IDUG

IDUG 2024 NA Db2 Tech Conference ZLN6 Unlock the new security functions in Db2 for z/OS

Speaker: Gayathiri (Gaya) Chandran

IBM

@IDUGDb2
#IDUG_NA24

Session Code: ZLN6 | Platform: z/OS

Agenda – Db2 13 for z/OS Security

Compliance

- IBM Z Security and Compliance Center Support
- CIS IBM 13 for z/OS Benchmark

Remote Access Security

- Granular filtering for monitoring secure connectivity with profiles
- Token-based authentication using RACF Identity Token (IDT) capability
- Cross-Origin Resource Sharing (CORS) support for Db2 REST services
- JDBC T2 driver Password phrase support

Data Access Security

- Temporal on security-related catalog tables
- Increased flexibility for object owner management
- Plan Authorization Cache
- View management authorization
- DISPLAY privilege enhancement for Db2 Commands

Compliance

Db2 13 for z/OS Enhancements

Compliance Challenges

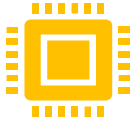
Interpret Regulations

Determine which regulations are relevant for your organization

Map IBM zSystems capabilities to those regulations

Easily show how IBM zSystems & IBM® LinuxONE capabilities meet or exceed industry standards.

Implement Controls



Discover new IBM zSystems capabilities to meet compliance

Engage IBM experts to deploy new features and submit RFEs to request new capabilities

Utilize new capabilities throughout the IBM stack to meet compliance.

Collect & Validate Evidence

Identify which data is essential for auditors.

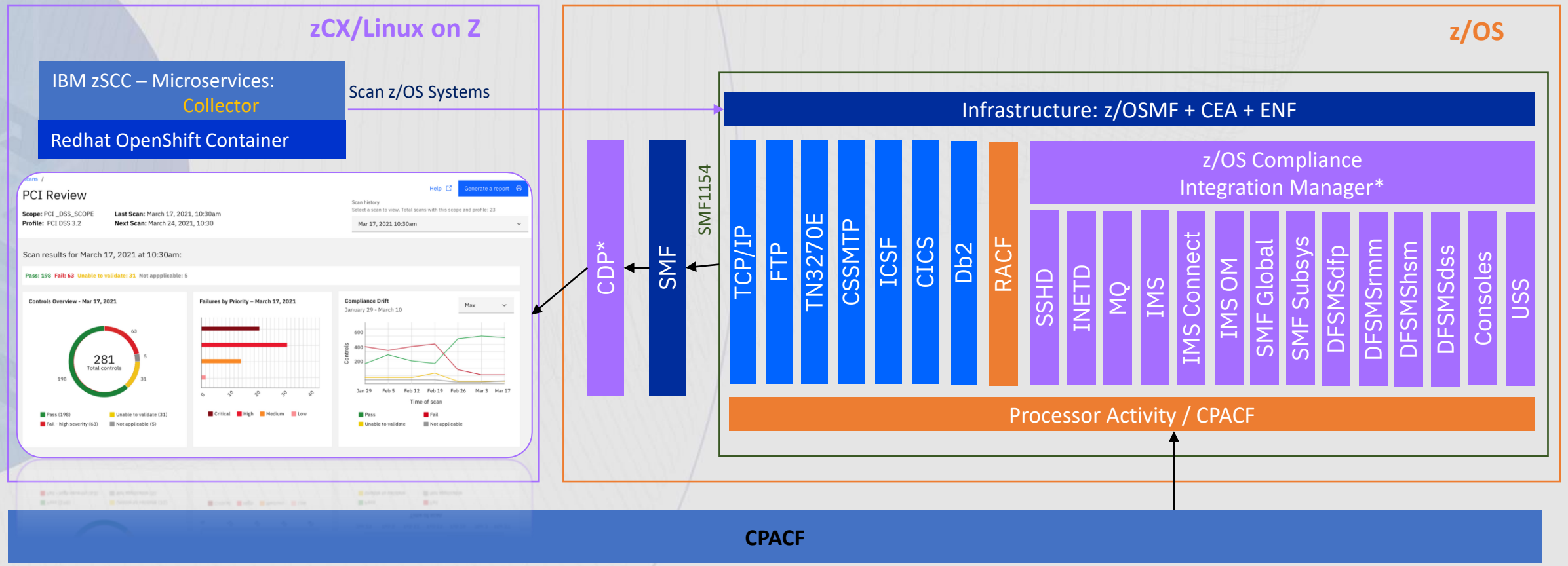
Regularly collect and validate compliance data

Optimize your audit process to reduce time and effort.

IBM Z Security and Compliance Center Solution

IBM Z Security & Compliance Center collectors connect to a resource, such as z/OS or Linux on Z, and scan for compliance data. For z/OS, the collector connects to a z/OSMF compliance REST API which triggers sysplex-wide compliance data collection using an ENF86 signal.

Participating z/OS components and products listen for the new ENF86 signal. When received, these components write compliance data to SMF 1154 records associated with a unique subtype. The SMF records are streamed to IBM Z Security & Compliance Center using the Common Data Provider. Then, the IBM Z Security & Compliance Center maps the compliance data to the appropriate regulatory controls associated with a profile for validation, display and reporting.



* The z/OS Compliance Integration Manager and CDP are delivered with the IBM Z Security & Compliance Center

Db2 for z/OS Goals: SMF 1154 Subtype 81 Records

- Db2 collects and writes SMF 1154 subtype 81 records on receiving an ENF 86 signal
- SMF 1154 subtype 81 records contain information to determine whether:
  - The installation specified default ID has been changed
  - The security port is configured
  - Authorization is enabled
  - Administrator authority is granted to a user, when native Db2 authorization is used
  - A RACF® user access change is reflected in Db2
  - Db2 is properly configured to terminate idle server threads
  - All remote connections to Db2 require secure credentials

Db2 SMF 1154 subtype 81 format:

https://www.ibm.com/docs/en/db2-for-zos/13?topic=dezcc-db2-data-smf-record-type-1154-x482-zos-compliance-evidence

CIS IBM Db2 13 for z/OS Benchmark

- CIS (Center for Internet Security) - Industry recognized standard that provides recommendations for establishing a secure configuration

- Db2 for z/OS Recommendations:
  - Installation and Configuration
  - Secure the database
  - Audit

CIS Db2 13 for z/OS Benchmark is available to download at:

https://downloads.cisecurity.org/#/

https://ncp.nist.gov/repository?sortBy=modifiedDate%7Cdesc&keyword=DB2
https://ncp.nist.gov/repository?sortBy=modifiedDate%7Cdesc&keyword=z%2FOS

Data Access Security

Db2 13 for z/OS Enhancements

Temporal on security-related catalog tables

Challenge

It is not easy to provide point-in-time evidence to address audit issues related to privilege management and security objects management such as changes to trusted contexts, audit policies, row permissions, and column masks

Temporal on security-related catalog tables

Support system-period temporal on the security-related catalog tables:

- SYSAUDITPOLICIES
- SYSCONTROLS
- SYSCONTEXT, SYSCONTEXTAUTHIDS, SYSCTXTTRUSTATTRS, SYSROLES
- SYSCOLAUTH, SYSDBAUTH, SYSPACKAUTH, SYSPLANAUTH, SYSRESAUTH, SYSROUTINEAUTH, SYSSCHEMAAUTH, SYSSEQUENCEAUTH, SYSTABAUTH, SYSUSERAUTH, SYSVARIABLEAUTH

Requires APAR PH59531 / PH60582

Enabling and Disabling Temporal

- Temporal support can be enabled using the ALTER TABLE statement ADD VERSIONING clause
  - Requires APPLCOMPAT V13R1M505
  - Requires SECADM authority (regardless of SEPARATE_SECURITY setting)
  - Enabling temporal is optional and can be enabled on one or more of the security-related catalog tables
- Temporal support can be disabled using the ALTER TABLE statement DROP VERSIONING clause
  - No specific APPLCOMPAT level required
  - Requires SECADM authority (regardless of SEPARATE_SECURITY setting)

```
ALTER TABLE SYSIBM.SYSTABAUTH
  ADD VERSIONING
  USE HISTORY TABLE SYSIBM.SYSTABAUTH_H;
```

Managing History Tables

- Operations that can add an entry to the corresponding security-related catalog history tables:
  - SQL statements: ALTER, DROP, REPLACE PROCEDURE, REVOKE, TRANSFER OWNERSHIP, UPDATE, DELETE from SYSIBM.SYSAUDITPOLICIES
  - Commands: BIND / REBIND PACKAGE /PLAN OWNER change, FREE
  - If insert into the history tables fails, Db2 will fail the SQL or command that triggered the operation.

- REORG TABLESPACE utility DISCARD option can be used to delete rows from the security-related catalog history tables
  - Requires Function Level V13R1M505
  - Requires SECADM authority (regardless of SEPARATE_SECURITY setting), in addition to REORG privilege

Increased Flexibility for Object Ownership

Challenge

A Db2 for z/OS DBA who manages plans, packages, and SQL routines cannot control the owner of those plans, packages, and SQL routine packages when using both a role and an authorization ID. Difficult to migrate to role-based security and achieve better compliance.

Increased Flexibility for object ownership

- Plans, Packages, and SQL routine packages can be owned by an authorization ID or a role regardless of the context specification
  - Provides flexibility for the adoption of trusted context and roles
  - Allows ownership of plans, packages, SQL routine packages to align with the organization policies
- Specified owner can be identified as:
  - ROLE that exists at the current server
  - USER that is an authorization ID

Increased Flexibility for object ownership

- SQL Routine Package owner type (AS ROLE / AS USER) can be specified for:
  - CREATE and ALTER compiled SQL scalar function
  - CREATE and ALTER native SQL procedure
  - Requires APPLCOMPAT V13R1M500
- New OWNERTYPE option can be specified for:
  - BIND and REBIND PACKAGE
  - BIND and REBIND PLAN
  - BIND SERVICE
  - Requires function level V13R1M500

Plan Authorization Cache Enhancements

Challenge

Db2 for z/OS system is impacted by performance issues due to plan authorization cache limitations such as plan authorization cache misses when using native security and lack of support for external security.

Plan Authorization Cache - Performance

- Statistics record Counters for plan authorization cache
  - QTAUCCH – Successful auth check for plans using a plan cache or PUBLIC
  - QTAUPUB – Successful auth checks for plan execute privilege held by PUBLIC
    - Not applicable when using external security for authorization
  - (New) QTAUCNOT – Checks that could not make use of the cache
  - (New) QTAUCOW1 – Number of times Db2 overwrote an auth ID in the cache
- Smarter Algorithm for Authorization ID management
  - Algorithm used to calculate the number of authorization IDs per plan cache enhanced to store more IDs
  - Authorization ID entries in the cache dynamically updated based on the size
- Cache Management
  - AUTHCACH subsystem parameter is removed. Default cache size is 4K per plan.
  - Can be controlled using the BIND PLAN command CACHESIZE option at the plan level.

Plan Authorization Cache and External Security

- Supports plan authorization caching when external security is used for access control
- Successful EXECUTE on a plan is cached, when access is allowed due to a profile in the RACF resource class for plan
  - Example: RACF MDSNPN class
- Requirements:
  - z/OS version 2.5 or later
  - System parameter, AUTHEXIT_CACHEREFRESH is set to ALL
- Cache entry refreshed when ENF signal is issued for:
  - User profile change (ENF Type 71)
  - Refresh plan resource access change (ENF Type 62 and Type 79)

View Management Authorization

Challenge

A Db2 for z/OS database administrator (DBA) with DBADM authority on databases cannot manage views that the DBA created for other users. These views are created based on one or more tables in any of the databases where the DBADM authority is held. The DBA requires elevated system-level authority to manage these views, which raises audit concern.

View Management Authorization

Enhanced Authorization for SELECT from a view and DROP a view, in addition to the existing privilege checks.

- Available in function level *V13R1M100*
- Required APARs: PH54863 (Db2); PH54936 (RACF Exit)

SELECT from a view:

- Required privileges such as SELECT for each table or view and EXECUTE for each function that is identified in the fullselect of the CREATE VIEW statement

DROP a view:

- DBADM authority on the database that contains one of the tables identified in the fullselect of the CREATE VIEW statement and the primary authorization ID that created the view

SYSIBM.SYSVIEWDEP table

- Can identify the objects that the user must have the required privileges on.

DISPLAY Privilege Enhancement

Challenge

An elevated system level authority is needed to issue DISPLAY commands such as DISPLAY PROFILE, DISPLAY ML. This raises audit concern and does not satisfy the minimum privilege requirement.

DISPLAY Privilege Enhancement

DISPLAY privilege added as an additional privilege that can be used to execute the commands:

- DISPLAY PROFILE
- DISPLAY DYNAMICQUERYCAPTURE
- DISPLAY RLIMIT
- DISPLAY ML

DIS PROFILE & DIS DYNAMICQUERYCAPTURE - PH56996 (RACF), PH56997 (Db2)

DIS RLIMIT & DIS ML – PH60536

Remote Access Security

Db2 13 for z/OS Enhancements

Granular connection control using Security Profiles

Challenge

Lack of granular control in Db2 beyond the TCPALVER and the SECPORT system parameters makes it difficult to migrate and enforce the Db2 client applications to use approved authentication methods and encrypted connections.

MONITOR CONNECTIONS FOR SECURITY

- DSN_PROFILE_ATTRIBUTES – KEYWORD: MONITOR product_type CONNECTIONS FOR SECURITY
  - Specifies that Db2 monitors all connections for the specified product type for connection compliant requirements
  - Specified only for profiles using the default locations filtering criteria
    - DSN_PROFILE_TABLE - LOCATION column contains '*', '::0', or '0.0.0.0'
  - Validation occurs only when new connections are established
  - Supported *product_type* values:
    - REST
    - JDBC
    - CLI
    - DB2CONNECT
    - DSN
    - * - Applied for application requestors not matching any of the supported product types
- Required APAR: PH48764 / PH53182

MONITOR CONNECTIONS FOR SECURITY - ATTRIBUTE

- ATTRIBUTE1
  - Specifies the actions to take when the policy requirements are not met
  - Supported values:
    - EXCEPTION, EXCEPTION_DIAGLEVELx (DSNT771I, DSNT772I, DSNT776I)
    - WARNING, WARNING_DIAGLEVELx (DSNT771I, DSNT772I, DSNT775I)
- ATTRIBUTE2
  - Specifies the desired authentication mechanisms
  - Supported values: NULL, 1, 2, 4, 5, 6
- ATTRIBUTE3
  - Specifies whether the connection must be secured with an AT-TLS policy
  - Supported values: NULL, 1

Steps to discover and control secure connectivity

- Create a profile by inserting a row in SYSIBM.DSN_PROFILE_TABLE table and specify the filtering criteria
- Specify the monitoring functions of the profile by inserting one or more rows in SYSIBM.DSN_PROFILE_ATTRIBUTES table
- Issue a –START PROFILE command to load or reload the profile tables in memory
- Check the status of all the newly added profiles in the STATUS column of DSN_PROFILE_HISTORY and DSN_PROFILE_ATTRIBUTES_HISTORY tables

Granular connection control using Security Profiles

- APAR PH57811 – Enforce security for new cloud-based clients or specific portions of the network more strictly
  - Filtering criteria in the LOCATION column for the security profiles is expanded to include:
    - IPv4 or IPv6 subnet address
    - IPv4 or IPv6 IP address of a remote client
    - Fully qualified domain name

Monitor Connections for Security - Sample

DSN_PROFILE_TABLE:

PROFILEID	LOCATION	ROLE	AUTHID	PRDID	COLLID	PKGNAME
1	::0	null	null	null	null	Null
2	9.61.0.0/16	null	null	null	null	Null
3	9.61.15.0/24	null	null	null	null	Null

Connections are monitored based on the LOCATION value and the KEYWORDS specified in the DSN_PROFILE_ATTRIBUTES table for that profile ID.

DSN_PROFILE_ATTRIBUTES:

PROFILEID	KEYWORDS	ATTRIBUTE1	ATTRIBUTE2	ATTRIBUTE3
1	MONITOR * CONNECTIONS FOR SECURITY	WARNING	5	1
1	MONITOR JDBC CONNECTIONS FOR SECURITY	EXCEPTION_DIAGLEVEL3	5	NULL
2	MONITOR * CONNECTIONS FOR SECURITY	EXCEPTION	1	1
3	MONITOR REST CONNECTIONS FOR SECURITY	EXCEPTION	4	NULL

REST connections are allowed from IP 9.61.15.0/24 only when using client certificate authentication

RACF Identity Token (IDT)

Challenge

Unable to login to a Db2 for z/OS server from a Db2 for z/OS requestor by a RACF protected user ID using an approved authentication method

RACF Identity Token (IDT)

- JASON Web Token (JWT) represents both an identification and authentication of a user
- IDTs are JWTs (JASON Web Tokens) issued by SAF
- Db2 IDT support provides the capability to
  - Obtain an IDT to be used as an authentication token in an outbound connection from Db2
  - Validate a provided IDT that represents a user ID including protected user IDs
  - Accept an IDT as an authentication token
- Requires Db2 function level, V13R1M505 and Db2 APAR PH55599
- Requires RACF IDT2 support for obtaining IDT for protected user IDs
  - RACF APAR OA63462 / SAF APAR OA63463

RACF Identity Token (IDT)

- Db2 for z/OS requester outbound connection support
  - SYSIBM.IPNAMES – SECURITY_OUT column:
    - New value, ‘T’ (Authentication Token)
  - If an outbound user ID translation is performed, the outbound user ID must exist at the Db2 for z/OS requester and server subsystems
  - Cannot be used when the remote connection is to be trusted
- DDF REST support
  - Uses the Bearer format of the Authorization request header field
    - Authorization: Bearer <Token>

RACF Identity Token (IDT)

- RACF IDTDATA profile must exist on the Db2 for z/OS requester and server systems
  - JWT.<*linkname*>.<*authid*>|*.SAF where <*linkname*> matches:
    - The LINKNAME column of the SYSIBM.LOCATIONS row of the remote location on the Db2 requester
    - Either LUNAME/Generic LUNAME/IPNAME of the serving Db2
  - Serving Db2 must have IDTDATA profile IDTPARMS PROTALLOWED set to YES to enable the use of RACF protected user IDs with IDTs

RACF Identity Token (IDT) - Audit

- New Db2 message, DSNL060I is issued when an authentication error occurs using an authentication token (IDT / JWT)
- New Db2 reason codes:
  - 00F3008A – Token format invalid
  - 00F3008B – Token expired
  - 00F3008C – Token signature invalid
  - 00D31060 - Unable to obtain an IDT at the Db2 for z/OS requestor
- New IFCID 0415 – Authentication Token Exception trace
  - Written each time an authentication token is unsuccessfully processed by RACF
  - Written when STATISTICS TRACE class 4 is ON
- Updated IFCIDs – IFCID 319 (Audit trail for security), IFCID 365 (Location Statistics)

IDT support for Granular Connection Control

- MONITOR CONNECTIONS FOR SECURITY – ATTRIBUTE2 column includes additional values:
  - 8 – Authentication token
    - Use RACF authentication token (JWT/IDT) for authentication
  - 10 – Basic authentication with MFA or Authentication token
    - Use the behavior of value 2 or 8
  - 12 – Client certificate or Authentication token
    - Use the behavior of value 4 or 8
  - 14 – Basic authentication with MFA or Client certificate or Authentication token
    - Use the behavior of value 2 or 4 or 8
- ATTRIBUTE3 column includes additional value:
  - Authentication token – Connection does not require AT-TLS policy

Db2 REST: Cross-Origin Resource Sharing

Challenge

JavaScript web applications which directly invoke Db2 for z/OS REST services cannot be developed and deployed easily due to Db2's lack of Cross-Origin Resource Sharing (CORS) support.

Db2 REST: Cross-Origin Resource Sharing

- Cross Origin Resource Sharing (CORS)
  - Protocol standard for permitting a web page from accessing content from a different location than where the web page was loaded.
- Supports CORS “Preflight” request and “simple” CORS enabled request
- CORS “Preflight” request
  - Determines if the actual request should be permitted
  - Utilizes the HTTP OPTIONS verb with the target resource URL and the other CORS related request header fields.
- “Simple” CORS enabled request
  - CORS HTTP request / response header fields
- Requires profiles in new z/OS RACF resource class, DSNRAUTH
  - Authorization ID associated with the DDF started task requires access to the profile

Db2 CORS - Configuration and Management

- Create a Db2 REST CORS RACF resource profile under the new SAF/RACF resource class, DSNRAUTH
- Permit the authorization ID associated with the Db2 DDF (ssid<DIST>) started task address space READ access to the profile.
- Db2 REST CORS RACF resource naming convention format:

DSNCORS.<ssid|group-attach>.<reversed-hostname>
e.g.: DSNCORS.DB2A.COM.SOMESERVER.WWW

<ssid|group-attach>

For Db2 non-data sharing, the Db2 *SUBSYSTEM NAME* (SSID) value is used. For Db2 data sharing, the *Db2-group-attachment-name* value is used.

<reversed-hostname>

The remote origin site's fully qualified domain name in reverse and uppercase.

Db2 for z/OS CORS - Audit

- New Db2 message, DSNL616I is issued when the service request include CORS and Db2 REST services CORS support is not enabled
- New Db2 reason codes:
  - 00D36063 – Request origin host not authorized
  - 00D36064 – Request did not include the required origin host value
  - 00D36065 – Unsupported IPV6 format origin host value
  - 00D36066 – Db2 REST services CORS support not enabled
- New IFCID 0416 – REST CORS Exception trace
  - Written each time when a Db2 REST CORS authorization request is unsuccessfully processed by Db2
  - Written when AUDIT TRACE class 12 is ON

JDBC T2 driver: Password phrase support

- Password phrases (Passphrase)
  - A string of 100 characters maximum length that consists of mixed-case letters, numbers, and special characters
- T2 driver normal connection Passphrase support
  - SQL CONNECT statement *authorization* USER/USING supports up to 100 characters password phrase
  - APAR PH40443 (DB2 for z/OS 12 and 13)
- T2 driver trusted connection Passphrase support
  - Db2 for z/OS APAR PH54501 (Db2 for z/OS 13)
  - IBM Data Server Driver for JDBC and SQLJ 4.33.39 - APAR PH60240

For more information …

https://www.ibm.com/products/z-security-and-compliance-center

https://www.redbooks.ibm.com/abstracts/sg248540.html

https://www.ibm.com/docs/en/db2-for-zos/13?topic=securing-db2

https://www.ibm.com/docs/en/db2-for-zos/13?topic=support-discovering-controlling-secure-connectivity-profile-tables

https://www.redbooks.ibm.com/abstracts/sg248527.html

https://www.ibm.com/support/z-content-solutions/z-security-compliance-center/

Thank you

IDUG

2024 NA Db2 Tech Conference

Unlock the new security functions in Db2 for z/OS

Gayathiri (Gaya) Chandran

gchandran@us.ibm.com

ZLN6

Please fill out your session evaluation!

@IDUGDb2
#IDUG_NA24