IBM i

# I servizi SQL di IBM i

## *sicurezza*

Marco Riva

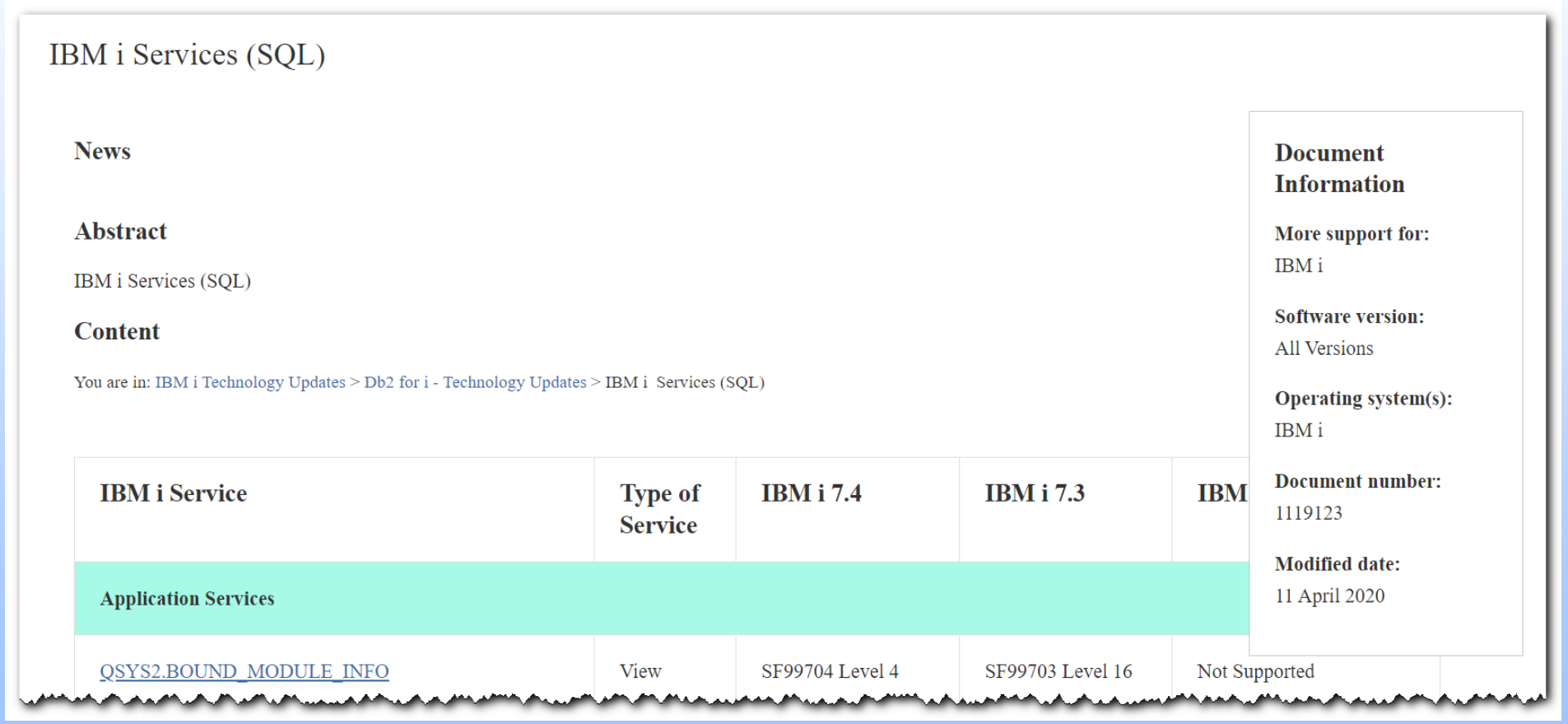
www.markonetools.it

IBM CHAMPION 2021 Power Systems area

Ultimo aggiornamento: 17/10/2021

# IBM i services – home page

- https://www.ibm.com/support/pages/node/1119123



IBM i Services (SQL)

**News**

**Abstract**

IBM i Services (SQL)

**Content**

You are in: IBM i Technology Updates > Db2 for i - Technology Updates > IBM i Services (SQL)

**Document Information**

**More support for:**
IBM i

**Software version:**
All Versions

**Operating system(s):**
IBM i

**Document number:**
1119123

**Modified date:**
11 April 2020

| IBM i Service | Type of Service | IBM i 7.4 | IBM i 7.3 | IBM |
|---|---|---|---|---|
| **Application Services** | | | | |
| QSYS2.BOUND_MODULE_INFO | View | SF99704 Level 4 | SF99703 Level 16 | Not Supported |

# Elenco e informazioni sui profili utenti

Power coffee 20/2021: https://www.markonetools.it/power-coffee-n-20-2021/

- **USERS**: funzione di tabella che restituisce l'elenco degli utenti (profilo e descrizione)
- USER_INFO_BASIC e USER_INFO: viste che restituiscono diverse informazioni sui profili utente. Simile a `DSPUSRPRF`.
- GROUP_PROFILE_ENTRIES: (vista) restituisce un record per ogni utente che fa parte di un gruppo utenti

| ODOBNM | ODOBTX |
|---|---|
| QSYSOPR | Operatore di sistema |
| QTCM | Profilo utente fornito da IBM. |
| QTCP | Profilo utente TCP/IP interno |
| QTFTP | Profilo utente fornito da IBM. |
| QTMHHTP1 | Profilo utente CGI server HTTP |
| QTMHHTTP | Profilo utente server HTTP |
| QTMPLPD | ALLOW REMOTE LPR REQUESTERS |
| QTSTRQS | Profilo utente richiesta test |
| QUSER | Utente della stazione di lavoro |
| QWEBADMIN | Profilo utente GUI ammin. Web |
| QWSERVICE | Utente predefinito servizi web integrati |
| QYCMCIMOM | Profilo utente fornito da IBM. |
| QYPSJSVR | Profilo utente fornito da IBM. |

| Utente | Descrizione | Ult.collegamento | Coll.non validi | Stato | Data/Ora mod.pwd | gg a scadenza password | Pwd a scad. | Classe | Aut.spec. |
|---|---|---|---|---|---|---|---|---|---|
| CORSOXG8 | Profilo-utente x | 2017-03-16 15:27:45.000000 | 0 | *ENABLED | 2017-04-14 09:35:57.000000 | [NULL] | NO | *PGMR | *ALLOBJ *JOBCTL *SAVSYS |
| CORSO0901 | Profilo-utente x | 2020-05-14 10:17:39.000000 | 0 | *ENABLED | 2019-10-07 11:40:06.000000 | [NULL] | NO | *PGMR | [NULL] |
| CORSO0902 | Profilo-utente x | 2020-05-14 10:17:47.000000 | 0 | *ENABLED | 2019-10-07 11:40:19.000000 | [NULL] | NO | *PGMR | [NULL] |
| CORSO0903 | Profilo-utente x | [NULL] | 0 | *ENABLED | 2019-10-07 11:32:13.000000 | [NULL] | NO | *PGMR | [NULL] |
| CORSO0904 | Profilo-utente x | [NULL] | 0 | *ENABLED | 2019-10-07 11:40:37.000000 | [NULL] | NO | *PGMR | [NULL] |
| CORSO0905 | Profilo-utente x | [NULL] | 0 | *ENABLED | 2019-10-07 11:40:56.000000 | [NULL] | NO | *PGMR | [NULL] |
| CORSO0906 | Profilo-utente x | [NULL] | 0 | *ENABLED | 2019-10-07 11:41:13.000000 | [NULL] | NO | *PGMR | [NULL] |

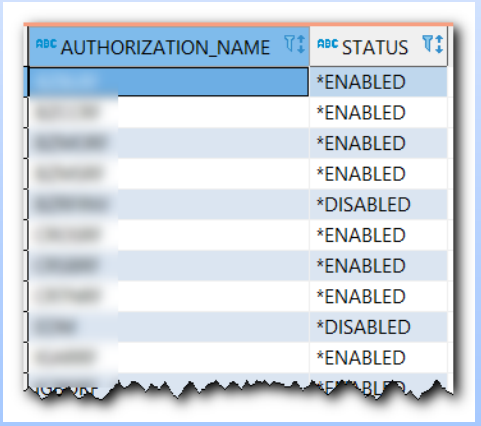
# Utenti molto potenti poco sicuri

da eseguire con un profilo utente con autorizzazione speciale *ALLOBJ o *SECADM

```
-- utenti di classe *SECOFR con password di default
select AUTHORIZATION_NAME, STATUS
  from USER_INFO U
  where USER_DEFAULT_PASSWORD = 'YES' and STATUS = '*ENABLED'
    and USER_CLASS_NAME = '*SECOFR'
  order by AUTHORIZATION_NAME;
```

```
-- utenti con autorizzazione *ALLOBJ con password di default
select AUTHORIZATION_NAME, STATUS
  from USER_INFO U
  where USER_DEFAULT_PASSWORD = 'YES' and STATUS = '*ENABLED'
    and (SPECIAL_AUTHORITIES like '%*ALLOBJ%'
     or AUTHORIZATION_NAME in
         (select USER_PROFILE_NAME
            from GROUP_PROFILE_ENTRIES
            where GROUP_PROFILE_NAME in
                   (select AUTHORIZATION_NAME
                      from USER_INFO
                      where SPECIAL_AUTHORITIES like '%*ALLOBJ%')))
  order by AUTHORIZATION_NAME;
```

https://blog.faq400.com/it/system-administration/ibmi-sysadmin-faq-part-4-it/



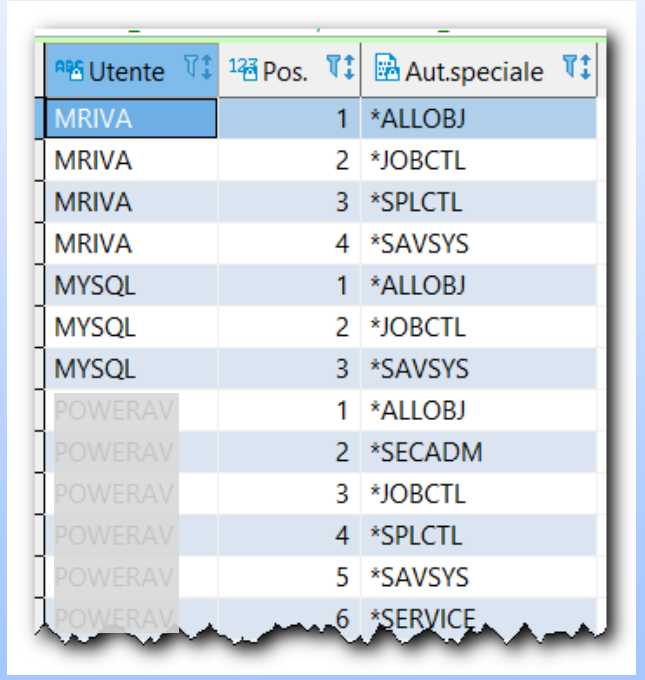
| AUTHORIZATION_NAME | STATUS |
|---|---|
| [redacted] | *ENABLED |
| [redacted] | *ENABLED |
| [redacted] | *ENABLED |
| [redacted] | *ENABLED |
| [redacted] | *DISABLED |
| [redacted] | *ENABLED |
| [redacted] | *ENABLED |
| [redacted] | *ENABLED |
| [redacted] | *DISABLED |
| [redacted] | *ENABLED |

Scott Forstie: https://gist.github.com/forstie/a47869f799aed5f7d552c7dc45489821

# Utenti e autorizzazioni speciali

- Sfruttiamo la funzione di tabella SPLIT per ottenere l'elenco delle autorizzazioni speciali per utente

```
select USER_NAME "Utente", ORDINAL_POSITION "Pos.", ltrim(ELEMENT) as
"Aut.speciale"
  from USER_INFO, table(
         systools.split(rtrim(SPECIAL_AUTHORITIES), '   ')) as SA
         -- seleziona solo profili utente
  where USER_NAME not in (select AUTHORIZATION_NAME
                          from AUTHIDS
                          where AUTHORIZATION_ATTR = 'GROUP')
  order by 1, 2;
```



| Utente | Pos. | Aut.speciale |
|---|---|---|
| MRIVA | 1 | *ALLOBJ |
| MRIVA | 2 | *JOBCTL |
| MRIVA | 3 | *SPLCTL |
| MRIVA | 4 | *SAVSYS |
| MYSQL | 1 | *ALLOBJ |
| MYSQL | 2 | *JOBCTL |
| MYSQL | 3 | *SAVSYS |
| POWERAV | 1 | *ALLOBJ |
| POWERAV | 2 | *SECADM |
| POWERAV | 3 | *JOBCTL |
| POWERAV | 4 | *SPLCTL |
| POWERAV | 5 | *SAVSYS |
| POWERAV | 6 | *SERVICE |

# Utenti disabilitati per NetServer

- Nella vista **USER_INFO** è stato aggiunto il campo NETSERVER_DISABLED

```
select AUTHORIZATION_NAME "Utente", TEXT_DESCRIPTION "Descrizione"
  from USER_INFO
  where NETSERVER_DISABLED = 'YES'
  order by AUTHORIZATION_NAME;
```

# Configurazione sicurezza

- SECURITY_INFO: informazioni sulla configurazione della sicurezza. Simile ai comandi DSPSECA e DSPSECAUD.

```
select SECURITY_LEVEL "Liv.sic.", PASSWORD_LEVEL "Liv.pwd", AUDIT_JOURNAL_EXISTS "Giorn.sic.",
       PASSWORD_CHANGE_BLOCK "Bl.cambio pwd", PASSWORD_EXPIRATION_INTERVAL "Durata pwd",
       PASSWORD_EXPIRATION_WARNING "GG avviso scad.pwd",
       'da ' concat char(PASSWORD_MINIMUM_LENGTH) concat ' a ' concat
        char(PASSWORD_MAXIMUM_LENGTH) "Lungh.pwd",
      MAXIMUM_SIGNON_ATTEMPTS "Num.tentativi coll.", MAXIMUM_SIGNON_ACTION "Az.coll.",
       CREATE_PUBLIC_AUTHORITY "Aut.pubb.creaz.", LIMIT_SECOFR_ACCESS "Limita accesso secofr",
       INACTIVE_JOB_TIMEOUT "Timeout lav.inatt.",
       DISCONNECTED_JOB_INTERVAL "Interv.disconness.job", AUTOCONFIGURE_DEVICES "Config.aut."
  from SECURITY_INFO;
```

| Liv.sic. | Liv.pwd | Giorn.sic. | Bl.cambio pwd | Durata pwd | GG avviso scad.pwd | Lungh.pwd | Num.tentativi coll. | Az.coll. | Aut.pubb.creaz. |
|---|---|---|---|---|---|---|---|---|---|
| 30 | 0 | YES | *NONE | 90 | 7 | da 8 a 10 | 10 | 3 | *CHANGE |

# Valori di sistema per sicurezza

- SYSTEM_VALUE_INFO

```
select SYSTEM_VALUE_NAME "Valore di sistema",
       trim(coalesce(char(CURRENT_NUMERIC_VALUE), CURRENT_CHARACTER_VALUE)) "Valore"
  from SYSTEM_VALUE_INFO
  where SYSTEM_VALUE_NAME like 'QAUD%'
     or SYSTEM_VALUE_NAME like 'QPWD%'
     or SYSTEM_VALUE_NAME like 'QSSL%'
     or SYSTEM_VALUE_NAME in ('QALWOBJRST', 'QALWUSRDMN', 'QCRTAUT', 'QCRTOBJAUD',
'QDSPSGNINF', 'QFRCCVNRST', 'QINACTITV', 'QINACTMSGQ', 'QLMTDEVSSN', 'QLMTSECOFR',
'QMAXSGNACN', 'QMAXSIGN', 'QRETSVRSEC', 'QRMTSIGN', 'QSCANFS', 'QSCANFSCTL',
'QSECURITY', 'QUSEADPAUT', 'QVFYOBJRST')
  order by SYSTEM_VALUE_NAME;
```

| Valore di sistema | Valore |
|---|---|
| QALWOBJRST | *ALL |
| QALWUSRDMN | *ALL |
| QAUDCTL | *AUDLVL |
| QAUDENDACN | *NOTIFY |
| QAUDFRCLVL | 0 |
| QAUDLVL | *AUTFAIL *JOBDTA |
| QAUDLVL2 | *NONE |
| QCRTAUT | *CHANGE |
| QCRTOBJAUD | *NONE |
| QDSPSGNINF | 0 |
| QFRCCVNRST | 1 |
| QINACTITV | *NONE |
| QINACTMSGQ | *DSCJOB |

# Autorizzazioni sugli oggetti

- OBJECT_PRIVILEGES: informazioni sulle autorizzazione degli oggetti nel file system delle librerie. Simile al comando DSPOBJAUT.

```
select OBJECT_NAME "Ogg.", TEXT_DESCRIPTION "Descrizione", OBJECT_TYPE "Tipo",
    SQL_OBJECT_TYPE "Tipo SQL", OWNER "Propr.", AUTHORIZATION_NAME "Utente",
    OBJECT_AUTHORITY "Autorizz.", AUTHORIZATION_LIST "Lista aut.",
    OBJECT_OPERATIONAL, OBJECT_MANAGEMENT, OBJECT_EXISTENCE, OBJECT_ALTER, OBJECT_REFERENCE,
    DATA_READ, DATA_ADD, DATA_UPDATE, DATA_DELETE, DATA_EXECUTE
  from OBJECT_PRIVILEGES
  where OBJECT_SCHEMA = 'MK1SAMPLE'
  order by OBJECT_NAME;
```

| Ogg. | Descrizione | Tipo | Tipo SQL | Propr. | Utente | Autorizz. | Lista aut. | OBJECT_OPERATIONAL | OBJECT_MANAGEMENT | OBJECT_EXIS |
|---|---|---|---|---|---|---|---|---|---|---|
| ACT | Activity | *FILE | TABLE | QPGMR | *PUBLIC | USER DEFINED | [NULL] | YES | YES | NO |
| ACT | Activity | *FILE | TABLE | QPGMR | QPGMR | *ALL | [NULL] | YES | YES | YES |
| ANAGRAFICAARTICOLI | Anagrafica articoli | *FILE | TABLE | QPGMR | *PUBLIC | *EXCLUDE | [NULL] | NO | NO | NO |
| ANAGRAFICAARTICOLI | Anagrafica articoli | *FILE | TABLE | QPGMR | QPGMR | *ALL | [NULL] | YES | YES | YES |
| ANAGRAFICAARTICOLI_01A | RI per codice articolo | *FILE | INDEX | QPGMR | *PUBLIC | *EXCLUDE | [NULL] | NO | NO | NO |
| ANAGRAFICAARTICOLI_01A | RI per codice articolo | *FILE | INDEX | QPGMR | QPGMR | *ALL | [NULL] | YES | YES | YES |
| ANAGRAFICAARTICOLI_01L | RI per codice articolo (no ann) | *FILE | INDEX | QPGMR | *PUBLIC | *EXCLUDE | [NULL] | NO | NO | NO |
| ANAGRAFICAARTICOLI_01L | RI per codice articolo (no ann) | *FILE | INDEX | QPGMR | QPGMR | *ALL | [NULL] | YES | YES | YES |

# Autorizzazioni sugli oggetti (IFS)

- IFS_OBJECT_PRIVILEGES: informazioni sulle autorizzazioni degli oggetti in IFS. Simile al comando `DSPAUT`

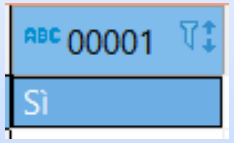
```
with
 LIST as
 (select PATH_NAME
    from table(IFS_OBJECT_STATISTICS(START_PATH_NAME => '/home/mriva')))
 select A.PATH_NAME "Percorso", OBJECT_TYPE "Tipo", OWNER "Propr.",
    AUTHORIZATION_NAME "Utente", DATA_AUTHORITY "Autorizz.", AUTHORIZATION_LIST "Lista aut.",
    OBJECT_OPERATIONAL, OBJECT_MANAGEMENT, OBJECT_EXISTENCE, OBJECT_ALTER, OBJECT_REFERENCE,
    DATA_READ, DATA_ADD, DATA_UPDATE, DATA_DELETE, DATA_EXECUTE
   from LIST as L, table(IFS_OBJECT_PRIVILEGES(PATH_NAME => L.PATH_NAME)) as A
   order by A.PATH_NAME;
```

| Percorso | Tipo | Propr. | Utente | Autorizz. | Lista aut. | OBJECT_OPERATIONAL | OBJECT_MANAGEMENT | OBJECT_EXISTENCE | OBJECT_ALTER |
|---|---|---|---|---|---|---|---|---|---|
| /home/mriva | *DIR | MRIVA | *PUBLIC | *RWX | [NULL] | YES | YES | YES | YES |
| /home/mriva | *DIR | MRIVA | MRIVA | *RWX | [NULL] | YES | YES | YES | YES |
| /home/mriva/.bash_history | *STMF | MRIVA | *PUBLIC | *NONE | [NULL] | NO | YES | YES | YES |
| /home/mriva/.bash_history | *STMF | MRIVA | MRIVA | *RW | [NULL] | YES | YES | YES | YES |
| /home/mriva/.eclipse | *DIR | MRIVA | *PUBLIC | *RWX | [NULL] | YES | YES | YES | YES |
| /home/mriva/.eclipse | *DIR | MRIVA | MRIVA | *RWX | [NULL] | YES | YES | YES | YES |
| /home/mriva/.eclipse/RSE | *DIR | MRIVA | *PUBLIC | *RWX | [NULL] | YES | YES | YES | YES |

# Controllo autorizzazione sui file

- La funzione SQL_CHECK_AUTHORITY restituisce l'indicazione se l'utente è autorizzato o meno all'oggetto di tipo `*FILE`.

```
values case when sql_check_authority('MK1SAMPLE', 'EMPLOYEE') = '0' then 'Sì' else 'No' end;
```




# Liste di autorizzazione: oggetti

- La vista AUTHORIZATION_LIST_INFO visualizza l'elenco degli oggetti protetti da una lista di autorizzazione. Simile al comando DSPAUTLOBJ.

```
select AUTHORIZATION_LIST "Lista", SYSTEM_OBJECT_SCHEMA concat '/' concat SYSTEM_OBJECT_NAME "Oggetto",
  SYSTEM_OBJECT_TYPE "Tipo", OBJECT_ATTRIBUTE "Attr.",
  coalesce(PATH_NAME, '/QDLS/' concat FOLDER_PATH concat '/' concat DLO_NAME) "Percorso",
  OBJECT_OWNER "Propr.", PRIMARY_GROUP "Gruppo", TEXT_DESCRIPTION "Descrizione"
 from AUTHORIZATION_LIST_INFO
 order by AUTHORIZATION_LIST, SYSTEM_OBJECT_SCHEMA, SYSTEM_OBJECT_NAME, "Percorso";
```

| Lista | Oggetto | Tipo | Attr. | Percorso | Propr. | Gruppo | Descrizione |
|---|---|---|---|---|---|---|---|
| QINAVMNTR | QNAVSRV/METAINF | *FILE | PF | [NULL] | QLWISVR | [NULL] | [NULL] |
| QINAVMNTR | QNAVSRV/MNTCMD | *FILE | PF | [NULL] | QLWISVR | [NULL] | [NULL] |
| QINAVMNTR | QNAVSRV/MNTEVT | *FILE | PF | [NULL] | QLWISVR | [NULL] | [NULL] |
| QINAVMNTR | QNAVSRV/MNTLOG | *FILE | PF | [NULL] | QLWISVR | [NULL] | [NULL] |
| QINAVMNTR | QNAVSRV/MNTSPEC | *FILE | PF | [NULL] | QLWISVR | [NULL] | [NULL] |
| QINAVMNTR | QNAVSRV/MNTSVR | *FILE | PF | [NULL] | QLWISVR | [NULL] | [NULL] |
| QINAVMNTR | QNAVSRV/QINAVMNDQ | *DTAQ | [NULL] | [NULL] | QLWISVR | [NULL] | Monitors data queue for IBM Navigator for i |
| QINAVMNTR | QNAVSRV/QINAVMNTRG | *FILE | PF | [NULL] | QLWISVR | [NULL] | [NULL] |
| QIWSADM | QDOC/GM5FG71853 | *FLR | [NULL] | [NULL] | QSECOFR | [NULL] | [NULL] |
| QIWSADM | QDOC/GM5FG71969 | *FLR | [NULL] | /QDLS/QIWSADM/MODEL | QSECOFR | [NULL] | [NULL] |
| QIWSADM | QDOC/GM5FG72023 | *FLR | [NULL] | /QDLS/QIWSADM/USER | QSECOFR | [NULL] | [NULL] |
| QLWISVR | [NULL] | *STMF | [NULL] | /QIBM/ProdData/OS400/Navigator/appdata/iWebNav.et | QLWISVR | [NULL] | [NULL] |
| QLWISVR | [NULL] | *STMF | [NULL] | /QIBM/ProdData/OS400/Navigator/appdata/iWebNav.et | QLWISVR | [NULL] | [NULL] |

# Liste di autorizzazione: utenti

- La vista AUTHORIZATION_LIST_USER_INFO visualizza le informazioni e gli utenti iscritti ad una lista di autorizzazione. Simile al comando `DSPAUTL`.

```
select AUTHORIZATION_LIST "Lista", TEXT_DESCRIPTION "Descrizione", AUTHORIZATION_NAME "Utente",
OBJECT_AUTHORITY "Autorizzazione", AUTHORIZATION_LIST_MANAGEMENT "Gest.lista", OWNER "Propr.",
       OBJECT_OPERATIONAL, OBJECT_MANAGEMENT, OBJECT_EXISTENCE, OBJECT_ALTER, OBJECT_REFERENCE,
       DATA_READ, DATA_ADD, DATA_UPDATE, DATA_DELETE, DATA_EXECUTE
  from AUTHORIZATION_LIST_USER_INFO
order by AUTHORIZATION_LIST, AUTHORIZATION_NAME;
```

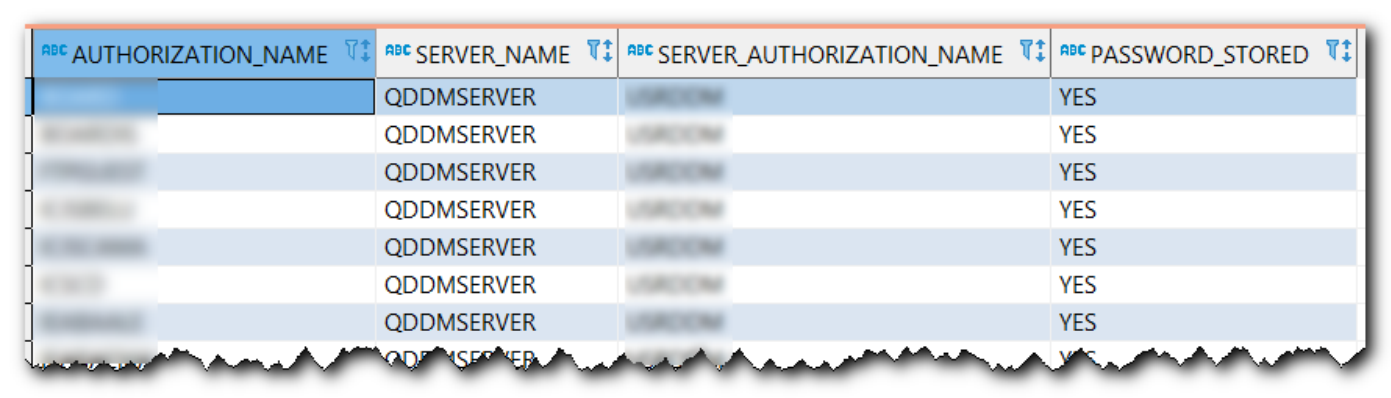
| Lista | Descrizione | Utente | Autorizzazione | Gest.lista | Propr. | OBJECT_OPERATIONAL | OBJECT_MANAGEMENT | OBJECT_EXISTENCE | OBJECT_ALTER | O |
|---|---|---|---|---|---|---|---|---|---|---|
| JDBC | Regolamentazione accesso JDBC/ODBC | *PUBLIC | *CHANGE | NO | QPGMR | YES | NO | NO | NO | NO |
| JDBC | Regolamentazione accesso JDBC/ODBC | QPGMR | *ALL | YES | QPGMR | YES | YES | YES | YES | YES |
| QINAVMNTR | IBM Navigator for i Monitors | *PUBLIC | *USE | NO | QLWISVR | YES | NO | NO | NO | NO |
| QINAVMNTR | IBM Navigator for i Monitors | QLWISVR | *ALL | YES | QLWISVR | YES | YES | YES | YES | YES |
| QIWSADM | Amministratori IBM i Access | *PUBLIC | *USE | NO | QSECOFR | YES | NO | NO | NO | NO |
| QIWSADM | Amministratori IBM i Access | QSECOFR | *ALL | YES | QSECOFR | YES | YES | YES | YES | YES |
| QLWISVR | [NULL] | *PUBLIC | *EXCLUDE | NO | QSYS | NO | NO | NO | NO | NO |
| QLWISVR | [NULL] | QSYS | *ALL | YES | QSYS | YES | YES | YES | YES | YES |
| QLWISVR | [NULL] | QTMHHTTP | *USE | NO | QSYS | YES | NO | NO | NO | NO |

# Liste di autorizzazione

- Con le viste AUTHORIZATION_LIST_INFO e AUTHORIZATION_LIST_USER_INFO posso quindi rispondere a domande come:
  - in quali liste di autorizzazione è presente l'utente XYZ?
  - con quali liste di autorizzazione sono protetti gli oggetti di una libreria?
  - …

# Voci di autorizzazione server

- La vista DRDA_AUTHENTICATION_ENTRY_INFO restituisce informazioni sulle voci di autorizzazione server . Simile al comando `DSPSVRAUTE`.



| AUTHORIZATION_NAME | SERVER_NAME | SERVER_AUTHORIZATION_NAME | PASSWORD_STORED |
|---|---|---|---|
| | QDDMSERVER | | YES |
| | QDDMSERVER | | YES |
| | QDDMSERVER | | YES |
| | QDDMSERVER | | YES |
| | QDDMSERVER | | YES |
| | QDDMSERVER | | YES |
| | QDDMSERVER | | YES |

# Function usage

- Le viste FUNCTION_INFO e FUNCTION_USAGE restituiscono informazioni sulle function usage. Simili ai comandi `DSPFCNUSG` e `WRKFCNUSG`.

```
select FUNCTION_CATEGORY "Categ.", I.FUNCTION_ID "Funzione", FUNCTION_TYPE "Tipo",
       coalesce(FUNCTION_DESCRIPTION_MESSAGE_TEXT, FUNCTION_NAME) "Descrizione",
       FUNCTION_PRODUCT_ID "Prodotto", DEFAULT_USAGE "Util.default", ALLOBJ_INDICATOR "Ut. *ALLOBJ",
       USAGE_INFORMATION_INDICATOR "Info util.",
       USER_NAME "Utente", USER_TYPE "Tipo utente", USAGE "Permesso"
  from FUNCTION_INFO as I inner join FUNCTION_USAGE as U
    on I.FUNCTION_ID = U.FUNCTION_ID
  order by FUNCTION_CATEGORY, I.FUNCTION_ID, USER_TYPE, USER_NAME;
```

| Categ. | Funzione | Tipo | Descrizione | Prodotto | Util.default | Ut. *ALLOBJ | Info util. | Utente | Tipo utente | Permesso |
|---|---|---|---|---|---|---|---|---|---|---|
| 3 - HOST | QIBM_DB_ZDA | ADMINISTRABLE | Fornisce il supporto per proteggere l'accesso al server d | QIBM_BASE_OPERATING_SYSTEM | ALLOWED | NOT USED | YES | [illegible] | GROUP | DENIED |
| 3 - HOST | QIBM_DB_ZDA | ADMINISTRABLE | Fornisce il supporto per proteggere l'accesso al server d | QIBM_BASE_OPERATING_SYSTEM | ALLOWED | NOT USED | YES | [illegible] | GROUP | DENIED |
| 3 - HOST | QIBM_QSY_SYSTEM_CERT_STORE | ADMINISTRABLE | Fornire l'accesso alla memorizzazione certificato *SYSTE | QIBM_QSY_DIGITAL_CERT_MGR | DENIED | USED | YES | QDIRSRV | USER | ALLOWED |
| 3 - HOST | QIBM_QSY_SYSTEM_CERT_STORE | ADMINISTRABLE | Fornire l'accesso alla memorizzazione certificato *SYSTE | QIBM_QSY_DIGITAL_CERT_MGR | DENIED | USED | YES | QTCP | USER | ALLOWED |
| 3 - HOST | QIBM_QSY_SYSTEM_CERT_STORE | ADMINISTRABLE | Fornire l'accesso alla memorizzazione certificato *SYSTE | QIBM_QSY_DIGITAL_CERT_MGR | DENIED | USED | YES | QYPSJSVR | USER | ALLOWED |

# Giornale sicurezza QAUDJRN

- Configurazione giornale sicurezza:

```
select AUDIT_JOURNAL_EXISTS "Giorn.sic.", CREATE_OBJECT_AUDITING "Aud.creaz.ogg.",
    AUDITING_CONTROL "Controllo auditing", '1/' concat trim(AUDITING_LEVEL) concat
    ' - 2/' concat trim(AUDITING_LEVEL_EXTENSION) "Liv. auditing",
    AUDIT_JOURNAL_RECEIVER_LIBRARY "Lib.ricevitori", AUDIT_JOURNAL_RECEIVER "Ricevitore"
  from SECURITY_INFO;
```

| Giorn.sic. | Aud.creaz.ogg. | Controllo auditing | Liv. auditing | Lib.ricevitori | Ricevitore |
|---|---|---|---|---|---|
| YES | *NONE | *AUDLVL | 1/*AUTFAIL *JOBDTA - 2/*NONE | AUDITING2 | AUDRCV8394 |

- Esistono un gruppo di funzioni che restituiscono le informazioni dal giornale della sicurezza formattate in base al tipo voce https://www.ibm.com/docs/en/i/7.4?topic=services-audit-journal-entry
  Tipi voce: AF, CA, CD, CO, CP, DO, EV, GR, M0, M6, M7, M8, M9, OW, PW, SV

# Giornale sicurezza QAUDJRN: esempio

- La funzione di tabella AUDIT_JOURNAL_PW estrae le voci di giornale di tipo PW che riguardono eventi relativi alla password

```
select timestamp(ENTRY_TIMESTAMP, 0) "Data/ora", QUALIFIED_JOB_NAME "Lavoro",
       trim(PROGRAM_LIBRARY) concat '/' concat trim(PROGRAM_NAME) "Programma",
       trim(REMOTE_ADDRESS) concat ':' concat trim(REMOTE_PORT) "Ind.remoto",
       VIOLATION_TYPE "Tipo violazione", VIOLATION_TYPE_DETAIL "Descrizione",
       AUDIT_USER_NAME "Utente", DEVICE_NAME "Device"
  from table(SYSTOOLS/AUDIT_JOURNAL_PW(STARTING_TIMESTAMP => current timestamp - 72 hours));
```

| Data/ora | Lavoro | Programma | Ind.remoto | Tipo violazione | Descrizione | Utente | Device |
|---|---|---|---|---|---|---|---|
| 2021-10-16 01:32:35.000 | 095353/QTCP/QTVDEVICE | QTCP/QTGCLSRV | 192.168.1.100:16493 | U | User name not valid | | [NULL] |
| 2021-10-16 08:13:12.000 | 517644/QTMHHTTP/ | QSYS/QLESPI | 192.168.90.3:64809 | P | Password not valid | | [NULL] |
| 2021-10-16 08:13:22.000 | 517644/QTMHHTTP/ | QSYS/QLESPI | 192.168.90.3:64847 | P | Password not valid | | [NULL] |
| 2021-10-16 08:13:26.000 | 517644/QTMHHTTP/ | QSYS/QLESPI | 192.168.90.3:64861 | P | Password not valid | | [NULL] |
| 2021-10-16 08:25:24.000 | 095089/QSYS/QINTER | QSYS/QLESPI | 192.168.0.222:3008 | P | Password not valid | | SASC1 |
| 2021-10-16 08:33:08.000 | 517645/QTMHHTTP | QSYS/QLESPI | :64619 | U | User name not valid | DONTEXISTS | [NULL] |

# Authority collection

- Esistono una serie di viste per gestire le authority collection. La principale è AUTHORITY_COLLECTION.
- Le authority collection consentono di monitorare per uno o più utenti l'accesso agli oggetti in una o più librerie o cartelle
- Sono molto utili per pianificare modifiche alle autorizzazioni sugli oggetti
- Si avviano/arrestano da Navigator for i (utenti > Gestisci collezioni) o con i comandi `STRAUTCOL/ENDAUTCOL`

IBM i 7.3 – Authority Collection Services, di Steve Bradshaw, 23-dic-2016:
https://powerwire.eu/ibm-i-7-3-authority-collection-services

# Certificati

- La funzione di tabella CERTIFICATE_INFO restituisce informazioni sui certificati. Per esempio per visualizzare i certificati memorizzati nello storage *SYSTEM:

```
select CERTIFICATE_LABEL "Desc.certificato", SUBJECT_COMMON_NAME "Desc.comune",
       SUBJECT_ORGANIZATION "Organizzazione",
       ISSUER_COMMON_NAME "Emittente: nome", ISSUER_ORGANIZATION "Emittente: organizzazione",
       timestamp(VALIDITY_START, 0) "Inizio val.",
       timestamp(VALIDITY_END, 0) "Fine val.", TRUSTED "Trusted",
       PRIVATE_KEY "Chiave privata", DOMAIN_NAMES "Nome dominio"
  from table(CERTIFICATE_INFO(CERTIFICATE_STORE_PASSWORD => 'xyz',
                              CERTIFICATE_STORE => '*SYSTEM'));
```

| Desc.certificato | Desc.comune | Organizzazione | Emittente: nome | Emittente: organizzazione | Inizio val. | Fine val. |
|---|---|---|---|---|---|---|
| [redacted] | [redacted] | [NULL] | Sectigo RSA Domain Validation Secure Server CA | Sectigo Limited | 2020-06-08 02:00:00.000 | 2022-07-09 0 |
| Trustico 3 AC | Sectigo RSA Domain Validation Secure Server CA | Sectigo Limited | USERTrust RSA Certification Authority | The USERTRUST Network | 2018-11-02 01:00:00.000 | 2031-01-01 0 |
| Comodo RSA Certification Authority | COMODO RSA Certification Authority | COMODO CA Limited | COMODO RSA Certification Authority | COMODO CA Limited | 2010-01-19 01:00:00.000 | 2038-01-19 0 |
| Comodo AC 2020-05 2 | USERTrust RSA Certification Authority | The USERTRUST Network | AAA Certificate Services | Comodo CA Limited | 2019-03-12 01:00:00.000 | 2029-01-01 0 |
| Comodo AC 2020-05 1 | AAA Certificate Services | Comodo CA Limited | AAA Certificate Services | Comodo CA Limited | 2004-01-01 01:00:00.000 | 2029-01-01 0 |
| Comodo Intermediate 2 CA | COMODO RSA Domain Validation Secure Server CA | COMODO CA Limited | COMODO RSA Certification Authority | COMODO CA Limited | 2014-02-12 01:00:00.000 | 2029-02-12 0 |
| [redacted] | [redacted] | [NULL] | COMODO RSA Domain Validation Secure Server CA | COMODO CA Limited | 2018-03-12 01:00:00.000 | 2020-06-10 0 |

# Riferimenti

- E-mail aziendale: mriva@sirio-is.it
- Blog: www.markonetools.it
- E-mail blog: info@markonetools.it
- Linkedin: www.linkedin.com/in/marcoriva-mk1
- Twitter: @MarcoRiva73
- Facebook: https://www.facebook.com/markonetools/
- YouTube: https://www.youtube.com/channel/UCb47YJQJCzU-5x4nnGzDu-w