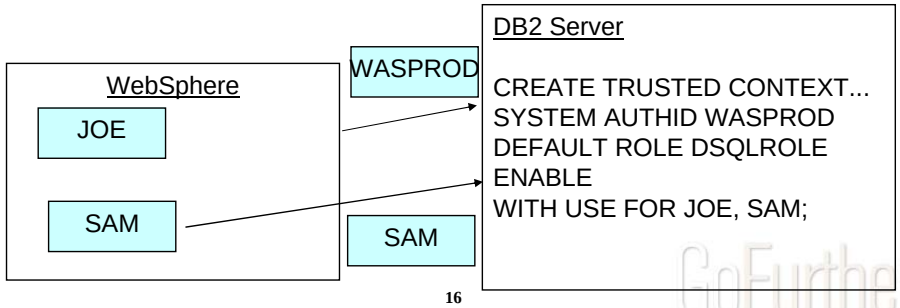


15

Role and Trusted Context can be used to provide added security for network-attached application servers. These new capabilities allow the DBA to make GRANT statements conditional, so that they can only be used if connection is established from a specified list of IP addresses. If someone steals the application server's userid/password, they won't be able to access the database server unless they are also able to execute the SQL statement on one of the approved application servers.

Usage 2: Dynamic SQL Auditing

- GRANT dynamic SQL privileges to a ROLE
- End user passwords can be optional
- No added complexity for administration of GRANTs, while retaining the ability to audit the end user's identity



Role and Trusted Context also enable customers to improve DB2 system auditing. Today, many customers use a "system" user id to access DB2 so that they don't have to grant dynamic SQL privileges to their end users.
With V9, customers will be able to grant dynamic SQL table privileges to a ROLE, and specify that the end user can only use that ROLE when the end user is running on an approved application server.
The benefits are:
A ROLE can be used as a single database authid that can be used to simplify administration of dynamic SQL privileges.
The end user's authid can be used to run database transactions, so that the DB2 audit is able to identify the end users individually (important capability for meeting some regulatory compliance requirements).

Usage 3: Secure DBA Activities

- Customers concerned about DBA access to sensitive data.
- An auditable DBA process can be done with trusted context and role:
  - Grant DBA privileges to a Role, AuditRole
  - When a DBA needs to perform a system change:
    - Create trusted context to assign AuditRole to a DBA auth ID
    - Enable trusted context to allow access to sensitive objects
    - DBA connects and performs activity against sensitive objects
    - Disable trusted context to protect sensitive objects
  - An auditor can review the audit trace

Using trusted context and role, DBA privileges can easily be disconnected and reconnected to individual employees. This provides function similar to shared SYSADM or DBADM user ids, but avoids the audit compliance problems associated with shared user ids.

Role has the ability to “own” DB2 objects, so that revoking a person’s ROLE does not cause the objects to be cascade deleted.

With these capabilities, customers are able to create DBA procedures that can be audited and protected so that one individual cannot violate the established rules without being detected during the audit review.

Usage 4: View Maintenance

- DBADM who created view for other IDs can DROP/ALTER view owned by that other IDs

```
 CREATE TRUSTED CONTEXT CTXLOCAL
  BASED UPON CONNECTION USING SYSTEM AUTHID PRODDBA1
  ATTRIBUTES (JOBNAME 'PRODDBA1')
  ENABLE
  WITH USE FOR PRODOWNR;

//PRODDBA1 JOB  USER='PRODDBA1'
//IKJEFT1B EXEC PGM=IKJEFT1B
//SYSTSPRT DD   SYSOUT=*
//SYSPRINT DD   SYSOUT=*
//SYSTSIN  DD   *
  DSN SYSTEM(DB1P) ASUSER(PRODOWNR)
  END
//SYSIN    DD   *
  ALTER VIEW PRODVIEW REGENERATE;
  COMMIT ;
//
```


DBADM under certain circumstances can create view for others. However, this same DBADM is not able to drop or grant privileges on these views to others. Since views do not have an underlying database, DBADM can not be recognized for views.

A trusted context can allow DBADM or any other permitted user to assume the identity of another user like view owner and then perform the desired actions.

To accomplish view maintenance on behalf of other user, create a trusted context at local DB2 with DBADM id as SYSTEM AUTHID and switch to view owner id.

Usage 5: Roles and Secondary Auth IDs

- RACF groups and roles can complement each other

```
Create a RACF group called PROD_BASIC – Assign basic DB2
privileges

CREATE ROLE PROD_LOAN_ROLE;

CREATE TRUSTED CONTEXT CTXLOCAL
  BASED UPON CONNECTION USING SYSTEM AUTHID PRODDBA1
  ATTRIBUTES (JOBNAME 'PRODDBA1')
  DEFAULT ROLE PROD_LOAN_ROLE WITH ROLE AS OBJECT OWNER
  ENABLE;
```

Best Practice: Ownership and authorization to groups and roles.

For the purpose of managing authorizations, roles are more flexible than groups or users.

Suppose there is a team of 5 production DBAs who maintain databases. The DBAs could acquire basic DB2 privileges like access to the catalog, some display capabilities, but no access to data or utilities through RACF group

The role, PROD_LOAN_ROLE is granted DBADM against application database, LOAN.

Each DBA could have a context defined with their user ID with default role PROD_LOAN_ROLE with ROLE as OBJECT OWNER. The context is disabled.

When the LOAN database needs to be enhanced and there is an implementation scheduled, one of the 5 DBA's context can be enabled.

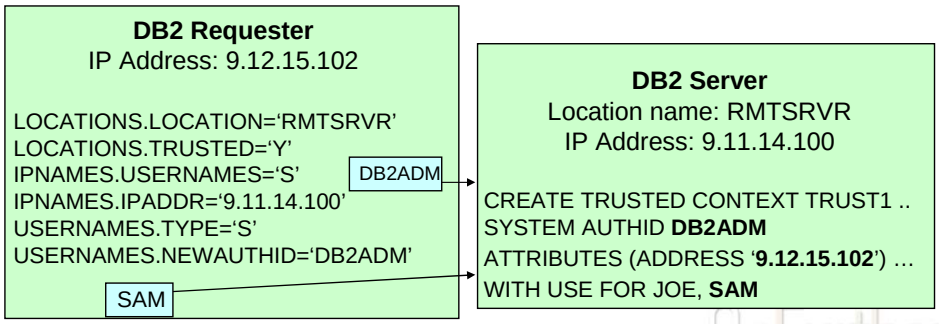
On the implementation weekend, the DBA acquires the required privileges which are in addition to what is available via the PROD_BASIC secondary auth ID.

Using a trusted connection the DBA makes the change and when the implementation is complete, the DBA's trusted context is disabled.

With this approach the objects in the LOAN database are always structurally changed via the role and the role owns all the objects in the LOAN database

Usage 6: z/OS Trusted Application

- Communications Database is configured for trusted connection and to specify “SYSTEM AUTHID” for the trusted connection
- End user identity is automatically propagated if SYSTEM AUTHID is different from the application end user

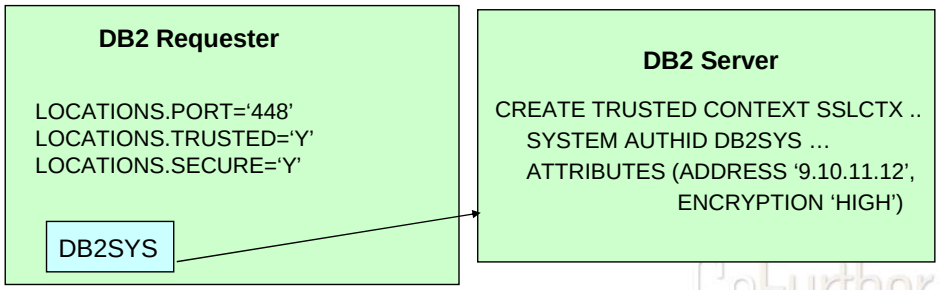


20

Trusted connection can be established from DB2 requester by configuring the communications database (CDB) tables with the new options. If the server returns a warning indicating that trusted connection can not be established, then a normal connection is established with out any additional privileges.

Usage 7: z/OS Application – SSL and Trusted Context

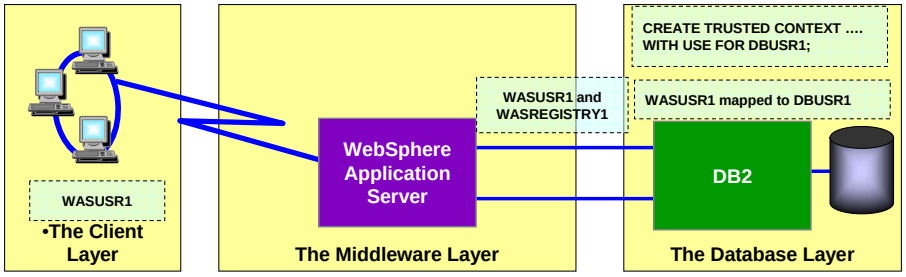
- Configure communication AT-TLS layer at the DB2 requester and server
- At the DB2 z/OS requester
  - Set Secure column in the SYSIBM.LOCATIONS table to 'Y'
  - Configure SYSIBM.IPNAMES and SYSIBM.USERNAMES tables
- Create trusted context at the server



21

See chapter 9 in the Securing DB2 and Implementing MLS on z/OS (SG24-6480-01) redbook for establishing SSL connection from WebSphere.

Usage 8: WebSphere – EIM and Trusted Context



- Configure WebSphere app server to create trusted connection and send the registry name to the server
- DB2 maps the registry name and client user ID to obtain DB2 auth ID
- DB2 checks if the DB2 auth ID is allowed to use the trusted connection
- Client user ID, DB2 auth ID, and registry name are recorded in RACF audit records

Trusted connection is established using application server's user id and password. The user is switched in the trusted connection and client id and registry name are sent to the DB2 server. DB2 maps the registry name and client id to obtain DB2 authorization id. DB2 authorization id is used to determine if the user is allowed to switch in the trusted connection.

See chapter 9 and appendix B in the Securing DB2 and Implementing MLS on z/OS (SG24-6480-01) redbook for more information on EIM scenario.

Improved Audit: Trace (IFCID) changes

- Correlation Header - Trusted context name, role name, original application user, security token
- IFCID 062 -Statement and object types for trusted contexts and roles
- New ID type is added to distinguish between auth ID and role:
  - IFCID 140 – Auth ID checked type
  - IFCID 141 – Grantor / Revoker type
  - IFCID 142 – Table owner type
- IFCID 169 – Identifier type 'S' traces system auth ID translation
- New Audit Trace Class 10
  - IFCID 269 – Establish trusted connection and Switch user
  - IFCID 270 – CREATE and ALTER TRUSTED CONTEXT statements
- IFCID 314 – Role name

The accounting, performance, audit, and monitor trace records can have a correlation header. The correlation header can now trace trusted context name, role name, original application user and security token.

IFCID 062 (Performance class 3) traces SQL events. IFCID 140 (Audit class 1) traces access attempts denied due to inadequate authorization. IFCID 141 (Audit class 2) traces explicit GRANTs and REVOKEs. IFCID 142 (Audit class 3) traces CREATE, ALTER, and DROP operations against audited tables. IFCID 169 (Audit class 7) traces assignment or change of authorization IDs. IFCID 314 (Performance class 22) traces authorization exit parameters. These traces have been modified to include information about the use of trusted contexts and roles.

Traces can be formatted using programs like DB2 Audit Management Expert and IBM Tivoli OMEGAMON XE for DB2 Performance Expert/Monitor on z/OS V410.

For more information about auditing, see DB2 V9.1 for z/OS Administration Guide (SC18-9840)

http://www.ibm.com/software/data/db2/zos/library.html

Improved Audit: Trace INCLUDE Filtering

- -START TRACE new filtering capabilities that INCLUDE based on the keywords:
  - USERID – client user ID
  - WRKSTN – client workstation name
  - APPNAME – client application name
  - PKGLOC – package LOCATION name
  - PKGCOL – package COLLECTION name
  - PKGPROG – PACKAGE name
  - CONNID – connection ID
  - CORRID – correlation ID
  - ROLE – end user's database Role
- Positional and terminating wildcards can be used

```
-STA TRACE … ROLE(DBAROLE, USRROLE)
-STA TRACE(ACCTG) CLASS(1,2,3) AUTHID(A_M*)
```


Originally filtering can be done using PLAN, AUTHID, LOCATION, and RMID. The new filtering capabilities provide greater flexibility.

Starting a trace with multiple arguments for any keyword will start one trace for each argument using OR logic.

Starting a trace with multiple arguments for any keyword starts one trace using AND logic.

Trace Filtering considerations:

For EXCLUDE keywords, a maximum of 8 arguments is allowed.

Combining 'EXCLUDE' and 'INCLUDE' filtering keywords produces AND combined qualifications. For example:

> -START TRACE(A) XPLAN(A,B,C) CORRID(D) would have 4 AND combined qualifications.
>
> -START TRACE(A) XPLAN(A,B) CORRID(D,E) would start 2 traces, each with 3 AND combined qualifications.

Any given trace can have at most 16 AND combined qualifications.

> If this number is exceeded, new message '`DSNW169I THE MAXIMUM OF 16 TRACE QUALIFICATIONS FOR A TRACE HAS BEEN EXCEEDED`' is issued, and the command does not complete.

Improved Audit: Trace Enhancements

- -DISPLAY TRACE DETAIL(2)
  - Displays EXCLUDE filtering details
- IFI READS interface
  - The WQAL block, as mapped by the DSNDWQAL macro, is changed to allow the specification of Roles
  - IFCIDs 124, 147, 148, and 150, which can be read via READS are eligible for filtering with the new qualifications.

The instrumentation facility interface (IFI) is designed for a program needing online trace information. The IFI READS function obtains monitor trace records synchronously. On READS requests, the qualification area, as mapped by DSNDQWAL macro, can be used by the monitor program to specify constraints on the data to be returned. This macro is changed to allow the specification of Roles.

IFCID 124 – Traces current SQL statement

IFCIDs 147, 148, and 150 – Monitor trace records

IFCIDs themselves are not modified. They are eligible to be filtered using the new qualifications.

If you have a program which reads trace records via IFI and want to exploit the new WQAL filters, then your program needs to be modified.

Summary

- Better manageability
- Better user accountability without compromising performance
- Improved security
- Improved compliance

Manageability

Selective access to applications is possible by enabling access control over objects within a trusted context that are not available to it outside.

Eliminates the need to manage multiple passwords at the client

Role object ownership eliminates object dependency on authorization IDs

Provide DBADM authority to perform CREATE, DROP, GRANT on aliases and views created for others

User accountability

Knowing end user's identity provides improved data access auditing capability - Sarbanes-Oxley (SOX) compliance.

Role object ownership can be used to eliminate shared user IDs and have each person audited and accountable with their own authorization IDs

Improved Security

Eliminates the concern about misusing the application servers "system authid" credentials to access the DB2 server

Allows authorization IDs to perform only the approved activities by allowing privileges granted to authorization IDs to be restricted

References

- DB2 V9.1 for z/OS publications:
  - Administration Guide (SC18-9840)
  - Application Programming and SQL Guide (SC18-9841)
  - Application Programming Guide and Reference for Java (SC18-9842)
  - Command Reference (SC18-9844)
  - Data Sharing: Planning and Administration (SC18-9845)
  - Installation Guide (GC18-9846)
  - RACF Access Control Module Guide (SC18-9852)
  - SQL Reference (SC18-9854)
  - Utility Guide & Reference (SC18-9855)
  - XML Guide (SC18-9858)
- DB2 information website:
  http://www.ibm.com/software/data/db2/zos/library.html

Here are some additional pointers for information about DB2

References

- Security Server (RACF) publications:
  - RACF Command Language Reference (SA22-7687)
  - RACF Security Administrator's Guide (SA22-7683)
  - RACF Callable Services Guide (SA22-7691)
  - z/OS Integrated Security Services LDAP Administration and Use (SC24-5923)
  - z/OS Integrated Security Services LDAP Client Programming (SC24-5924)
  - z/OS Integrated Security Services Enterprise Identity Mapping (EIM) Guide and Reference (SA22-7875)
- z/OS Publications
  - z/OS Communications Server: IP Configuration Guide (SC31-8775)
- z/OS information website

  http://www.ibm.com/servers/eserver/zseries/zos/bkserv/

Here are some additional pointers for information about RACF

Updated Redbook

SG24-6480-01

Trusted Context
Roles
Multilevel security

30

Today's computing environment is subject to increasing regulatory pressures and potentially malicious attacks. Regulatory compliance, security and audit are in the daily headlines and growing more prominent. We have a responsibility to secure all business data and especially sensitive customer data. DB2 V9 for z/OS, z/OS 1.8, and RACF provide additional capability while assisting with security management.

In this book, an update is provided to major existing security functionality covering RACF, Multilevel Security, Security Labels, and DB2 row level security. This book explains how to use the Vanguard Administrator software (third party) to facilitate/simplify implementation of MLS and security labels. Some significant new DB2 functionalities, Network Trusted Contexts and Roles are also described.

The Redbook is located at http://www.redbooks.ibm.com/

Disclaimer and Trademarks

Information contained in this material has not been submitted to any formal IBM review and is distributed on "as is" basis without any warranty either expressed or implied. Measurements data have been obtained in laboratory environment. Information in this presentation about IBM's future plans reflect current thinking and is subject to change at IBM's business discretion. You should not rely on such information to make business plans. The use of this information is a customer responsibility.

IBM MAY HAVE PATENTS OR PENDING PATENT APPLICATIONS COVERING SUBJECT MATTER IN THIS DOCUMENT. THE FURNISHING OF THIS DOCUMENT DOES NOT IMPLY GIVING LICENSE TO THESE PATENTS.

TRADEMARKS: THE FOLLOWING TERMS ARE TRADEMARKS OR ® REGISTERED TRADEMARKS OF THE IBM CORPORATION IN THE UNITED STATES AND/OR OTHER COUNTRIES: AIX, AS/400, DATABASE 2, DB2, e-business logo, Enterprise Storage Server, ESCON, FICON, OS/390, OS/400, ES/9000, MVS/ESA, Netfinity, RISC, RISC SYSTEM/6000, iSeries, pSeries, xSeries, SYSTEM/390, IBM, Lotus, NOTES, WebSphere, z/Architecture, z/OS, zSeries,

The FOLLOWING TERMS ARE TRADEMARKS OR REGISTERED TRADEMARKS OF THE MICROSOFT CORPORATION IN THE UNITED STATES AND/OR OTHER COUNTRIES: MICROSOFT, WINDOWS, WINDOWS NT, ODBC, WINDOWS 95

For additional information see ibm.com/legal/copytrade.phtml

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in the 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 measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only. This information may contain 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.

Session: C08

Security enhancements in DB2 9 for z/OS

Gayathiri Chandran

IBM

gchandran@us.ibm.com

GoFurther