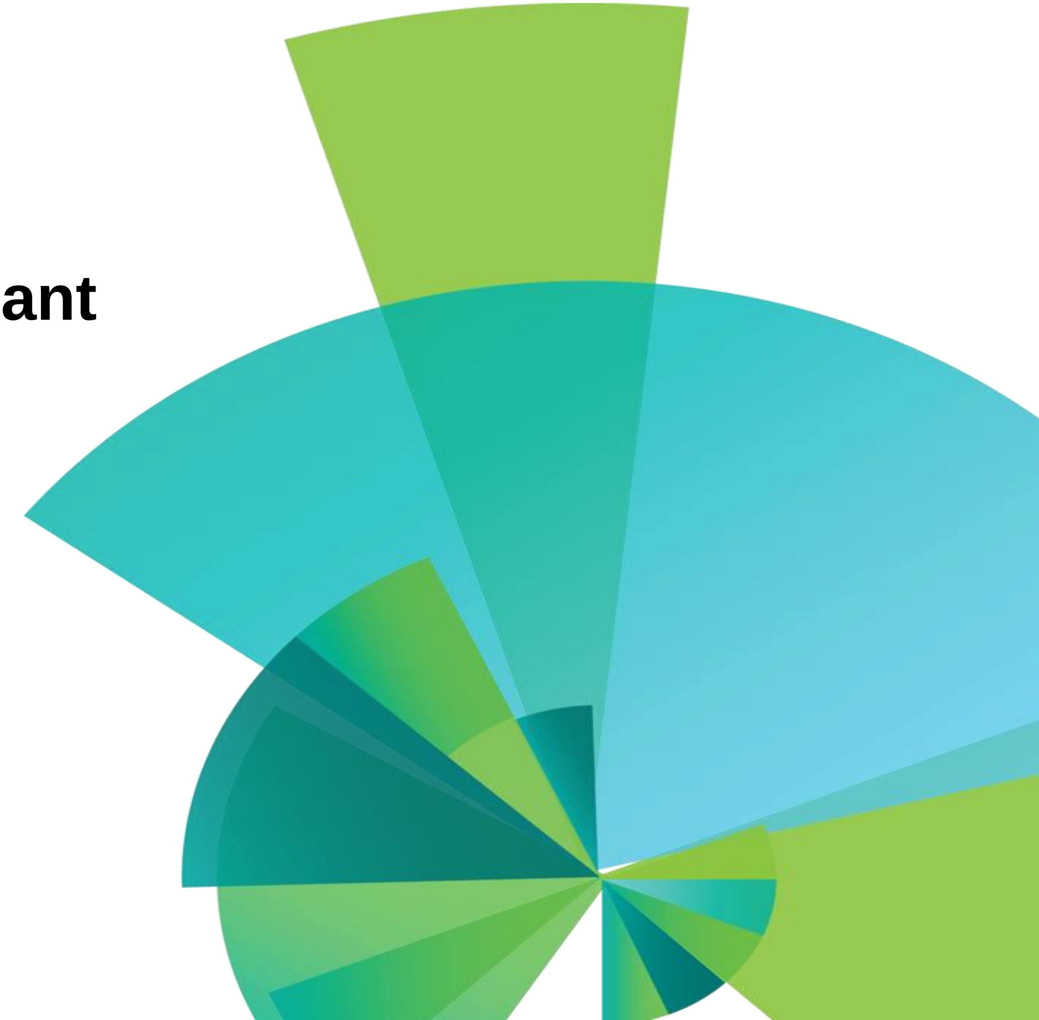
What’s New in IBM i 7.1, 7.2 & 7.3 Security

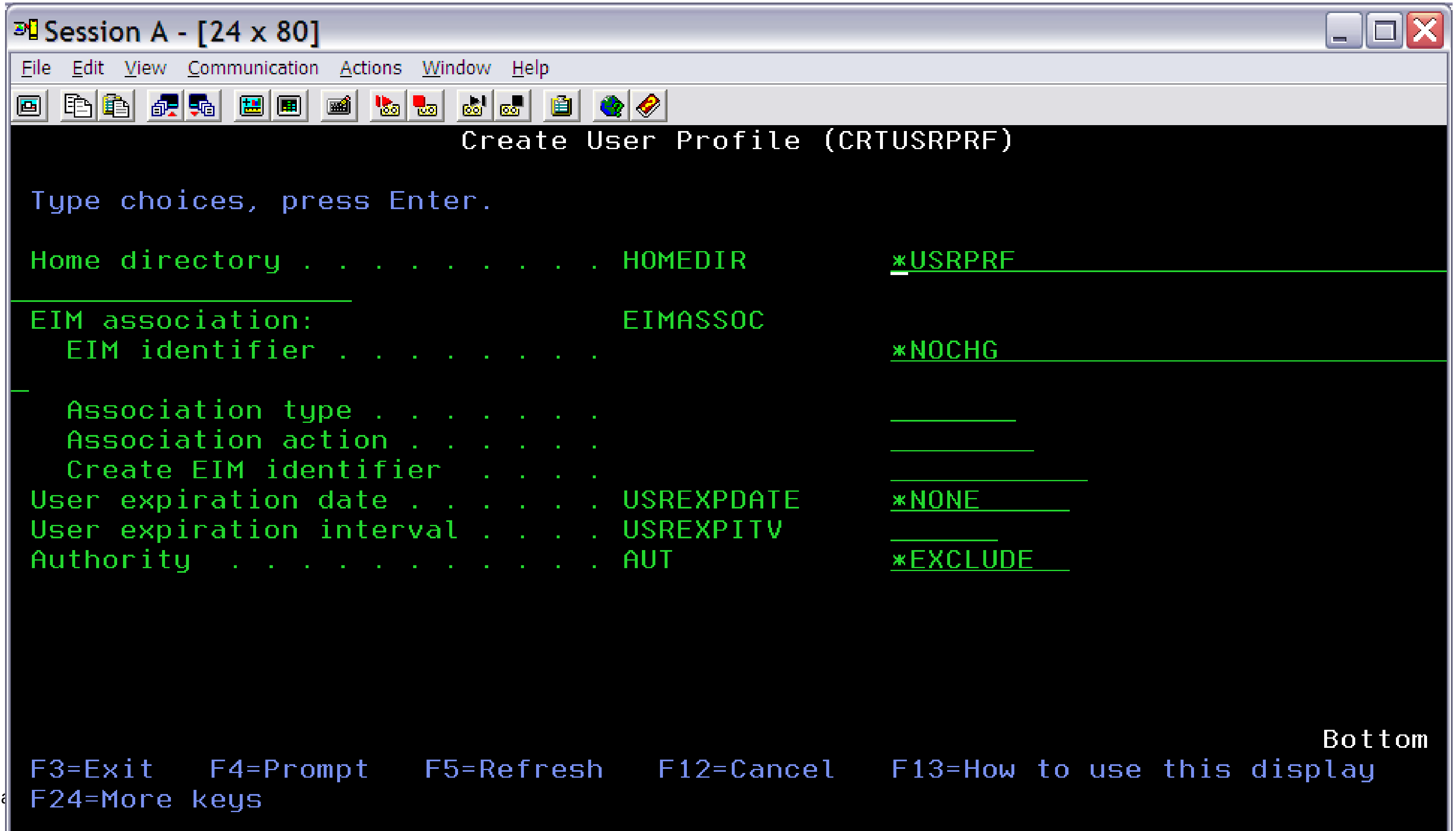
Robert D. Andrews
IBM i Security Managing Consultant
robert.andrews@us.ibm.com



7.1 Security Enhancements Overview

New User Profile Parameters – 7.1

- New user profile “expiration” parameters in 7.1
  - USREXPDATE, User Expiration Date (Date when profile is *DISABLED)
  - USREXPITV, User Expiration interval (1-366 days)



```
                        Create User Profile (CRTUSRPRF)

 Type choices, press Enter.

 Home directory . . . . . . . . .   HOMEDIR         *USRPRF

 EIM association:                   EIMASSOC
   EIM identifier . . . . . . . .                   *NOCHG

   Association type . . . . . . .
   Association action . . . . . .
   Create EIM identifier  . . . .
 User expiration date . . . . . .   USREXPDATE      *NONE
 User expiration interval . . . .   USREXPITV
 Authority  . . . . . . . . . . .   AUT             *EXCLUDE




                                                                         Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

7.1 IBM i DB2 Field Procedures

Column Level Encryption Enablement

DB2 Field Procedures – 7.1

- **DB2 Column Level (field) exit support**
  - Exit program (Field Procedure) called on insert/update/read of a column
  - Similar to "Triggers" but additional support to enable encryption
  - Exit added via SQL Alter Table
    - One exit per column
  - Masking of Data is also supported

- **Enables Column Level Encryption**
  - Encrypt/Decrypt data in a DB2 column
    - No need to change column attributes like field length or data type
  - Encryption Key management must be implemented by the Exit Program (Field Procedure)

- **Field Procedure is a user written program**
  - Business partner solutions from Enforcive, Raz-Lee, Linoma and Towsend Security

DB2 Field Procedures continued – 7.1

- **Additional Security Checks within the Field Procedure**
  - To make the support meaningful, additional security checks should be implemented by the exit
    - Is the user listed on the Authorization list (*AUTL)?
    - If so, decrypt the SS# (data), otherwise return '*********' or '000000000'

- **DB2 handles all length and data type issues**
  - I/O buffer doesn't change but encrypted data length and data type can change
    - I/O buffer for SS# is 9 and type character
    - Result of encryption is, for example, length 16 and data type binary
      - Managed by DB2 internally

DB2 Field Procedures continued – 7.1

- **Performance Considerations**
  - Field Procedure replaces application level code
    - Encryption/Decryption performance will be the same regardless of where it is implemented (in application vrs field procedure)
    - No application source code available to make updates
    - Implement all encryption/decryption in one place
    - No need to deal with length/data type changes on the column

- **SQL Programming Guide will contain examples for Field Procedure implementation**

7.2 Security Enhancements

7.2 DB2 Security Enhancements

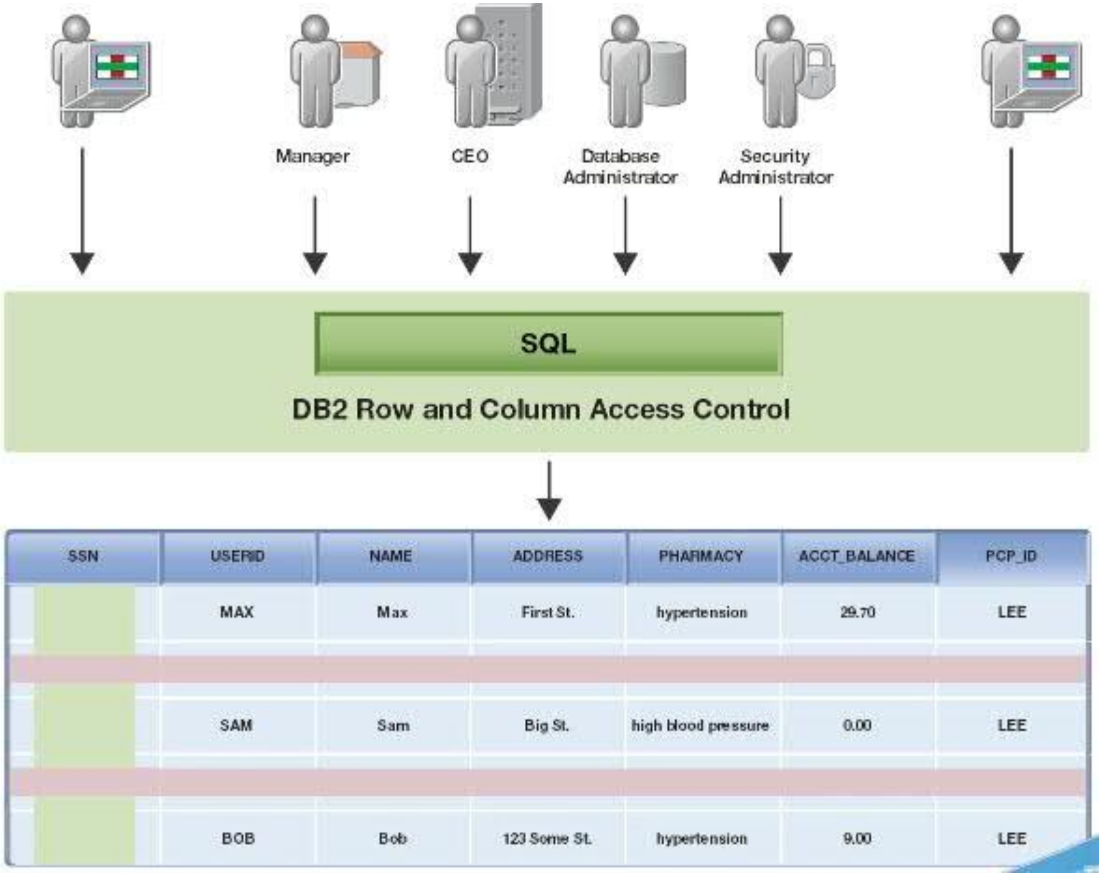
What is RCAC (Row & Column Access Control)?

IBM Advanced Data Security for i

(**Boss option 47**)

No Charge

- Additional layer of data security available with DB2 in 7.2
- Complementary to table level security (object authority checking)
- Controls access to table data at the **ROW, COLUMN or BOTH**
- Two sets of rules
  - Permissions for rows
  - Masks for columns
- IBM Advanced Data Security for i
  - No-charge feature, OS Option 47 required for RCAC



SSN	USERID	NAME	ADDRESS	PHARMACY	ACCT_BALANCE	PCP_ID
🟩	MAX	Max	First St.	hypertension	29.70	LEE
🟩	SAM	Sam	Big St.	high blood pressure	0.00	LEE
🟩	BOB	Bob	123 Some St.	hypertension	9.00	LEE

http://www.redbooks.ibm.com/redbooks.nsf/RedpieceAbstracts/redp5110.html?Open

IBM Advanced Data Security for i (Boss Option 47)

- Option must be installed to:
  - CREATE PERMISSION and CREATE MASK
  - Open a file that has RCAC activated

- RCAC does not replace object authorization requirements
  - If you pass the object authorization check:
    - Row permissions reduce the set of rows returned
    - Column Masks limit full or partial access to sensitive column data

- RCAC is comprehensive and applies to any interface (Native DB, SQL, RPG, APIs, etc)

- Row Permissions are a replacement technology for Views / Logical Files

Security - Separation of Duties

Before 7.2

Problem:

Anyone who has the authority to grant privileges also has the authority to perform operations that require those privileges.

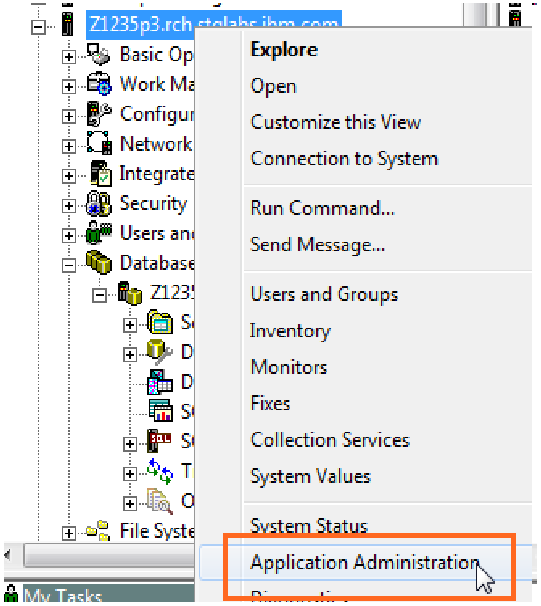
Should the security administrator be able to access the data within tables?

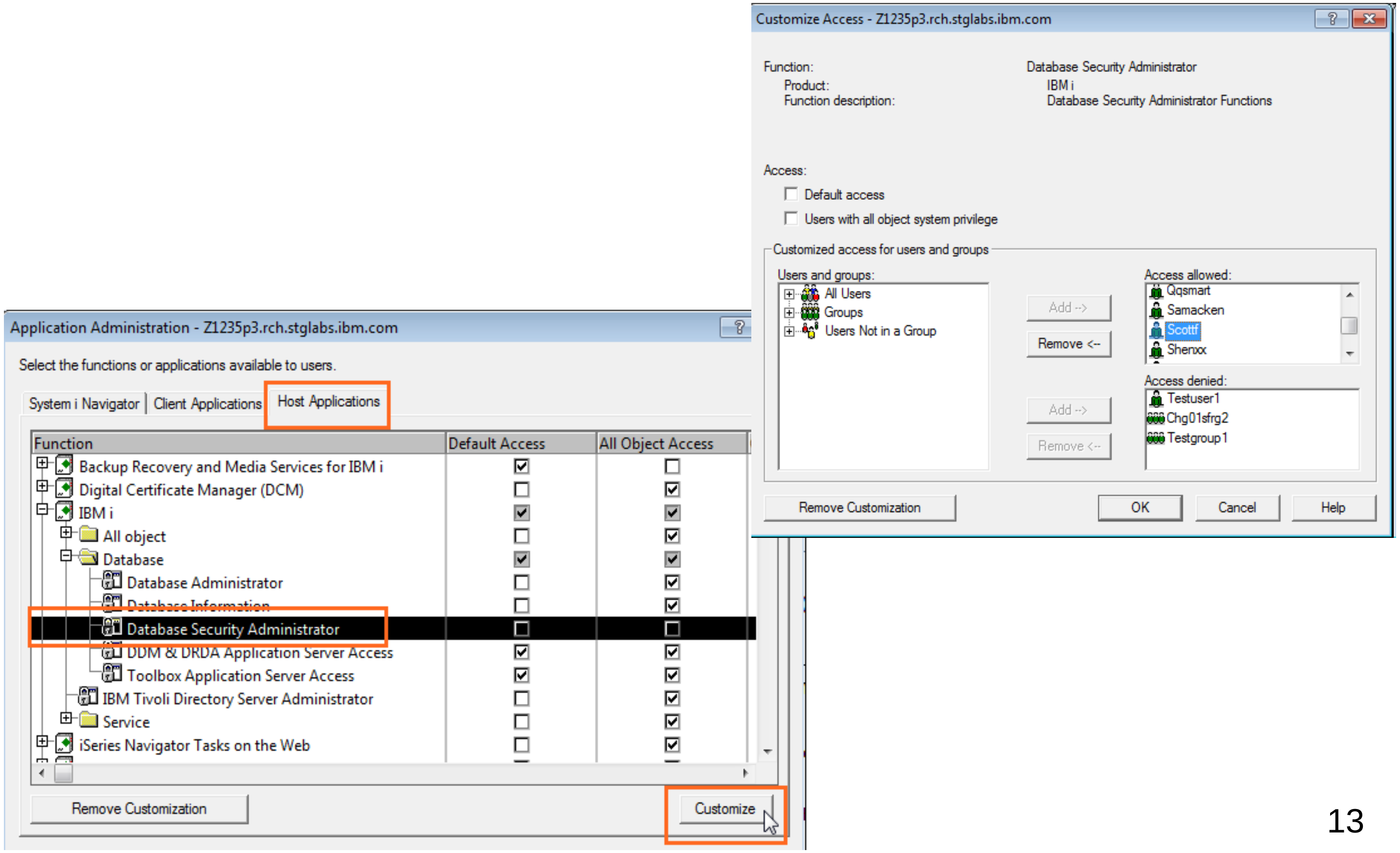
IBM i 7.2 with RCAC (Row and Column Access Control)

- Enable the management of security, **without exposing the data** to be read or modified.
- A user with security administration function usage (QIBM_DB_SECADM) will be able to grant or revoke privileges on any object to anyone, even if they do not have the those privileges.

Setting up QIBM_DB_SECADM for an Administrator

- Authorization to the Database Security Administrator function of IBM i can be assigned through Application Administration in IBM Navigator for i and via the Change Function Usage (WRK/CHGFCNUSG) command.
- Navigator → Right click on the connection name and select Application Administration.




Application Administration - Z1235p3.rch.stglabs.ibm.com

Select the functions or applications available to users.

Function	Default Access	All Object Access
Backup Recovery and Media Services for IBM i	☑	☐
Digital Certificate Manager (DCM)	☐	☑
IBM i	☑	☑
All object	☐	☑
Database	☑	☑
Database Administrator	☐	☑
Database Information	☐	☑
Database Security Administrator	☐	☐
DDM & DRDA Application Server Access	☑	☑
Toolbox Application Server Access	☑	☑
IBM Tivoli Directory Server Administrator	☐	☑
Service	☐	☑
iSeries Navigator Tasks on the Web	☐	☑

Customize Access - Z1235p3.rch.stglabs.ibm.com

Function: Database Security Administrator
Product: IBM i
Function description: Database Security Administrator Functions

Access:
☐ Default access
☐ Users with all object system privilege

Customized access for users and groups

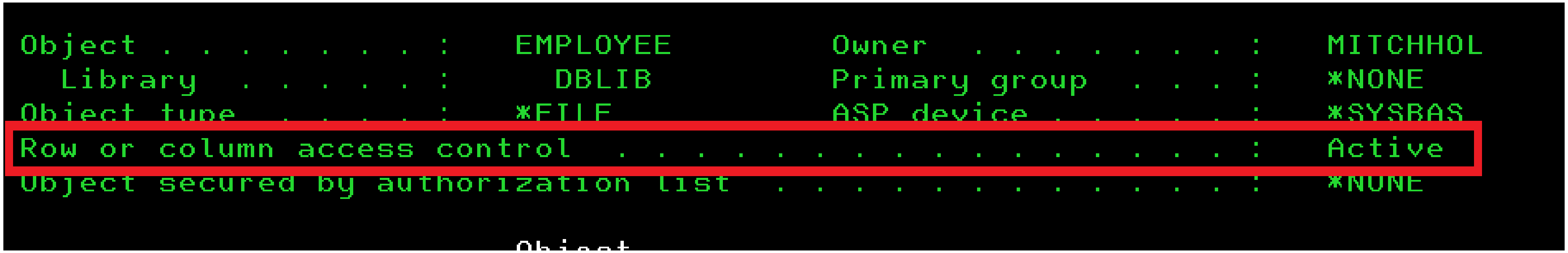
Users and groups:
All Users
Groups
Users Not in a Group

Access allowed:
Qqsmart
Samacken
Scottf
Shenxx

Access denied:
Testuser1
Chg01sfrg2
Testgroup1

How do I determine if RCAC is enabled for a file?

- DSPOBJAUT command

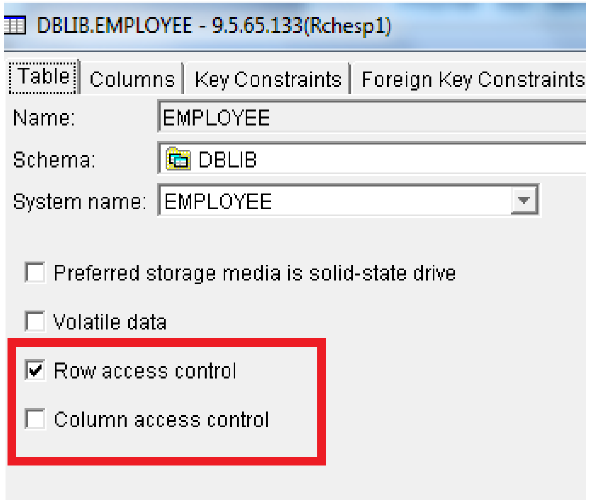


```
Object . . . . . . . . :   EMPLOYEE        Owner . . . . . . . :   MITCHHOL
  Library  . . . . . . :     DBLIB         Primary group . . . :   *NONE
Object type  . . . . . :   *FILE           ASP device  . . . . :   *SYSBAS
Row or column access control . . . . . . . . . . . . . . . . . :   Active
Object secured by authorization list . . . . . . . . . . . . . :   *NONE

                         Object
```

- Query new QSYS2/SYSCONTROLS catalog
- Navigator for i

Column Masks/Row Permissions under Schemas

Right click on table → Definition



DBLIB.EMPLOYEE - 9.5.65.133(Rchesp1)

Name: EMPLOYEE

Schema: DBLIB

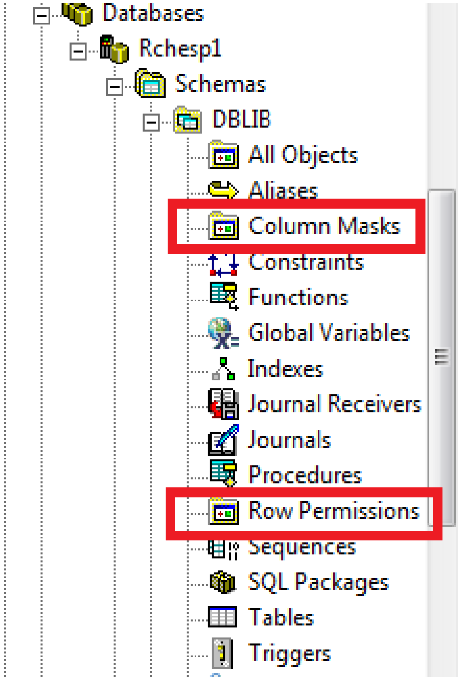
System name: EMPLOYEE

☐ Preferred storage media is solid-state drive

☐ Volatile data

☑ Row access control

☐ Column access control



- Databases
  - Rchesp1
    - Schemas
      - DBLIB
        - All Objects
        - Aliases
        - Column Masks
        - Constraints
        - Functions
        - Global Variables
        - Indexes
        - Journal Receivers
        - Journals
        - Procedures
        - Row Permissions
        - Sequences
        - SQL Packages
        - Tables
        - Triggers

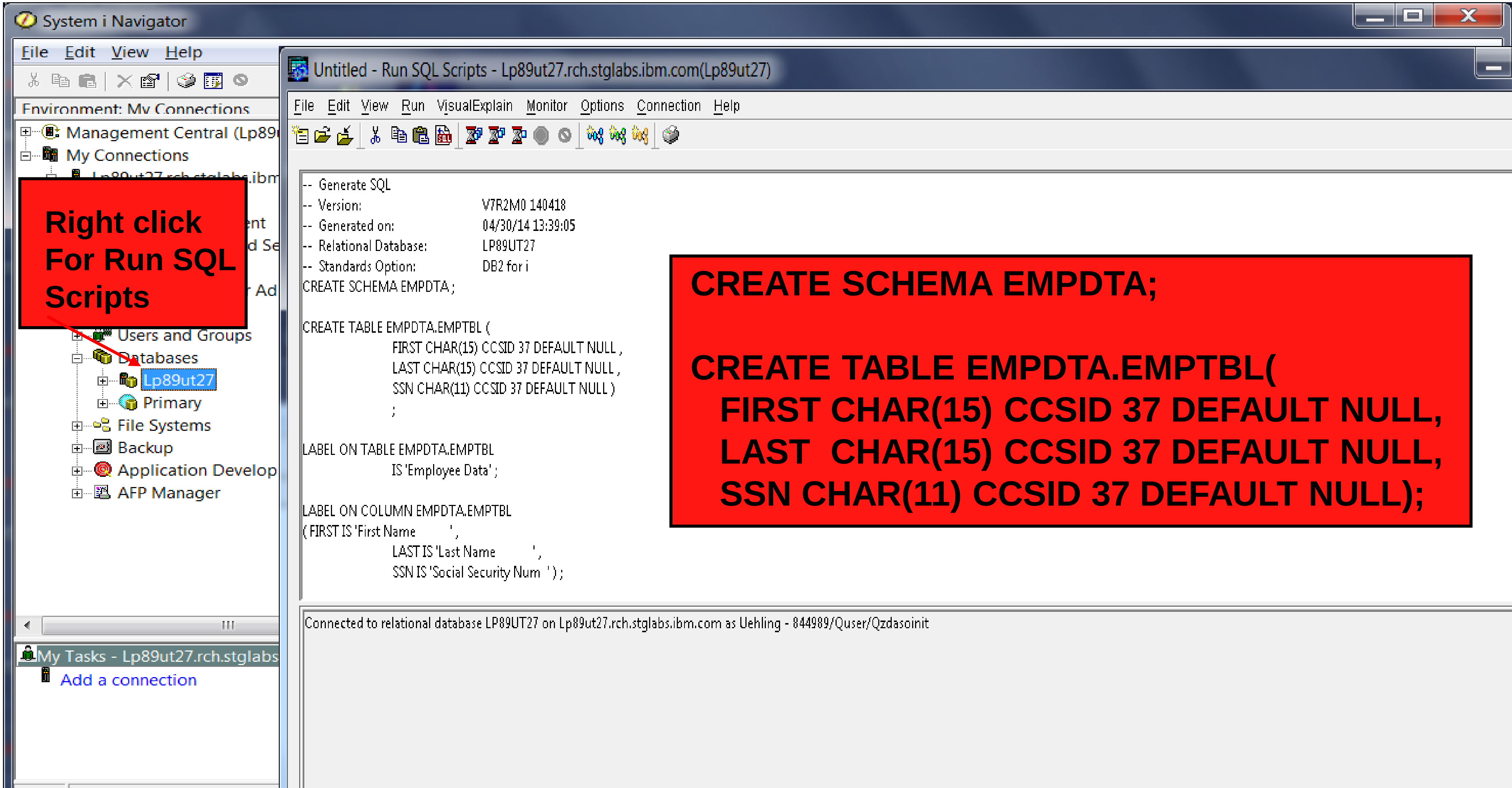
Special registers – similar names, different purposes

The name CURRENT USER could easily be misunderstood.

Special Register	Definition
USER **or** **SESSION_USER**	The effective user of the thread Is returned.
SYSTEM_USER	The authorization ID that initiated the connection is returned.
CURRENT USER **or** **CURRENT_USER**	The most recently program adopted authorization ID within the thread will be returned. When no adopted authority is active, the effective user of the thread Is returned.

Example: Step by Step, very simple scenario

- Create Schema “EMPDTA” and Table “EMPTBL” via “Run SQL Scripts”
  - Schema contains a library, journal and receiver plus DB2 catalog objects
  - After creating the schema “EMPDTA”, right click on Schemas in iNav and “select schemas to display” to add “EMPDTA” to your schema list



Right click For Run SQL Scripts

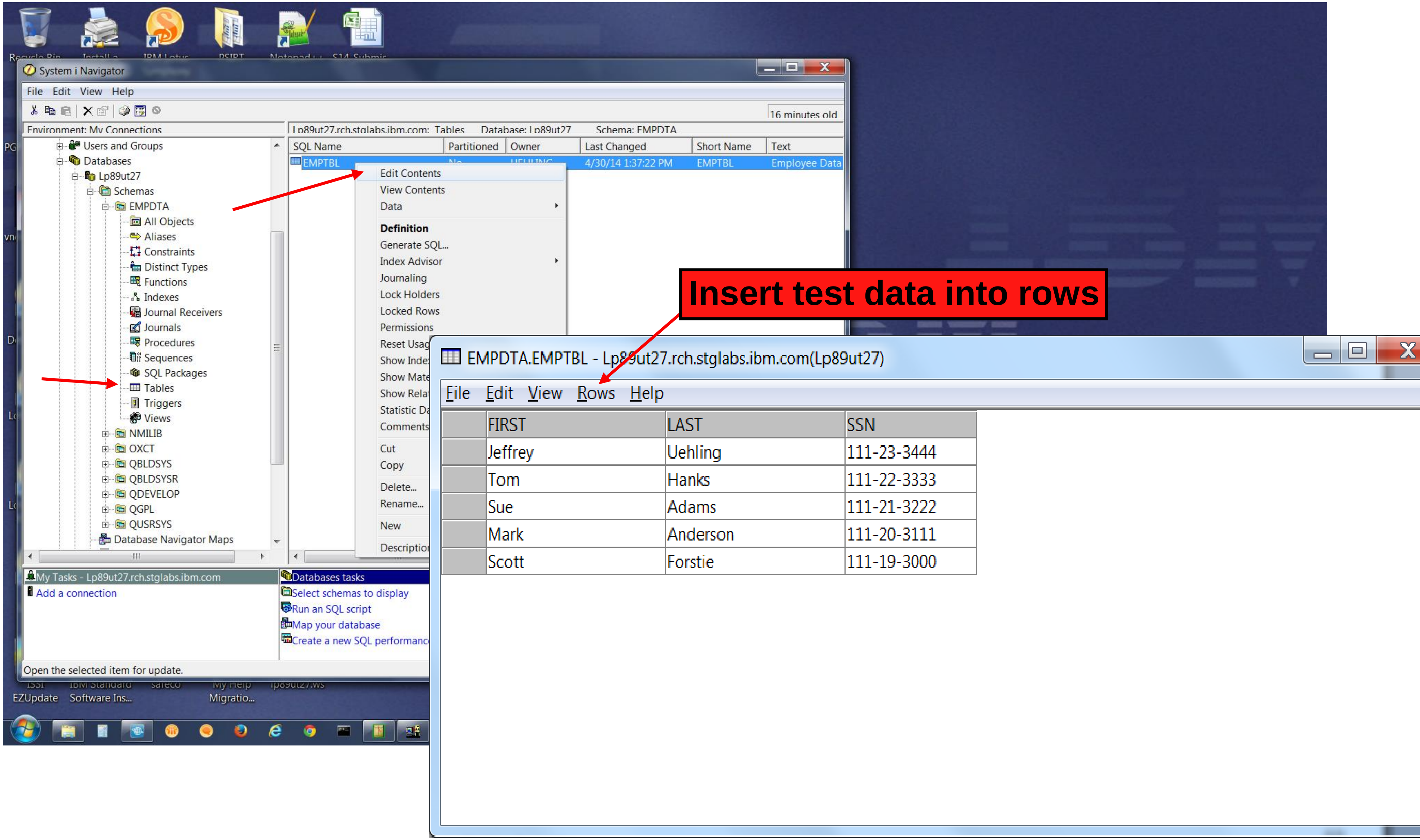
```
-- Generate SQL
-- Version:                   V7R2M0 140418
-- Generated on:              04/30/14 13:39:05
-- Relational Database:       LP89UT27
-- Standards Option:          DB2 for i
CREATE SCHEMA EMPDTA ;

CREATE TABLE EMPDTA.EMPTBL (
              FIRST CHAR(15) CCSID 37 DEFAULT NULL ,
              LAST CHAR(15) CCSID 37 DEFAULT NULL ,
              SSN CHAR(11) CCSID 37 DEFAULT NULL )
              ;

LABEL ON TABLE EMPDTA.EMPTBL
              IS 'Employee Data' ;

LABEL ON COLUMN EMPDTA.EMPTBL
( FIRST IS 'First Name          ' ,
              LAST IS 'Last Name           ' ,
              SSN IS 'Social Security Num  ' ) ;
```

```
Connected to relational database LP89UT27 on Lp89ut27.rch.stglabs.ibm.com as Uehling - 844989/Quser/Qzdasoinit
```

```
CREATE SCHEMA EMPDTA;

CREATE TABLE EMPDTA.EMPTBL(
   FIRST CHAR(15) CCSID 37 DEFAULT NULL,
   LAST  CHAR(15) CCSID 37 DEFAULT NULL,
   SSN CHAR(11) CCSID 37 DEFAULT NULL);
```

Example: Step by Step, very simple scenario (cont…)

- Edit data in the Table via iNav

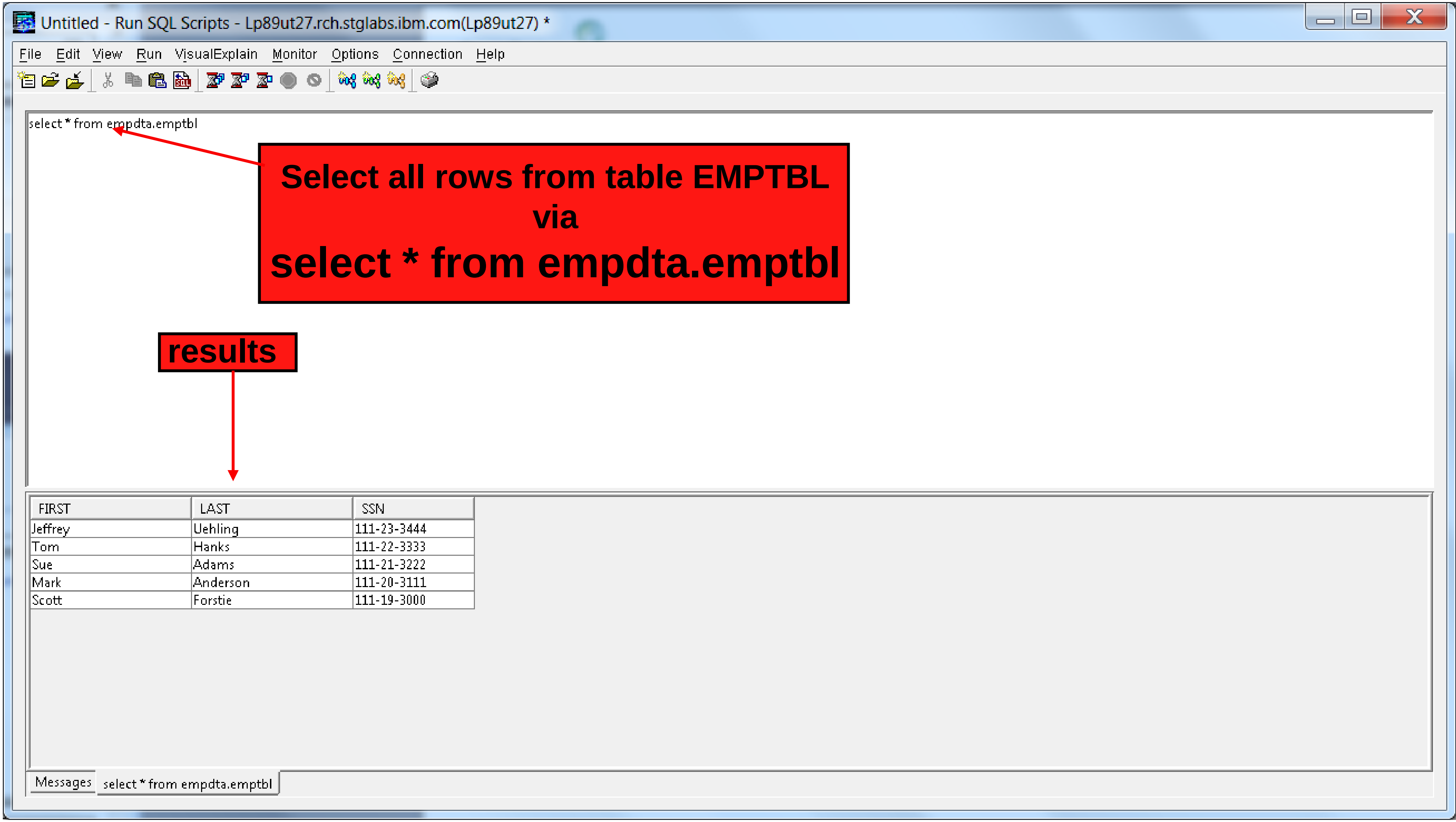


Insert test data into rows

FIRST	LAST	SSN
Jeffrey	Uehling	111-23-3444
Tom	Hanks	111-22-3333
Sue	Adams	111-21-3222
Mark	Anderson	111-20-3111
Scott	Forstie	111-19-3000

Example: Step by Step, very simple scenario (cont…)

- View the data via “Run SQL Scripts” and SQL “select” statement


Untitled - Run SQL Scripts - Lp89ut27.rch.stglabs.ibm.com(Lp89ut27) *
File
Edit
View
Run
VisualExplain
Monitor
Options
Connection
Help
Messages
select * from empdta.emptbl

```
select * from empdta.emptbl
```

Select all rows from table EMPTBL via

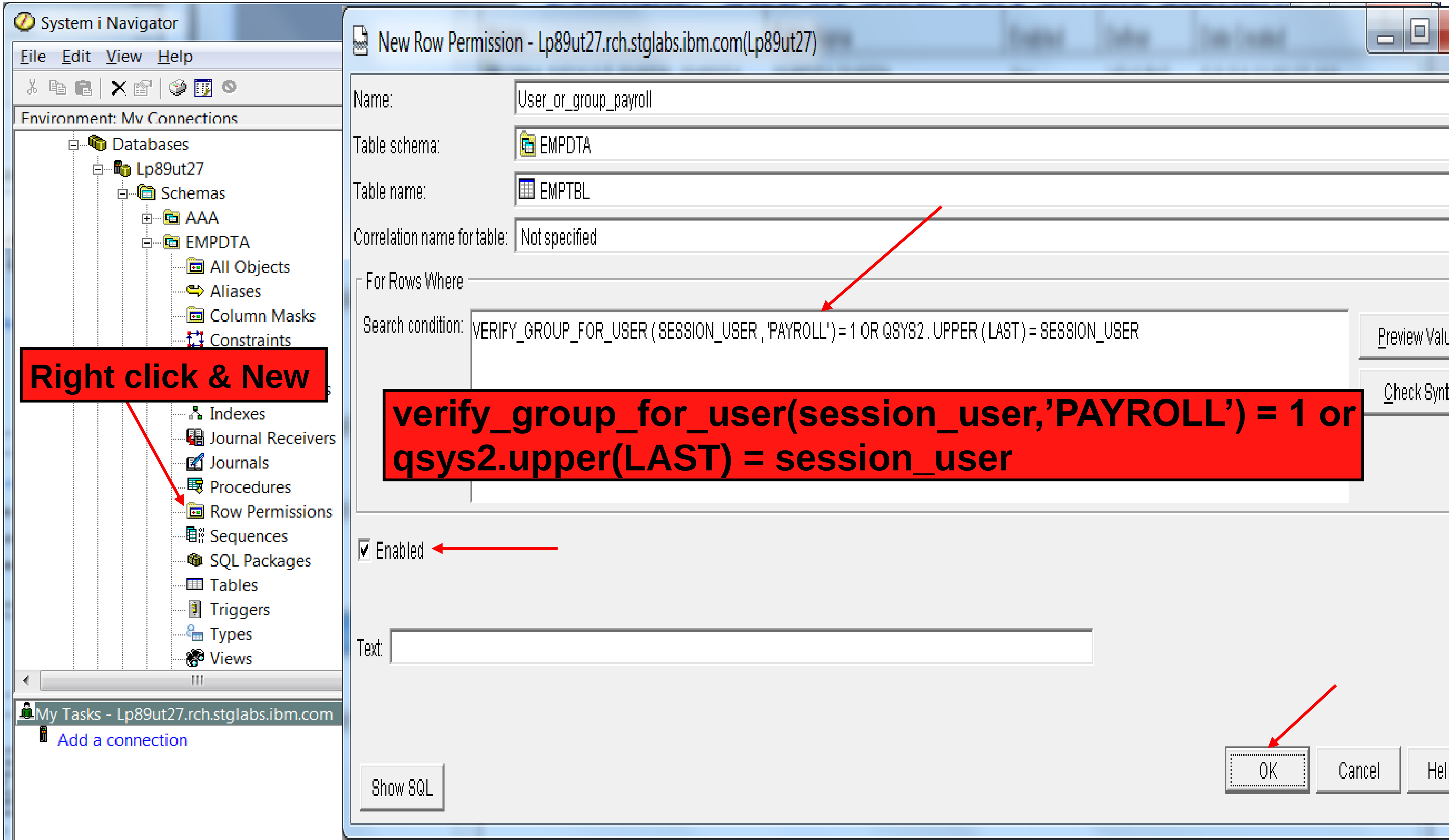
select * from empdta.emptbl

results

FIRST	LAST	SSN
Jeffrey	Uehling	111-23-3444
Tom	Hanks	111-22-3333
Sue	Adams	111-21-3222
Mark	Anderson	111-20-3111
Scott	Forstie	111-19-3000

Example: Step by Step, very simple scenario (cont…)

- Create “Row” Permissions
  - Return all ROWS for group profile = PAYROLL or return just the ROW where process user profile = column LAST



Name: User_or_group_payroll

Table schema: EMPDTA

Table name: EMPTBL

Correlation name for table: Not specified

For Rows Where

Search condition: VERIFY_GROUP_FOR_USER (SESSION_USER , 'PAYROLL') = 1 OR QSYS2 . UPPER (LAST) = SESSION_USER

☑ Enabled

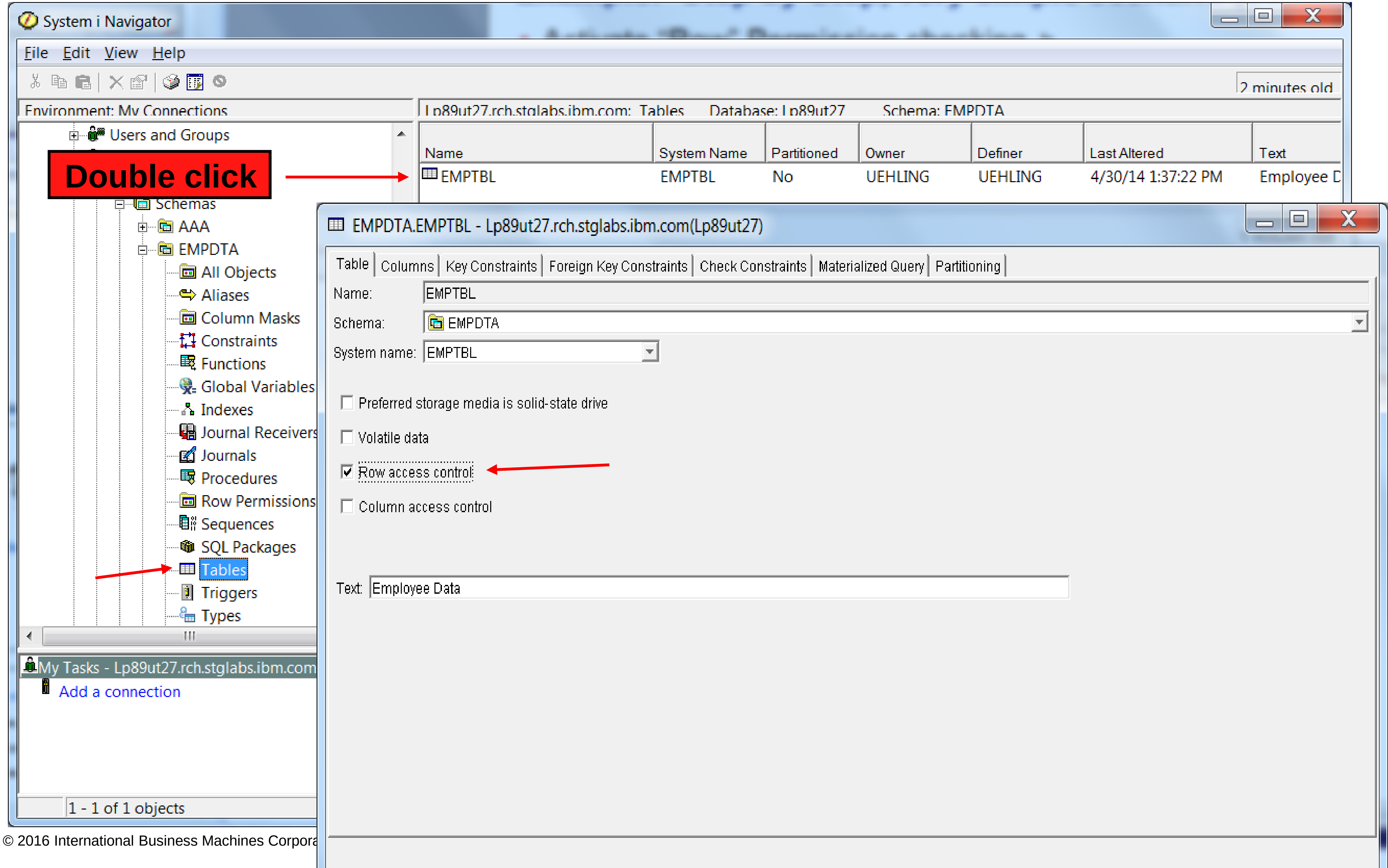
Text:

Right click & New

verify_group_for_user(session_user,’PAYROLL’) = 1 or qsys2.upper(LAST) = session_user

Example: Step by Step, very simple scenario (cont…)

- Activate “Row Access Control”



Double click

Environment: My Connections

Lp89ut27.rch.stglabs.ibm.com: Tables   Database: Lp89ut27   Schema: EMPDTA

Name	System Name	Partitioned	Owner	Definer	Last Altered	Text
EMPTBL	EMPTBL	No	UEHLING	UEHLING	4/30/14 1:37:22 PM	Employee D

1 - 1 of 1 objects

EMPDTA.EMPTBL - Lp89ut27.rch.stglabs.ibm.com(Lp89ut27)

Name: EMPTBL

Schema: EMPDTA

System name: EMPTBL

☐ Preferred storage media is solid-state drive

☐ Volatile data

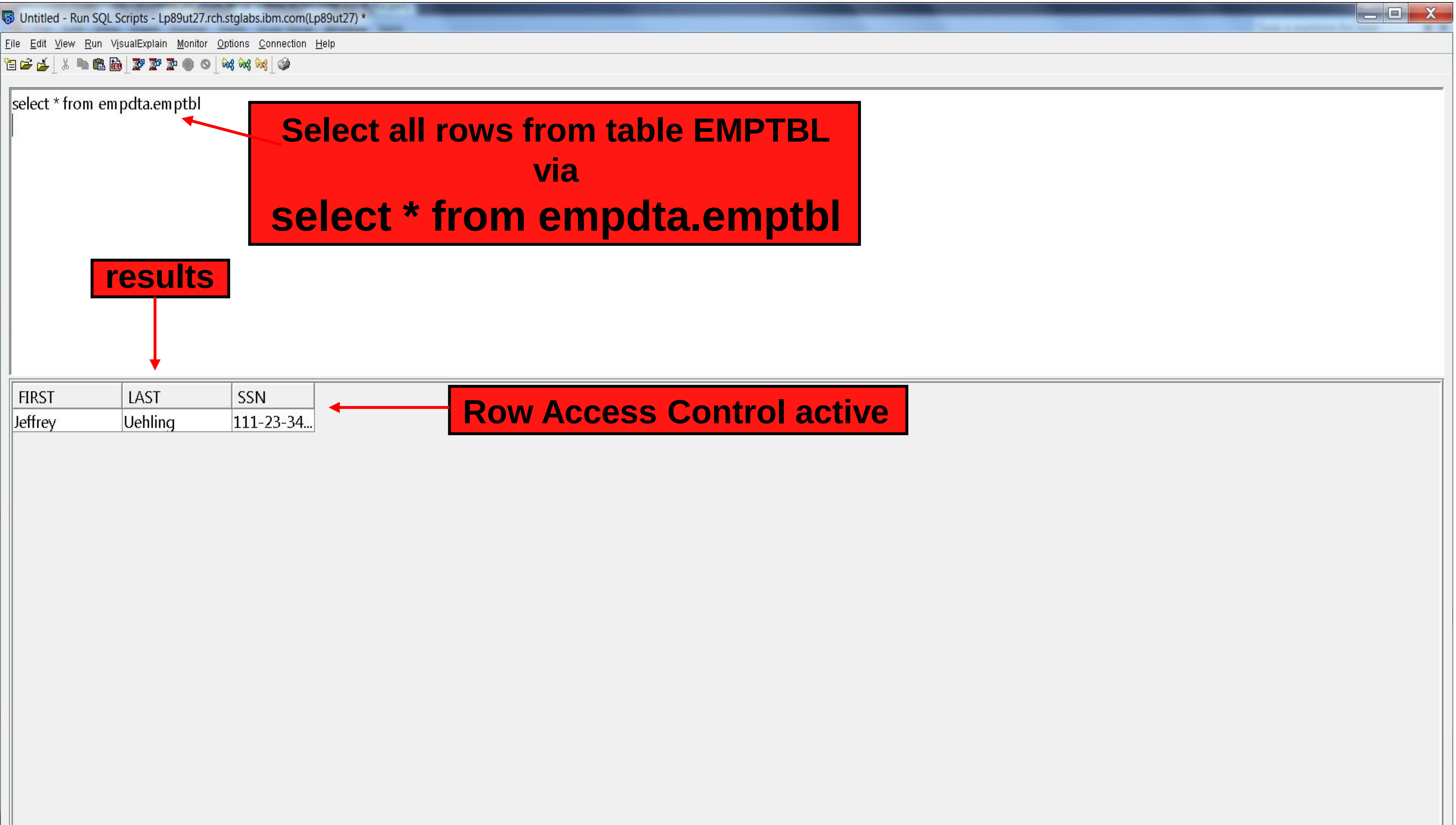
☑ Row access control

☐ Column access control

Text: Employee Data

Example: Step by Step, very simple scenario (cont…)

- View the data via “Run SQL Scripts” and SQL select statement
  - iNav session user is “UEHLING” & no group profile



Untitled - Run SQL Scripts - Lp89ut27.rch.stglabs.ibm.com(Lp89ut27) *
File Edit View Run VisualExplain Monitor Options Connection Help

```
select * from empdta.emptbl
```

Select all rows from table EMPTBL via **select * from empdta.emptbl**

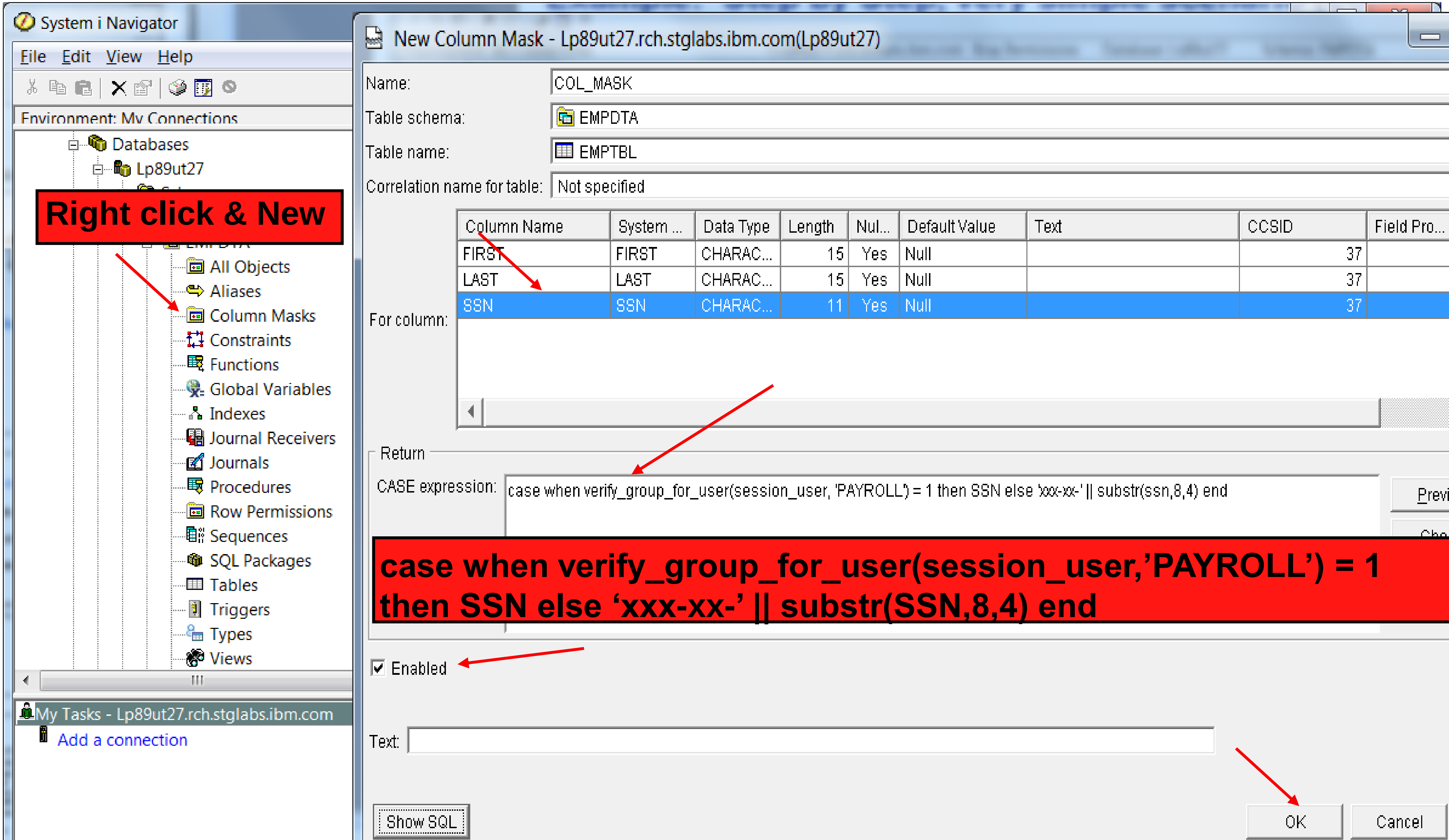
results

FIRST	LAST	SSN
Jeffrey	Uehling	111-23-34...

Row Access Control active

Example: Step by Step, very simple scenario (cont…)

- Create “Column” Mask
  - Return all COLUMN data, SSN, for group profile = PAYROLL or return masked data for the SSN column where the user is not part of the PAYROLL group



Right click & New

New Column Mask - Lp89ut27.rch.stglabs.ibm.com(Lp89ut27)

Name: COL_MASK

Table schema: EMPDTA

Table name: EMPTBL

Correlation name for table: Not specified

For column:

Column Name	System ...	Data Type	Length	Nul...	Default Value	Text	CCSID	Field Pro...
FIRST	FIRST	CHARAC...	15	Yes	Null		37	
LAST	LAST	CHARAC...	15	Yes	Null		37	
SSN	SSN	CHARAC...	11	Yes	Null		37	

Return

CASE expression: case when verify_group_for_user(session_user, 'PAYROLL') = 1 then SSN else 'xxx-xx-' || substr(ssn,8,4) end

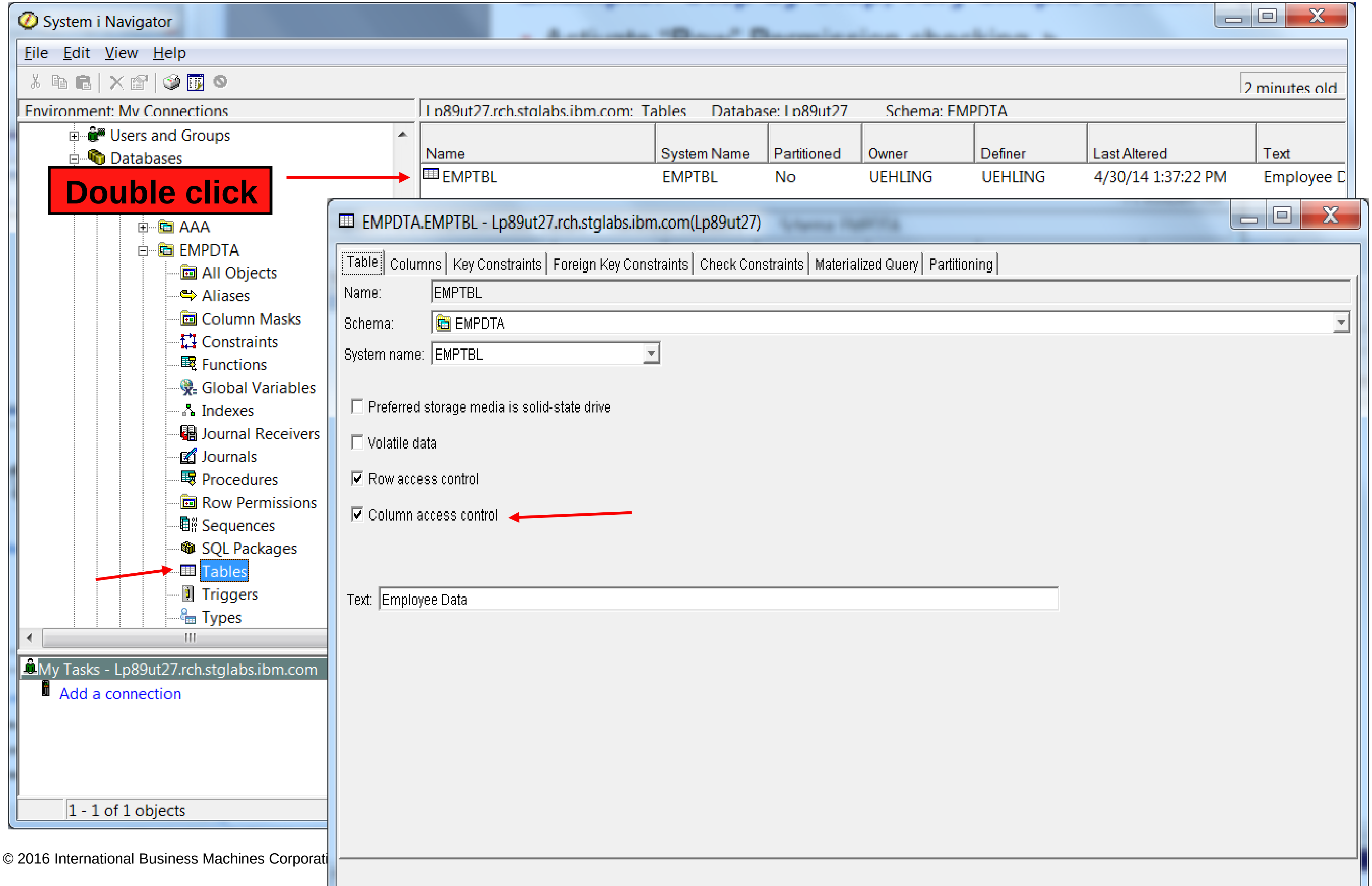
case when verify_group_for_user(session_user,’PAYROLL’) = 1 then SSN else ‘xxx-xx-’ || substr(SSN,8,4) end

☑ Enabled

Text:

Example: Step by Step, very simple scenario (cont…)

- Activate "Column Access Control"



Double click

Lp89ut27.rch.stglabs.ibm.com: Tables Database: Lp89ut27 Schema: EMPDTA

Name	System Name	Partitioned	Owner	Definer	Last Altered	Text
EMPTBL	EMPTBL	No	UEHLING	UEHLING	4/30/14 1:37:22 PM	Employee D

EMPDTA.EMPTBL - Lp89ut27.rch.stglabs.ibm.com(Lp89ut27)

Table | Columns | Key Constraints | Foreign Key Constraints | Check Constraints | Materialized Query | Partitioning

Name: EMPTBL

Schema: EMPDTA

System name: EMPTBL

☐ Preferred storage media is solid-state drive

☐ Volatile data

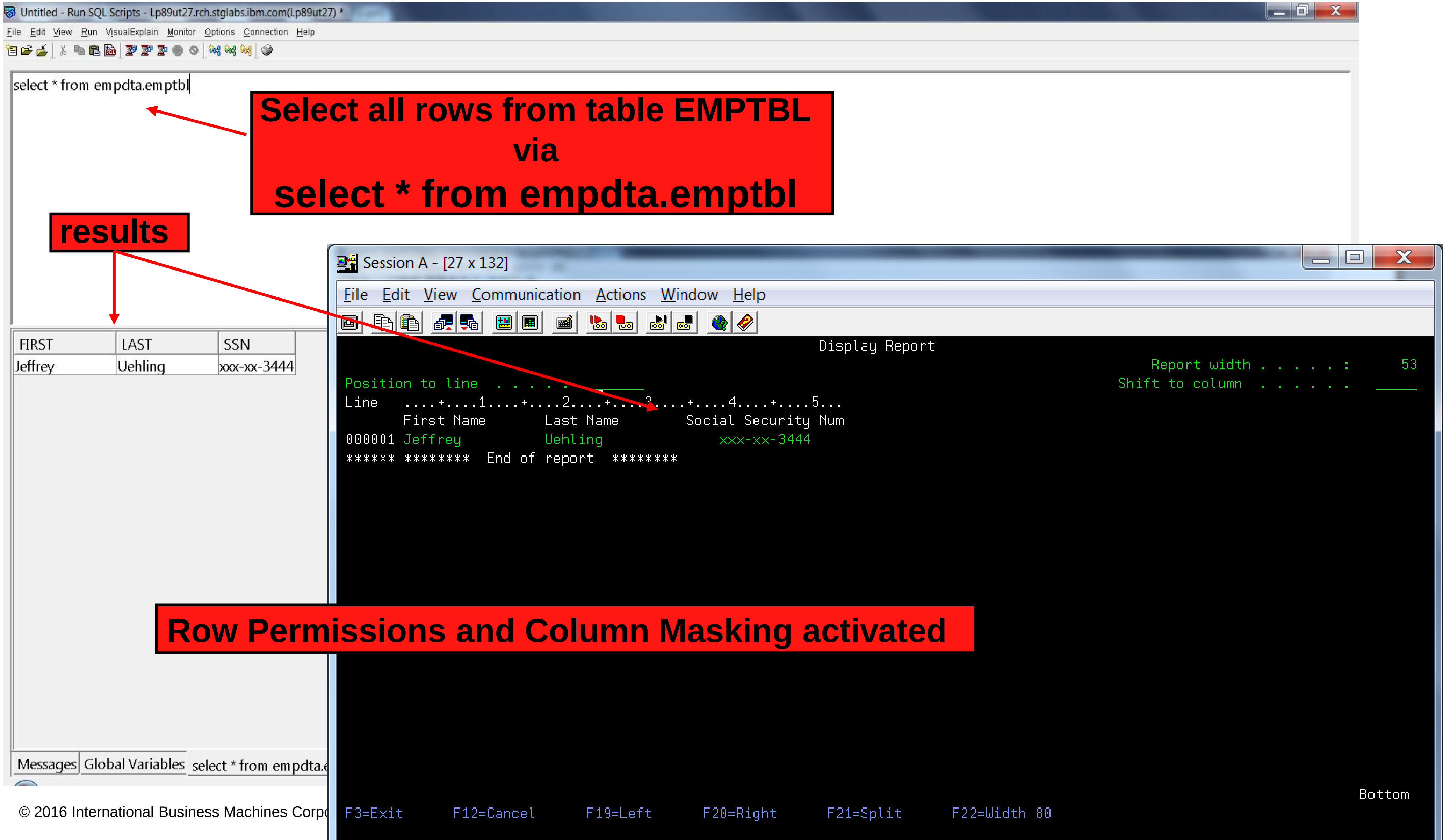
☑ Row access control

☑ Column access control

Text: Employee Data

Example: Step by Step, very simple scenario (cont…)

- View the data via “Run SQL Scripts” and SQL “select” statement & RUNQRY
  – iNav session user is “UEHLING” & no group profile



Untitled - Run SQL Scripts - Lp89ut27.rch.stglabs.ibm.com(Lp89ut27) *
File Edit View Run VisualExplain Monitor Options Connection Help
Messages
Global Variables
select * from empdta.e
Session A - [27 x 132]
File Edit View Communication Actions Window Help

```
select * from empdta.emptbl
```

Select all rows from table EMPTBL via select * from empdta.emptbl

results

FIRST	LAST	SSN
Jeffrey	Uehling	xxx-xx-3444

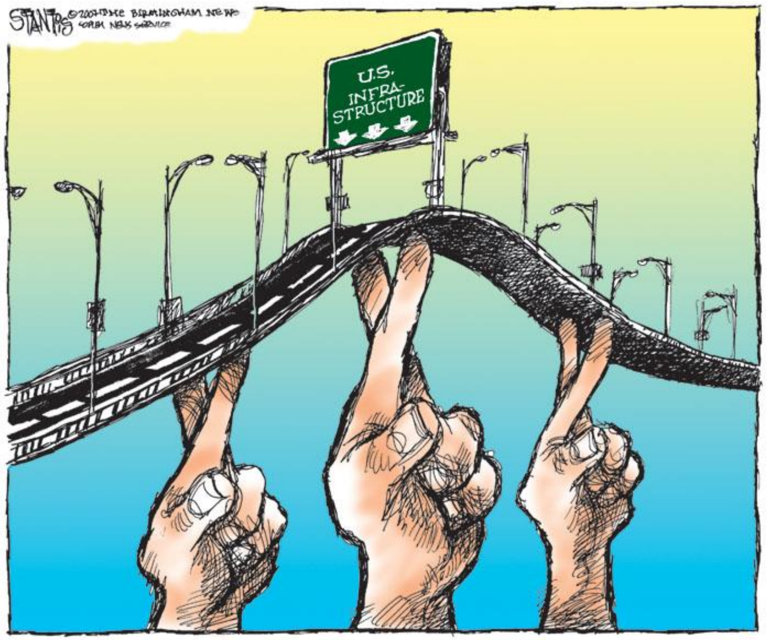
```
                                      Display Report
                                                          Report width . . . . . :      53
Position to line  . . . . .   ______                      Shift to column  . . . . . .   _____
Line   ....+....1....+....2....+....3....+....4....+....5...
       First Name        Last Name         Social Security Num
000001 Jeffrey           Uehling               xxx-xx-3444
****** ********  End of report  ********

                                                                                  Bottom
F3=Exit      F12=Cancel      F19=Left      F20=Right      F21=Split      F22=Width 80
```

Row Permissions and Column Masking activated

7.2 Security Enhancements Continued

Security Enhancements – infrastructure currency

- System SSL (security updates to industry standards)
- Java – latest version (with quarterly updates)
- Web Servers – updated to latest levels for security compliance
- PASE Updates
  - Latest AIX release, 7.1 (this is not IBM i 7.1)
  - OpenSSL to latest version 1.0.2g

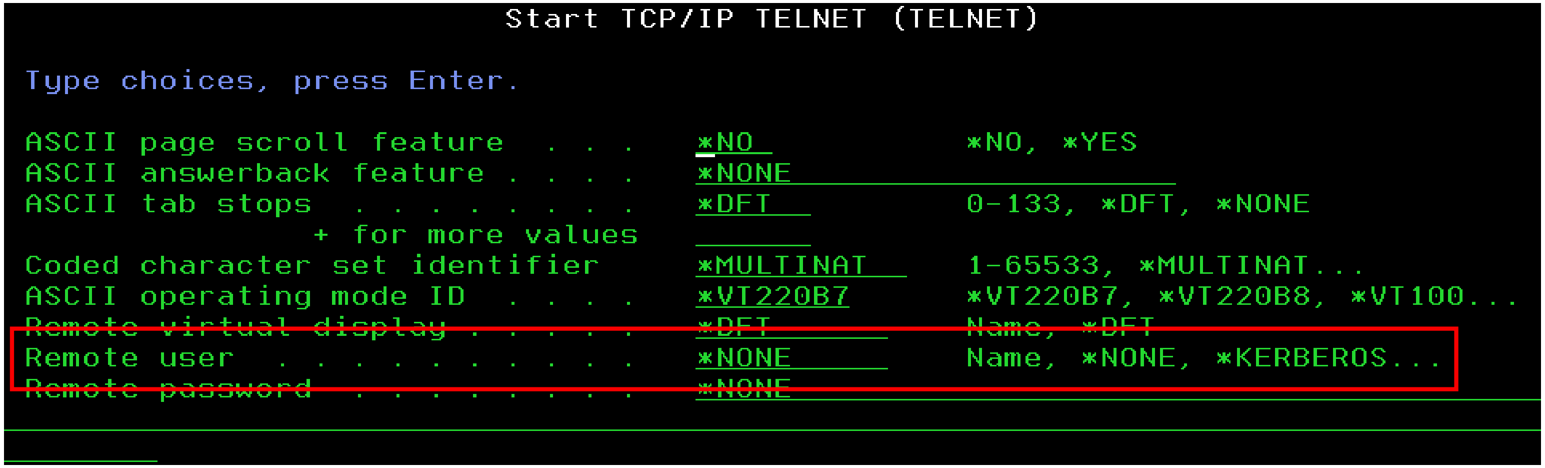


Security Enhancements – Crypto Performance

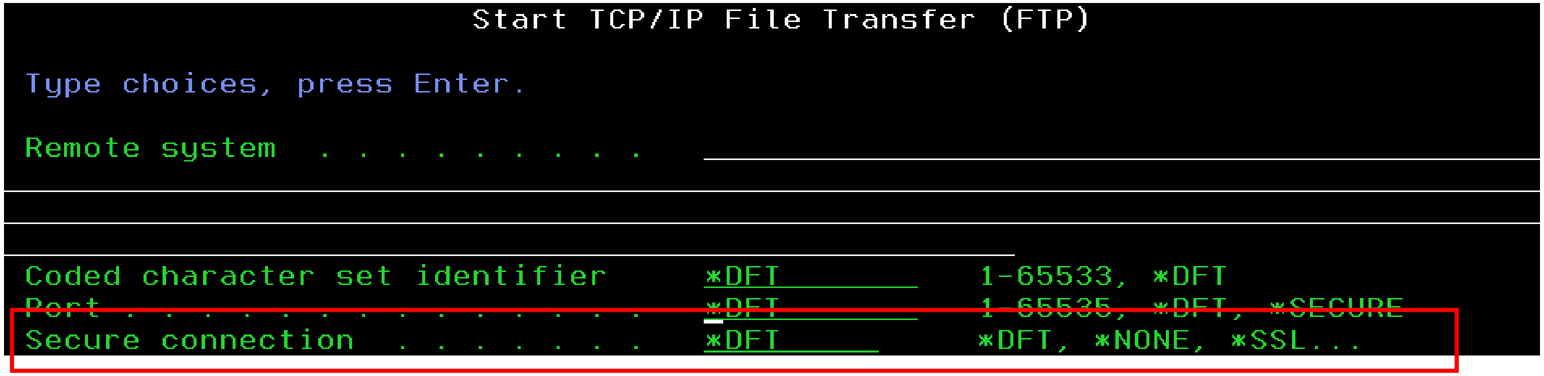
- Power 8 in-core Cryptographic Performance Acceleration
  - Support within the processor itself, no additional products or HW required
  - “Automatic” performance acceleration for certain cryptographic algorithms
    - AES & SHA-2 message digest
  - Does not support “cryptographic key” storage
    - Certain customers will still need the HW Cryptographic Coprocessor Card
  - Performance gains will be realized in support such as:
    - Customer applications that use the Crypto Services APIs
    - SSL (Secure Socket Layer)
    - VPN (Virtual Private Network)
    - Software Tape Encryption

Security Enhancements – Single Sign-on

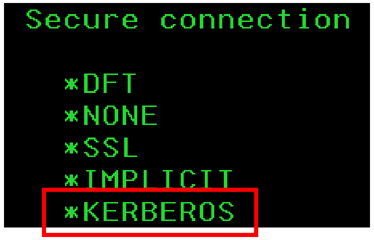
- Enhance both FTP and TELNET to support authenticating with Kerberos (SSO)
  - Kerberos authentication and Enterprise Identity Mapping integrated in FTP & TELNET
  - Integrates into the IBM i SSO application suite
    - FTP client and server support
    - Telnet client and server support



```
                          Start TCP/IP TELNET (TELNET)

 Type choices, press Enter.

 ASCII page scroll feature  . . .   *NO            *NO, *YES
 ASCII answerback feature . . . .   *NONE
 ASCII tab stops  . . . . . . . .   *DFT           0-133, *DFT, *NONE
               + for more values
 Coded character set identifier     *MULTINAT      1-65533, *MULTINAT...
 ASCII operating mode ID  . . . .   *VT220B7       *VT220B7, *VT220B8, *VT100...
 Remote virtual display . . . . .   *DFT           Name, *DFT
 Remote user  . . . . . . . . . .   *NONE          Name, *NONE, *KERBEROS...
 Remote password  . . . . . . . .   *NONE
```



```
                      Start TCP/IP File Transfer (FTP)

 Type choices, press Enter.

 Remote system  . . . . . . . . .




 Coded character set identifier     *DFT           1-65533, *DFT
 Port . . . . . . . . . . . . . .   *DFT           1-65535, *DFT, *SECURE
 Secure connection  . . . . . . .   *DFT           *DFT, *NONE, *SSL...
```

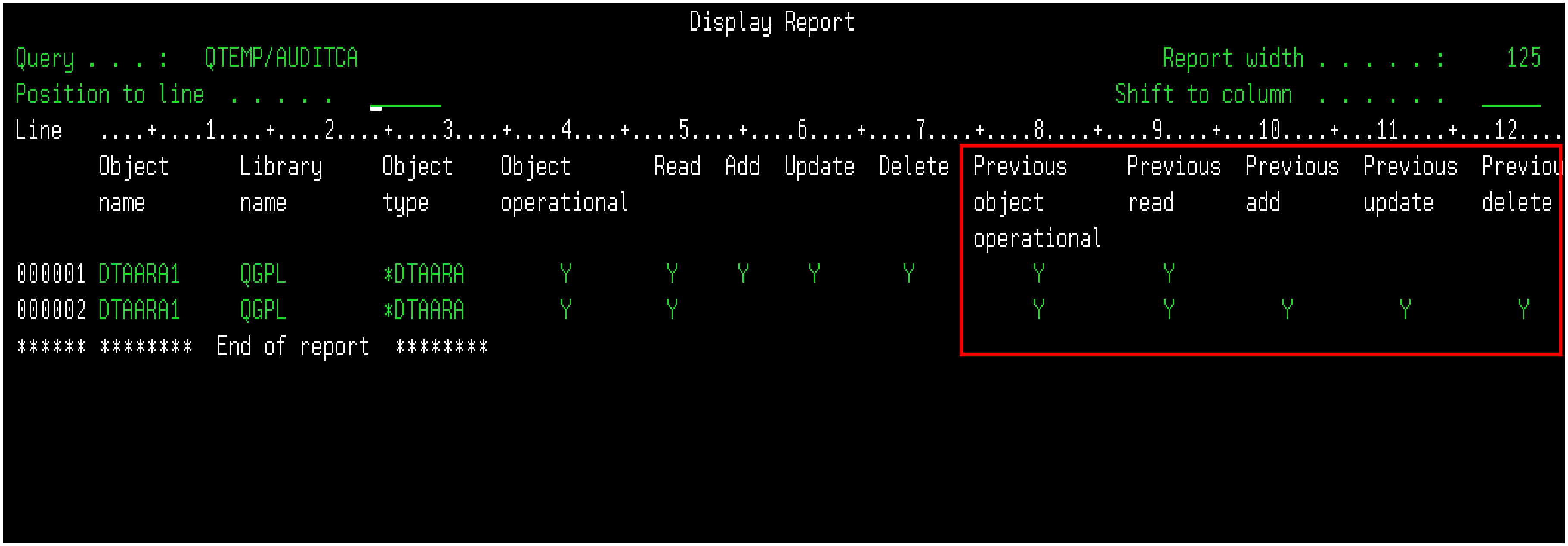


```
 Secure connection

   *DFT
   *NONE
   *SSL
   *IMPLICIT
   *KERBEROS
```

Security Enhancements – Audit Record Changes

- Additional data logged in security audit records
  - Both “before” and “after” values logged in the audit record
    - Prior release had only the “after” values
    - **Many audit records** have been updated to log before/after data
      - See appendix F of the security reference pdf in knowledge center

Example: Query of CA (Change Authority) audit record data from QAUDJRN

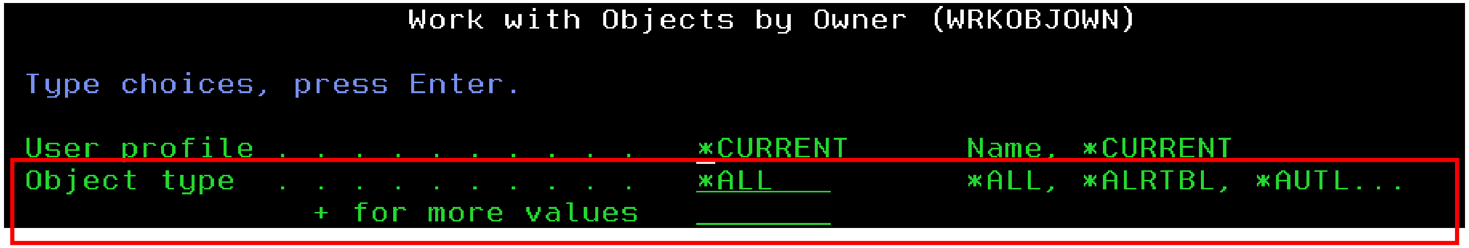


```
                                   Display Report
Query . . . :   QTEMP/AUDITCA                                             Report width . . . . . :     125
Position to line  . . . . .  _____                                      Shift to column  . . . . . .  _____
Line   ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+...10....+...11....+...12....
       Object     Library    Object    Object       Read  Add  Update  Delete  Previous     Previous  Previous  Previous  Previou
       name       name       type      operational                            object       read      add       update    delete
                                                                              operational
000001 DTAARA1    QGPL       *DTAARA        Y        Y     Y     Y       Y        Y            Y
000002 DTAARA1    QGPL       *DTAARA        Y        Y                            Y            Y         Y         Y         Y
****** ********  End of report  ********
```

Security Enhancements - continued

- New option, via QPWDRULES system value, to enforce password composition rules for security officers/admins
  - *ALLCRTCHG value added to QPWDRULES
  - CRTUSRPRF & CHGUSRPRF will honor password syntax rules

- New Object Type parameter added to the Security “WRK” commands
  - WRKOBJOWN, WRKOBJPGP, WRKOBJPVT



```
                     Work with Objects by Owner (WRKOBJOWN)

Type choices, press Enter.

User profile . . . . . . . . . .   *CURRENT      Name, *CURRENT
Object type  . . . . . . . . . .   *ALL          *ALL, *ALRTBL, *AUTL...
               + for more values
```

System SSL - New in 7.2 (PTFs back to 7.1)

- Transport Layer Security version 1.1 & 1.2 protocol (TLSv1.1 and TLSv1.2) RFC 4346 & RFC 5246
  - SHA2 support

  WARNING: Payment Card Industry (PCI) will require TLS 1.1 or TLS 1.2 in June, 2018.   IBM i 6.1 does not support TLS 1.1 or TLS 1.2.

- Online Certificate Status Protocol (OCSP)
  - A method to determine the revocation status for a digital certificate.

System SSL New in IBM i 7.2

- Elliptic Curve Cryptography (ECC)
  - Asymmetric encryption algorithm similar to RSA. ECC has an advantage over RSA in that it has smaller key sizes and better computational performance.
- Elliptic Curve Digital Signature Algorithm (ECDSA) certificates
- Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) key exchange method
- Galois/Counter Mode (GCM) – a mode of operation for symmetric key cryptographic block ciphers. Considered more secure than Cipher Block Chaining (CBC) mode.

- New 7.2 SSL Ciphersuites
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384

System SSL 7.2 Multiple Certificate Support

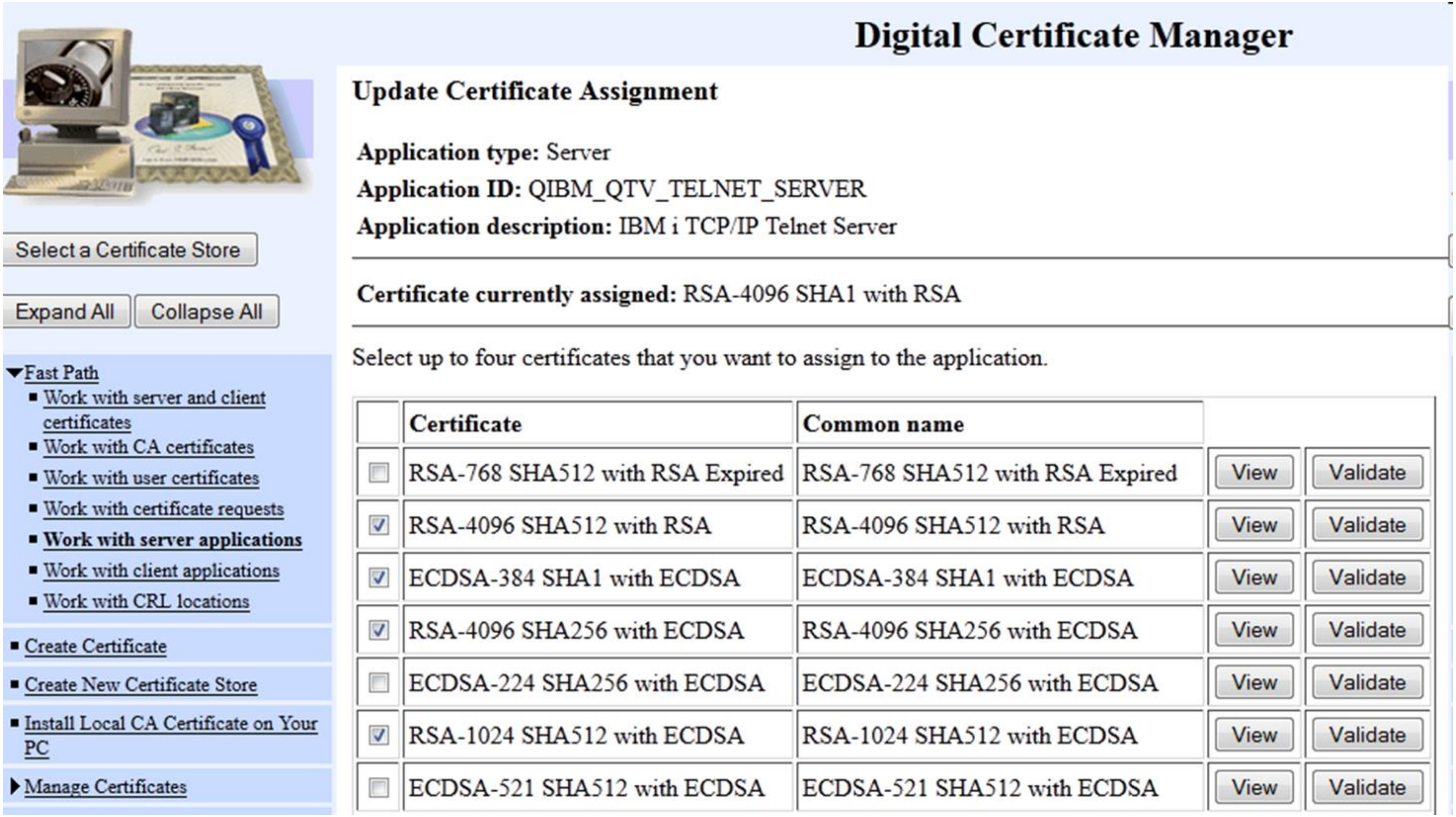
- Up to four unique certificates can be assigned to a server at one time.
  - One certificate is selected during each secure session negotiation.
    - Server configuration
    - Client capabilities and preferences

- Allows both RSA and ECDSA certificates to be used during transition phase.
  - The transition phase could last indefinitely.

- Configured via Application Definition or with GSKit API

- DCM allows multiple local CAs
  - RSA and ECDSA CAs and certificates can be created locally

Multiple Server Certificates



Select a Certificate Store
Expand All
Collapse All
Fast Path
Work with server and client certificates
Work with CA certificates
Work with user certificates
Work with certificate requests
Work with server applications
Work with client applications
Work with CRL locations
Create Certificate
Create New Certificate Store
Install Local CA Certificate on Your PC
Manage Certificates

Digital Certificate Manager

Update Certificate Assignment

Application type: Server

Application ID: QIBM_QTV_TELNET_SERVER

Application description: IBM i TCP/IP Telnet Server

Certificate currently assigned: RSA-4096 SHA1 with RSA

Select up to four certificates that you want to assign to the application.

	Certificate	Common name		
□	RSA-768 SHA512 with RSA Expired	RSA-768 SHA512 with RSA Expired	View	Validate
☑	RSA-4096 SHA512 with RSA	RSA-4096 SHA512 with RSA	View	Validate
☑	ECDSA-384 SHA1 with ECDSA	ECDSA-384 SHA1 with ECDSA	View	Validate
☑	RSA-4096 SHA256 with ECDSA	RSA-4096 SHA256 with ECDSA	View	Validate
□	ECDSA-224 SHA256 with ECDSA	ECDSA-224 SHA256 with ECDSA	View	Validate
☑	RSA-1024 SHA512 with ECDSA	RSA-1024 SHA512 with ECDSA	View	Validate
□	ECDSA-521 SHA512 with ECDSA	ECDSA-521 SHA512 with ECDSA	View	Validate

7.3 Security Enhancements

Miscellaneous 7.3 Security Changes

- Expand the CP (Create/Change Profile) audit record
  - Audit all parameter changes in the CP audit record
  - Prior to 7.2, CP contained “security related” CRT/CHGUSRPRF parameter changes in the audit record
  - In 7.3, all security and “environmental” CRT/CHGUSRPRF parameter changes are included in the audit record

- Enhance Digital Certificate Manager
  - Fully support digital certificate dates beyond 2038
    - PTF support back to previous releases

Issue: Monitoring Network Traffic to & from IBM i

- Admins may not be aware of all inbound and outbound communication sessions

- Is the communication channel secure?

- How secure is the connection?

- IBM recommends or disables a weak security algorithm or cipher suite. Is the weak algorithm or cipher suite being used?

7.3 Solution: Network Auditing

New Support to audit inbound and outbound network connections

- New/Updated QAUDLVL2 values (audit system value)
  - *NETSECURE
    - Network Connections are audited (Secure Connections)
    - *NETSCK (existing QAUDLVL value) required to audit unsecure connections
  - *NETUDP
    - User Datagram Protocol audit (Secure and Unsecure Connections)
    - One record per UDP audit interval per unique four-tuple
    - UDP audit interval defaults to 12 hours
    - IPCONFIG option udpAuditInterval controls interval setting
  - *NETTELSVR
    - Telnet auditing (Secure and Unsecure Connections)
  - Audit Data that is captured:
    - Local/Remote IP Addresses, Port information, Cipher Suite

7.3 Authority Collection

NOTE: See chapter 10 of the Security Reference PDF in the Knowledge Center for Authority Collection documentation.

Background: Security and Compliance - the Issue

- Customers run many applications on a single partition
  - No detailed knowledge of the applications… where is the data?
    - Data in DB2 or IFS … **but where**?
  - Once found, how do you lock down security without application breakage?
    - What is the **"minimum"** authority level that can be granted for the end user?
  - Many customers have little to no knowledge of what interfaces an application uses so the authority requirements cannot be determined
  - Applications are shipped with excessive public authority (common problem) which leads to security exposures
- The problem: customers don't change security leaving data exposed
  - Example: Think about your personal device, over 1 million files on a single user system
  - What if this device was a multi-user system… how would you lock it down?
    - No knowledge of the application or data objects so very difficult to secure the objects

Solution: Authority Collection

- Build a utility that captures pertinent data associated with an authority check (included as part of the base OS)
  - The collection covers all native IBM i file systems
  - Focus on capturing only unique instances of the authority check
  - Run-time performance, while the collection is active, will degrade 2-3%
  - Storage consideration for long running authority collection

- The collection includes key pieces of information… (including)

“What authority is **<u>required</u>** for this authority check”

Implementation

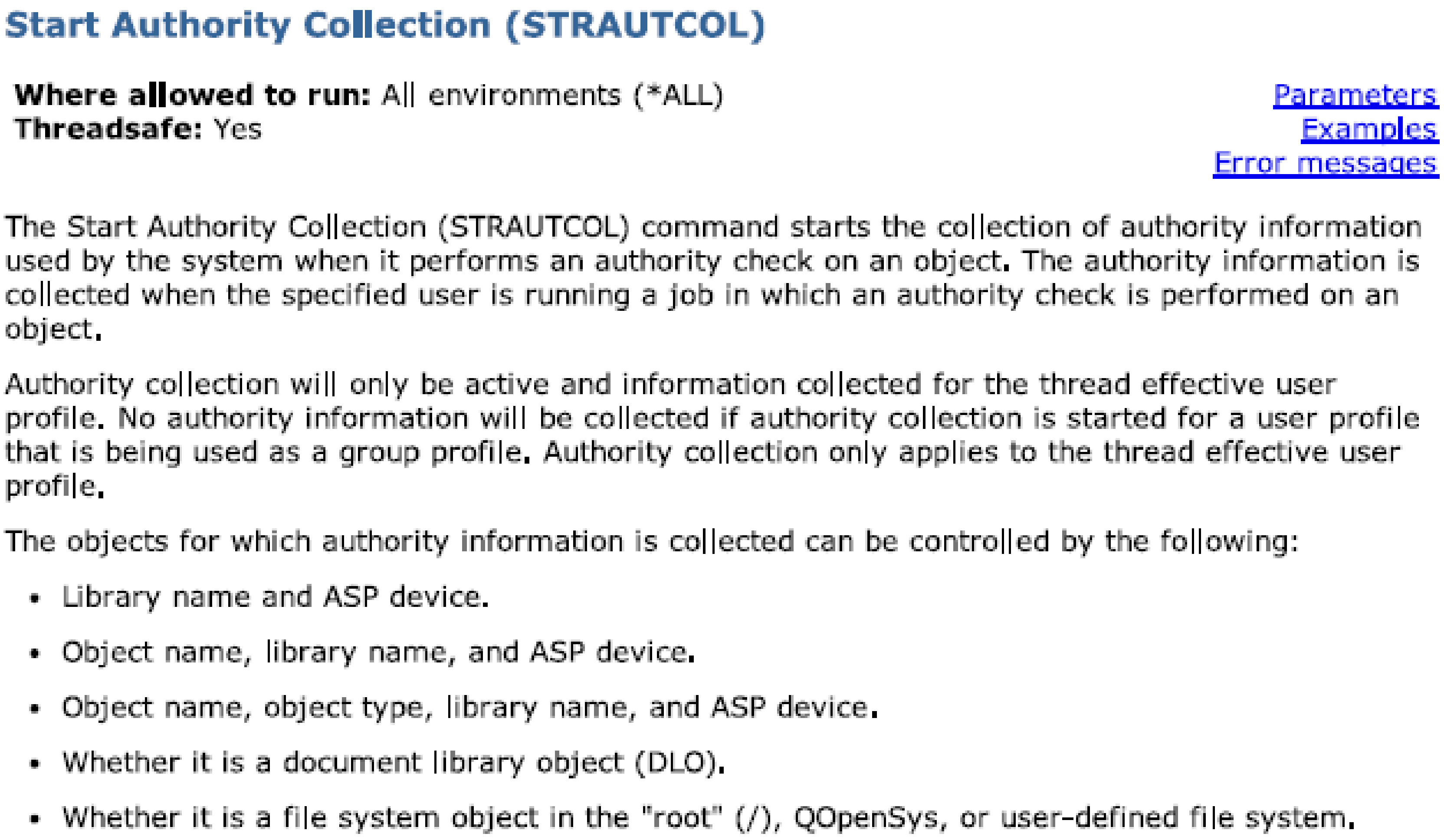
- The Authority collection is “user” based in the 7.3 release

  – Turn on the authority collection for a given user(s)

  – Collect authority information for the user… run the application(s)
    - Cannot collect information on the group level but object access allowed via a group profile authority is collected
    - Adopted authority information collected

  – QSYS file system has object level selectivity but IFS (root, QOpenSys, UDFs do not have object level selectivity (all or nothing))

Turning on Authority Collection



Start Authority Collection (STRAUTCOL)

Where allowed to run: All environments (*ALL)
Threadsafe: Yes

Parameters
Examples
Error messages

The Start Authority Collection (STRAUTCOL) command starts the collection of authority information used by the system when it performs an authority check on an object. The authority information is collected when the specified user is running a job in which an authority check is performed on an object.

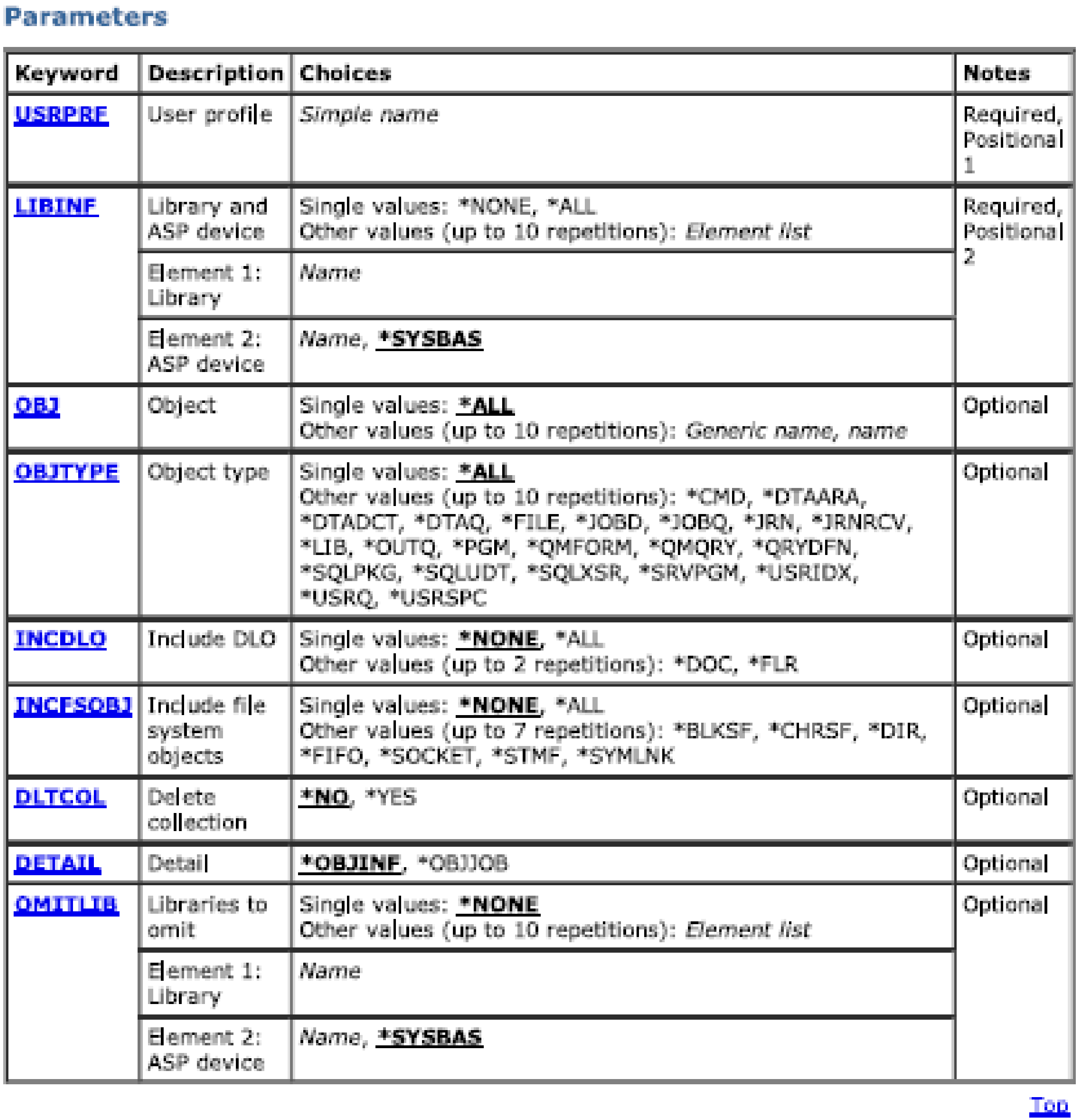
Authority collection will only be active and information collected for the thread effective user profile. No authority information will be collected if authority collection is started for a user profile that is being used as a group profile. Authority collection only applies to the thread effective user profile.

The objects for which authority information is collected can be controlled by the following:

- Library name and ASP device.
- Object name, library name, and ASP device.
- Object name, object type, library name, and ASP device.
- Whether it is a document library object (DLO).
- Whether it is a file system object in the "root" (/), QOpenSys, or user-defined file system.

NOTE: Authority collection can be managed via users/groups in Navigator

Start Authority Collection (STRAUTCOL)



Parameters

Keyword	Description	Choices	Notes
USRPRF	User profile	*Simple name*	Required, Positional 1
LIBINF	Library and ASP device	Single values: *NONE, *ALL Other values (up to 10 repetitions): *Element list*	Required, Positional 2
	Element 1: Library	*Name*	
	Element 2: ASP device	*Name*, ***SYSBAS**	
OBJ	Object	Single values: ***ALL** Other values (up to 10 repetitions): *Generic name, name*	Optional
OBJTYPE	Object type	Single values: ***ALL** Other values (up to 10 repetitions): *CMD, *DTAARA, *DTADCT, *DTAQ, *FILE, *JOBD, *JOBQ, *JRN, *JRNRCV, *LIB, *OUTQ, *PGM, *QMFORM, *QMQRY, *QRYDFN, *SQLPKG, *SQLUDT, *SQLXSR, *SRVPGM, *USRIDX, *USRQ, *USRSPC	Optional
INCDLO	Include DLO	Single values: ***NONE**, *ALL Other values (up to 2 repetitions): *DOC, *FLR	Optional
INCFSOBJ	Include file system objects	Single values: ***NONE**, *ALL Other values (up to 7 repetitions): *BLKSF, *CHRSF, *DIR, *FIFO, *SOCKET, *STMF, *SYMLNK	Optional
DLTCOL	Delete collection	***NO**, *YES	Optional
DETAIL	Detail	***OBJINF**, *OBJJOB	Optional
OMITLIB	Libraries to omit	Single values: ***NONE** Other values (up to 10 repetitions): *Element list*	Optional
	Element 1: Library	*Name*	
	Element 2: ASP device	*Name*, ***SYSBAS**	

Top

Authority Collection Data (subset of what is collected)

The Start Authority Collection (STRAUTCOL) command starts the collection of information used by the system when it performs an authority check on an object. The authority information is collected when the specified user is running a job in which an authority check is performed on a object.

The collected information contains the following:

- Object name
- Library name
- ASP device
- Object type
- SQL name
- SQL object type
- SQL schema name
- Path name and object name
- Authorization list for the object
- Required authority
- Current authority
- Authority source for the user that satisfies the authority request
- Adopted authority indicator (adopt was used to satisfy the authority request)
- Current adopted authority
- Adopted authority source
- Adopting program name and indicator (adopting program that was used to satisfy the authority request)
- Adopting program library
- Adopting program object type (*PGM or *SRVPGM)
- Adopting program owner
- Stack info (most recent invocation and most recent user state invocation including procedure name and statement)
- Job name
- Job user
- Job number
- Current job user profile
- Group profile and indicator (group profile that was used to satisfy the authority request)
- Date and time of authority check

Where does the users authority to this object come from?

The authority collection information will tell you!

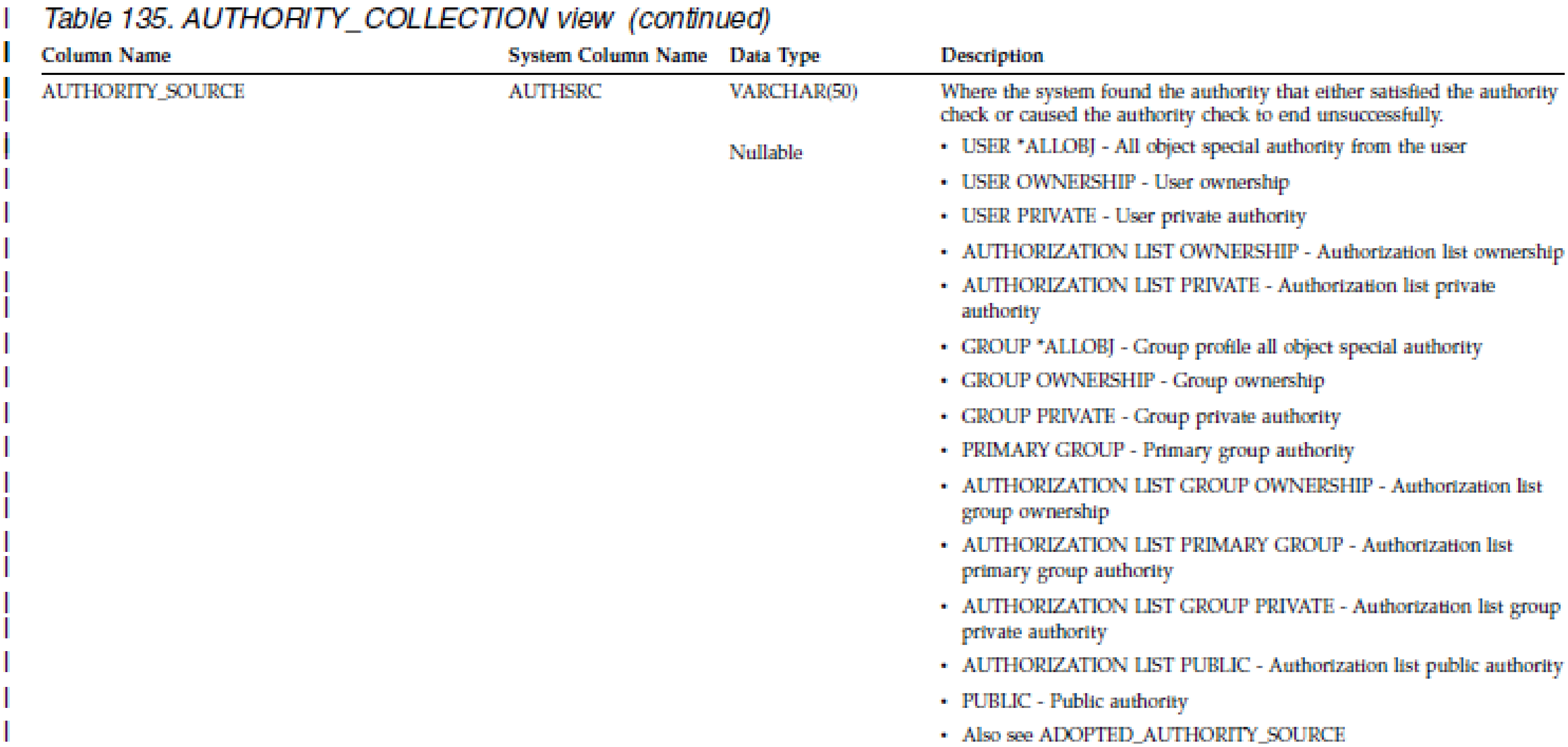
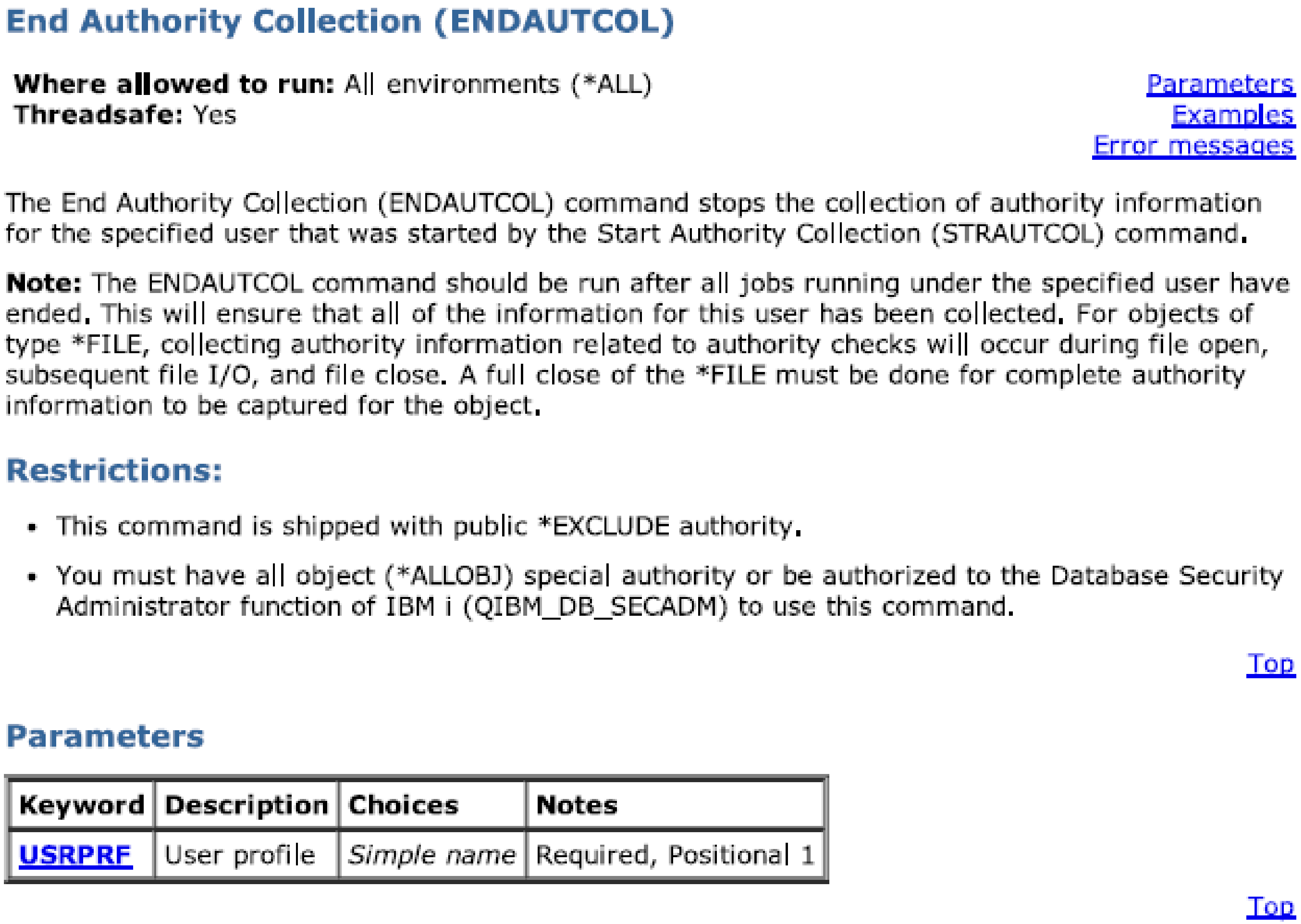


Table 135. AUTHORITY_COLLECTION view (continued)

Column Name	System Column Name	Data Type	Description
AUTHORITY_SOURCE	AUTHSRC	VARCHAR(50) Nullable	Where the system found the authority that either satisfied the authority check or caused the authority check to end unsuccessfully. • USER *ALLOBJ - All object special authority from the user • USER OWNERSHIP - User ownership • USER PRIVATE - User private authority • AUTHORIZATION LIST OWNERSHIP - Authorization list ownership • AUTHORIZATION LIST PRIVATE - Authorization list private authority • GROUP *ALLOBJ - Group profile all object special authority • GROUP OWNERSHIP - Group ownership • GROUP PRIVATE - Group private authority • PRIMARY GROUP - Primary group authority • AUTHORIZATION LIST GROUP OWNERSHIP - Authorization list group ownership • AUTHORIZATION LIST PRIMARY GROUP - Authorization list primary group authority • AUTHORIZATION LIST GROUP PRIVATE - Authorization list group private authority • AUTHORIZATION LIST PUBLIC - Authorization list public authority • PUBLIC - Public authority • Also see ADOPTED_AUTHORITY_SOURCE



End Authority Collection (ENDAUTCOL)

Where allowed to run: All environments (*ALL)
Threadsafe: Yes

Parameters
Examples
Error messages

The End Authority Collection (ENDAUTCOL) command stops the collection of authority information for the specified user that was started by the Start Authority Collection (STRAUTCOL) command.

Note: The ENDAUTCOL command should be run after all jobs running under the specified user have ended. This will ensure that all of the information for this user has been collected. For objects of type *FILE, collecting authority information related to authority checks will occur during file open, subsequent file I/O, and file close. A full close of the *FILE must be done for complete authority information to be captured for the object.

Restrictions:

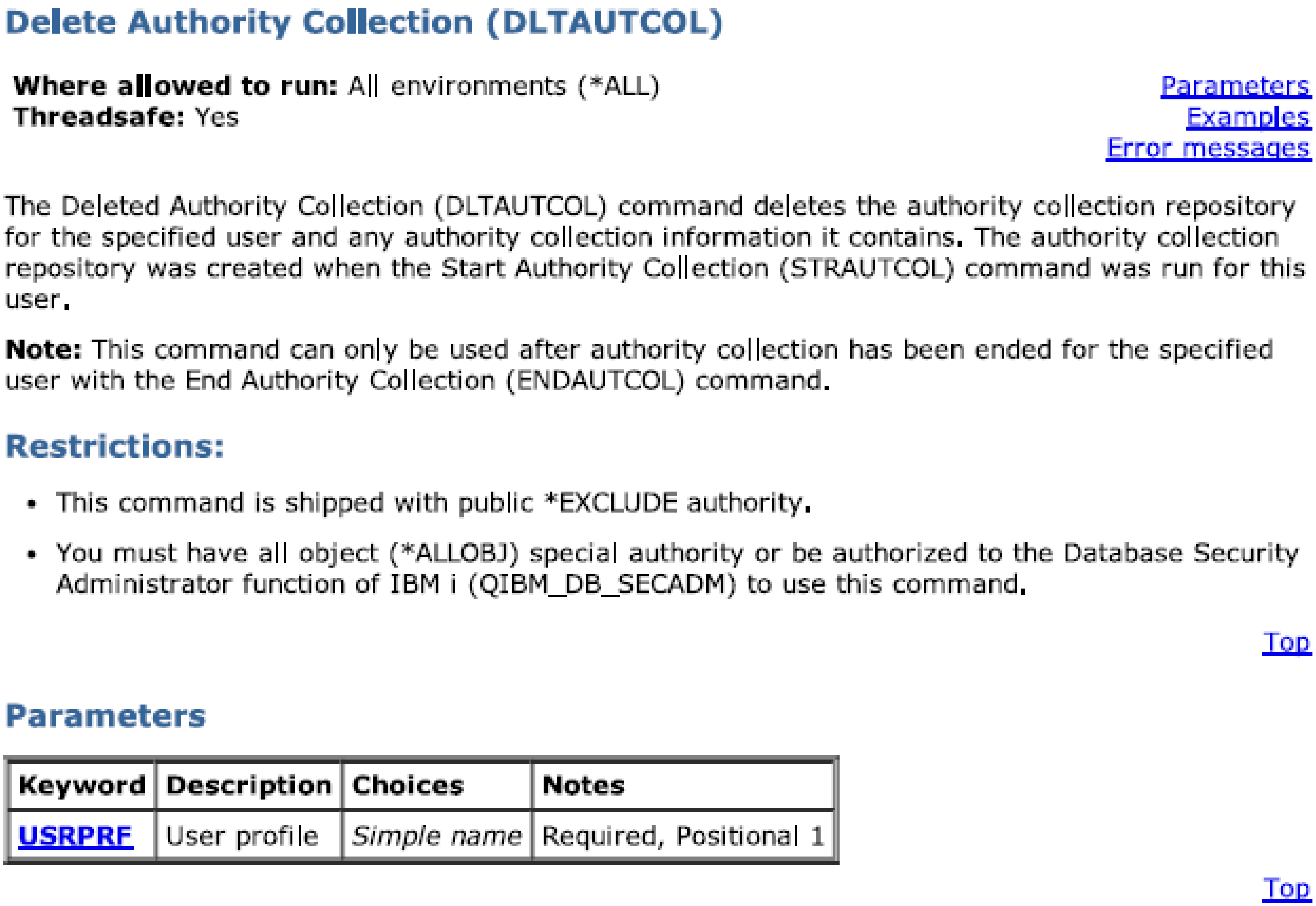
- This command is shipped with public *EXCLUDE authority.
- You must have all object (*ALLOBJ) special authority or be authorized to the Database Security Administrator function of IBM i (QIBM_DB_SECADM) to use this command.

Top

Parameters

Keyword	Description	Choices	Notes
USRPRF	User profile	*Simple name*	Required, Positional 1

Top



Delete Authority Collection (DLTAUTCOL)

Where allowed to run: All environments (*ALL)
Threadsafe: Yes

Parameters
Examples
Error messages

The Deleted Authority Collection (DLTAUTCOL) command deletes the authority collection repository for the specified user and any authority collection information it contains. The authority collection repository was created when the Start Authority Collection (STRAUTCOL) command was run for this user.

Note: This command can only be used after authority collection has been ended for the specified user with the End Authority Collection (ENDAUTCOL) command.

Restrictions:

- This command is shipped with public *EXCLUDE authority.
- You must have all object (*ALLOBJ) special authority or be authorized to the Database Security Administrator function of IBM i (QIBM_DB_SECADM) to use this command.

Top

Parameters

Keyword	Description	Choices	Notes
USRPRF	User profile	*Simple name*	Required, Positional 1

Top

Authority Collection example

Authority Collection Data – Example

Sign on as an “Administrator” with *ALLOBJ & *SECADM authority

- Turn on Authority Collection for user “FRED1”
- **STRAUTCOL USRPRF(FRED1) LIBINF(*ALL) INCFSOBJ(*ALL) DLTCOL(*YES)**

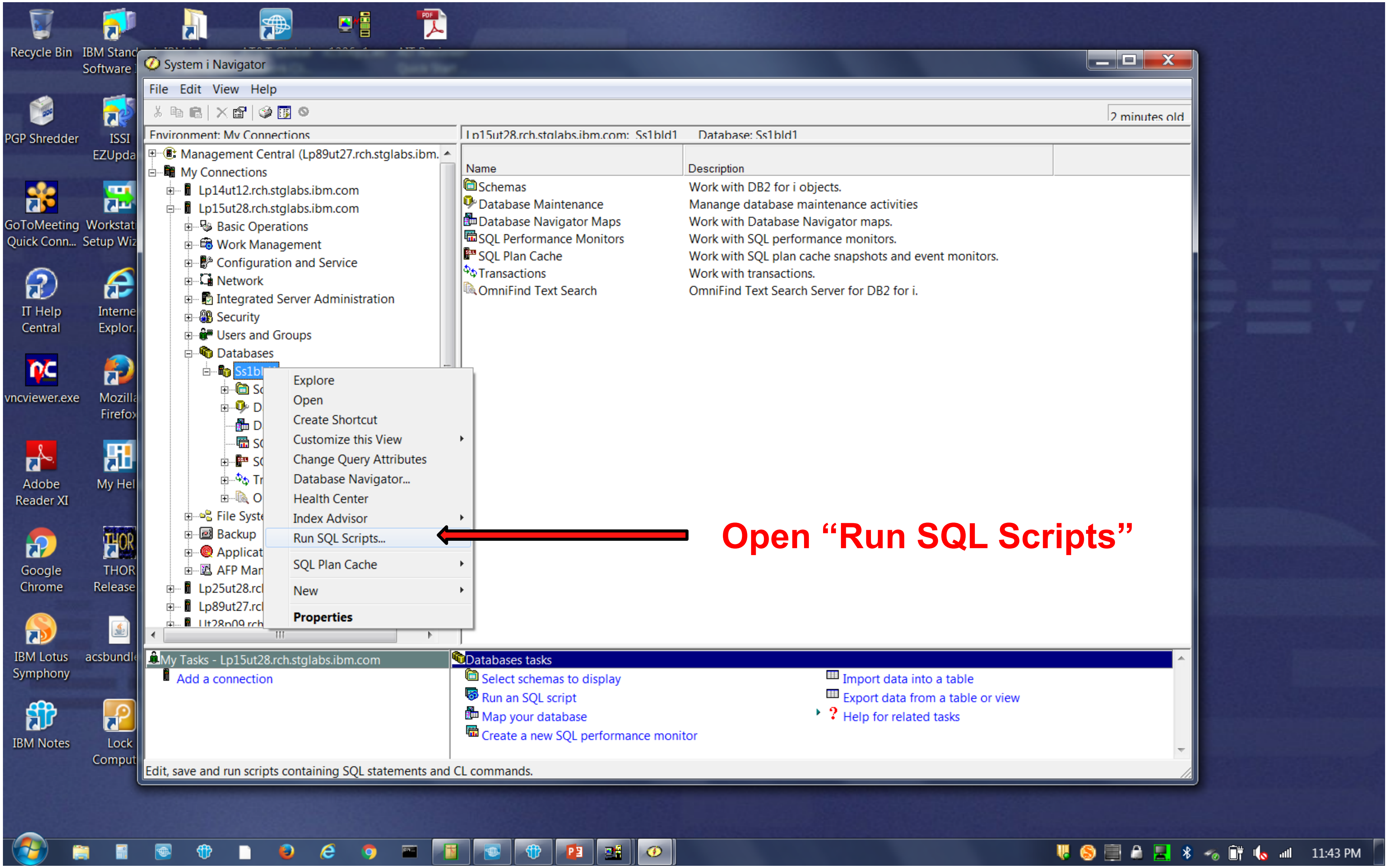
Sign on as user “FRED1”

- Call a simple CL program, AUTCOL, that runs several CL commands
- **CALL PGM(QGPL/AUTCOL)**

```
PGM  /* program AUTCOL */
   DSPPFM FILE(QGPL/TESTFILE1)
   CALL PGM(QGPL/PAYPGM1)
   DSPDTAARA DTAARA(QGPL/PAYDTAARA)
ENDPGM
```

Authority Collection View – Display the Data

Launch “Run SQL Scripts” from Navigator (as an administrator)



Open “Run SQL Scripts”

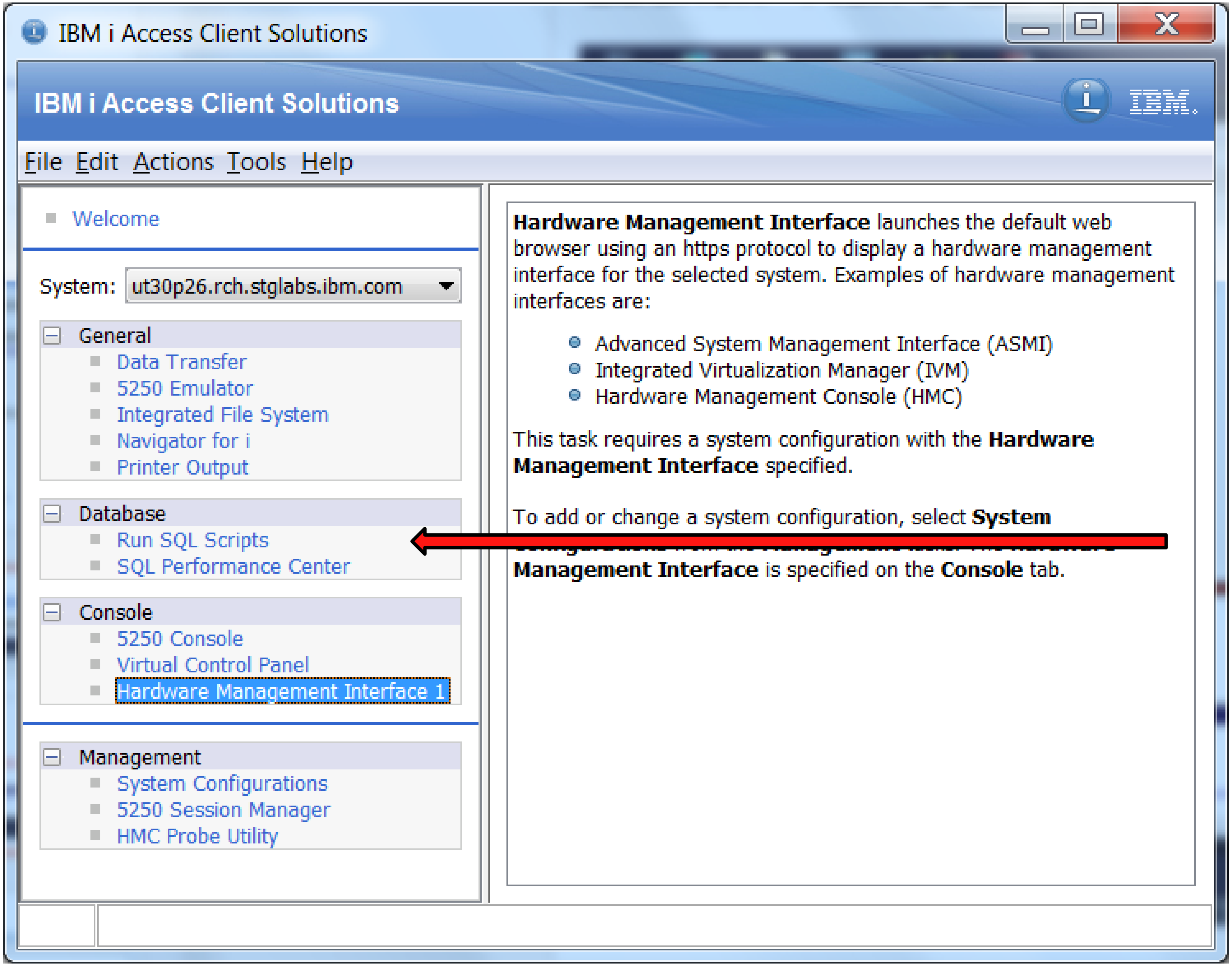
Lp15ut28.rch.stglabs.ibm.com: Ss1bld1   Database: Ss1bld1

Name	Description
Schemas	Work with DB2 for i objects.
Database Maintenance	Manange database maintenance activities
Database Navigator Maps	Work with Database Navigator maps.
SQL Performance Monitors	Work with SQL performance monitors.
SQL Plan Cache	Work with SQL plan cache snapshots and event monitors.
Transactions	Work with transactions.
OmniFind Text Search	OmniFind Text Search Server for DB2 for i.

Edit, save and run scripts containing SQL statements and CL commands.

Authority Collection View – Display the Data

Or… Launch “Run SQL Scripts” from ACS (as an administrator)



Hardware Management Interface launches the default web browser using an https protocol to display a hardware management interface for the selected system. Examples of hardware management interfaces are:

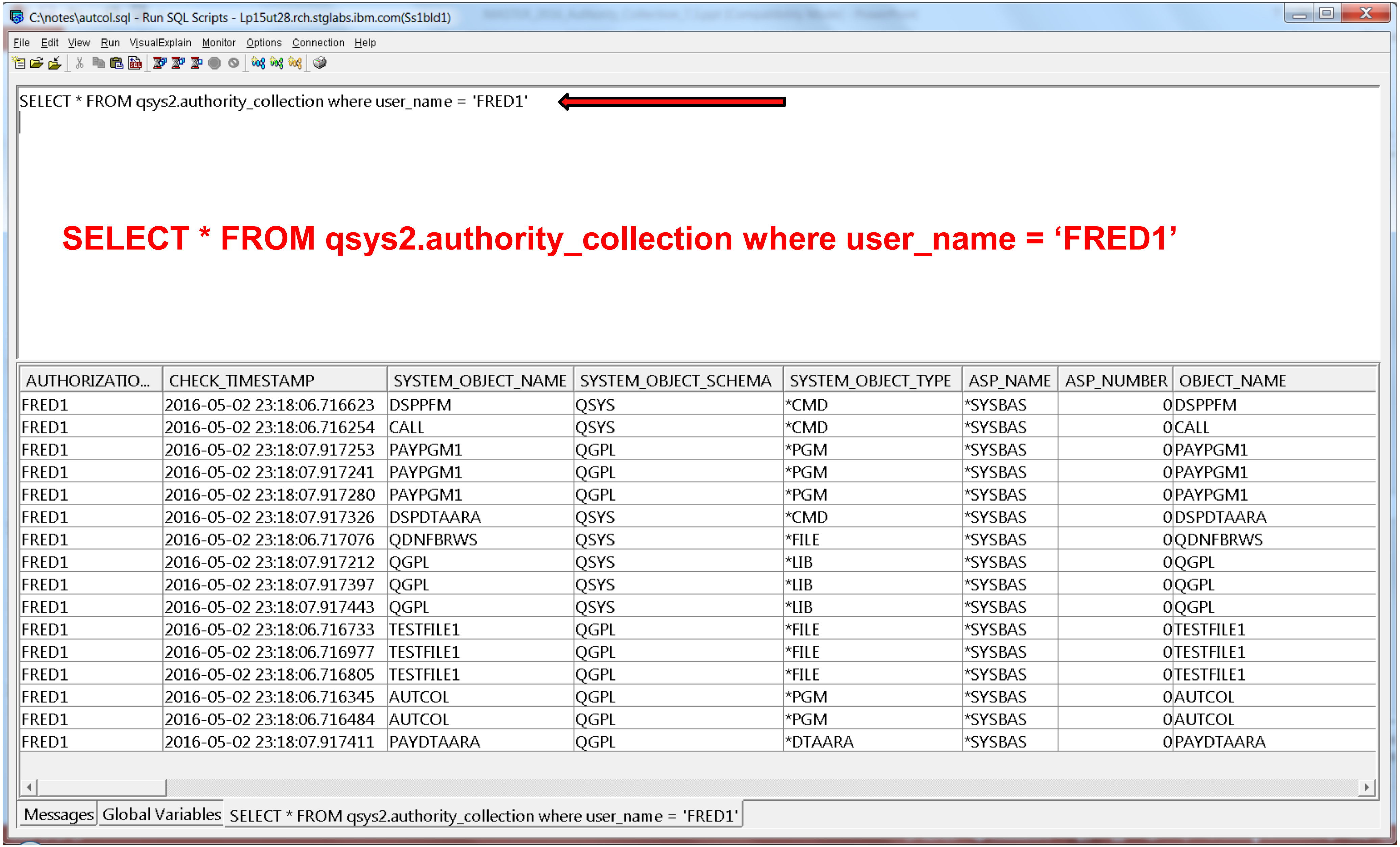
- Advanced System Management Interface (ASMI)
- Integrated Virtualization Manager (IVM)
- Hardware Management Console (HMC)

This task requires a system configuration with the **Hardware Management Interface** specified.

To add or change a system configuration, select **System Configurations** from the **Management** tasks. The **Hardware Management Interface** is specified on the **Console** tab.

Open “Run SQL Scripts”

Authority Collection – View


C:\notes\autcol.sql - Run SQL Scripts - Lp15ut28.rch.stglabs.ibm.com(Ss1bld1)
File Edit View Run VisualExplain Monitor Options Connection Help

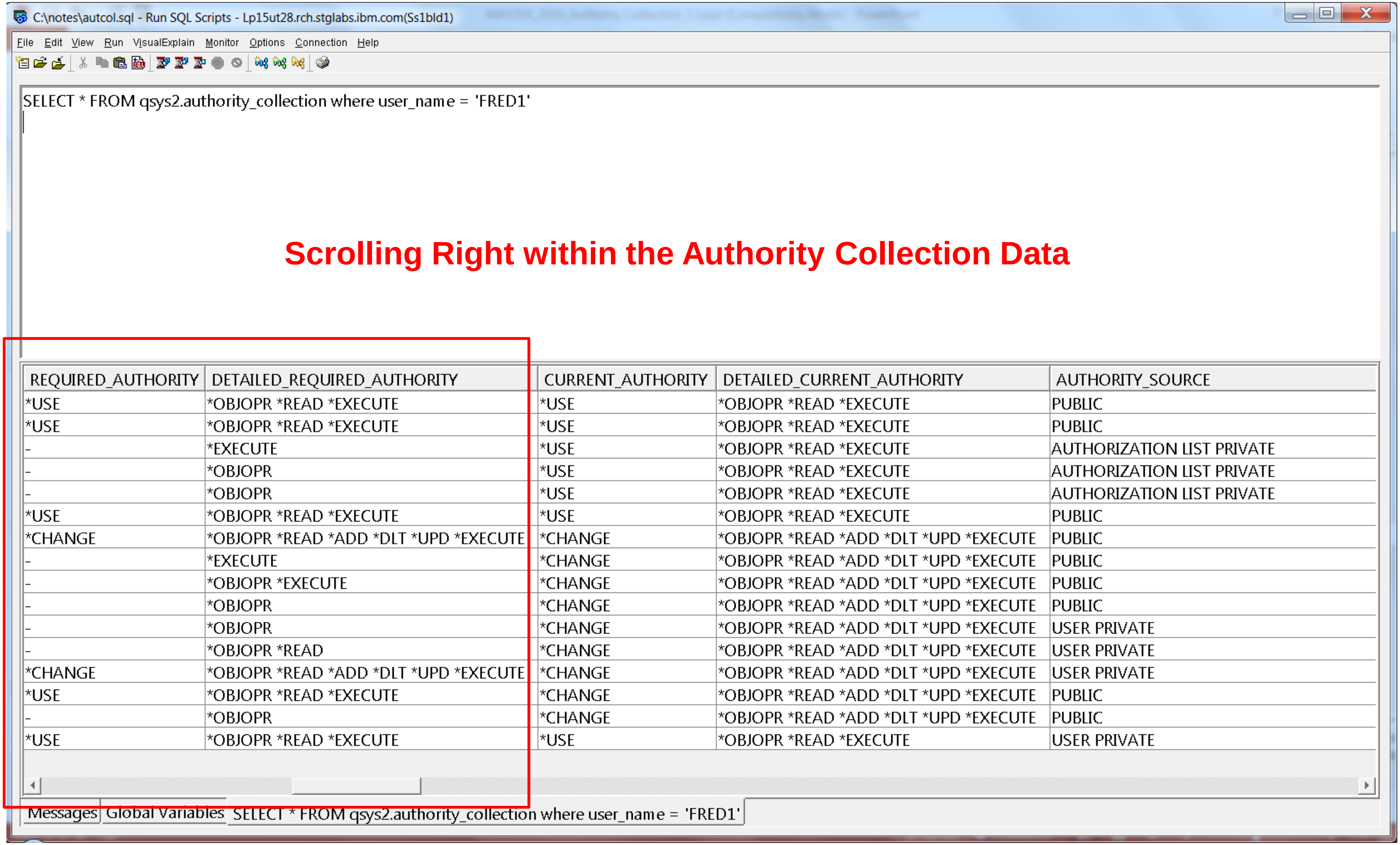
```
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1'
```

SELECT * FROM qsys2.authority_collection where user_name = ‘FRED1’

AUTHORIZATIO...	CHECK_TIMESTAMP	SYSTEM_OBJECT_NAME	SYSTEM_OBJECT_SCHEMA	SYSTEM_OBJECT_TYPE	ASP_NAME	ASP_NUMBER	OBJECT_NAME
FRED1	2016-05-02 23:18:06.716623	DSPPFM	QSYS	*CMD	*SYSBAS	0	DSPPFM
FRED1	2016-05-02 23:18:06.716254	CALL	QSYS	*CMD	*SYSBAS	0	CALL
FRED1	2016-05-02 23:18:07.917253	PAYPGM1	QGPL	*PGM	*SYSBAS	0	PAYPGM1
FRED1	2016-05-02 23:18:07.917241	PAYPGM1	QGPL	*PGM	*SYSBAS	0	PAYPGM1
FRED1	2016-05-02 23:18:07.917280	PAYPGM1	QGPL	*PGM	*SYSBAS	0	PAYPGM1
FRED1	2016-05-02 23:18:07.917326	DSPDTAARA	QSYS	*CMD	*SYSBAS	0	DSPDTAARA
FRED1	2016-05-02 23:18:06.717076	QDNFBRWS	QSYS	*FILE	*SYSBAS	0	QDNFBRWS
FRED1	2016-05-02 23:18:07.917212	QGPL	QSYS	*LIB	*SYSBAS	0	QGPL
FRED1	2016-05-02 23:18:07.917397	QGPL	QSYS	*LIB	*SYSBAS	0	QGPL
FRED1	2016-05-02 23:18:07.917443	QGPL	QSYS	*LIB	*SYSBAS	0	QGPL
FRED1	2016-05-02 23:18:06.716733	TESTFILE1	QGPL	*FILE	*SYSBAS	0	TESTFILE1
FRED1	2016-05-02 23:18:06.716977	TESTFILE1	QGPL	*FILE	*SYSBAS	0	TESTFILE1
FRED1	2016-05-02 23:18:06.716805	TESTFILE1	QGPL	*FILE	*SYSBAS	0	TESTFILE1
FRED1	2016-05-02 23:18:06.716345	AUTCOL	QGPL	*PGM	*SYSBAS	0	AUTCOL
FRED1	2016-05-02 23:18:06.716484	AUTCOL	QGPL	*PGM	*SYSBAS	0	AUTCOL
FRED1	2016-05-02 23:18:07.917411	PAYDTAARA	QGPL	*DTAARA	*SYSBAS	0	PAYDTAARA

Messages
Global Variables
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1'

Authority Collection – View

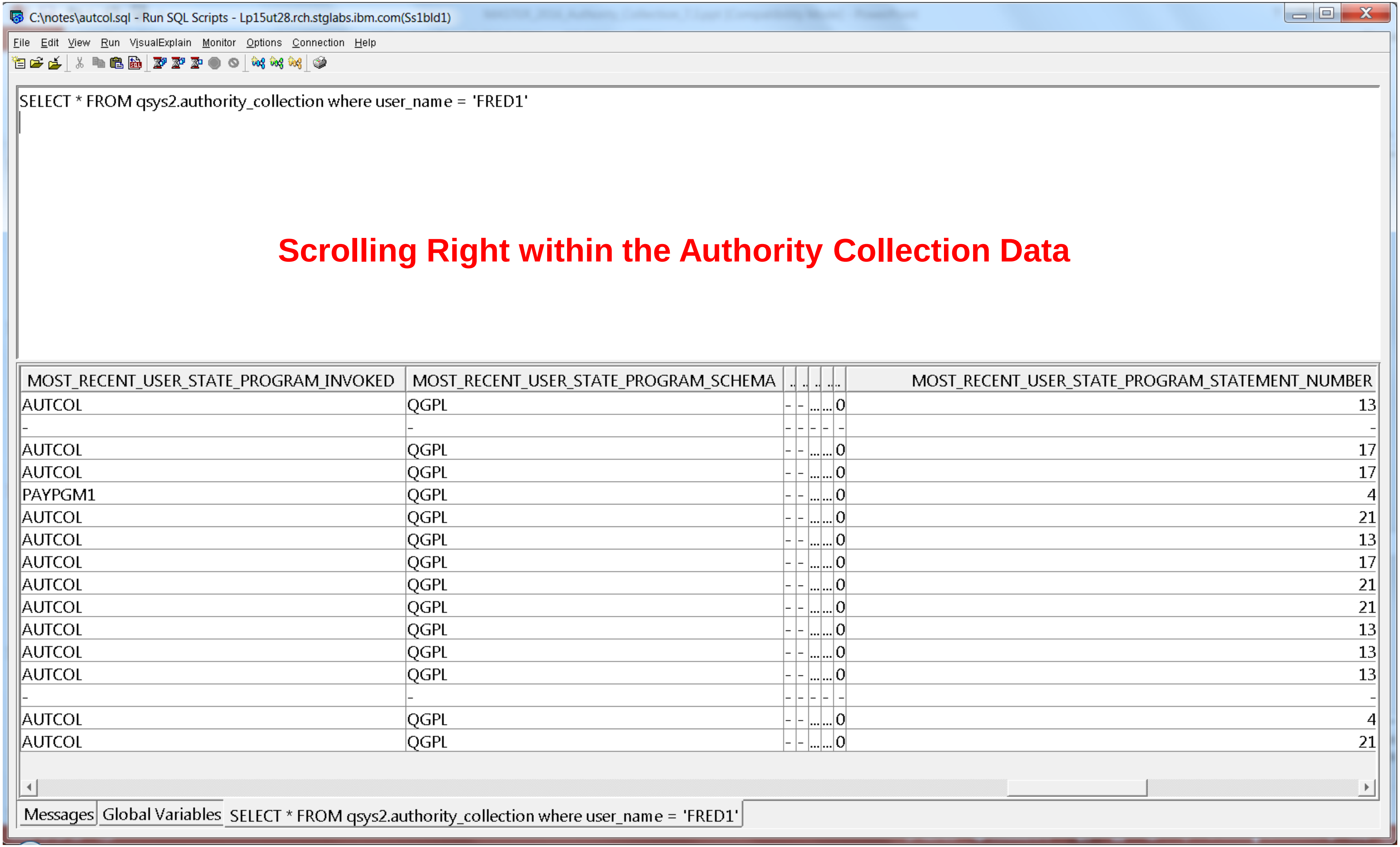

C:\notes\autcol.sql - Run SQL Scripts - Lp15ut28.rch.stglabs.ibm.com(Ss1bld1)
File Edit View Run VisualExplain Monitor Options Connection Help
Messages
Global Variables
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1'

```
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1'
```

Scrolling Right within the Authority Collection Data

REQUIRED_AUTHORITY	DETAILED_REQUIRED_AUTHORITY	CURRENT_AUTHORITY	DETAILED_CURRENT_AUTHORITY	AUTHORITY_SOURCE
*USE	*OBJOPR *READ *EXECUTE	*USE	*OBJOPR *READ *EXECUTE	PUBLIC
*USE	*OBJOPR *READ *EXECUTE	*USE	*OBJOPR *READ *EXECUTE	PUBLIC
-	*EXECUTE	*USE	*OBJOPR *READ *EXECUTE	AUTHORIZATION LIST PRIVATE
-	*OBJOPR	*USE	*OBJOPR *READ *EXECUTE	AUTHORIZATION LIST PRIVATE
-	*OBJOPR	*USE	*OBJOPR *READ *EXECUTE	AUTHORIZATION LIST PRIVATE
*USE	*OBJOPR *READ *EXECUTE	*USE	*OBJOPR *READ *EXECUTE	PUBLIC
*CHANGE	*OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*CHANGE	*OBJOPR *READ *ADD *DLT *UPD *EXECUTE	PUBLIC
-	*EXECUTE	*CHANGE	*OBJOPR *READ *ADD *DLT *UPD *EXECUTE	PUBLIC
-	*OBJOPR *EXECUTE	*CHANGE	*OBJOPR *READ *ADD *DLT *UPD *EXECUTE	PUBLIC
-	*OBJOPR	*CHANGE	*OBJOPR *READ *ADD *DLT *UPD *EXECUTE	PUBLIC
-	*OBJOPR	*CHANGE	*OBJOPR *READ *ADD *DLT *UPD *EXECUTE	USER PRIVATE
-	*OBJOPR *READ	*CHANGE	*OBJOPR *READ *ADD *DLT *UPD *EXECUTE	USER PRIVATE
*CHANGE	*OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*CHANGE	*OBJOPR *READ *ADD *DLT *UPD *EXECUTE	USER PRIVATE
*USE	*OBJOPR *READ *EXECUTE	*CHANGE	*OBJOPR *READ *ADD *DLT *UPD *EXECUTE	PUBLIC
-	*OBJOPR	*CHANGE	*OBJOPR *READ *ADD *DLT *UPD *EXECUTE	PUBLIC
*USE	*OBJOPR *READ *EXECUTE	*USE	*OBJOPR *READ *EXECUTE	USER PRIVATE

Authority Collection – View



C:\notes\autcol.sql - Run SQL Scripts - Lp15ut28.rch.stglabs.ibm.com(Ss1bld1)
File Edit View Run VisualExplain Monitor Options Connection Help

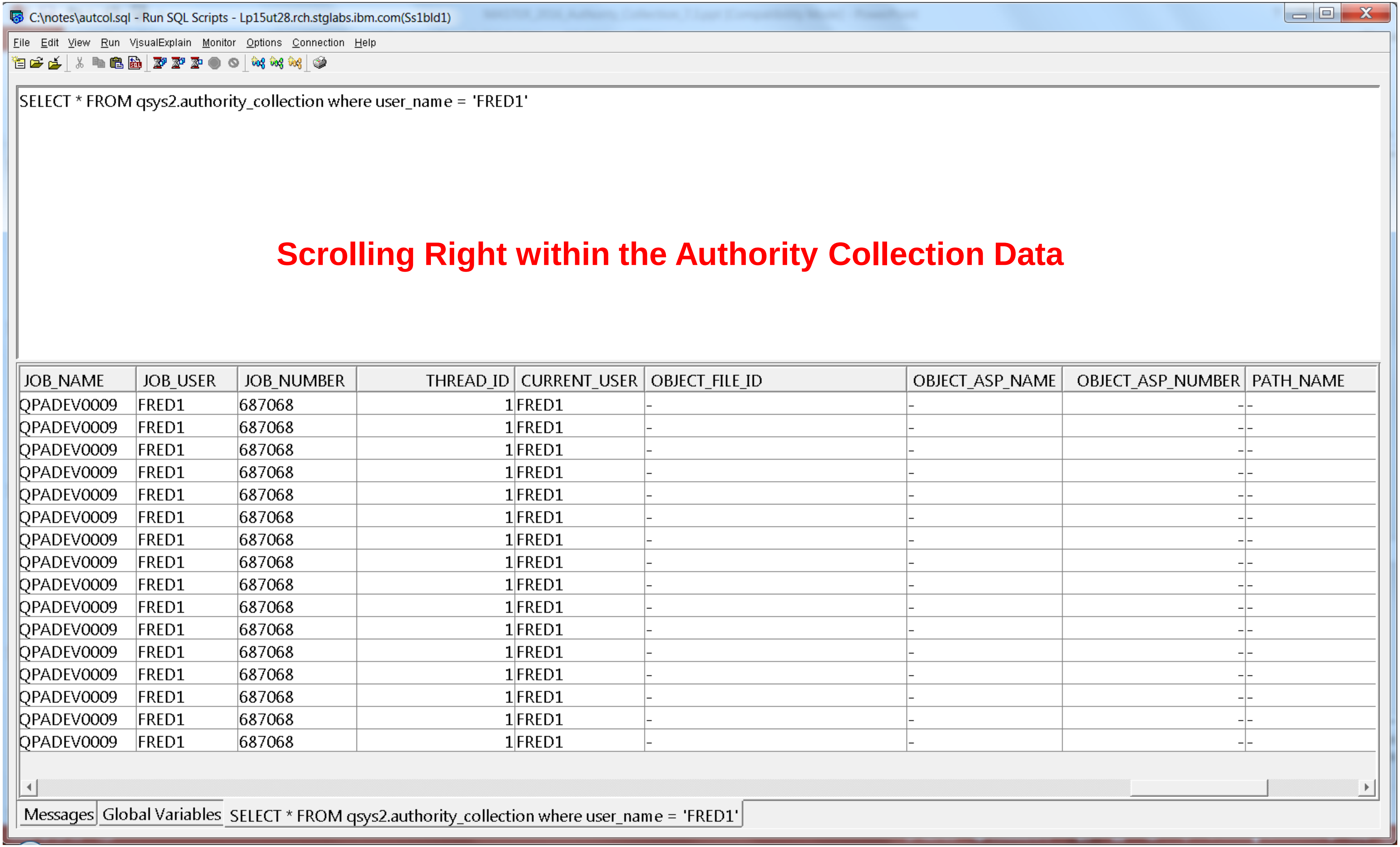
```
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1'
```

Scrolling Right within the Authority Collection Data

MOST_RECENT_USER_STATE_PROGRAM_INVOKED	MOST_RECENT_USER_STATE_PROGRAM_SCHEMA	..	..	..	..	..	MOST_RECENT_USER_STATE_PROGRAM_STATEMENT_NUMBER
AUTCOL	QGPL	-	-	...	...	0	13
-	-	-	-	-	-	-	-
AUTCOL	QGPL	-	-	...	...	0	17
AUTCOL	QGPL	-	-	...	...	0	17
PAYPGM1	QGPL	-	-	...	...	0	4
AUTCOL	QGPL	-	-	...	...	0	21
AUTCOL	QGPL	-	-	...	...	0	13
AUTCOL	QGPL	-	-	...	...	0	17
AUTCOL	QGPL	-	-	...	...	0	21
AUTCOL	QGPL	-	-	...	...	0	21
AUTCOL	QGPL	-	-	...	...	0	13
AUTCOL	QGPL	-	-	...	...	0	13
AUTCOL	QGPL	-	-	...	...	0	13
-	-	-	-	-	-	-	-
AUTCOL	QGPL	-	-	...	...	0	4
AUTCOL	QGPL	-	-	...	...	0	21

Messages
Global Variables
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1'

Authority Collection – View


C:\notes\autcol.sql - Run SQL Scripts - Lp15ut28.rch.stglabs.ibm.com(Ss1bld1)
File Edit View Run VisualExplain Monitor Options Connection Help
Messages
Global Variables
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1'

```
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1'
```

Scrolling Right within the Authority Collection Data

JOB_NAME	JOB_USER	JOB_NUMBER	THREAD_ID	CURRENT_USER	OBJECT_FILE_ID	OBJECT_ASP_NAME	OBJECT_ASP_NUMBER	PATH_NAME
QPADEV0009	FRED1	687068	1	FRED1	-	-	-	-
QPADEV0009	FRED1	687068	1	FRED1	-	-	-	-
QPADEV0009	FRED1	687068	1	FRED1	-	-	-	-
QPADEV0009	FRED1	687068	1	FRED1	-	-	-	-
QPADEV0009	FRED1	687068	1	FRED1	-	-	-	-
QPADEV0009	FRED1	687068	1	FRED1	-	-	-	-
QPADEV0009	FRED1	687068	1	FRED1	-	-	-	-
QPADEV0009	FRED1	687068	1	FRED1	-	-	-	-
QPADEV0009	FRED1	687068	1	FRED1	-	-	-	-
QPADEV0009	FRED1	687068	1	FRED1	-	-	-	-
QPADEV0009	FRED1	687068	1	FRED1	-	-	-	-
QPADEV0009	FRED1	687068	1	FRED1	-	-	-	-
QPADEV0009	FRED1	687068	1	FRED1	-	-	-	-
QPADEV0009	FRED1	687068	1	FRED1	-	-	-	-
QPADEV0009	FRED1	687068	1	FRED1	-	-	-	-
QPADEV0009	FRED1	687068	1	FRED1	-	-	-	-

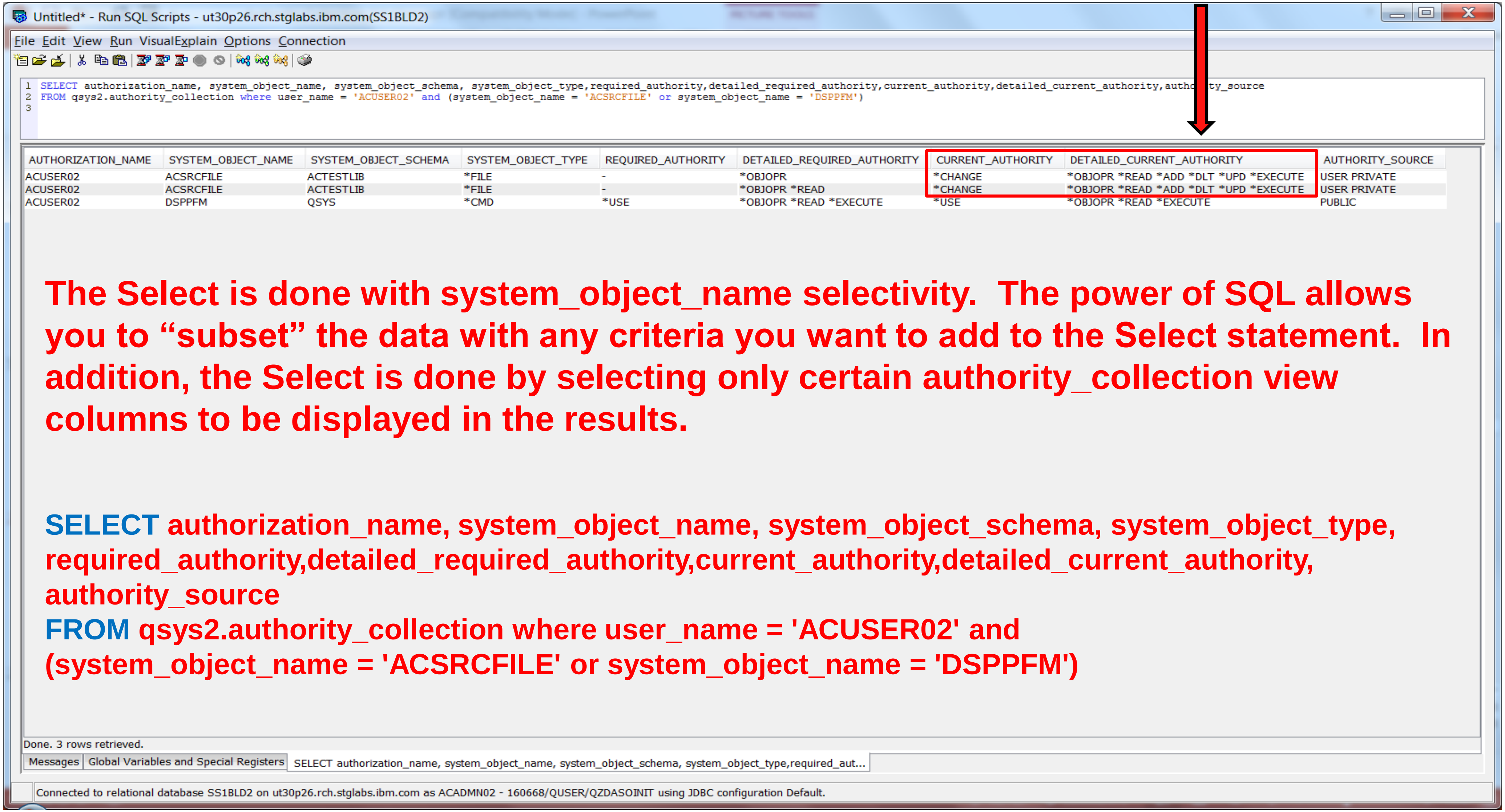
A simple example

Authority Collection – Example

Run this command:

DSPPFM ACTESTLIB/ACSRCFILE ACMBR

Excessive Authority?



Untitled* - Run SQL Scripts - ut30p26.rch.stglabs.ibm.com(SS1BLD2)
File Edit View Run VisualExplain Options Connection

```
SELECT authorization_name, system_object_name, system_object_schema, system_object_type,required_authority,detailed_required_authority,current_authority,detailed_current_authority,authority_source
FROM qsys2.authority_collection where user_name = 'ACUSER02' and (system_object_name = 'ACSRCFILE' or system_object_name = 'DSPPFM')
```

AUTHORIZATION_NAME	SYSTEM_OBJECT_NAME	SYSTEM_OBJECT_SCHEMA	SYSTEM_OBJECT_TYPE	REQUIRED_AUTHORITY	DETAILED_REQUIRED_AUTHORITY	CURRENT_AUTHORITY	DETAILED_CURRENT_AUTHORITY	AUTHORITY_SOURCE
ACUSER02	ACSRCFILE	ACTESTLIB	*FILE	-	*OBJOPR	*CHANGE	*OBJOPR *READ *ADD *DLT *UPD *EXECUTE	USER PRIVATE
ACUSER02	ACSRCFILE	ACTESTLIB	*FILE	-	*OBJOPR *READ	*CHANGE	*OBJOPR *READ *ADD *DLT *UPD *EXECUTE	USER PRIVATE
ACUSER02	DSPPFM	QSYS	*CMD	*USE	*OBJOPR *READ *EXECUTE	*USE	*OBJOPR *READ *EXECUTE	PUBLIC

The Select is done with system_object_name selectivity. The power of SQL allows you to “subset” the data with any criteria you want to add to the Select statement. In addition, the Select is done by selecting only certain authority_collection view columns to be displayed in the results.

SELECT authorization_name, system_object_name, system_object_schema, system_object_type, required_authority,detailed_required_authority,current_authority,detailed_current_authority, authority_source
FROM qsys2.authority_collection where user_name = 'ACUSER02' and (system_object_name = 'ACSRCFILE' or system_object_name = 'DSPPFM')

Done. 3 rows retrieved.

Messages | Global Variables and Special Registers | SELECT authorization_name, system_object_name, system_object_schema, system_object_type,required_aut...

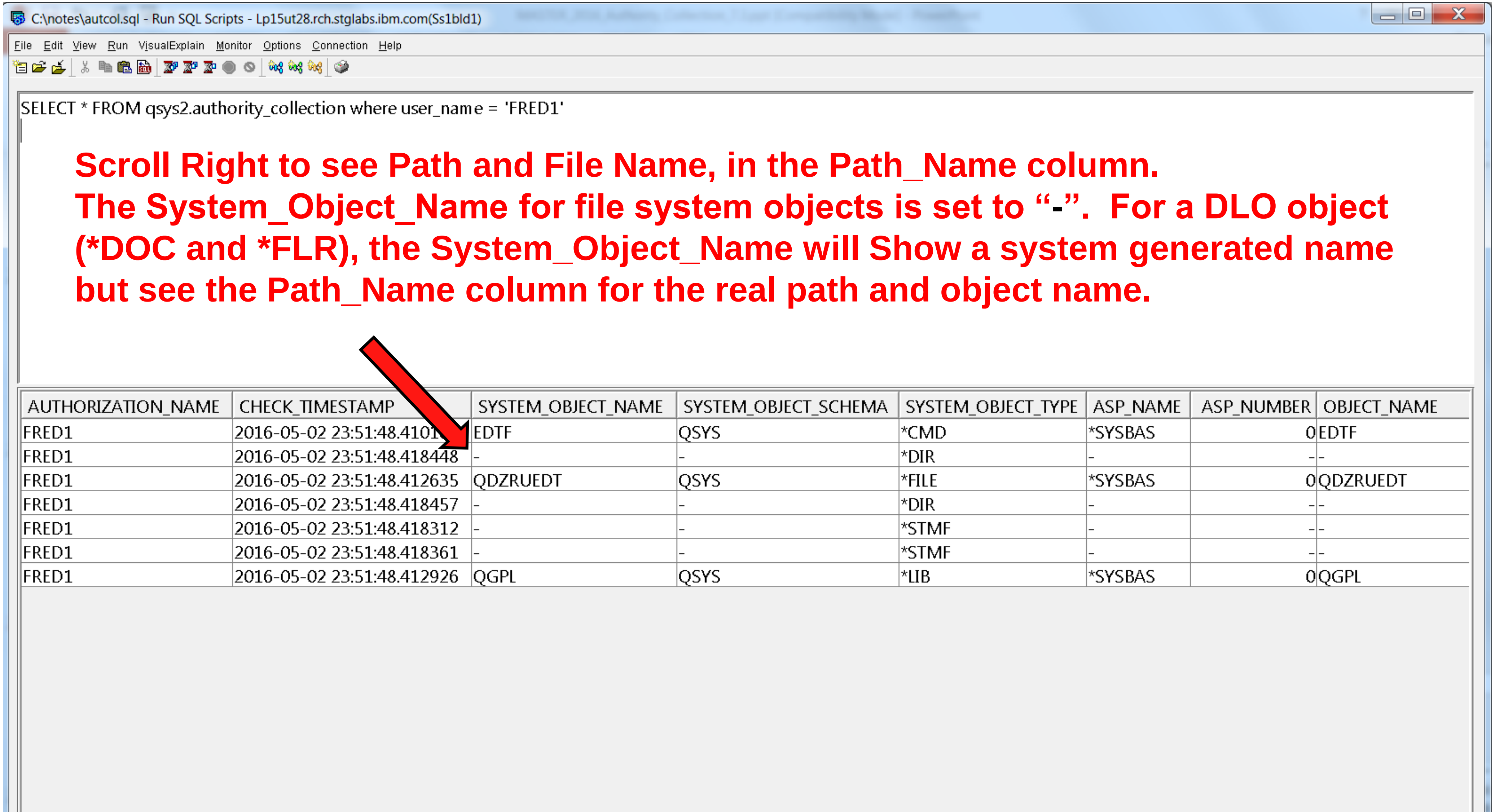
Connected to relational database SS1BLD2 on ut30p26.rch.stglabs.ibm.com as ACADMN02 - 160668/QUSER/QZDASOINIT using JDBC configuration Default.

File System Example

Authority Collection – File System Example

Run this command:

EDTF STMF('/fred1/streamfil1')

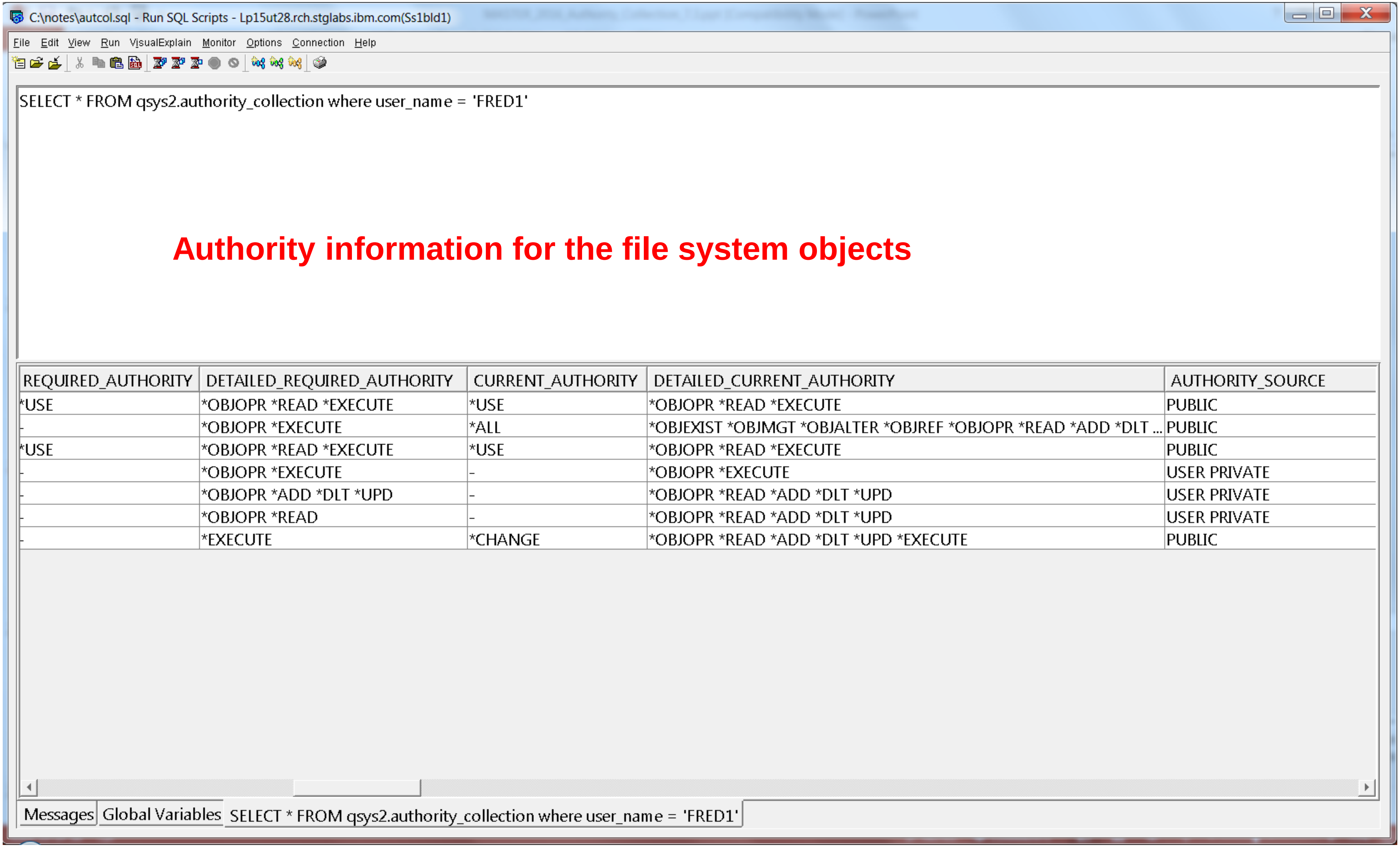

C:\notes\autcol.sql - Run SQL Scripts - Lp15ut28.rch.stglabs.ibm.com(Ss1bld1)
File Edit View Run VisualExplain Monitor Options Connection Help

```
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1'
```

Scroll Right to see Path and File Name, in the Path_Name column. The System_Object_Name for file system objects is set to "-". For a DLO object (*DOC and *FLR), the System_Object_Name will Show a system generated name but see the Path_Name column for the real path and object name.

AUTHORIZATION_NAME	CHECK_TIMESTAMP	SYSTEM_OBJECT_NAME	SYSTEM_OBJECT_SCHEMA	SYSTEM_OBJECT_TYPE	ASP_NAME	ASP_NUMBER	OBJECT_NAME
FRED1	2016-05-02 23:51:48.41010	EDTF	QSYS	*CMD	*SYSBAS	0	EDTF
FRED1	2016-05-02 23:51:48.418448	-	-	*DIR	-	-	-
FRED1	2016-05-02 23:51:48.412635	QDZRUEDT	QSYS	*FILE	*SYSBAS	0	QDZRUEDT
FRED1	2016-05-02 23:51:48.418457	-	-	*DIR	-	-	-
FRED1	2016-05-02 23:51:48.418312	-	-	*STMF	-	-	-
FRED1	2016-05-02 23:51:48.418361	-	-	*STMF	-	-	-
FRED1	2016-05-02 23:51:48.412926	QGPL	QSYS	*LIB	*SYSBAS	0	QGPL

Authority Collection – File System Example

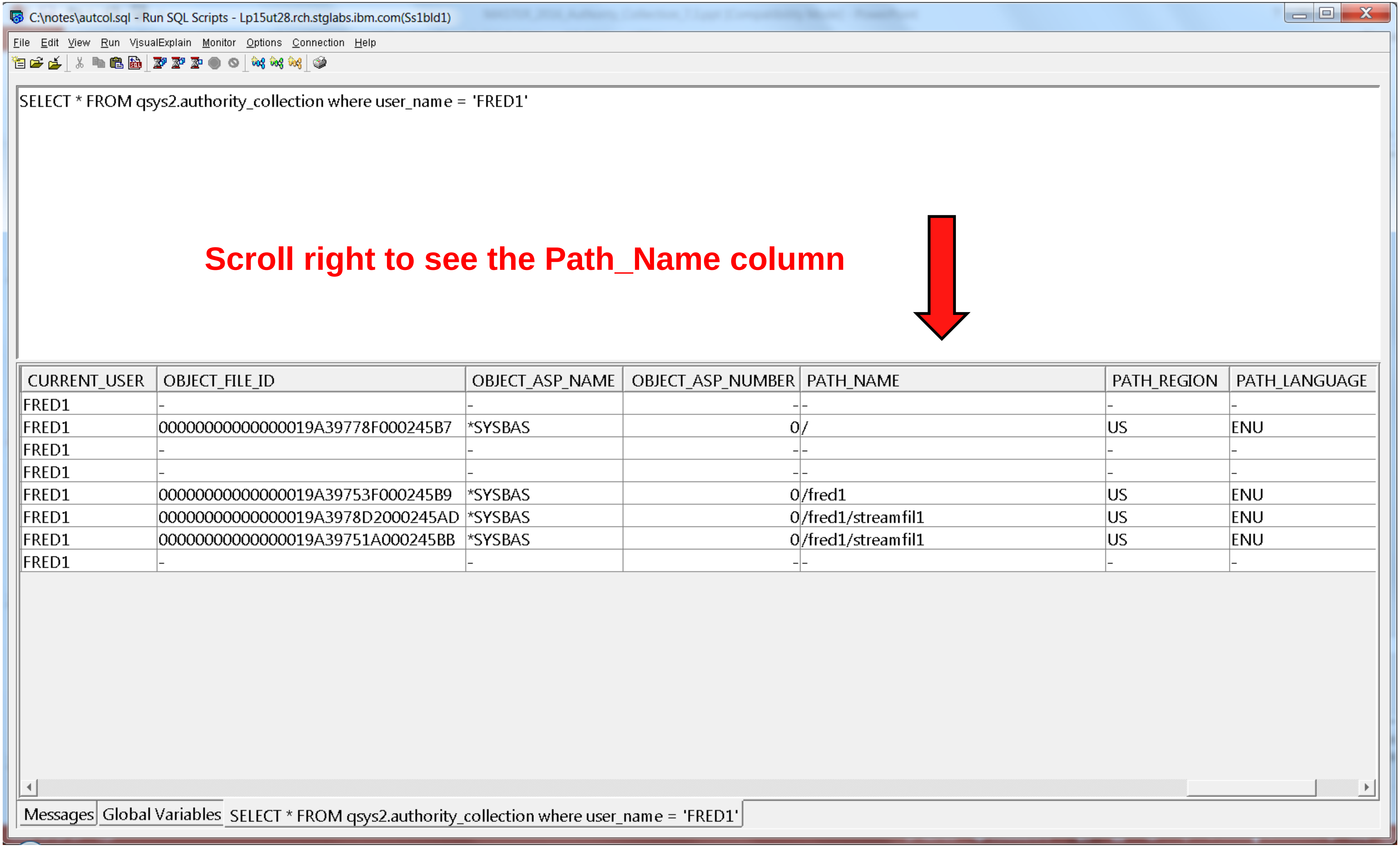

C:\notes\autcol.sql - Run SQL Scripts - Lp15ut28.rch.stglabs.ibm.com(Ss1bld1)
File Edit View Run VisualExplain Monitor Options Connection Help
Messages
Global Variables
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1'

```
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1'
```

Authority information for the file system objects

REQUIRED_AUTHORITY	DETAILED_REQUIRED_AUTHORITY	CURRENT_AUTHORITY	DETAILED_CURRENT_AUTHORITY	AUTHORITY_SOURCE
*USE	*OBJOPR *READ *EXECUTE	*USE	*OBJOPR *READ *EXECUTE	PUBLIC
-	*OBJOPR *EXECUTE	*ALL	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT ...	PUBLIC
*USE	*OBJOPR *READ *EXECUTE	*USE	*OBJOPR *READ *EXECUTE	PUBLIC
-	*OBJOPR *EXECUTE	-	*OBJOPR *EXECUTE	USER PRIVATE
-	*OBJOPR *ADD *DLT *UPD	-	*OBJOPR *READ *ADD *DLT *UPD	USER PRIVATE
-	*OBJOPR *READ	-	*OBJOPR *READ *ADD *DLT *UPD	USER PRIVATE
-	*EXECUTE	*CHANGE	*OBJOPR *READ *ADD *DLT *UPD *EXECUTE	PUBLIC

Authority Collection – File System Example



C:\notes\autcol.sql - Run SQL Scripts - Lp15ut28.rch.stglabs.ibm.com(Ss1bld1)
File Edit View Run VisualExplain Monitor Options Connection Help

```
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1'
```

Scroll right to see the Path_Name column

CURRENT_USER	OBJECT_FILE_ID	OBJECT_ASP_NAME	OBJECT_ASP_NUMBER	PATH_NAME	PATH_REGION	PATH_LANGUAGE
FRED1	-	-	-	-	-	-
FRED1	00000000000000019A39778F000245B7	*SYSBAS	0	/	US	ENU
FRED1	-	-	-	-	-	-
FRED1	-	-	-	-	-	-
FRED1	00000000000000019A39753F000245B9	*SYSBAS	0	/fred1	US	ENU
FRED1	00000000000000019A3978D2000245AD	*SYSBAS	0	/fred1/streamfil1	US	ENU
FRED1	00000000000000019A39751A000245BB	*SYSBAS	0	/fred1/streamfil1	US	ENU
FRED1	-	-	-	-	-	-

Messages
Global Variables
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1'

Adopted Authority Example

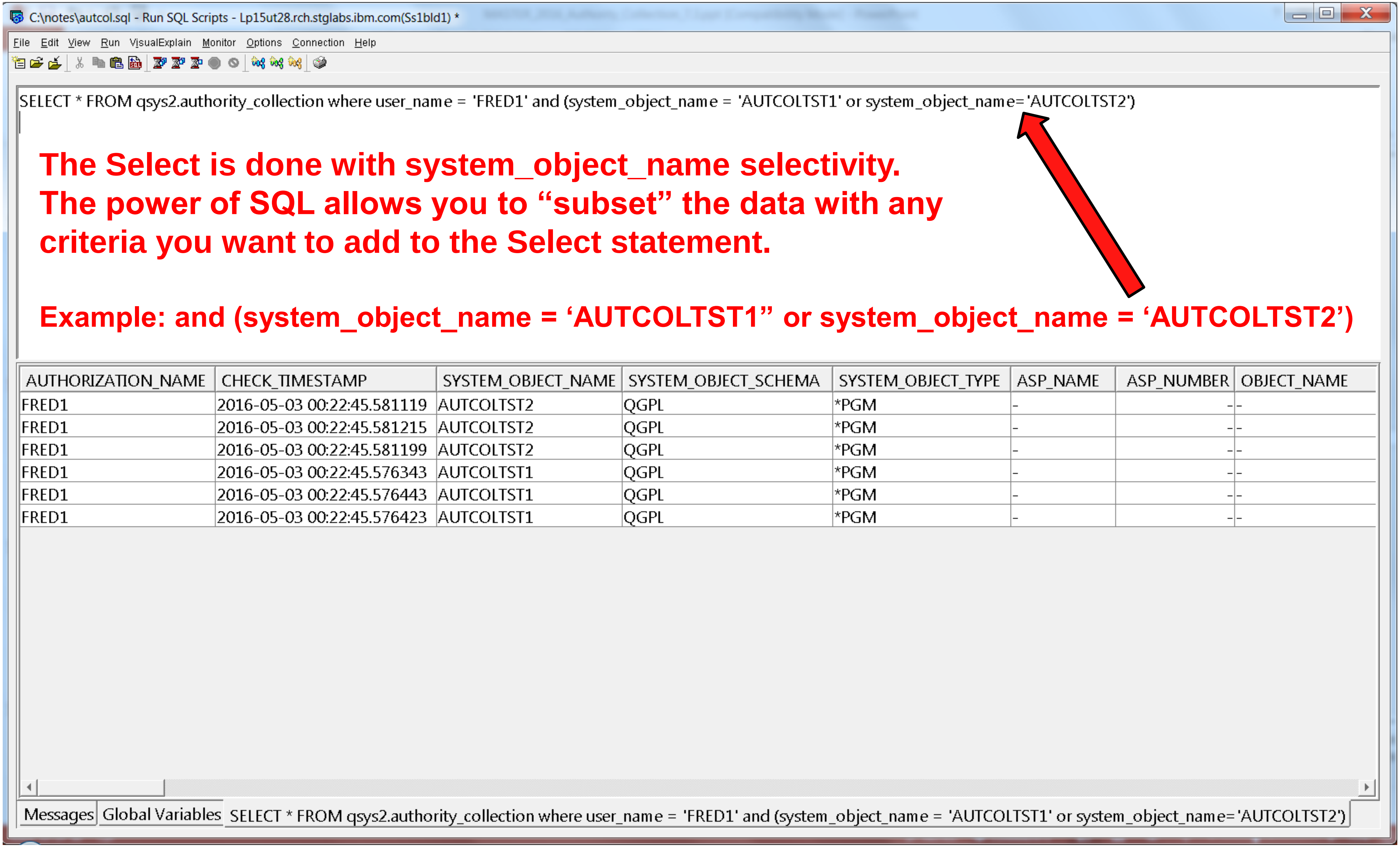
Authority Collection – Adopted Authority Example

Call a simple CL program, that adopts owner authority, to run two DLTPGM commands. Program AUTCOLADP adopts its owners, “UEHLING”, authority.

```
CALL PGM(QGPL/AUTCOLADP) /* PGM created with USRPRF(*OWNER) */
```

```
PGM
   DLTPGM PGM(QGPL/AUTCOLTST1)  /* Public authority = *EXCLUDE) */
   DLTPGM PGM(QGPL/AUTCOLTST2)  /* Public authority = *ALL         */
ENDPGM
```

Authority Collection – Adopted Authority Example


C:\notes\autcol.sql - Run SQL Scripts - Lp15ut28.rch.stglabs.ibm.com(Ss1bld1) *
File Edit View Run VisualExplain Monitor Options Connection Help
Messages
Global Variables

```
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1' and (system_object_name = 'AUTCOLTST1' or system_object_name='AUTCOLTST2')
```

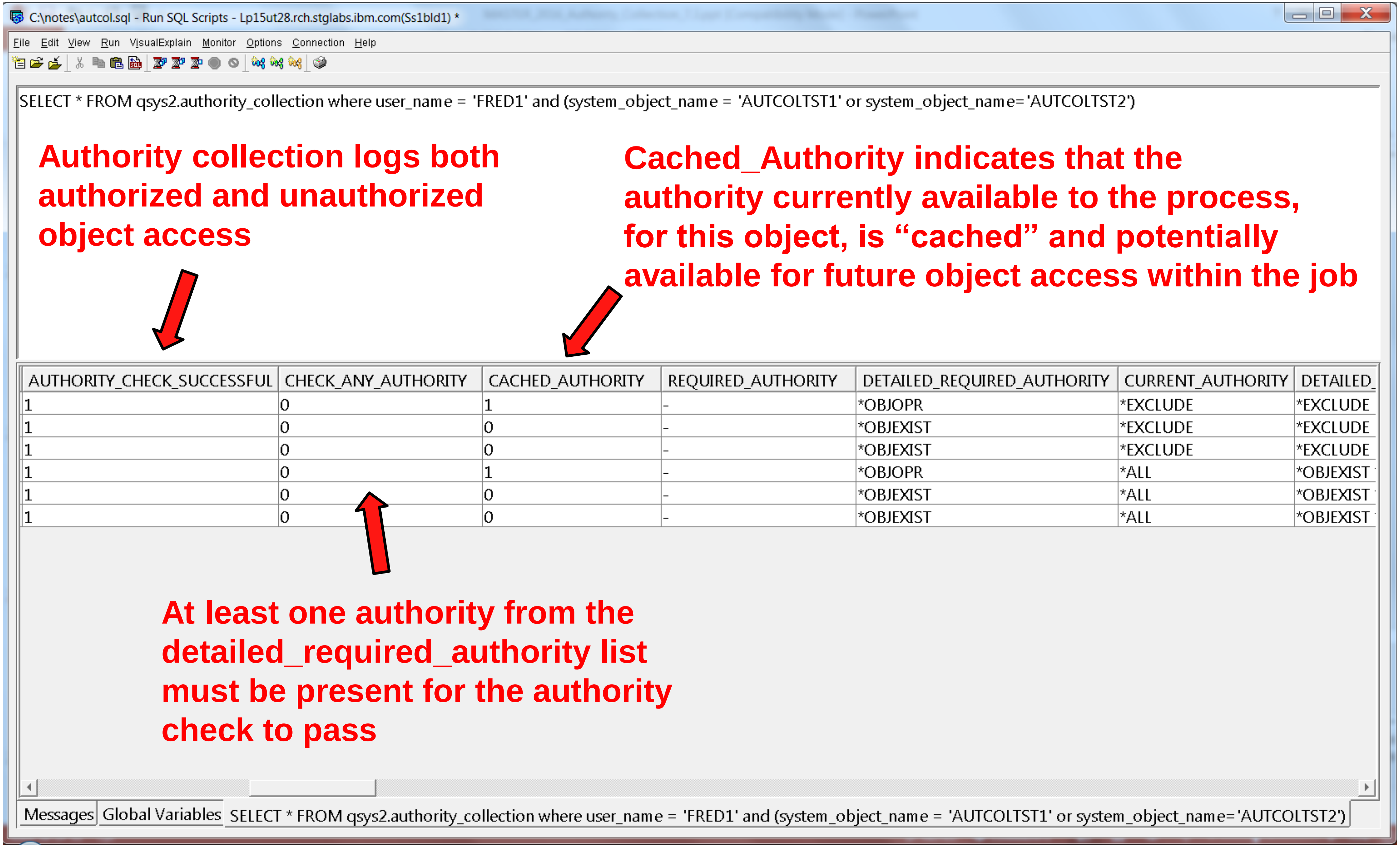
The Select is done with system_object_name selectivity. The power of SQL allows you to "subset" the data with any criteria you want to add to the Select statement.

Example: and (system_object_name = 'AUTCOLTST1" or system_object_name = 'AUTCOLTST2')

AUTHORIZATION_NAME	CHECK_TIMESTAMP	SYSTEM_OBJECT_NAME	SYSTEM_OBJECT_SCHEMA	SYSTEM_OBJECT_TYPE	ASP_NAME	ASP_NUMBER	OBJECT_NAME
FRED1	2016-05-03 00:22:45.581119	AUTCOLTST2	QGPL	*PGM	-	-	-
FRED1	2016-05-03 00:22:45.581215	AUTCOLTST2	QGPL	*PGM	-	-	-
FRED1	2016-05-03 00:22:45.581199	AUTCOLTST2	QGPL	*PGM	-	-	-
FRED1	2016-05-03 00:22:45.576343	AUTCOLTST1	QGPL	*PGM	-	-	-
FRED1	2016-05-03 00:22:45.576443	AUTCOLTST1	QGPL	*PGM	-	-	-
FRED1	2016-05-03 00:22:45.576423	AUTCOLTST1	QGPL	*PGM	-	-	-

```
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1' and (system_object_name = 'AUTCOLTST1' or system_object_name='AUTCOLTST2')
```

Authority Collection – Adopted Authority Example



C:\notes\autcol.sql - Run SQL Scripts - Lp15ut28.rch.stglabs.ibm.com(Ss1bld1) *
File Edit View Run VisualExplain Monitor Options Connection Help

```
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1' and (system_object_name = 'AUTCOLTST1' or system_object_name='AUTCOLTST2')
```

Authority collection logs both authorized and unauthorized object access

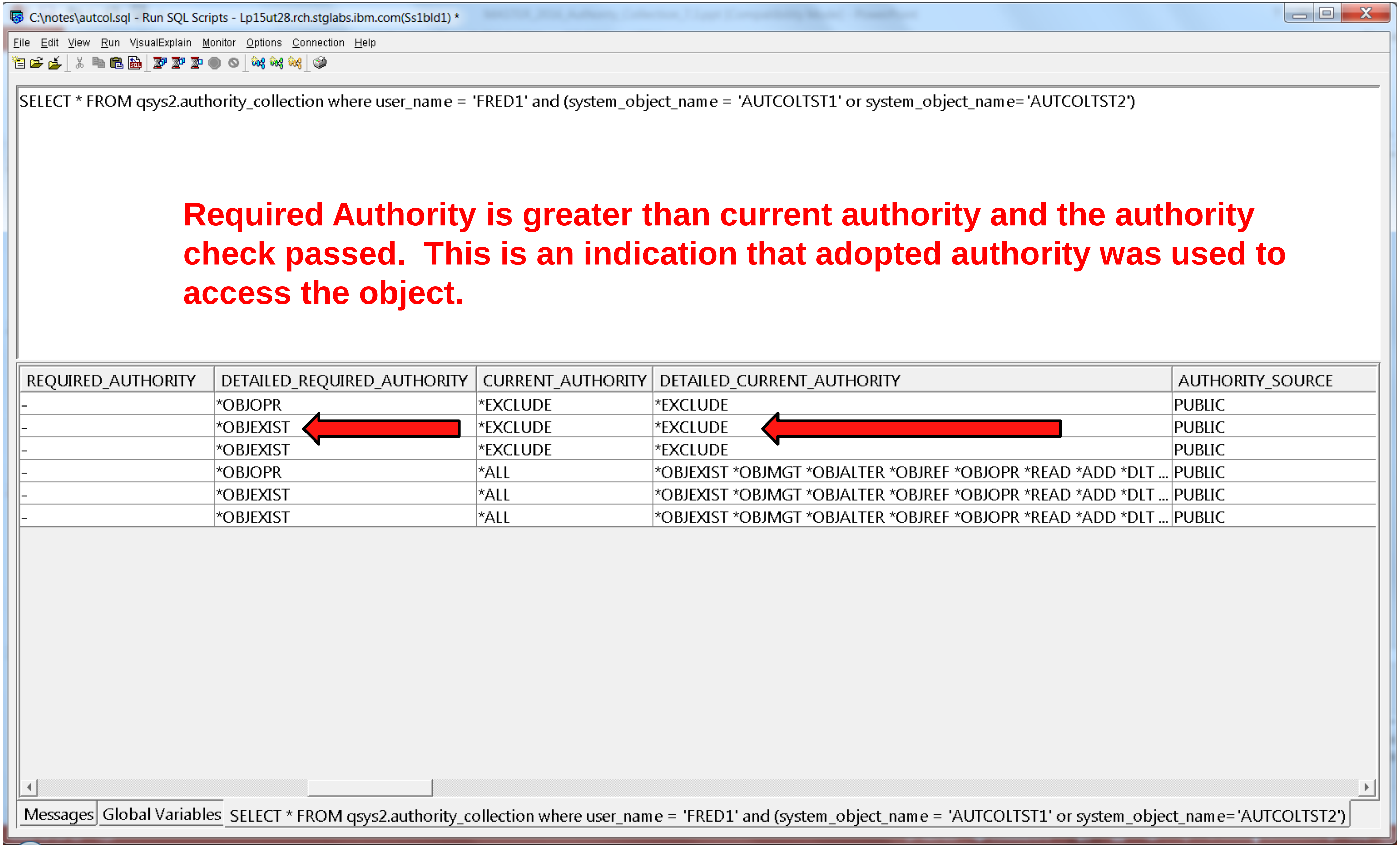
Cached_Authority indicates that the authority currently available to the process, for this object, is "cached" and potentially available for future object access within the job

AUTHORITY_CHECK_SUCCESSFUL	CHECK_ANY_AUTHORITY	CACHED_AUTHORITY	REQUIRED_AUTHORITY	DETAILED_REQUIRED_AUTHORITY	CURRENT_AUTHORITY	DETAILED_
1	0	1	-	*OBJOPR	*EXCLUDE	*EXCLUDE
1	0	0	-	*OBJEXIST	*EXCLUDE	*EXCLUDE
1	0	0	-	*OBJEXIST	*EXCLUDE	*EXCLUDE
1	0	1	-	*OBJOPR	*ALL	*OBJEXIST
1	0	0	-	*OBJEXIST	*ALL	*OBJEXIST
1	0	0	-	*OBJEXIST	*ALL	*OBJEXIST

At least one authority from the detailed_required_authority list must be present for the authority check to pass

```
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1' and (system_object_name = 'AUTCOLTST1' or system_object_name='AUTCOLTST2')
```

Authority Collection – Adopted Authority Example



C:\notes\autcol.sql - Run SQL Scripts - Lp15ut28.rch.stglabs.ibm.com(Ss1bld1) *
File Edit View Run VisualExplain Monitor Options Connection Help
Messages
Global Variables

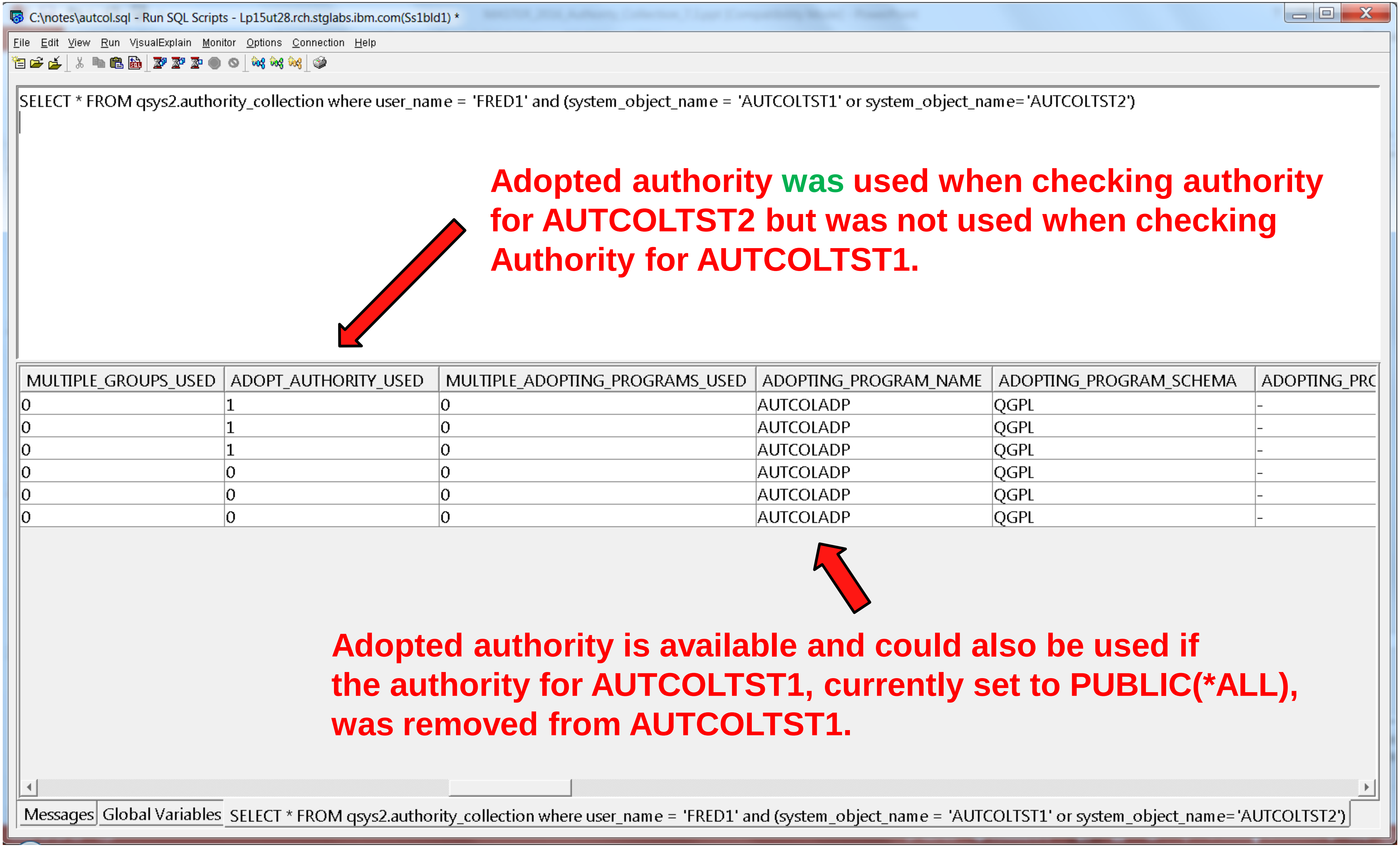
```
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1' and (system_object_name = 'AUTCOLTST1' or system_object_name='AUTCOLTST2')
```

Required Authority is greater than current authority and the authority check passed. This is an indication that adopted authority was used to access the object.

REQUIRED_AUTHORITY	DETAILED_REQUIRED_AUTHORITY	CURRENT_AUTHORITY	DETAILED_CURRENT_AUTHORITY	AUTHORITY_SOURCE
-	*OBJOPR	*EXCLUDE	*EXCLUDE	PUBLIC
-	*OBJEXIST	*EXCLUDE	*EXCLUDE	PUBLIC
-	*OBJEXIST	*EXCLUDE	*EXCLUDE	PUBLIC
-	*OBJOPR	*ALL	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT ...	PUBLIC
-	*OBJEXIST	*ALL	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT ...	PUBLIC
-	*OBJEXIST	*ALL	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT ...	PUBLIC

```
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1' and (system_object_name = 'AUTCOLTST1' or system_object_name='AUTCOLTST2')
```

Authority Collection – Adopted Authority Example


C:\notes\autcol.sql - Run SQL Scripts - Lp15ut28.rch.stglabs.ibm.com(Ss1bld1) *
File
Edit
View
Run
VisualExplain
Monitor
Options
Connection
Help
Messages
Global Variables
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1' and (system_object_name = 'AUTCOLTST1' or system_object_name='AUTCOLTST2')

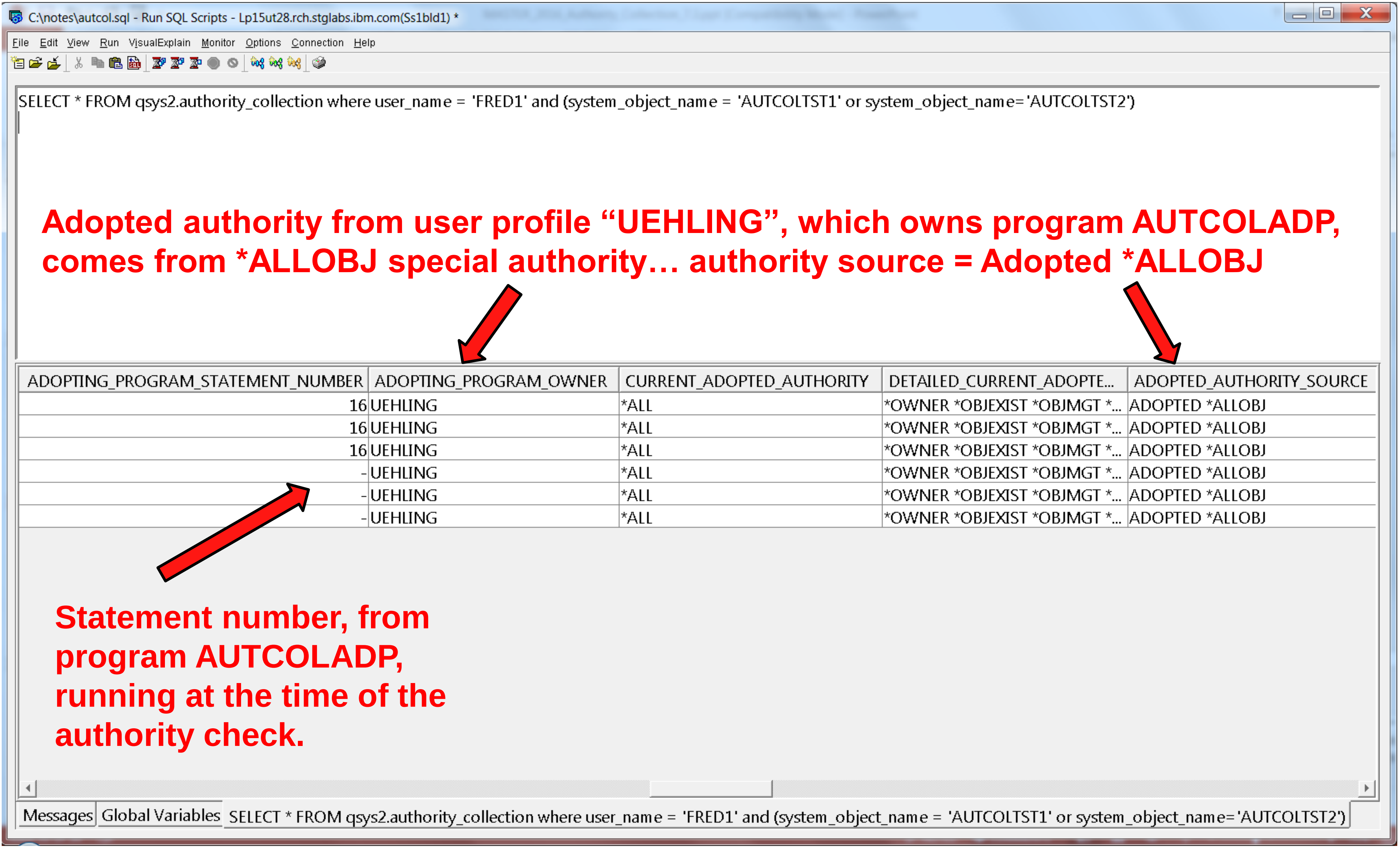
```
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1' and (system_object_name = 'AUTCOLTST1' or system_object_name='AUTCOLTST2')
```

Adopted authority was used when checking authority for AUTCOLTST2 but was not used when checking Authority for AUTCOLTST1.

MULTIPLE_GROUPS_USED	ADOPT_AUTHORITY_USED	MULTIPLE_ADOPTING_PROGRAMS_USED	ADOPTING_PROGRAM_NAME	ADOPTING_PROGRAM_SCHEMA	ADOPTING_PRC
0	1	0	AUTCOLADP	QGPL	-
0	1	0	AUTCOLADP	QGPL	-
0	1	0	AUTCOLADP	QGPL	-
0	0	0	AUTCOLADP	QGPL	-
0	0	0	AUTCOLADP	QGPL	-
0	0	0	AUTCOLADP	QGPL	-

Adopted authority is available and could also be used if the authority for AUTCOLTST1, currently set to PUBLIC(*ALL), was removed from AUTCOLTST1.

Authority Collection – Adopted Authority Example



```
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1' and (system_object_name = 'AUTCOLTST1' or system_object_name='AUTCOLTST2')
```

Adopted authority from user profile “UEHLING”, which owns program AUTCOLADP, comes from *ALLOBJ special authority… authority source = Adopted *ALLOBJ

ADOPTING_PROGRAM_STATEMENT_NUMBER	ADOPTING_PROGRAM_OWNER	CURRENT_ADOPTED_AUTHORITY	DETAILED_CURRENT_ADOPTE...	ADOPTED_AUTHORITY_SOURCE
16	UEHLING	*ALL	*OWNER *OBJEXIST *OBJMGT *...	ADOPTED *ALLOBJ
16	UEHLING	*ALL	*OWNER *OBJEXIST *OBJMGT *...	ADOPTED *ALLOBJ
16	UEHLING	*ALL	*OWNER *OBJEXIST *OBJMGT *...	ADOPTED *ALLOBJ
-	UEHLING	*ALL	*OWNER *OBJEXIST *OBJMGT *...	ADOPTED *ALLOBJ
-	UEHLING	*ALL	*OWNER *OBJEXIST *OBJMGT *...	ADOPTED *ALLOBJ
-	UEHLING	*ALL	*OWNER *OBJEXIST *OBJMGT *...	ADOPTED *ALLOBJ

Statement number, from program AUTCOLADP, running at the time of the authority check.

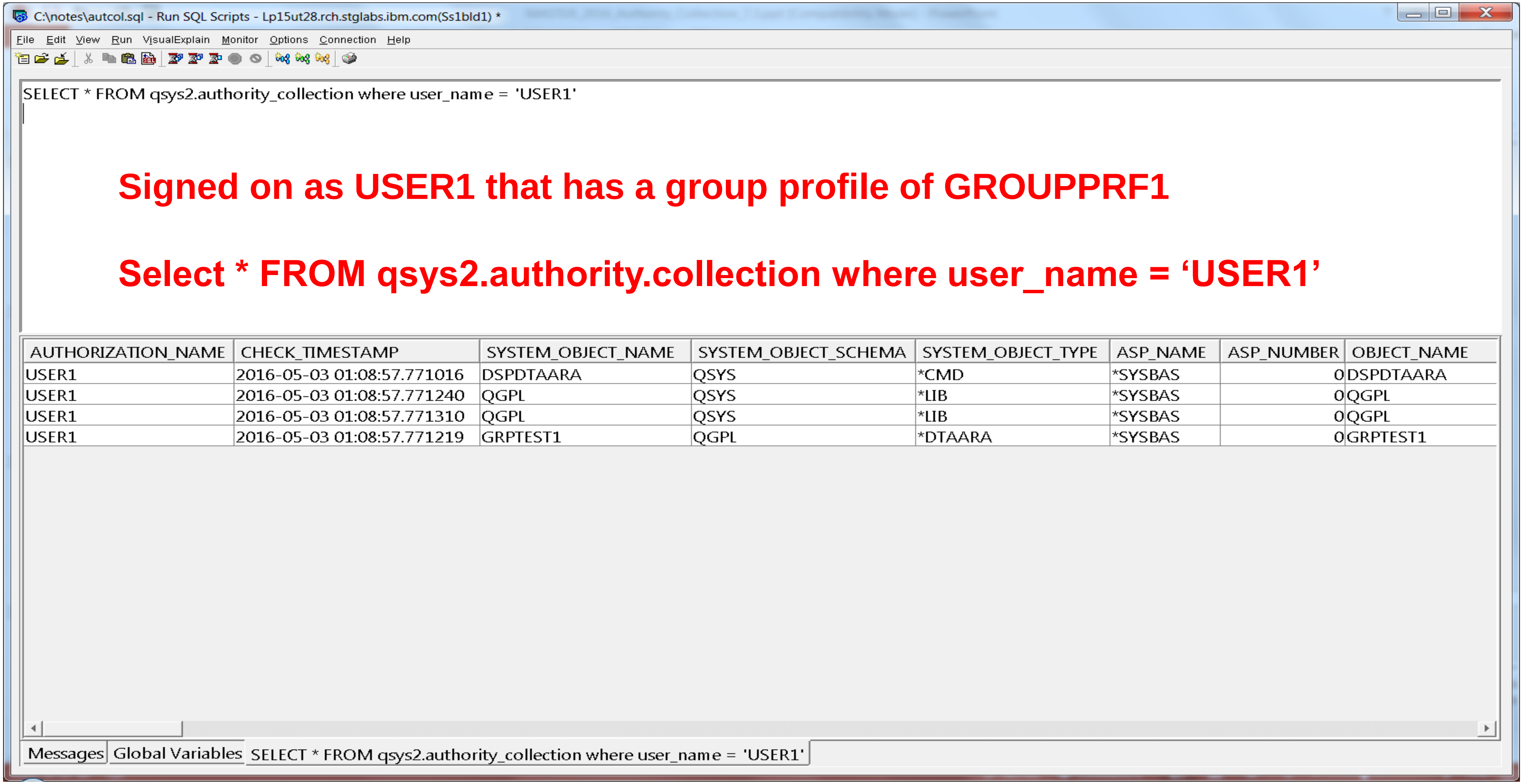
```
SELECT * FROM qsys2.authority_collection where user_name = 'FRED1' and (system_object_name = 'AUTCOLTST1' or system_object_name='AUTCOLTST2')
```

Group Profile Example

Authority Collection – Group Profile Example

Run this command:

DSPDTAARA DTAARA(GRPTEST1)


C:\notes\autcol.sql - Run SQL Scripts - Lp15ut28.rch.stglabs.ibm.com(Ss1bld1) *
File Edit View Run VisualExplain Monitor Options Connection Help
Messages
Global Variables
SELECT * FROM qsys2.authority_collection where user_name = 'USER1'

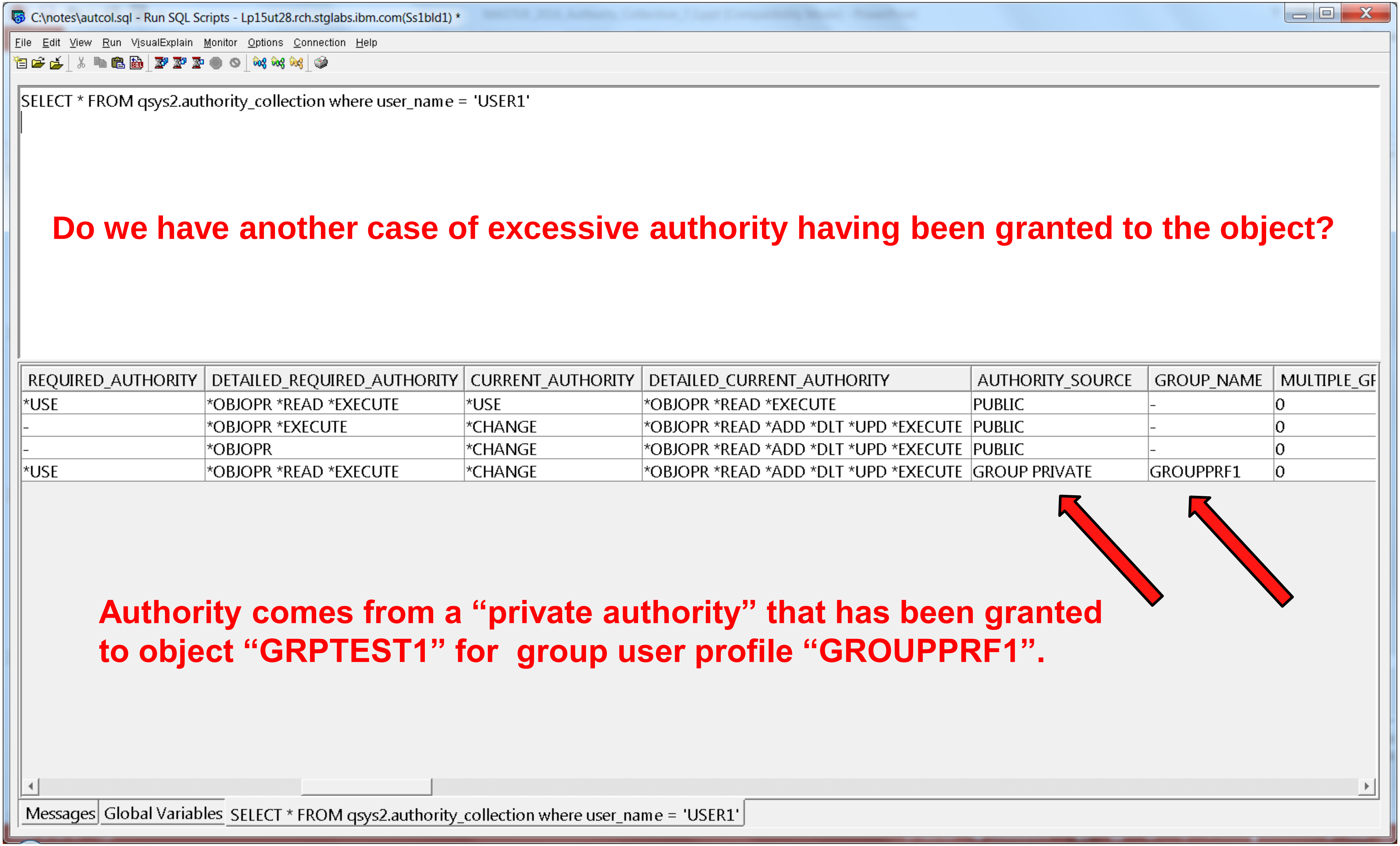
```
SELECT * FROM qsys2.authority_collection where user_name = 'USER1'
```

Signed on as USER1 that has a group profile of GROUPPRF1

Select * FROM qsys2.authority.collection where user_name = ‘USER1’

AUTHORIZATION_NAME	CHECK_TIMESTAMP	SYSTEM_OBJECT_NAME	SYSTEM_OBJECT_SCHEMA	SYSTEM_OBJECT_TYPE	ASP_NAME	ASP_NUMBER	OBJECT_NAME
USER1	2016-05-03 01:08:57.771016	DSPDTAARA	QSYS	*CMD	*SYSBAS	0	DSPDTAARA
USER1	2016-05-03 01:08:57.771240	QGPL	QSYS	*LIB	*SYSBAS	0	QGPL
USER1	2016-05-03 01:08:57.771310	QGPL	QSYS	*LIB	*SYSBAS	0	QGPL
USER1	2016-05-03 01:08:57.771219	GRPTEST1	QGPL	*DTAARA	*SYSBAS	0	GRPTEST1

Authority Collection – Group Profile Example


C:\notes\autcol.sql - Run SQL Scripts - Lp15ut28.rch.stglabs.ibm.com(Ss1bld1) *
File Edit View Run VisualExplain Monitor Options Connection Help
Messages Global Variables

```
SELECT * FROM qsys2.authority_collection where user_name = 'USER1'
```

Do we have another case of excessive authority having been granted to the object?

REQUIRED_AUTHORITY	DETAILED_REQUIRED_AUTHORITY	CURRENT_AUTHORITY	DETAILED_CURRENT_AUTHORITY	AUTHORITY_SOURCE	GROUP_NAME	MULTIPLE_GF
*USE	*OBJOPR *READ *EXECUTE	*USE	*OBJOPR *READ *EXECUTE	PUBLIC	-	0
-	*OBJOPR *EXECUTE	*CHANGE	*OBJOPR *READ *ADD *DLT *UPD *EXECUTE	PUBLIC	-	0
-	*OBJOPR	*CHANGE	*OBJOPR *READ *ADD *DLT *UPD *EXECUTE	PUBLIC	-	0
*USE	*OBJOPR *READ *EXECUTE	*CHANGE	*OBJOPR *READ *ADD *DLT *UPD *EXECUTE	GROUP PRIVATE	GROUPPRF1	0

Authority comes from a “private authority” that has been granted to object “GRPTEST1” for group user profile “GROUPPRF1”.

```
SELECT * FROM qsys2.authority_collection where user_name = 'USER1'
```

Questions?

Special notices

This document was developed for IBM offerings in the United States as of the date of publication. IBM may not make these offerings available in other countries, and the information is subject to change without notice. Consult your local IBM business contact for information on the IBM offerings available in your area.

Information in this document concerning non-IBM products was obtained from the suppliers of these products or other public sources. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. Send license inquires, in writing, to IBM Director of Licensing, IBM Corporation, New Castle Drive, Armonk, NY 10504-1785 USA.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The information contained in this document has not been submitted to any formal IBM test and is provided "AS IS" with no warranties or guarantees either expressed or implied.

All examples cited or described in this document are presented as illustrations of the manner in which some IBM products can be used and the results that may be achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions.

IBM Global Financing offerings are provided through IBM Credit Corporation in the United States and other IBM subsidiaries and divisions worldwide to qualified commercial and government clients. Rates are based on a client's credit rating, financing terms, offering type, equipment type and options, and may vary by country. Other restrictions may apply. Rates and offerings are subject to change, extension or withdrawal without notice.

IBM is not responsible for printing errors in this document that result in pricing or information inaccuracies.

All prices shown are IBM's United States suggested list prices and are subject to change without notice; reseller prices may vary.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

Any performance data contained in this document was determined in a controlled environment. Actual results may vary significantly and are dependent on many factors including system hardware configuration and software design and configuration. Some measurements quoted in this document may have been made on development-level systems. There is no guarantee these measurements will be the same on generally-available systems. Some measurements quoted in this document may have been estimated through extrapolation. Users of this document should verify the applicable data for their specific environment.

Special notices (cont.)

IBM, the IBM logo, ibm.com AIX, AIX (logo), AIX 6 (logo), AS/400, BladeCenter, Blue Gene, ClusterProven, DB2, ESCON, i5/OS, i5/OS (logo), IBM Business Partner (logo), IntelliStation, LoadLeveler, Lotus, Lotus Notes, Notes, Operating System/400, OS/400, PartnerLink, PartnerWorld, PowerPC, pSeries, Rational, RISC System/6000, RS/6000, THINK, Tivoli, Tivoli (logo), Tivoli Management Environment, WebSphere, xSeries, z/OS, zSeries, AIX 5L, Chiphopper, Chipkill, Cloudscape, DB2 Universal Database, DS4000, DS6000, DS8000, EnergyScale, Enterprise Workload Manager, General Purpose File System, , GPFS, HACMP, HACMP/6000, HASM, IBM Systems Director Active Energy Manager, iSeries, Micro-Partitioning, POWER, PowerExecutive, PowerVM, PowerVM (logo), PowerHA, Power Architecture, Power Everywhere, Power Family, POWER Hypervisor, Power Systems, Power Systems (logo), Power Systems Software, Power Systems Software (logo), POWER2, POWER3, POWER4, POWER4+, POWER5, POWER5+, POWER6, POWER6+, System i, System p, System p5, System Storage, System z, Tivoli Enterprise, TME 10, Workload Partitions Manager and X-Architecture are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

The Power Architecture and Power.org wordmarks and the Power and Power.org logos and related marks are trademarks and service marks licensed by Power.org.

UNIX is a registered trademark of The Open Group in the United States, other countries or both.

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

Microsoft, Windows and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries or both.

Intel, Itanium, Pentium are registered trademarks and Xeon is a trademark of Intel Corporation or its subsidiaries in the United States, other countries or both.

AMD Opteron is a trademark of Advanced Micro Devices, Inc.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries or both.

TPC-C and TPC-H are trademarks of the Transaction Performance Processing Council (TPPC).

SPECint, SPECfp, SPECjbb, SPECweb, SPECjAppServer, SPEC OMP, SPECviewperf, SPECapc, SPEChpc, SPECjvm, SPECmail, SPECimap and SPECsfs are trademarks of the Standard Performance Evaluation Corp (SPEC).

NetBench is a registered trademark of Ziff Davis Media in the United States, other countries or both.

AltiVec is a trademark of Freescale Semiconductor, Inc.

Cell Broadband Engine is a trademark of Sony Computer Entertainment Inc.

InfiniBand, InfiniBand Trade Association and the InfiniBand design marks are trademarks and/or service marks of the InfiniBand Trade Association.
Other company, product and service names may be trademarks or service marks of others.