# NetIQ Security Solutions for IBM i
# TGAudit 2.4
## Report Reference Guide
**Revised September 2021**

## Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.

**Copyright© 2021 Trinity Guard LLC. All rights reserved.**

1. What's New . . . 9
2. TGAudit Report Reference Introduction . . . 10
3. Authority Collection Reports . . . 11
3.1 Authority Collection for Object IFS Report . . . 12
3.2 Authority Collection for Object Native Report . . . 13
3.3 Authority Collection for Users and IFS Report . . . 14
3.4 Authority Collection for Users and Native Object Report . . . 15
3.5 Authority Collection Report (*ALL) . . . 16
4. Configuration Management Reports . . . 17
4.1 Access Control List Changes . . . 21
4.2 Actions that Affect a Job are Audited . . . 22
4.3 Active Job Information . . . 24
4.4 Adopting Authority from a Program Owner is Audited . . . 25
4.5 All Deletions of External Objects on the System are Audited . . . 26
4.6 All Object Creations are Audited . . . 28
4.7 All Optical Functions are Audited . . . 30
4.8 All Security Functions are Audited . . . 32
4.9 Alternate Subsystem Configurations . . . 35
4.10 Attention Events are Audited . . . 36
4.11 Auditing End Action set to Power Down System . . . 37
4.12 Authority Changes to Restored Objects . . . 38
4.13 Authorization Failures are Audited . . . 39
4.14 Authorization List or Object Authority Changes . . . 41
4.15 Basic Product Information on the System . . . 42
4.16 Certificate Details . . . 43
4.17 Certificates Expired . . . 44
4.18 Certificates Expiring in 90 Days . . . 45
4.19 Change Request Descriptor Changes . . . 46
4.20 Columns with Field Procedures . . . 47
4.21 Cryptographic Configuration Changes . . . 48
4.22 Current Cumulative PTF Level . . . 49
4.23 Current Job's Reply List Entry Information . . . 50
4.24 Dependencies of Row Permissions and Column Masks . . . 51
4.25 Disk Information . . . 52
4.26 DRDA and DDM User Access . . . 53
4.27 EIM Attribute Changes . . . 54
4.28 Environment Variable Changes . . . 55
4.29 Exit Point Information . . . 56
4.30 Exit Program Information . . . 57
4.31 Function Usage Configuration Details . . . 58
4.32 Function Usage Identifiers . . . 59
4.33 Group PTFs Information . . . 60
4.34 IBM i Temporary Storage Pool Detail . . . 61
4.35 IPv4 and IPv6 Network Connection Details . . . 62
4.36 Installed Products . . . 63
4.37 Job Description Details . . . 64
4.38 Job Descriptions that Contain User Profile Names were Restored . . . 65
4.39 Job Descriptions – USER Parameter Changes . . . 66
4.40 Job Descriptions with Logging . . . 67
4.41 Job Descriptions with Request Data . . . 68
4.42 Job Descriptions with Specific Initial Library Lists . . . 69
4.43 Job Schedule Entry Information . . . 70
4.44 Journal and Remote Journal Information . . . 71
4.45 Key Ring File Changes . . . 72
4.46 Limit Device Sessions Not Enabled . . . 73
4.47 Line Description Details . . . 74
4.48 Media Library Status Details . . . 75
4.49 Memory Pool Details . . . 76
4.50 Message Queue Data by Date Range . . . 77
4.51 Message Queue Data for All Queues . . . 78

4.52 Message Queue Data QSYSOPR . . . 79
4.53 Message Queue Data Severity Greater than 30 . . . 80
4.54 Message Queue Details . . . 81
4.55 Networking and Communications Functions are Audited . . . 82
4.56 Object Auditing Attribute Changes . . . 84
4.57 Object Lock Information . . . 85
4.58 Object Management Tasks are Audited . . . 86
4.59 OfficeVision Tasks are Audited . . . 88
4.60 Operating System Product Info . . . 90
4.61 Output Queue Details . . . 91
4.62 Ownership Changes for Restored Objects . . . 92
4.63 Partition Information . . . 93
4.64 Permission or Column Mask Defined . . . 94
4.65 Primary Group Changes for Restored Objects . . . 95
4.66 Printing Functions are Audited . . . 96
4.67 Product Information on the System . . . 98
4.68 Product Registration ID Information . . . 100
4.69 Products License Information . . . 101
4.70 Products with Load Errors . . . 102
4.71 Program Changes to Adopt Owner Authority . . . 103
4.72 Program Failures are Audited . . . 105
4.73 Programs Restored that Adopt Owner Authority . . . 107
4.74 Programs that Adopt Authority were Executed . . . 108
4.75 PTF Status for all Products . . . 109
4.76 PTFs Applied to the Licensed Internal Code . . . 110
4.77 PTFs for WDS . . . 111
4.78 PTFs Requiring IPL . . . 112
4.79 PTFs that are Loaded but not Applied . . . 113
4.80 Record Lock Information . . . 114
4.81 Restrict Use of Use Adopted Authority . . . 115
4.82 QHST Message Information . . . 116
4.83 QHST Messages with Severity Greater Than 40 . . . 117
4.84 Save and Restore Information is Audited . . . 118
4.85 Security Auditing Level . . . 120
4.86 Security System Values . . . 121
4.87 Server Security Data is Retained . . . 124
4.88 Server Security User Information Actions . . . 125
4.89 Service Tasks are Audited . . . 126
4.90 Service Tools Actions . . . 128
4.91 Software Product Information . . . 129
4.92 Spooled File Functions are Audited . . . 130
4.93 Spooled File in Output Queue . . . 131
4.94 Storage Usage by User Profile . . . 132
4.95 Strong System Security Level . . . 133
4.96 Subsystem Autostart Details . . . 134
4.97 Subsystem Communication Details . . . 135
4.98 Subsystem Information Details . . . 136
4.99 Subsystem Job Queue Details . . . 137
4.100 Subsystem Pool Data Details . . . 138
4.101 Subsystem Prestart Job Details . . . 139
4.102 Subsystem Remote Entries . . . 140
4.103 Subsystem Routing Entries . . . 141
4.104 Subsystem Routing Entry Changes . . . 142
4.105 Subsystem Workstation Names . . . 143
4.106 Subsystem Workstation Types . . . 144
4.107 Superseded PTFs . . . 145
4.108 System, User, and Object Auditing Control Configuration . . . 146
4.109 System Management Tasks are Audited . . . 147
4.110 System Software Resources . . . 149
4.111 System Value Changes . . . 150

4.112 System Value Configuration Changes . . . 151
4.113 System Value Configuration Details . . . 153
4.114 System Value Default Changes . . . 155
4.115 System Value Defaults . . . 157
4.116 System Value Valid Value Changes . . . 159
4.117 System Value Valid Values . . . 161
4.118 Systems Management Changes . . . 163
4.119 Time Adjustment Software Installed . . . 165
4.120 User Profile Changes . . . 166
4.121 User Profile Information . . . 167
5. Databases Management Reports . . . 168
5.1 Cross Reference Physical File . . . 169
5.2 Data Area Changes . . . 170
5.3 Database Access . . . 171
5.4 Database Changes . . . 172
5.5 Database Content . . . 173
5.6 Database Operations . . . 174
5.7 Database Operations by Journal . . . 175
5.8 Field Level Authorities . . . 176
5.9 Row and Column Access Control . . . 177
5.10 Schedule Master File . . . 178
5.11 Sensitive Database Content . . . 179
6. Log Management Reports . . . 180
6.1 Job Activity Details . . . 181
6.2 Job Activity Summary . . . 182
7. Network Management Reports . . . 183
7.1 Actions to IP Rules . . . 185
7.2 APPN Endpoint Filter Violations . . . 187
7.3 Asynchronous Signals Processed . . . 189
7.4 Cluster Operations . . . 190
7.5 Connections Started, Ended, or Rejected . . . 191
7.6 Controller Description Details . . . 193
7.7 Controllers and Attached Devices . . . 194
7.8 Database Server Initialization Report . . . 195
7.9 Database Server Native DB Report . . . 196
7.10 Database Server Object Info Report . . . 197
7.11 Database Server SQL Requests Report . . . 198
7.12 Device Description Data . . . 199
7.13 Device Descriptions - *APPC . . . 200
7.14 DNS Configuration Details . . . 201
7.15 Integrated File System Exits Installed . . . 202
7.16 Internet Security Management Events . . . 203
7.17 Inter-process Communication Events . . . 205
7.18 Intrusion Monitor Events . . . 206
7.19 NetServer Configuration . . . 208
7.20 NetServer Shares . . . 209
7.21 Network Attribute Details . . . 210
7.22 Network Authentication Events . . . 211
7.23 Network Connection Details . . . 213
7.24 Network Interface Details IPv4 . . . 214
7.25 Network Interface Details IPv6 . . . 215
7.26 Network Route Details IPv4 . . . 216
7.27 Network Route Details IPv6 . . . 217
7.28 Network Server Descriptions . . . 218
7.29 Network Server Encryption Status . . . 219
7.30 Network Servers with Encryption Verified . . . 220
7.31 Network Servers with Failed or Unknown Encryption . . . 221
7.32 Object Management Changes . . . 222
7.33 OfficeVision Mail Services Actions . . . 223
7.34 Remote Power On and IPL . . . 224

7.35 Remote Service Attribute . . . 225
7.36 Remote Sign-on Control . . . 226
7.37 Secure Socket Connections . . . 227
7.38 Server Sessions Started or Ended . . . 229
7.39 Server Share Information . . . 230
7.40 Service Status Change Events . . . 231
7.41 Sockets-related Exit Points Not Secured . . . 233
7.42 SSL Cipher Control and Specification List . . . 234
7.43 TCP_IP IPv4 Stack Attributes . . . 236
7.44 TCP_IP IPv6 Stack Attributes . . . 237
7.45 Unsecured Remote Server Exit Points . . . 238
8. Profile Management Reports . . . 240
8.1 All User Profiles . . . 242
8.2 Authority Failures . . . 243
8.3 Authority Restored for User Profiles . . . 245
8.4 Block Password Change . . . 246
8.5 Changes to Service Tools Profiles . . . 247
8.6 Connection Verifications . . . 249
8.7 Directory Server Extensions . . . 250
8.8 Disable Profile After Maximum Failed Signon Attempts . . . 251
8.9 Duplicate Password Control . . . 252
8.10 Enabled IBM Profiles . . . 254
8.11 Exceeded Account Limit Events . . . 255
8.12 Group Profile Information . . . 257
8.13 Group Profiles with *ALLOBJ *SECADM or *SERVICE Special Authorities . . . 258
8.14 Group Profiles with Special Authorities . . . 259
8.15 IBM Profile Details Report . . . 260
8.16 Identity Token Events . . . 261
8.17 Inactive Job Message Queue . . . 263
8.18 Inactive Job Time-out . . . 264
8.19 Invalid Sign-on Attempts . . . 265
8.20 Limit Adjacent Digits in Password . . . 267
8.21 Limit Characters in Password . . . 268
8.22 Limit Password Character Positions . . . 269
8.23 Limit Repeating Characters in Password . . . 270
8.24 Limit Security Officer Device Access . . . 271
8.25 Maximum Password Length . . . 272
8.26 Minimum Password Length . . . 273
8.27 Network Attribute Changes . . . 274
8.28 Network Log on and Logoff Events . . . 275
8.29 Network Password Errors . . . 277
8.30 Network Profile Changes . . . 278
8.31 Object Authorities of User Profiles . . . 279
8.32 Ownership Changes for Restored Objects0 . . . 280
8.33 Password Expiration Interval . . . 281
8.34 Password Expiration Warning . . . 283
8.35 Password Level . . . 284
8.36 Password Rules . . . 286
8.37 Password Validation Program . . . 287
8.38 Powerful User Profiles . . . 288
8.39 Profile Object Auditing Values . . . 290
8.40 Profile with Password Expiration Interval not *SYSVAL . . . 291
8.41 Profiles that are *DISABLED . . . 292
8.42 Profiles with Expired Passwords . . . 293
8.43 Profiles with Limit Capabilities = *NO . . . 294
8.44 Profiles with Multiple Groups . . . 295
8.45 Profiles with Pwd = *NONE or *DISABLED . . . 296
8.46 Publicly Accessible User Profiles . . . 297
8.47 Require Digit in Password . . . 298
8.48 Security Officer Profiles . . . 299

8.49 Service Tool Security Attributes . . . 300
8.50 Swap Profile Events . . . 301
8.51 System Service Tools Users . . . 303
8.52 User Profile = Password . . . 305
8.53 User Profiles Not Used in 90 Days . . . 306
8.54 Users with Job Control Special Authority . . . 307
8.55 Users with Save System Special Authority . . . 308
8.56 Users with Unlimited Device Sessions . . . 309
9. Resource Management Reports . . . 310
9.1 *PUBLIC User with *RWX Authorities -*PUBLIC with *ALL . . . 313
9.2 Actions on Validation Lists . . . 314
9.3 Allow Object Restore Option . . . 316
9.4 Allow User Domain Objects in Libraries . . . 317
9.5 ASCII Files Stored in the IFS . . . 318
9.6 Attributes for QSYS.LIB . . . 319
9.7 Authorization List Details . . . 320
9.8 Authorization Lists with Public Access . . . 321
9.9 Authorized Users via Authorization Lists . . . 322
9.10 Change Request Descriptors Restored . . . 323
9.11 Changed Data Files in Last 30 Days . . . 324
9.12 Close Operations on Server Files . . . 325
9.13 Commands Available in QSH . . . 327
9.14 Commands Executed . . . 328
9.15 Configuration Files . . . 330
9.16 Create Operations . . . 331
9.17 Damages Objects . . . 332
9.18 Data Queue Entries . . . 333
9.19 Database Files Larger than 100Mb . . . 334
9.20 Database Files with Over 1,000,000 Read Operations . . . 335
9.21 Database Files with Over 100,000 Delete Operations . . . 336
9.22 Database Files with Over 100,000 Insert Operations . . . 337
9.23 Database Files with 10000 Delete Records . . . 338
9.24 Db2 Mirror Communication Services . . . 339
9.25 Db2 Mirror Product Services . . . 340
9.26 Db2 Mirror Replication Services . . . 341
9.27 Db2 Mirror Replication State . . . 342
9.28 Db2 Mirror Setup Tools . . . 343
9.29 Delete Operations . . . 344
9.30 Directory Link, Unlink, and Search Operations . . . 346
9.31 Directory Search Violations . . . 348
9.32 DLO Object Changes . . . 349
9.33 DLO Object Reads . . . 350
9.34 Dual Optical Object Accesses . . . 351
9.35 Exit Point Maintenance Operations . . . 353
9.36 File Statistics . . . 355
9.37 File Usage Information . . . 357
9.38 Files Checked Out Status . . . 358
9.39 Files Not Secured by Authorization Lists . . . 359
9.40 Files Not Used in the Last 30 Days . . . 360
9.41 Files with RWX Authorities . . . 361
9.42 HTTP Server and Web Files Status . . . 362
9.43 HTTP Server File Authorities . . . 363
9.44 IFS Directory Information . . . 364
9.45 IFS Files Being Journaled . . . 365
9.46 Integrated File System Content . . . 366
9.47 Integrated File System Security . . . 367
9.48 Job Changes . . . 368
9.49 Job Descriptions - USER Parameter Changes . . . 370
9.50 Journaled Files . . . 371
9.51 Journaled Objects . . . 372

9.52 Largest Files Report >100Mb . . . 373
9.53 LDAP Operations . . . 374
9.54 Library QGPL Database Files not Backed up in 30 Days . . . 376
9.55 Library Statistics . . . 377
9.56 Maximum sign-on attempts allowed is NOMAX . . . 379
9.57 Network Resource Accesses . . . 380
9.58 New Data Files in Last 30 Days . . . 382
9.59 New Library in Last 30 Days . . . 383
9.60 New Objects in the Last 30 Days . . . 384
9.61 Object Authority . . . 385
9.62 Object Changes . . . 386
9.63 Object Details . . . 387
9.64 Object Ownership Changes . . . 388
9.65 Object Reads . . . 389
9.66 Object Source . . . 390
9.67 Object Statistics . . . 391
9.68 Objects Changed in the Last 30 Days . . . 393
9.69 Objects Created in the Last 30 Days . . . 394
9.70 Objects Larger than 100MB . . . 395
9.71 Objects Owned by QSECOFR . . . 396
9.72 Objects Restored . . . 397
9.73 Objects Used in the Last 30 Days . . . 398
9.74 Optical Volume Accesses . . . 399
9.75 Primary Group Changes . . . 401
9.76 Printer Output Changes . . . 402
9.77 Program Reference Details . . . 404
9.78 Programs that Adopt Authority . . . 405
9.79 PTF Object Changes . . . 406
9.80 PTF Operations . . . 407
9.81 Public Access to Commands in QSYS . . . 408
9.82 Public Access to Devices . . . 409
9.83 Public Access to Journal Receivers in QGPL . . . 410
9.84 Public Access to Objects in QGPL . . . 411
9.85 Regular Files on the IFS . . . 412
9.86 Restored Objects in the Last 30 Days . . . 413
9.87 Single Optical Object Accesses . . . 414
9.88 Socket Descriptor Details . . . 416
9.89 Source Changes in Last 30 Days . . . 418
9.90 Spooled File Actions . . . 419
9.91 System Directory Changes . . . 421
9.92 System Security Audit Journal Exists . . . 423
9.93 TGAudit Report Configuration . . . 424
9.94 TGCentral Agent Configuration . . . 426
9.95 Unsaved Objects in the Last 30 Days . . . 428
9.96 User-defined File Systems (UDFS's) . . . 429
9.97 Verify Object on Restore . . . 430
10. Appendices . . . 432
10.1 APPENDIX - TGAudit Report Reference Revisions . . . 433
10.1.1 Version 2.4 - TGAudit Report Reference . . . 434
10.1.2 Version 2.3 - TGAudit Report Reference . . . 435
10.1.3 Version 2.2 - TGAudit Report Reference . . . 436
10.1.4 Version 2.1 - TGAudit Report Reference . . . 438
10.2 APPENDIX - TGAudit Collectors . . . 439

# What's New

**Version 2.4 - TGAudit Report Reference**

**Collectors**

The following new collectors are now available:

- SYS_VAL_CONFIG
- SYS_VAL_DEFAULT
- SYS_VAL_VALID
- NETSERVER_CONFIG
- NETSERVER_SHARES
- QSYS2.DATA_QUEUE_ENTRIES
- QSYS2.EXIT_POINT_INFO
- QSYS2.EXIT_PROGRAM_INFO
- QSYS2.JOURNALED_OBJECTS
- QSYS2.SERVER_SHARE_INFO
- QSYS2.SOFTWARE_PRODUCT

**Reports**

**Configuration Reports**

The following new **Configuration** reports are now available:

- Exit Point Information
- Exit Program Information
- Software Product Information
- System Value Configuration Changes
- System Value Configuration Details
- System Value Default Changes
- System Value Defaults
- System Value Valid Value Changes
- System Value Valid Values

**Network Reports**

- NetServer Shares
- NetServer Configuration
- Server Share Information

**Resource Reports**

- Data Queue Entries
- Journaled Objects

### See also

APPENDIX - TGAudit Report Reference Revisions

# TGAudit Report Reference Introduction

This reference guide provides information about the built-in reports provided in TGAudit.  Use this reference guide to learn why a report passed or failed in a pre-defined TGAudit Report Card, as well as learn information about report topics and recommendations on how to address existing vulnerabilities.

> **Note**: Refer to the TGAudit User Guide for detailed information and concepts on how to use TGAudit.

The TGAudit reports fall into the following categories:

- Authority Collection Reports
- Configuration Management Reports
- Database Management Reports
- Log Management Reports
- Network Management Reports
- Profile Management Reports
- Resource Management Reports

# Authority Collection Reports

This section includes descriptions of the following **Authority Collection** reports:

- Authority Collection for Object IFS Report
- Authority Collection for Object Native Report
- Authority Collection for Users and IFS Report
- Authority Collection for Users and Native Object Report
- Authority Collection Report (*ALL)

# Authority Collection for Object IFS Report

If a user is enrolled in Authority Collection through the STRAUTCOL command with DLO and file system objects selected for inclusion, then the Authority Collection data collected for IFS objects will be displayed in this report. Information about current and required authorities to applications is displayed for enrolled users.

> ⚠ **Important**: This report is only available for OS 7.4 or higher.

**Collector ID**: AUTHORITY_COL_IFS

**Report ID**: AUTHORITY_COL_IFS

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **4** (Authority Collection).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **20** (Authority Collection Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **4** (Auth Collection For Objects IFS Report).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> ⓘ **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> ✓ **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Authority Collection for Object Native Report

If a user is enrolled in Authority Collection through the STRAUTCOL command, then the Authority Collection data collected for native (QSYS.LIB) objects will be displayed in this report.  Information about current and required authorities to applications is displayed for enrolled users.

> ⚠ **Important**: This report is only available for OS 7.4 or higher.

**Collector ID**:  AUTHORITY_COL_OBJECT

**Report ID**: AUTHORITY_COL_OBJECT

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **4** (Authority Collection).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **20** (Authority Collection Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **3** (Auth Collection For Objects Native Report).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> ⓘ **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> ✓ **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Authority Collection for Users and IFS Report

If a user is enrolled in Authority Collection through the STRAUTCOL command, then the Authority Collection data collected for IFS objects will be displayed in this report and categorized by user. Information about current and required authorities to applications is displayed for enrolled users.

> ⚠ **Important**: This report is only available for OS 7.3 or higher.

**Collector ID**: AUTHORITY_COLLECTION

**Report ID**: AUTHORITY_IFS

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **4** (Authority Collection).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **20** (Authority Collection Reports).

5) Press **Enter**.

6 At the **Selection or command** prompt, enter **2** (Auth Collection For Users and Native Object Report).

7) Press **Enter**.

8) Modify the run criteria as necessary.

> ⚠ **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

> ✓ **Tip**: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

9) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**See also**

Resource Management Reports

# Authority Collection for Users and Native Object Report

If a user is enrolled in Authority Collection through the STRAUTCOL command, then the Authority Collection data collected for native (QSYS.LIB) objects will be displayed in this report and categorized by user. Information about current and required authorities to applications is displayed for enrolled users.

> **Important**: This report is only available for OS 7.3 or higher.

**Collector ID**: AUTHORITY_COLLECTION

**Report ID**: AUTHORITY_OBJECTS

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **4** (Authority Collection).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **20** (Authority Collection Reports).

5) Press **Enter**.

6 At the **Selection or command** prompt, enter **1** (Auth Collection For Users and Native Object Report).

7) Press **Enter**.

8) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

> **Tip**: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

9) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**See also**

Resource Management Reports

# Authority Collection Report (*ALL)

If a user is enrolled in Authority Collection through the STRAUTCOL command with DLO and file system objects selected for inclusion, then the Authority Collection data collected for all objects will be displayed in this report. Information about current and required authorities to applications is displayed for enrolled users.

> ⚠ **Important**: This report is only available for OS 7.4 or higher.

**Collector ID**: AUTHORITY_COL_ALL

**Report ID**: AUTHORITY_COL_ALL

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **4** (Authority Collection).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **20** (Authority Collection Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **5** (Auth Collection Report *ALL).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> ⓘ **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> ✓ **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Configuration Management Reports

This section includes descriptions of the following **Configuration Management** reports:

- Access Control List Changes
- Actions that Affect a Job are Audited
- Active Job Information
- Adopting Authority from a Program Owner is Audited
- All Deletions of External Objects on the System are Audited
- All Object Creations are Audited
- All Optical Functions are Audited
- All Security Functions are Audited
- Alternate Subsystem Configurations
- Attention Events are Audited
- Auditing End Action set to Power Down System
- Authority Changes to Restored Objects
- Authorization Failures are Audited
- Authorization List or Object Authority Changes
- Basic Product Information on the System
- Certificate Details
- Certificates Expired
- Certificates Expiring in 90 Days
- Change Request Descriptor Changes
- Columns with Field Procedures
- Cryptographic Configuration Changes
- Current Cumulative PTF Level
- Current Job's Reply List Entry Information
- Dependencies of Row Permissions and Column Masks
- Disk Information
- DRDA and DDM User Access
- EIM Attribute Changes
- Environment Variable Changes
- Exit Point Information
- Exit Program Information
- Function Usage Configuration Details
- Function Usage Identifiers
- Group PTFs Information
- IBM i Temporary Storage Pool Detail
- IPv4 and IPv6 Network Connection Details
- Installed Products

- Job Description Details
- Job Descriptions that Contain User Profile Names were Restored
- Job Descriptions – USER Parameter Changes
- Job Descriptions with Logging
- Job Descriptions with Request Data
- Job Descriptions with Specific Initial Library Lists
- Job Schedule Entry Information
- Journal and Remote Journal Information
- Key Ring File Changes
- Limit Device Sessions Not Enabled
- Line Description Details
- Media Library Status Details
- Memory Pool Details
- Message Queue Data by Date Range
- Message Queue Data for All Queues
- Message Queue Data QSYSOPR
- Message Queue Data Severity Greater than 30
- Message Queue Details
- Networking and Communications Functions are Audited
- Object Auditing Attribute Changes
- Object Lock Information
- Object Management Tasks are Audited
- OfficeVision Tasks are Audited
- Operating System Product Info
- Output Queue Details
- Ownership Changes for Restored Objects
- Partition Information
- Permission or Column Mask Defined
- Primary Group Changes for Restored Objects
- Printing Functions are Audited
- Product Information on the System
- Product Registration ID Information
- Products License Information
- Products with Load Errors
- Program Changes to Adopt Owner Authority
- Program Failures are Audited
- Programs Restored that Adopt Owner Authority
- Programs that Adopt Authority were Executed
- PTF Status for all Products

- PTFs Applied to the Licensed Internal Code
- PTFs for WDS
- PTFs Requiring IPL
- PTFs that are Loaded but not Applied
- Record Lock Information
- Restrict Use of Use Adopted Authority
- QHST Message Information
- QHST Messages with Severity Greater Than 40
- Save and Restore Information is Audited
- Security Auditing Level
- Security System Values
- Server Security Data is Retained
- Server Security User Information Actions
- Service Tasks are Audited
- Service Tools Actions
- Software Product Information
- Spooled File Functions are Audited
- Spooled File in Output Queue
- Storage Usage by User Profile
- Strong System Security Level
- Subsystem Autostart Details
- Subsystem Communication Details
- Subsystem Information Details
- Subsystem Job Queue Details
- Subsystem Pool Data Details
- Subsystem Prestart Job Details
- Subsystem Remote Entries
- Subsystem Routing Entries
- Subsystem Routing Entry Changes
- Subsystem Workstation Names
- Subsystem Workstation Types
- Superseded PTFs
- System, User, and Object Auditing Control Configuration
- System Management Tasks are Audited
- System Software Resources
- System Value Changes
- System Value Configuration Changes
- System Value Configuration Details
- System Value Default Changes

- System Value Defaults
- System Value Valid Value Changes
- System Value Valid Values
- Systems Management Changes
- Time Adjustment Software Installed
- User Profile Changes
- User Profile Information

**See also**

TGAudit Report Reference Introduction

# Access Control List Changes

This report displays changes to Access Control Lists. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is VA.

**Collector ID**: JOURNAL_VA

**Report ID**: *BASE

> **Tip**: For VA journal entries to be generated, the QAUDLVL system value must contain *SECCFG and *SECURITY.

PASS = VA journal entries were not found in QAUDJRN.

FAIL = VA journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **21** (Access Control List Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Actions that Affect a Job are Audited

This report displays the values of the QAUDLVL (Auditing level) or QAUDLVL2 (Auditing level extension) system value if *JOBDTA is specified.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDLVL_JOBDTA

PASS = Value *JOBDTA is specified in the QAUDLVL or QAUDLVL2 system value.

FAIL = Value * JOBDTA is not specified in QAUDLVL or QAUDLVL2 system value.

Actions that affect a job are audited. (*JOBDTA) The following are some examples:

- Job start and stop data
- Hold, release, stop, continue, change, disconnect, end, end abnormal, PSR-attached to prestart job entries
- Changing a thread's active user profile or group profiles

> **Note**: *JOBDTA is composed of two values to allow you to better customize your auditing. If you specify both of the values, you will get the same auditing as if you specified *JOBDTA. The following values make up *JOBDTA.

*JOBBAS

*JOBCHGUSR

When you have this value set, the following security audit journal entry types are generated:

JS – A change was made to job data

SG – Asynchronous signals

VC – Connection started or ended

VN – A logon or logoff operation on the network

VS – A server session started or ended

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **2** (Actions that Affect a Job are Audited).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Active Job Information

This report displays a list of active jobs.

**Collector ID**: QSYS2.ACTIVE_JOB_INFO

**Report ID:** QSYS2_ACTIVE_JOB_INFO

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Adopting Authority from a Program Owner is Audited

This report displays the values of the QAUDLVL (Auditing level) or QAUDLVL2 (Auditing level extension) system value if *PGMADP is specified.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDLVL_PGMADP

PASS = Value *PGMADP is specified in the QAUDLVL or QAUDLVL2 system value.

FAIL = Value *PGMADP is not specified in QAUDLVL or QAUDLVL2 system value.

Adopting authority from a program owner is audited. (*PGMADP)

When you have this value set, the following security audit journal entry types are generated:

AP – A change was made to program adopt

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **3** (Adopting Authority from a Program Owner is Audited).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# All Deletions of External Objects on the System are Audited

This report displays the values of the QAUDLVL (Auditing level) or QAUDLVL2 (Auditing level extension) system value if *DELETE is specified.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDLVL_DELETE

PASS = Value *DELETE is specified in the QAUDLVL or QAUDLVL2 system value.

FAIL = Value * DELETE is not specified in QAUDLVL or QAUDLVL2 system value.

> **Tip**: All deletions of external objects on the system are audited. (*DELETE) Objects deleted from library QTEMP are not audited.

When you have this value set, the following security audit journal entry types are generated:

DO – Object deleted. Pending delete committed. Pending create rolled back. Delete pending. Pending delete rolled back.

DI – Object deleted.

XD – Group names (associated with DI entry)

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **4** (All Deletions of External Objects on the System are Audited).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# All Object Creations are Audited

This report displays the values of the QAUDLVL (Auditing level) or QAUDLVL2 (Auditing level extension) system value if *CREATE is specified.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDLVL_CREATE

PASS = Value *CREATE is specified in the QAUDLVL or QAUDLVL2 system value.

FAIL = Value *CREATE is not specified in QAUDLVL or QAUDLVL2 system value.

All object creations are audited. (*CREATE) Objects created in library QTEMP are not audited. The following are some examples:

- Newly-created objects
- Objects created to replace an existing object

When you have this value set, the following security audit journal entry types are generated:

CO - Creation of a new object, except creation of objects in QTEMP library.

DI - Object created.

XD - Group names (associated with DI entry)

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **5** (All Object Creations are Audited).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

**Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# All Optical Functions are Audited

This report displays the values of the QAUDLVL (Auditing level) or QAUDLVL2 (Auditing level extension) system value if *OPTICAL is specified.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDLVL_OPTICAL

PASS = Value *OPTICAL is specified in the QAUDLVL or QAUDLVL2 system value.

FAIL = Value * OPTICAL is not specified in QAUDLVL or QAUDLVL2 system value.

All optical functions are audited. (*OPTICAL) The following are some examples:

- Add or remove optical cartridge
- Change the authorization list used to secure an optical volume
- Open optical file or directory
- Create or delete optical directory
- Change or retrieve optical directory attributes
- Copy, move, or rename optical file
- Copy optical directory
- Back up optical volume
- Initialize or rename optical volume
- Convert backup optical volume to a primary volume
- Save or release held optical file
- Absolute read of an optical volume

When you have this value set, the following security audit journal entry types are generated:

O1 - Single optical object access

O2- Dual optical object access

O3- Optical volume access

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **6** (All Optical Functions are Audited).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface..

**See also**

Configuration Management Reports

# All Security Functions are Audited

This report displays the values of the QAUDLVL (Auditing level) or QAUDLVL2 (Auditing level extension) system value if *SECURITY is specified.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDLVL_SECURITY

PASS = Value *SECURITY is specified in the QAUDLVL or QAUDLVL2 system value.

FAIL = Value *SECURITY is not specified in QAUDLVL or QAUDLVL2 system value.

> **Note**: *SECURITY is composed of several values to allow you to better customize your auditing. If you specify all of the values, you will get the same auditing as if you specified *SECURITY. The following values make up *SECURITY.
>
> - *SECCFG
> - *SECDIRSRV
> - *SECIPC
> - *SECNAS
> - *SECRUN
> - *SECSCKD
> - *SECVFY
> - *SECVLDL

All security-related functions are audited (*SECURITY).

- Security configuration
- Changes or updates when doing directory service functions
- Changes to inter-process communications
- Network authentication service actions
- Security run time functions
- Socket descriptor
- Use of verification functions
- Changes to validation list objects

When you have this value set, the following security audit journal entry types are generated:

AD - A change was made to the auditing attribute

X1- Identity token

AU - Attribute change

CA - Changes to object authority (authorization list or object)

CP - Create, change, and restore user profiles

CV - Connection verification

CY - Cryptographic configuration

DI - Directory services

DS - DST security officer password reset

EV - Environment variable

GR - General purpose audit record

GS - A descriptor was given

IP - Inter-process communication event

JD - Changes to the USER parameter of a job description

KF - Key ring file name

NA - Changes to network attributes

OW - Changes to object ownership

PA - Changes to programs (CHGPGM) that will now adopt the owner's authority

PG - Changes to an object's primary group

PS - Profile swap

SE - Changes to subsystem routing

SO - A change was made by server security

SV - Changes to system values

VA - Changes to access control list

VO - Actions on validation lists

VU - A network profile was changed

X0 - Network authentication

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **7** (All Security Functions are Audited).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Alternate Subsystem Configurations

This report returns information about the users who have alternate subsystem configurations for some IBM i servers. When a user profile listed in this view attempts to use TCP/IP to form a connection to the server, an attempt is made to use the alternate subsystem instead of the default subsystem for that server.

**Collector ID**: QSYS2.SERVER_SBS_ROUTING

**Report ID**: QSYS2_SERVER_SBS_ROUTING

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Attention Events are Audited

This report displays the values of the QAUDLVL (Auditing level) or QAUDLVL2 (Auditing level extension) system value if *ATNEVT is specified.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDLVL_ATNEVT

PASS = Value *ATNEVT is specified in the QAUDLVL or QAUDLVL2 system value.

FAIL = Value *ATNEVT is not specified in QAUDLVL or QAUDLVL2 system value.

> **Tip**: Attention events are audited. (*ATNEVT)  Attention events are conditions that require further evaluation to determine the condition's security significance.

The following is an example: Intrusion monitor events need to be examined to determine whether the condition is an intrusion or a false positive

When you have this value set, it generates security audit journal entries of type IM in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **8** (Attention Events are Audited).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Auditing End Action set to Power Down System

This report displays the value of the QAUDENDACN (Auditing End Action) system value if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDENDACN

PASS = System value QRETSVRSEC is set to *PWRDWNSYS

FAIL = System value QRETSVRSEC is set to *NOTIFY.

The Auditing End Action system value specifies the action that should be taken by the system when audit records cannot be sent to the auditing journal because of errors that occur when the journal entry is sent.

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Authority Changes to Restored Objects

This report displays authority changes to restored objects. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is RA.

**Collector ID**: JOURNAL_RA

**Report ID**: *BASE

> **Tip**: For RA journal entries to be generated, the QAUDLVL system value must contain *SAVRST. Also, object auditing on the object must be set to *CHANGE. To set object auditing, use the CHGOBJAUD command.

PASS = RA journal entries were not found in QAUDJRN.

FAIL = RA journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **10** (Authority Changes to Restored Objects).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Authorization Failures are Audited

This report displays the values of the QAUDLVL (Auditing level) or QAUDLVL2 (Auditing level extension) system value if *AUTFAIL is specified.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDLVL_AUTFAIL

PASS = Value *AUTFAIL is specified in the QAUDLVL or QAUDLVL2 system value.

FAIL = Value *AUTFAIL is not specified in QAUDLVL or QAUDLVL2 system value.

Authorization failures are audited (*AUTFAIL). The following are some examples:

- All access failures (sign-on, authorization, job submission)
- Incorrect password or user ID entered from a device

When you have this value set, the following security audit journal entry types are generated:

AF - All Authority Failures

CV - Connection verification - Connection ended abnormally.

DI - Directory services - Authority failures. Password failures.

GR - General purpose audit record - Function registration operations.

KF - Key ring file name - An incorrect password was entered.

IP - Inter-process communication event - Authority failure for an IPC request.

PW - Passwords used that are not valid.

VC - A connection was rejected because of an incorrect password.

VO - Unsuccessful verification of a validation list entry.

VN - A network logon was rejected because of expired account, incorrect hours, incorrect user ID, or incorrect password.

VP - An incorrect network password was used.

X1 - Delegate of identity token failed, Get user from identity token failed, Get user from identity token failed.

XD - Group names (associated with DI entry).

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **9** (Authorization Failures are Audited).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Authorization List or Object Authority Changes

This report displays changes to object authorities. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is CA.

**Collector ID**: JOURNAL_CA

**Report ID**: *BASE

> **Tip**: For CA journal entries to be generated, the QAUDLVL system value must contain *SECRUN and *SECURITY.

PASS = CA journal entries were not found in QAUDJRN.

FAIL = CA journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **4** (Authorization List or Object Authority Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Basic Product Information on the System

This report displays product information.

**Collector ID**: PRODUCT_INFO

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **8** (Product Information Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **3** (Basic Product Information on the System).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Certificate Details

This report displays the details of your security certificates.

**Collector ID**: KEYSTORE_DATA

**Report ID**: CERTIFICATE_DETAILS

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **10** (Keystore Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **1** (Certificate Details).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Certificates Expired

This report displays expired security certificates.

**Collector ID**: KEYSTORE_DATA

**Report ID**: CERTIFICATE_EXPIRED

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **10** (Keystore Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **2** (Certificates Expired).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Certificates Expiring in 90 Days

This report displays security certificates that will expire in 90 days.

**Collector ID**: KEYSTORE_DATA

**Report ID**:  CERTIFICATE_EXP90

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **10** (Keystore Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **3** (Certificates Expiring in 90 Days).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Change Request Descriptor Changes

This report displays changes made to Change Requestor Descriptors. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is CQ.

**Collector ID**: JOURNAL_CQ

**Report ID**: *BASE

> **Tip**: For CQ journal entries to be generated, the QAUDLVL system value must contain *SECCFG and *SECURITY.

PASS = CQ journal entries were not found in QAUDJRN.

FAIL = CQ journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **5** (Change Request Descriptor Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Columns with Field Procedures

This report displays the characteristics of columns and fields within a database table.

**Collector ID**: ACCESS_ESCAL_ACC_CONTROL

**Report ID**: SYSFIELDS

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Cryptographic Configuration Changes

This report displays changes to cryptographic configuration. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is CY.

**Collector ID**: JOURNAL_CY

**Report ID**: *BASE

> **Tip**: For CY journal entries to be generated, the QAUDLVL system value must contain *SECCFG and *SECURITY.

PASS = CY journal entries were not found in QAUDJRN.

FAIL = CY journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **6** (Cryptographic Configuration Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Current Cumulative PTF Level

This report displays the current Cumulative PTF level for the operating system. Cumulative PTF ID's begin with "TC" and are followed by a numerical value.  The highest numerical value represents the most recently installed Cumulative PTF.

Keeping current with Cumulative PTF packages is a very important part of maintaining your operating system and limiting exposure to vulnerabilities.

**Collector ID**:  PTF_DATA

**Report ID**: PTF_TO_GET_CUMULATIVE

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **8** (PTF Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **4** (Current Cumulative PTF Level).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Current Job's Reply List Entry Information

This report displays the list of current jobs and the associated entry information.

**Collector ID**: QSYS2.REPLY_LIST_INFO

**Report ID**: QSYS2_REPLY_LIST_INFO

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Dependencies of Row Permissions and Column Masks

This report displays the dependencies of row permissions and column masks.

**Collector ID**: QSYS2.SYSCONTROLSDEP

**Report ID**: QSYS2_SYSCONTROLSDEP

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Disk Information

This report displays information about the disk.

**Collector ID**: QSYS2.SYSDISKSTAT

**Report ID**: QSYS2_SYSDISKSTAT

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# DRDA and DDM User Access

This report displays DRDA and DDM User access.

**Collector ID**: QSYS2.DRDA_AUTHENTICATION

**Report ID**: QSYS2_DRDA_AUTHENTICATION

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# EIM Attribute Changes

This report displays Enterprise Identity Mapping (EIM) configuration attribute changes. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is AU.

**Collector ID**: JOURNAL_AU

**Report ID**: *BASE

> **Tip**: For AU journal entries to be generated, the QAUDLVL system value must contain *SECCFG and *SECURITY.

PASS = AU journal entries were not found in QAUDJRN.

FAIL = AU journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **3** (EIM Attribute Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Environment Variable Changes

This report displays changes to Environment Variables. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is EV.

**Collector ID**: JOURNAL_EV

**Report ID**: *BASE

> **Tip**: For EV journal entries to be generated, the QAUDLVL system value must contain *SECCFG and *SECURITY.

PASS = EV journal entries were not found in QAUDJRN.

FAIL = EV journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **7** (Environment Variable Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Exit Point Information

This report displays lists of registration information. The data returned can also be obtained by running the WRKREGINF CL command and by the Retrieve Exit Information (QUSRTVEI, QusRetrieveExitInformation) API.

**Collector ID**: QSYS2.EXIT_POINT_INFO

**Report ID**: EXIT_POINT_INFO

> **Note**: See the IBM documentation for additional information: https://www.ibm.com/support/pages/ibm-i-74-tr3-enhancements

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Exit Program Information

This report displays the lists exit program details. The data returned can also be obtained by running the WRKREGINF CL command and by the Retrieve Exit Information (QUSRTVEI, QusRetrieveExitInformation) API.

**Collector ID**: QSYS2.EXIT_PROGRAM_INFO

**Report ID**: EXIT_PROGRAM_INFO

> **Note**: See the IBM documentation for additional information: https://www.ibm.com/support/pages/ibm-i-74-tr3-enhancements

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Function Usage Configuration Details

This report displays function usage configuration details.  The detail returned corresponds to the data returned by the Retrieve Function Usage Information (QSYRTFUI, QsyRetrieveFunctionUsageInfo) API.

**Collector ID**:  QSYS2.FUNCTION_USAGE

**Report ID**: QSYS2_FUNCTION_USAGE

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Function Usage Identifiers

This report displays details about function usage identifiers.

**Collector ID**: QSYS2.FUNCTION_INFO

**Report ID**: QSYS2_FUNCTION_INFO

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Group PTFs Information

This report displays information about the group PTFs for the server.

**Collector ID**: QSYS2.GROUP_PTF_INFO

**Report ID**: QSYS2_GROUP_PTF_INFO

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# IBM i Temporary Storage Pool Detail

This report displays the IBM i temporary storage pool detail.

**Collector ID**: QSYS2.SYSTMPSTG

**Report ID**: QSYS2_GROUP_PTF_INFO

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# IPv4 and IPv6 Network Connection Details

This report displays IPv4 and IPv6 connection details.

**Collector ID**: QSYS2.NETSTAT_JOB_INFO

**Report ID**: QSYS2_NETSTAT_JOB_INFO

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Installed Products

This report displays information for all products currently installed on the system. All product options for each Product ID are included.

**Collector ID**: PRODUCT_INFO

**Report ID**: Installed_Products

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **8** (Product Information Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **4** (Installed Products).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Job Description Details

This report displays all job descriptions on the system, as well as configuration information about each.

**Collector ID**: JOB_DESCSRIPTIONS

**Report ID**: JOB_DESCRIPTION_DETAILS

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **5** (Job Description Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **1** (Job Description Details).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Job Descriptions that Contain User Profile Names were Restored

This report displays job descriptions restored that had a user profile name in the USER parameter. The data related to this report is retrieved from the system security audit journal (QAUDJRN.  The journal entry type associated with this event is RJ.

**Collector ID**: JOURNAL_RJ

**Report ID**: *BASE

> **Tip**: For RJ journal entries to be generated, the QAUDLVL system value must contain *SAVRST.

PASS = RJ journal entries were not found in QAUDJRN.

FAIL = RJ journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **11** (Job Descriptions that Contain User Profile Names were Restored).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Job Descriptions – USER Parameter Changes

This report displays changes to the USER parameter of Job Descriptions. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is JD.

**Collector ID**: JOURNAL_JD

**Report ID**: *BASE

> **Tip**: For JD journal entries to be generated, the QAUDLVL system value must contain *SECCFG and *SECURITY.

PASS = JD journal entries were not found in QAUDJRN.

FAIL = JD journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Job Descriptions with Logging

This report displays information about job descriptions on the system that have logging defined as anything other than 0, 99, *NOLIST, *NO.

**Collector ID**: JOB_DESCSRIPTIONS

**Report ID**: JOB_DESCRIPTION_LOGGING

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **5** (Job Description Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **2** (Job Descriptions with Logging).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Job Descriptions with Request Data

This report displays information about job descriptions on the system that have Request Data values defined.

**Collector ID**: JOB_DESCSRIPTIONS

**Report ID**: JOB_DESCRIPTIONS_REQUEST_DATA

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **5** (Job Description Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **4** (Job Descriptions with Request Data).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Job Descriptions with Specific Initial Library Lists

This report displays information about job descriptions on the system that have initial library lists defined as anything other than *SYSVAL.

**Collector ID**: JOB_DESCSRIPTIONS

**Report ID**:  JOB_DESCRIPTIONS_LIBL

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **5** (Job Description Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **3** (Job Descriptions with Specific Initial Library List).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Job Schedule Entry Information

This report displays information that can also be seen through the Work with Job Schedule Entries (WRKJOBSCDE) command interface. Each job schedule entry contains the information to automatically submit a batch job once or at regularly scheduled intervals.

**Collector ID**: QSYS2.SCHEDULED_JOB_INFO

**Report ID**: QSYS2_SCHEDULED_JOB_INFO

### To run this report

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

### See also

Configuration Management Reports

# Journal and Remote Journal Information

This report displays information about journals, including remote journals. The values returned for the columns in the view are closely related to the values returned by the QjoRetrieveJournalInformation() API. Refer to the API for more detailed information.

**Collector ID**: QSYS2.JOURNAL_INFO

**Report ID**: QSYS2_JOURNAL_INFO

### To run this report

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

### See also

Configuration Management Reports

# Key Ring File Changes

This report displays changes to Key Ring Files which store certificates. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is KF.

**Collector ID**: JOURNAL_KF

**Report ID**: *BASE

> **Tip**: For KF journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL, *SECCFG, and *SECURITY.

PASS = KF journal entries were not found in QAUDJRN.

FAIL = KF journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **9** (Key Ring File Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Limit Device Sessions Not Enabled

This report displays the value of the QLMTDEVSSN (Limit Device Sessions) system value if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QLMTDEVSSN

> **Tip**: The Limit Device Sessions system value controls the number of device sessions a user can sign on. This does not prevent the user from using group jobs or making a system request (pressing the System Request key) at the same workstation.

PASS = System value QLMTDEVSSN is set to 1 - 9.

FAIL = System value QLMTDEVSSN is set to 0.

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Line Description Details

This report displays configuration information about line descriptions available on the system.  Line description configuration is crucial for ensuring system communications are available.

**Collector ID**: LINE_DESCRIPTION_DATA

**Report ID**: LINE_DESCRIPTION_DETAILS

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Network Settings Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **10** (Line Description Details).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Media Library Status Details

This report displays information that can also be seen through the Work with Media Library Status (WRKMLBSTS) command interface.

**Collector ID**: QSYS2.MEDIA_LIBRARY_INFO

**Report ID**: QSYS2_MEDIA_LIBRARY_INFO

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Memory Pool Details

This report displays one row for every pool.

**Collector ID**: QSYS2.MEMORY_POOL

**Report ID**: QSYS2_MEMORY_POOL

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Message Queue Data by Date Range

This report shows messages for a date range.

**Collector ID**: QSYS2.MESSAGE_QUEUE_INFO

**Report ID**: MESSAGE_QUEUE_DATA

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **4** (Message Queue Report).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **7** (Message Queue Data by Time Range).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Message Queue Data for All Queues

This report displays all messages in all message queues on the system.  If you need message data for a particular user or a particular message ID or severity, this is a good report to copy and edit to suit the needs of your search.

**Collector ID**: MESSAGE_QUEUE_DATA

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **4** (Message Queue Report).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **2** (Message Queue Data for All Queues).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Message Queue Data QSYSOPR

This report shows all messages in the QSYSOPR system operator message queue.  Important messages regarding the operations of the overall system are sent to this message queue and should monitored frequently to ensure system operations are not interrupted and important system functions are operating normally.

**Collector ID**: MESSAGE_QUEUE_DATA

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **4** (Message Queue Report).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **1** (Message Queue Data QSYSOPR).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Message Queue Data Severity Greater than 30

This report shows messages that have a severity of 30 or higher.  Messages with a severity of 30 or higher indicate errors that have occurred on the system and should be monitored to ensure significant issues do not exist and disrupt system operations.

**Collector ID**: MESSAGE_QUEUE_DATA

**Report ID**: MESSAGE_QUEUE_DATA_SEV_30

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **4** (Message Queue Report).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **3** (Message Queue Data Severity Greater than 30).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Message Queue Details

This report contains general information about message queues defined on the system, such as the number of messages in each queue, the message delivery type, break handling programs, storage information, etc.

**Collector ID**: MESSAGE_QUEUE

**Report ID**: MESSAGE_QUEUE

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **4** (Message Queue Report).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **4** (Message Queue Details).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Networking and Communications Functions are Audited

This report displays the values of the QAUDLVL (Auditing level) or QAUDLVL2 (Auditing level extension) system value if *NETCMN is specified.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDLVL_NETCMN

PASS = Value *NETCMN is specified in the QAUDLVL or QAUDLVL2 system value.

FAIL = Value * NETCMN is not specified in QAUDLVL or QAUDLVL2 system value.

> **Note**: *NETCMN is composed of several values to allow you to better customize your auditing. If you specify all of the values, you will get the same auditing as if you specified *NETCMN. The following values make up *NETCMN.
>
> - *NETBAS
> - *NETCLU
> - *NETFAIL
> - *NETSCK

Networking and communications functions are audited (*NETCMN). The following are some examples:

- Network base functions (See *NETBAS)
- Cluster or cluster resource group operations (See *NETCLU)
- Network failures (See *NETFAIL)
- Sockets functions (See *NETSCK)

When you have this value set, the following security audit journal entry types are generated:

CU - Creation of an object by the cluster control operation.

CV - Connection established. Connection ended normally.

IR - IP rules have been loaded from a file.

IS - Internet security management

ND - Directory search violations

NE - End point violations

SK - Secure sockets connection

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **12** (Networking and Communications Functions are Audited).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Object Auditing Attribute Changes

This report displays changes made to auditing attributes of objects. The data on this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is AD.

**Collector ID**: JOURNAL_AD

**Report ID**: *BASE

> **Tip**: For AD journal entries to be generated, the QAUDLVL system value must contain values *SECCFG and *SECURITY. Also, object auditing on the object must be set to *CHANGE. To set object auditing, use the CHGOBJAUD command.

PASS = AD journal entries were not found in QAUDJRN.

FAIL = AD journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **1** (Object Auditing Attribute Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Object Lock Information

This report displays one row for every lock held for every object on the partition.

**Collector ID**: QSYS2.OBJECT_LOCK_INFO

**Report ID**: QSYS2_OBJECT_LOCK_INFO

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Object Management Tasks are Audited

This report displays the values of the QAUDLVL (Auditing level) or QAUDLVL2 (Auditing level extension) system value if *OBJMGT is specified.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDLVL_OBJMGT

PASS = Value *OBJMGT is specified in the QAUDLVL or QAUDLVL2 system value.

FAIL = Value * OBJMGT is not specified in QAUDLVL or QAUDLVL2 system value.

Generic object tasks are audited (*OBJMGT). The following are some examples:

- Moves of objects
- Renames of objects

When you have this value set, the following security audit journal entry types are generated:

DI - Object rename

OM - An object was moved to a different library

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **11** (Object Management Tasks are Audited).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# OfficeVision Tasks are Audited

This report displays the values of the QAUDLVL (Auditing level) or QAUDLVL2 (Auditing level extension) system value if *OFCSRV is specified.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDLVL_OFCSRV

PASS = Value *OFCSRV is specified in the QAUDLVL or QAUDLVL2 system value.

FAIL = Value * OFCSRV is not specified in QAUDLVL or QAUDLVL2 system value.

OfficeVision tasks are audited (*OFCSRV). The following are some examples:

- Changes to the system distribution directory
- Tasks involving electronic mail

When you have this value set, the following security audit journal entry types are generated:

ML - A mail log was opened.

SD - A change was made to the system distribution directory.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **13** (OfficeVision Tasks are Audited).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Operating System Product Info

This report displays information related to the current version of the Operating System (OS) installed.  Several product options are typically associated with the OS licensed product.

**Collector ID**: SOFTWARE_RESOURCES

**Report ID**: OS400_Product_Installed

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **8** (Product Information Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **2** (Operating System Product Info).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Output Queue Details

This report displays all output queues on the system, as well as configuration information about each.

**Collector ID**: OUTPUT_QUEUE

**Report ID**: OUTPUT_QUEUE_DETAILS

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Output Queue Details).
7) Press **Enter**.
8) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

9) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Ownership Changes for Restored Objects

This report displays ownership changes to objects during restore operations. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is RO.

**Collector ID**: JOURNAL_RO

**Report ID**: *BASE

> **Tip**: For RO journal entries to be generated, the QAUDLVL system value must contain *SAVRST. Also, object auditing on the object must be set to *CHANGE. To set object auditing, use the CHGOBJAUD command.

PASS = RO journal entries were not found in QAUDJRN.

FAIL = RO journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **12** (Ownership Changes for Restored Objects).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Partition Information

This report displays a single row containing details about the current partition.

**Collector ID**: QSYS2.SYSTEM_STATUS_INFO

**Report ID**: QSYS2_SYSTEM_STATUS_INFO

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Permission or Column Mask Defined

This report displays one row for each row permission or column mask defined by the CREATE PERMISSION or CREATE MASK statements.

**Collector ID**: QSYS2.SYSCONTROLS

**Report ID**: QSYS2_SYSCONTROLS

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Primary Group Changes for Restored Objects

This report displays changes to Primary Groups for objects during restore operations. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is RZ.

**Collector ID**: JOURNAL_RZ

**Report ID**: *BASE

> **Tip**: For RZ journal entries to be generated, the QAUDLVL system value must contain *SAVRST. Also, object auditing on the object must be set to *CHANGE. To set object auditing, use the CHGOBJAUD command.

PASS = RZ journal entries were not found in QAUDJRN.

FAIL = RZ journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **15** (Primary Group Changes for Restored Objects).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Printing Functions are Audited

This report displays the values of the QAUDLVL (Auditing level) or QAUDLVL2 (Auditing level extension) system value if *PRTDTA is specified.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QSYS2_SYSCONTROLS

PASS = Value *PRTDTA is specified in the QAUDLVL or QAUDLVL2 system value.

FAIL = Value *PRTDTA is not specified in QAUDLVL or QAUDLVL2 system value.

Printing functions are audited (*PRTDTA). The following are some examples:

- Printing a spooled file
- Printing with parameter SPOOL(*NO)

When you have this value set, the following security audit journal entry types are generated:

PO - A change was made to printed output

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **14** (Printing Functions are Audited).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

# Product Information on the System

This report displays all the software license product information available on the system. Information is shown for products that are installed as well as for products that are not installed.

**Collector ID**: PRODUCT_INFO

**Report ID**: PRODUCT_INFORMATION

The list of products displayed can be in the following Load States:

- All installed products.
- All supported products.
- All defined products.
- A user-specified subset of all defined products.
- All products that are supported, installed, or both installed and supported.

> **Note**: A product can be supported and unsupported by using the Work with Supported Products (WRKSPTPRD) command. This command is part of the System Manager for i5/OS® licensed program.

A defined product is one which is known to the system. This includes all installed products, but also includes products which are known to the system without the products being installed. For example, V5R4M0 of the System Manager for i5/OS licensed program (5722SM1) is known to the system once V5R4M0 of the operating system is installed. Therefore V5R4M0 of 5722SM1 is a defined product once V5R4M0 of the operating system is installed.

A product is also a defined product when a product definition (*PRDDFN) object exists for that product on the system.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **8** (Product Information Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **3** (Basic Product Information on the System).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Product Registration ID Information

This report displays Registration ID information for licensed products. A combination of the registration type and registration value makes up the Registration ID for a product.

**Collector ID**: PRODUCT_INFO

**Report ID**: PRODUCT_REGISTRATION

The registration type associated with the product could have the following values:

| | |
|---|---|
| *02* | Registration type *PHONE was specified when the product load or product definition was created. |
| *04* | The registration value is the same as the registration value for i5/OS®. |
| *08* | Registration type *CUSTOMER was specified when the product load or product definition was created. |

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **8** (Product Information Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **6** (Product Registration ID Information).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Products License Information

This report displays information about all products or features that contain license information.

**Collector ID**: QSYS2.LICENSE_INFO

**Report ID**: QSYS2_LICENSE_INFO

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Products with Load Errors

This report displays products with Load Errors. Data on this report is determined by the Check Product Option (CHKPRDOPT) command.

A Load Error can be caused by a restore, delete, or save licensed program function that might be in progress or might not have completed. The product may need to be reloaded to rectify the issue.

**Collector ID**: PRODUCT_INFO

**Report ID**: PRODUCT_WITH_LOAD_ERRORS

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **8** (Product Information Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **5** (Products with Load Errors).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Program Changes to Adopt Owner Authority

This report displays the program adopt details. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is PA.

**Collector ID**: JOURNAL_PA

**Report ID**: *BASE

> **Tip**: For PA journal entries to be generated, the QAUDLVL system value must contain *SECCFG and *SECURITY.

PASS = PA journal entries were not found in QAUDJRN.

FAIL = PA journal entries were found in QAUDJRN.

**Types of entries:**

A - Change program to adopt owner's authority.

J - Java program adopts owner's authority.

M - Change object's SETUID, SETGID, or Restricted rename and unlink mode indicator.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **13** (Program Changes to Adopt Owner Authority).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

## Configuration Management Report

# Program Failures are Audited

This report displays the values of the QAUDLVL (Auditing level) or QAUDLVL2 (Auditing level extension) system value if *PGMFAIL is specified.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDLVL_PGMFAIL

PASS = Value *PGMFAIL is specified in the QAUDLVL or QAUDLVL2 system value.

FAIL = Value *PGMFAIL is not specified in QAUDLVL or QAUDLVL2 system value.

Program failures are audited (*PGMFAIL). The following are some examples:

- Blocked instruction
- Validation value failure
- Domain violation

When you have this value set, the following security audit journal entry types are generated:

AF - All authority failures

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **15** (Program Failures are Audited).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Programs Restored that Adopt Owner Authority

This report displays restored programs that inherit the owner's authority. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is RO.

**Collector ID**: JOURNAL_RP

**Report ID**: *BASE

> **Tip**: For RP journal entries to be generated, the QAUDLVL system value must contain *SAVRST.

PASS = RP journal entries were not found in QAUDJRN.

FAIL = RP journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **13** (Programs Restored that Adopt Owner Authority).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Programs that Adopt Authority were Executed

This report displays program executions where the programs inherited the authority of the program user or program owner. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is AP.

**Collector ID**: JOURNAL_AP

**Report ID**: *BASE

> **Tip**: For AP journal entries to be generated, the QAUDLVL system value must contain *PGMADP.

PASS = AP journal entries were not found in QAUDJRN.

FAIL = AP journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **2** (Programs that Adopt Authority were Executed).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# PTF Status for all Products

This report displays the Program Temporary Fix (PTF) status and related information for all licensed products installed on the system.

**Collector ID**: PTF_DATA

**Report ID**: DISPLAY_PTF_STATUS

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **8** (PTF Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **1** (PTF Status for all Products).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# PTFs Applied to the Licensed Internal Code

This report displays PTFs which have been applied to the Licensed Internal Code (LIC). The data displayed in this report is based on the Product ID ending with 999 and having a PTF status of permanently or temporarily applied.

The LIC Product ID changes based on OS version.  For example, the LIC Product ID for V6R1 is 5761999 and, for V7R1, it is 5770999.

**Collector ID**: PTF_DATA

**Report ID**: LIC_PTFS

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **8** (PTF Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **3** (PTFs Applied to the Licensed Internal Code).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# PTFs for WDS

This report displays PTFs that are installed on the system for WebSphere Development Studio (WDS).

**Collector ID**: PTF_DATA

**Report ID**: WEBSPHERE_DEV_S_PTF

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **8** (PTF Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **7** (PTFs for WDS).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# PTFs Requiring IPL

This report displays PTFs waiting for the next IPL in order to be applied. Fixes within these PTFs are not implemented until the next IPL is complete.

**Collector ID**: PTF_DATA

**Report ID**: PTF_WAITING_FOR_IPL

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **8** (PTF Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **5** (PTFs Requiring IPL).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# PTFs that are Loaded but not Applied

This report displays Program Temporary Fixes (PTFs) that are loaded on the system but have not been applied. The status of these PTFs is "Not Applied."

On the IBM i, to complete the installation of a PTF for a licensed product, two steps must be performed – loading the PTF, and applying the PTF.  If the PTF remains in a load state and is never applied, then the fix contained in it is not installed and may result in potential vulnerabilities on the system.

**Collector ID**: PTF_DATA

**Report ID**: LOADED_PTFS

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **8** (PTF Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **2** (PTFs that are Loaded but not Applied).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Record Lock Information

This report displays one row for every record lock for the partition.

**Collector ID**: QSYS2.RECORD_LOCK_INFO

**Report ID**: QSYS2_RECORD_LOCK_INFO

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Restrict Use of Use Adopted Authority

This report displays the value of the QUSEADPAUT (Use Adopted Authority) system value if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QUSEADPAUT

PASS = System value QUSEADPAUT is set to anything other than *NONE.

FAIL = System value QUSEADPAUT is set to *NONE.

The Use Adopted Authority system value defines which users can create programs with the use adopted authority (*USEADPAUT(*YES)) attribute. All users can create, change, or update programs and service programs to use adopted authority if the user has the necessary authority to the program or service program.

This value should be set to an authorization list that contains a list of trusted users who are authorized to create programs that can adopt authority.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **21** (Restricted use of Use Adopted Authority).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# QHST Message Information

This report list the History Log details for a specified date range.

**Collector ID**: QHST_MSG_INFO

**Report ID**: QHST_MSG_INFO

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **4** (Message Queue Report).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **5** (QHST Message Information).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# QHST Messages with Severity Greater Than 40

This report lists the History Log details with Severity of 40 or higher for a specified date range.

**Collector ID**: QHST_MSG_INFO

**Report ID**: QHST_MSG_INFO_40

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **4** (Message Queue Report).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **6** (QHST Messages with Severity Greater than 40).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Save and Restore Information is Audited

This report displays the values of the QAUDLVL (Auditing level) or QAUDLVL2 (Auditing level extension) system value if *SAVRST is specified.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDLVL_SAVRST

PASS = Value *SAVRST is specified in the QAUDLVL or QAUDLVL2 system value.

FAIL = Value *SAVRST is not specified in QAUDLVL or QAUDLVL2 system value.

Save and restore information is audited (*SAVRST). The following are some examples:

- When programs that adopt their owner's user profile are restored
- When job descriptions that contain user names are restored
- When ownership and authority information changes for objects that are restored
- When the authority for user profiles is restored
- When a system state program is restored
- When a system command is restored
- When an object is restored

When you have this value set, the following security audit journal entry types are generated:

OR - Object restored

RA - Restore of objects when authority changes

RJ - Restore of job descriptions that contain user profile names

RO - Restore of objects when ownership information changes

RP - Restore of programs that adopt their owner's authority

RQ - A change request descriptor was restored

RU - Restore of authority for user profiles

RZ - The primary group for an object was changed during a restore operation

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **17** (Save and Restore Information is Audited).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Security Auditing Level

This report displays the security auditing levels.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDLVL

There is no pass/fail criteria associated with this report since it is informational only.

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Security System Values

This report displays the security-related system values and their contents.

**Collector ID**: SYSTEM_VALUES

**Report ID**: SECURITY_SYSTEM_VALUES

> **Note**: There are no pass/fail criteria associated with this report since it is informational only.

## To run this report

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

### Report Column Description

| System Value | Description |
|---|---|
| QALWOBJRST | Allow object restore option |
| QALWUSRDMN | Allow user domain objects in libraries |
| QAUDCTL | Auditing control |
| QAUDENDACN | Auditing end action |
| QAUDFRCLVL | Force auditing data |
| QAUDLVL | Security auditing level |
| QAUDLVL2 | Security auditing level extension |
| QCRTAUT | Create default public authority |
| QCRTOBJAUD | Create object auditing |

| | |
|---|---|
| QDSPSGNINF | Sign-on display information control |
| QFRCCVNRST | Force conversion on restore |
| QINACTITV | Inactive job time-out |
| QINACTMSGQ | Inactive job message queue |
| QLMTDEVSSN | Limit device sessions |
| QLMTSECOFR | Limit security officer device access |
| QMAXSGNACN | Action to take for failed signon attempts |
| QMAXSIGN | Maximum sign-on attempts allowed |
| QPWDCHGBLK | Block password change |
| QPWDEXPITV | Password expiration interval |
| QPWDEXPWRN | Password expiration warning |
| QPWDLMTAJC | Limit adjacent digits in password |
| QPWDLMTCHR | Limit characters in password |
| QPWDLMTREP | Limit repeating characters in password |
| QPWDLVL | Password level |
| QPWDMAXLEN | Maximum password length |
| QPWDMINLEN | Minimum password length |
| QPWDPOSDIF | Limit password character positions |
| QPWDRQDDGT | Require digit in password |
| QPWDRQDDIF | Duplicate password control |
| QPWDRULES | Password rules |
| QPWDVLDPGM | Password validation program |
| QRETSVRSEC | Retain server security data |
| QRMTSIGN | Remote sign-on control |
| QSCANFS | Scan file systems |
| QSCANFSCTL | Scan file systems control |
| QSECURITY | System security level |
| QSHRMEMCTL | Shared memory control |
| QSSLCSL | Secure sockets layer cipher specification list |
| QSSLCSLCTL | Secure sockets layer cipher control |
| QSSLPCL | Secure sockets layer protocols |

| | |
|---|---|
| QUSEADPAUT | Use adopted authority |
| QVFYOBJRST | Verify object on restore |

**See also**

Configuration Management Reports

# Server Security Data is Retained

This report displays the value of the QRETSVRSEC (Retain Server Security Data) system value if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QRETSVRSEC

PASS = System value QRETSVRSEC is set to 1.

FAIL = System value QRETSVRSEC is set to 0.

The Retain Server Security Data system value determines whether the security data needed by a server to authenticate a user on a target system through client-server interfaces can be retained on the host system.

It is recommended to retain server security data by setting this value to 1.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **16** (Server Security Data is Retained).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface..

**See also**

Configuration Management Reports

# Server Security User Information Actions

This report displays actions to Server Security User Information. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is SO.

**Collector ID**: JOURNAL_SO

**Report ID**: *BASE

> **Tip**: For SO journal entries to be generated, the QAUDLVL system value must contain *SECCFG and *SECURITY.

PASS = SO journal entries were not found in QAUDJRN.

FAIL = SO journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **18** (Server Security User Information Actions).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Service Tasks are Audited

This report displays the values of the QAUDLVL (Auditing level) or QAUDLVL2 (Auditing level extension) system value if *SERVICE is specified.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDLVL_SERVICE

PASS = Value *SERVICE is specified in the QAUDLVL or QAUDLVL2 system value.

FAIL = Value *SERVICE is not specified in QAUDLVL or QAUDLVL2 system value.

All service commands are audited. (*SERVICE)

When you have this value set, the following security audit journal entry types are generated:

ST - A change was made by system tools

VV - Service status was changed

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **10** (Service Tasks are Audited).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

## Configuration Management Reports

# Service Tools Actions

This report displays Service Tools actions performed. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is ST.

**Collector ID**: JOURNAL_ST

**Report ID**: *BASE

> **Tip**: For ST journal entries to be generated, the QAUDLVL system value must contain *SERVICE.

PASS = ST journal entries were not found in QAUDJRN.

FAIL = ST journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **18** (Server Security User Information Actions).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Software Product Information

This report displays software product information. You can also obtain this information by running the Display Software Resources (DSPSFWRSC) command and the Retrieve Product Information (QSZRTVPR) API.

**Collector ID**: QSYS2.SOFTWARE_PRODUCT

**Report ID**: SOFTWARE_PRODUCT

> **Note**: See the IBM documentation for additional information: https://www.ibm.com/support/pages/ibm-i-74-tr3-enhancements

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Spooled File Functions are Audited

This report displays the status of spooled file functions.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDLVL_SPLFDTA

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **18** (Spooled File Functions are Audited).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Spooled File in Output Queue

This report displays the values of the QAUDLVL (Auditing level) or QAUDLVL2 (Auditing level extension) system value if *SPLFDTA is specified.

**Collector ID**: QSYS2.OUTPUT_QUEUE_ENTRIES

**Report ID**: QSYS2_OUTPUT_QUEUE_ENTRIES

PASS = Value *SPLFDTA is specified in the QAUDLVL or QAUDLVL2 system value.

FAIL = Value *SPLFDTA is not specified in QAUDLVL or QAUDLVL2 system value.

Spooled file functions are audited. The following are some examples:

- Create, delete, display, copy, hold, and release a spooled file
- Get data from a spooled file (QSPGETSP)
- Change spooled file attributes (CHGSPLFA command)

When you have this value set, the following security audit journal entry types are generated:

SF - A change was made to a spooled output file

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Storage Usage by User Profile

This report displays details about storage by user profile.

**Collector ID**: QSYS2.USER_STORAGE

**Report ID**: QSYS2_USER_STORAGE

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Strong System Security Level

This report displays the value of the QSECURITY (System Security Level) system value if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QSECURITY

PASS = System value QSECURITY is set to 40 or above.

FAIL = System value QSECURITY is less than 40.

The System Security Level system value specifies the level of security on the system.

This value should be set to at least 40.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **20** (Strong System Security Level).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Subsystem Autostart Details

This report displays subsystem description information for autostart job entries.

**Collector ID**: SUBSYSTEM_AUTOSTART

**Report ID**: SUBSYSTEM_AUTOSTART_DETAILS

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **6** (Subsystem Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **2** (Subsystem Autostart Details).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Subsystem Communication Details

This report displays subsystem description information for communication entries.

**Collector ID**: SUBSYSTEM_COMMUNICATIONS

**Report ID**: SUBSYSTEM_COMMUNICATIONS

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **6** (Subsystem Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **3** (Subsystem Communication Details).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Subsystem Information Details

This report displays general subsystem description information.

**Collector ID**: SUBSYSTEM_INFORMATION

**Report ID**: SUBSYSTEM_INFORMATION

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **6** (Subsystem Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **1** (Subsystem Information Details).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Subsystem Job Queue Details

This report displays subsystem description information for job queue entries.

**Collector ID**: SUBSYSTEM_JOB_QUEUE

**Report ID**:  SUBSYSTEM_JOB_QUEUE

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **6** (Subsystem Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **4** (Subsystem Job Queue Details).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Subsystem Pool Data Details

This report displays subsystem description information for pool definitions.

**Collector ID**: SUBSYSTEM_POOL_DATA

**Report ID**: SUBSYSTEM_POOL_DATA

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **6** (Subsystem Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **5** (Subsystem Job Queue Details).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Subsystem Prestart Job Details

This report displays subsystem description information for prestart job entries.

**Collector ID**: SUBSYSTEM_PRESTART

**Report ID**: SUBSYSTEM_PRESTART_JOBS

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **6** (Subsystem Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **8** (Subsystem PreStart Job Details).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Subsystem Remote Entries

This report displays subsystem description information for remote location name entries.

**Collector ID**: SUBSYSTEM_REMOTE

**Report ID**: SUBSYSTEM_REMOTE_ENTRIES

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **6** (Subsystem Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **9** (Subsystem Remote Entries).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Subsystem Routing Entries

This report displays subsystem description information for routing entries.

**Collector ID**: SUBSYSTEM_ROUTING

**Report ID**: SUBSYSTEM_ROUTING_ENTRIES

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **6** (Subsystem Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **10** (Subsystem Routing Entries).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Subsystem Routing Entry Changes

This report displays changes in subsystem routing entries. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is SE.

**Collector ID**: JOURNAL_SE

**Report ID**: *BASE

> **Tip**: For SE journal entries to be generated, the QAUDLVL system value must contain *SECURITY.

PASS = SE journal entries were not found in QAUDJRN.

FAIL = SE journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **16** (Subsystem Routing Entry Change).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Subsystem Workstation Names

This report displays subsystem description information for workstation name entries.

**Collector ID**: SUBSYSTEM_WORKSTATION_NAMES

**Report ID**: SUBSYSTEM_WORKSTATION_NAMES

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **6** (Subsystem Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **6** (Subsystem Workstation Names).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Subsystem Workstation Types

This report displays subsystem description information for workstation type entries.

**Collector ID**: SUBSSTEM_WORKSTATION_TYPES

**Report ID**: SUBSYSTEM_WORKSTATION_TYPES

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **6** (Subsystem Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **7** (Subsystem Workstation Types).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Superseded PTFs

This report displays PTFs on the system that have been superseded by more recent PTFs. Superseding PTFs include the fixes supplied in the superseded PTFs.

**Collector ID**: PTF_DATA

**Report ID**: SUSPERSEDED_PTFS

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **8** (PTF Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **6** (Superseded PTFs).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# System, User, and Object Auditing Control Configuration

This report displays the value of the QAUDCTL (Auditing control) system value if *AUDLVL and *OBJAUD are not specified.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDCTL

PASS = System value QAUDCTL has both *AUDLVL and *OBJAUD specified.

FAIL = System value QAUDCTL does not have both *AUDLVL and *OBJAUD specified.

This system value controls whether or not auditing is performed on the system. If *AUDLVL is specified, then the system auditing configuration in system values QAUDLVL and QAUDLVL2 is activated. If *OBJAUD is specified, then object and user auditing is enabled for configuration done through the Change Object Auditing (CHGOBJAUD) and Change User Auditing (CHGUSRAUD) commands.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **1** (System, User, and Object Auditing Control Configuration).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# System Management Tasks are Audited

This report displays the values of the QAUDLVL (Auditing level) or QAUDLVL2 (Auditing level extension) system value if *SYSMGT is specified.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QAUDLVL_SYSMGT

PASS = Value *SYSMGT is specified in the QAUDLVL or QAUDLVL2 system value.

FAIL = Value *SYSMGT is not specified in QAUDLVL or QAUDLVL2 system value.

System management tasks are audited (*SYSMGT). The following are some examples:

- Hierarchical file system registration
- Changes for Operational Assistant functions
- Changes to the system reply list
- Changes to the DRDA relational database directory
- Network file operations

When you have this value set, the following security audit journal entry types are generated:

DI - Directory services

SM - A change was made by system management

VL - An account limit was exceeded

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **2** (Security Configuration System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **19** (System Management Tasks are Audited).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# System Software Resources

This report displays software resources installed on the system. Any licensed products installed through the IBM installation process will be displayed.

**Collector ID**: SOFTWARE_RESOURCES

**Report ID**: SOFTWARE_RESOURCES_DATA

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **8** (Product Information Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **1** (System Software Resources).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# System Value Changes

This report displays changes made to system values. The data relating to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is SV.

**Collector ID**: JOURNAL_SE

**Report ID**: *BASE

> **Tip**: For SV journal entries to be generated, the QAUDLVL system value must contain *SECCFG and *SECURITY.

PASS = SV journal entries were not found in QAUDJRN.

FAIL = SV journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **20** (System Values Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# System Value Configuration Changes

This report displays changes to the TGSecure System Value Management configuration values.

**Collector ID**: DATABASE_AUDITING

**Report ID**: SYS_VAL_CONFIG

**To run this report**

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **7** (System Value Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (System Value Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (System Value Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (System Value Configuration Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

**Report Column Description**

| Description | |
|---|---|
| Type | Journal entry code for the type of operation:<br><br>**DL** - Record delete<br>**PT** - Record add<br>**PX** - Record added by RRN (a relative record number) to a physical file member<br>**UB** - Record edit (before-change)<br>**UP** - Record edit (after-change) |
| Timestamp | Time at which the remote server attempted communication with the target server |
| Job Name | Name assigned to the job |
| User Name | Name of the user executing the job |
| Job Number | Numbered assigned to the job |
| Program Name | Name of the program used to perform encryption |

| | |
|---|---|
| Program Library | Name of the library in which the program resides |
| Object Name | Name of the object changed |
| Library Name | Name of the library in which the object resides |
| Member Name | Name of member |
| User Profile | Profile name of the user executing the change request |
| System Name | Name of system submitting the change request |
| Remote Address | IP address used to submit the change request |
| Audit Status | Flag indicating whether auditing is enabled<br>**Y** - Auditing is enabled<br>**N** - Auditing is disabled<br><br>**Note**: Auditing must be enabled to capture data for reporting purposes |
| Audit Journal Name | Name of audit journal |
| Audit Journal Library | Library in which audit journal resides |
| Alert Status | Flag indicating whether alerting is enabled:<br>**Y** - Alerting is enabled<br>**N** - Alerting is disabled |
| Alert Message Queue | Queue in which to store triggered alerts |
| Alert Message Queue Library | Library in which the message queue resides |
| Journal Type | Code that identifies the type of journal |

**See also**

System Value Change Reports

# System Value Configuration Details

This report displays the TGSecure System Value Management configuration details.

**Collector ID**: SYS_VAL_CONFIG

**Report ID**: SYS_VAL_CONFIG

## To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **7** (System Value Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (System Value Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (System Value Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (System Value Configuration).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

### Report Column Description

| Column | Description |
|---|---|
| System Value | Name assigned to the system value |
| Category | System value category |
| Description | Description of system value |
| OS Version | OS version installed |
| Field Type | Type of field value allowed (CHAR, DECIMAL) |
| Field Size | Max length of system value entry |
| Value | Value currently assigned to system value |

### See also

System Value Configuration Changes

# System Value Default Changes

This report displays changes to the TGSecure System Value Management default values.

**Collector ID**: DATABASE_AUDITING

**Report ID**: SYS_VAL_DEFAULT

**To run this report**

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **7** (System Value Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (System Value Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (System Value Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (System Value Default Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

**Report Column Description**

| Column | Description |
|---|---|
| Type | Journal entry code for the type of operation:<br><br>**DL** - Record delete<br>**PT** - Record add<br>**PX** - Record added by RRN (a relative record number) to a physical file member<br>**UB** - Record edit (before-change)<br>**UP** - Record edit (after-change) |
| Timestamp | Time at which the remote server attempted communication with the target server |
| Job Name | Name assigned to the job |
| User Name | Name of the user executing the job |
| Job Number | Numbered assigned to the job |
| Program Name | Name of the program used to perform encryption |

| | |
|---|---|
| Program Library | Name of the library in which the program resides |
| Object Name | Name of the object changed |
| Library Name | Name of the library in which the object resides |
| Member Name | Name of member |
| User Profile | Profile name of the user executing the change request |
| System Name | Name of system submitting the change request |
| Remote Address | IP address used to submit the change request |
| Journal Name | Journal in which configuration changes are stored |
| Journal Library | Library in which the journal resides |
| Default Swap | Profile to be used in place of the user profile associated with the transactions |
| Time-out interval | Max amount of time allowed for the remote server to attempt to communicate with the target server |
| Command Execution Entry | Journal entry code for the type of transaction |
| Audit Configuration | Flag indicating whether auditing is enabled for configuration changes:<br>**Y** - Auditing enabled (enable tracking and reporting)<br>**N** - Auditing disabled (disable tracking and reporting) |
| Alert Message Queue | Queue in which alerts are stored |
| Alert Message Queue Library | Library in which the queue resides |

**See also**

System Value Change Reports

# System Value Defaults

This report displays the TGSecure System Value Management configuration default values.

**Collector ID**: SYS_VAL_DEFAULT

**Report ID**: SYS_VAL_DEFAULT

**To run this report**

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **7** (System Value Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (System Value Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (System Value Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (System Value Defaults).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

**Report Column Description**

| Column | Description |
|---|---|
| Audit Journal Name | Name of the journal in which system value transactions are stored<br><br>**Note**: The default journal is **TGJRN** in the library **TGDATA**. |
| Audit Journal Library | Library in which the journal resides |
| Audit Configuration | Flag indicating whether journaling is enabled:<br>**Y** - Journaling is enabled<br>**N** - Journaling is disabled |
| Alert Status | Flag indicating whether alerting is enabled:<br>**Y** - Alerting is enabled<br>**N** - Alerting is disabled |
| Alert Message Queue Name | Name of the message queue<br><br>**Note**: The default alert queue is **TGMSGQ** in the library **TGDATA**. |

| | |
|---|---|
| Alert Message Queue Library | Library in which the alert queue resides |
| Enforcement (Enabled/Disabled) | Flag indicating whether system value rules enforcement is enabled:<br>**Y** - Enable enforcement of system value rules<br>**N** - Disable enforcement of system value rules |

**See also**

System Value Configuration Changes

# System Value Valid Value Changes

This report displays changes to the TGSecure System Value Management valid values.

**Collector ID**: DATABASE_AUDITING

**Report ID**: SYS_VAL_VALID

**To run this report**

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **7** (System Value Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (System Value Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (System Value Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **3** (System Value Valid Value Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

**Report Column Description**

**Report Column Description**

| Column | Description |
|---|---|
| Type | Journal entry code for the type of operation:<br><br>**DL** - Record delete<br>**PT** - Record add<br>**PX** - Record added by RRN (a relative record number) to a physical file member<br>**UB** - Record edit (before-change)<br>**UP** - Record edit (after-change) |
| Timestamp | Time at which the remote server attempted communication with the target server |
| Job Name | Name assigned to the job |
| User Name | Name of the user executing the job |
| Job Number | Numbered assigned to the job |

| | |
|---|---|
| Program Name | Name of the program used to perform encryption |
| Program Library | Name of the library in which the program resides |
| Object Name | Name of the object changed |
| Library Name | Name of the library in which the object resides |
| Member Name | Name of member |
| User Profile | Profile name of the user executing the change request |
| System Name | Name of system submitting the change request |
| Remote Address | IP address used to submit the change request |

**See also**

System Value Change Reports

# System Value Valid Values

This report displays the TGSecure System Value Management configuration valid values (used for validation).

**Collector ID**: SYS_VAL_VALID

**Report ID**: SYS_VAL_VALID

**To run this report**

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **7** (System Value Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (System Value Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (System Value Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (System Value Configuration).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

**Report Column Description**

| Column | Description |
|---|---|
| System Value | Name assigned to the system value |
| System Val Seq | Sequence order (position) |
| System Val Data | Parameter value |
| Data Type | Type of field value allowed (CHAR, DECIMAL) |
| Data Len | Max length of system value entry |
| Data Single (Y /N) | Does the system value consist of single or multiple values?<br><br>**Y** - Single Value<br>**N** - Multiple Value |
| Data Min Val | Minimum value allowed |

| | |
|---|---|
| Data Max Val | Maximum value allowed |
| Error Msg ID | Number assigned to the error produced when the validation criteria defined for the system value are not met |

**See also**

System Value Configuration Changes

# Systems Management Changes

This report displays Systems Management changes. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is SM.

**Collector ID**: JOURNAL_SM

**Report ID**: *BASE

> **Tip**: For SM journal entries to be generated, the QAUDLVL system value must contain *SYSMGT.

PASS = SM journal entries were not found in QAUDJRN.

FAIL = SM journal entries were found in QAUDJRN.

The following are the types of changes:

B - Backup list changed

C - Automatic cleanup options

D - DRDA

F - HFS file system

N - Network file operation

O - Backup options changed

P - Power on/off schedule

S - System reply list

T - Access path recovery times changed

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **17** (Systems Management Changes).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Time Adjustment Software Installed

This report displays the value of the Time Adjustment (QTIMADJ) system value.  This value will be set to *NONE if there is no software installed to automatically handle time changes for such events as daylight savings time.

**Collector ID**:  SYSTEM_VALUES

**Report ID**: QTIMADJ

**See also**

Configuration Management Reports

# User Profile Changes

This report displays changes to user profiles on the system. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is CP.

**Collector ID**: JOURNAL_CP

**Report ID**: *BASE

> **Tip**: For CP journal entries to be generated, the QAUDLVL system value must contain *SECCFG and *SECURITY.

PASS = CP Journal entries were not found in QAUDJRN.

FAIL = CP Journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Profile Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **1** (User Profile Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# User Profile Information

This report displays information about user profiles.

**Collector ID**: QSYS2.USER_INFO

**Report ID**: QSYS2_USER_INFO

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Databases Management Reports

This section includes descriptions of the following **Database Management** reports:

- Cross Reference Physical File
- Data Area Changes
- Database Access
- Database Changes
- Database Content
- Database Operations
- Database Operations by Journal
- Field Level Authorities
- Row and Column Access Control
- Schedule Master File
- Sensitive Database Content

**See also**

TGAudit Report Reference Introduction

# Cross Reference Physical File

This report returns the list of database files (file definition).

> **Tip**: If you enter ***ALL** in the Object field, the system returns a list of all database files (objects) in the specified library.

**Collector ID**: DATABASE_CONTENT

**Report ID**: DTABASE_CROSS_REF_FILE

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **2** (Data Level Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **6** (Cross Reference Physical File).

5) Press **Enter**.

6) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

7) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Data Area Changes

This report returns the changes made to data areas.

**Collector ID**: DATA_AREA_AUDITING

**Collector Name**: DATA AREA CHANGES

**Report ID**: *NONE

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **2** (Data Level Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Data Area Changes).
5) Press **Enter**.
6) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

7) Press **Enter**.

**See also**

Databases Management Reports

# Database Access

This report returns database file access detail.

**Collector ID**: DATABASE_ACCESS

**Collector Name**: DATABASE_FILE_ACCESS

**Report ID**: *NONE

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **2** (Data Level Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **8** (Database Access).
5) Press **Enter**.
6) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

7) Press **Enter**.

**See also**

Databases Management Reports

# Database Changes

This report returns database change details.

**Collector ID**: DATABASE_AUDITING

**Collector Name**: DATABASE_CHANGES

**Report ID**: *NONE

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **2** (Data Level Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Database Changes).
5) Press **Enter**.
6) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

7) Press **Enter**.

**See also**

Databases Management Reports

# Database Content

This report returns the content of a database file (columns and records).

> **Tip**: The **Object** field defaults to ***All**. You will need to clear this parameter value and enter the specific (singular) database object for which you want details.

**Collector ID**: DATABASE_CONTENT

**Report ID**: DATABASE CONTENT

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **2** (Data Level Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **5** (Database Content).

5) Press **Enter**.

6) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

7) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Database Operations

This report returns database operation details.

**Collector ID**: DATABASE_OPERATIONS

**Collector Name**: DATABASE_OPERATIONS

**Report ID**: *NONE

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **2** (Data Level Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **9** (Database Operations).
5) Press **Enter**.
6) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

7) Press **Enter**.

**See also**

Databases Management Reports

# Database Operations by Journal

This report returns database operation details grouped by journal.

**Collector ID**: DTBASE_OPERATIONS_JRN

**Collector Name**: DATABASE_OPERATIONS BY JOURNAL

**Report ID**: *NONE

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **2** (Data Level Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **10** (Database Operations by Journal).
5) Press **Enter**.
6) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

7) Press **Enter**.

**See also**

Databases Management Reports

# Field Level Authorities

This report returns database field level authority details.

**Collector ID**: FIELD_AUTHORITY

**Collector Name**: FIELD LEVEL AUTHORITIES

**Report ID**: *NONE

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **2** (Data Level Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Field Level Authorities).
5) Press **Enter**.
6) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

7) Press **Enter**.

**See also**

Databases Management Reports

# Row and Column Access Control

This report displays Row and Column Access Control (RCAC) events on the system. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is AX.

**Collector ID**: JOURNAL_AX

**Report ID**: *BASE

> **Tip**: For AX journal entries to be generated, the QAUDLVL system value must contain *SECRUN.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **2** (Data Level Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Row and Column Access Control).

5) Press **Enter**.

6) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

7) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Schedule Master File

This report returns the IBM internal job schedule.

**Collector ID**: DATABASE_CONTENT

**Report ID**: Dtabase_Schd_Mast_File

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **2** (Data Level Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **7** (Schedule Master File).
5) Press **Enter**.
6) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

7) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Sensitive Database Content

This report identifies and lists database files on your IBM i server that contain sensitive data. By default, this report is configured to find credit card information, but you can expand the search to meet the needs of your organization.

> **Tip**: If you desire customization of the Sensitive Database Content report, contact Trinity Guard customer support for assistance.

**Collector ID**: SENSTIIVE_DATABASE_CONTENT

**Report ID**: SENSITIVE_DATABASE CONTENT

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **2** (Data Level Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **11** (Sensitive Database Content).

5) Press **Enter**.

6) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

7) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Configuration Management Reports

# Log Management Reports

This section includes descriptions of the following **Log Management** reports:

- Job Activity Details
- Job Activity Summary

**See also**

TGAudit Report Reference Introduction

# Job Activity Details

This report displays the activities identified for monitoring by the Job Activity Monitor.

**Connector ID**: JOB_ACTIVITY_DETAILS

**Report ID**: JOB_ACTIVITY_DETAILS

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Log Management Reports

# Job Activity Summary

This report displays a summary of the activities identified for monitoring by the Job Activity Monitor.

**Connector ID**: JOB_ACTIVITY_SUMMARY

**Report ID**: JOB_ACTIVITY_SUMMARY

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Log Management Reports

# Network Management Reports

This section includes descriptions of the following **Network Management** reports:

- Actions to IP Rules
- APPN Endpoint Filter Violations
- Asynchronous Signals Processed
- Cluster Operations
- Connections Started, Ended, or Rejected
- Controller Description Details
- Controllers and Attached Devices
- Database Server Initialization Report
- Database Server Native DB Report
- Database Server Object Info Report
- Database Server SQL Requests Report
- Device Description Data
- Device Descriptions - *APPC
- DNS Configuration Details
- Integrated File System Exits Installed
- Internet Security Management Events
- Inter-process Communication Events
- Intrusion Monitor Events
- NetServer Configuration
- NetServer Shares
- Network Attribute Details
- Network Authentication Events
- Network Connection Details
- Network Interface Details IPv4
- Network Interface Details IPv6
- Network Route Details IPv4
- Network Route Details IPv6
- Network Server Descriptions
- Network Server Encryption Status
- Network Servers with Encryption Verified
- Network Servers with Failed or Unknown Encryption
- Object Management Changes
- OfficeVision Mail Services Actions
- Remote Power On and IPL
- Remote Service Attribute
- Remote Sign-on Control

- Secure Socket Connections
- Server Sessions Started or Ended
- Server Share Information
- Service Status Change Events
- Sockets-related Exit Points Not Secured
- SSL Cipher Control and Specification List
- TCP_IP IPv4 Stack Attributes
- TCP_IP IPv6 Stack Attributes
- Unsecured Remote Server Exit Points

**See also**

TGAudit Report Reference Introduction

# Actions to IP Rules

This report displays actions to IP Rules. The data relating to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is IR.

**Collector ID**: JOURNAL_IR

**Report ID**: *BASE

> **Tip**: For IR journal entries to be generated, the QAUDLVL system value must contain *NETBAS and *NETCMN.

PASS = IR journal entries were not found in QAUDJRN.

FAIL = IR journal entries were found in QAUDJRN.

**Types of entries**

L - IP rules have been loaded from a file.

N - IP rules have been unloaded for an IP Security connection.

P - IP rules have been loaded for an IP Security connection.

R - IP rules have been read and copied to a file.

U - IP rules have been unloaded (removed).

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **9** (Actions to IP Rules).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

**Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# APPN Endpoint Filter Violations

This report displays information about APPN Endpoint Filter Violations. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is NE.

**Collector ID**: JOURNAL_NE

**Report ID**: *BASE

> **Tip**: For NE journal entries to be generated, the QAUDLVL system value must contain *NETBAS and *NETCMN.

PASS = NE journal entries were not found in QAUDJRN.

FAIL = NE journal entries were found in QAUDJRN.

### Types of entries

A - Change to network attribute

T - Change to TCP/IP attribute

### To run this report

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **13** (APPN Endpoint Filter Violations).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

### See also

Network Management Reports

# Asynchronous Signals Processed

This report displays information about Asynchronous Signals Processed. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is SG.

**Collector ID**: JOURNAL_SG

**Report ID**: *BASE

> **Tip**: For SG journal entries to be generated, the QAUDLVL system value must contain *JOBDTA.

PASS = SG journal entries were not found in QAUDJRN.

FAIL = SG journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **14** (Asynchronous Signals Processed).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Cluster Operations

This report displays Cluster Operations. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is CU.

**Collector ID**: JOURNAL_CU

**Report ID**: *BASE

> **Tip**: For CU journal entries to be generated, the QAUDLVL system value must contain *NETCLU and *NETCMN.

PASS = CU journal entries were not found in QAUDJRN.

FAIL = CU journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **5** (Cluster Operations).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Connections Started, Ended, or Rejected

This report displays information for connections that were started, ended, or rejected on the system. The data relating to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is VC.

**Collector ID**: JOURNAL_VC

**Report ID**: *BASE

> **Tip**: For VC journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL and *JOBDTA.

PASS = VC journal entries were not found in QAUDJRN.

FAIL = VC journal entries were found in QAUDJRN.

**Types of entries**

S - Start

E - End

R - Reject

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **16** (Connections Started, Ended, or Rejected).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Controller Description Details

This report displays information about controller descriptions available on the system.

**Collector ID**: CONTROLLER_DESCRIPTION_DATA

**Report ID**: CONTROLLER_DESCRIPTION_DATA

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Network Settings Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **11** (Controller Description Details).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Controllers and Attached Devices

This report displays information about controller descriptions on the system and the related devices attached to each controller description.

**Collector ID**: CONTROLLER_ATTACHED_DEVICES

**Report ID**: CONTROLLER_ATTACHED_DEVICES

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Network Settings Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **12** (Controllers and Attached Devices).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Database Server Initialization Report

This report displays DB server transactions of type DBINIT - Perform server initiation.

**Collector IDs**:

- NETWORK_TRANS_DATABASE
- NETWORK_TRANSACTIONS_DATABASE

**Report ID**: DATABASE_SERVER_INITLZ_REPORT

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Network Management Reports

# Database Server Native DB Report

This report displays DB server transactions of type DBNDB - Perform native database requests.

**Collector IDs**:

- NETWORK_TRANS_DATABASE
- NETWORK_TRANSACTIONS_DATABASE

**Report ID**: DATABASE_SERVER_NATIVE_REPORT

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Network Management Reports

# Database Server Object Info Report

This report displays DB server transactions of type DBROI - Retrieve object information and catalog function.

**Collector IDs**:

- NETWORK_TRANS_DATABASE
- NETWORK_TRANSACTIONS_DATABASE

**Report ID**: DATABASE_SERVER_OBJECT_REPORT

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Network Management Reports

# Database Server SQL Requests Report

This report displays DB server transactions of type DBSQL - Perform SQL requests

**Collector IDs**:

- NETWORK_TRANS_DATABASE
- NETWORK_TRANSACTIONS_DATABASE

**Report ID**: DATABASE_SERVER_SQL_REQUESTS

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Network Management Reports

# Device Description Data

This report displays information about device descriptions configured on the system.

**Collector ID**: DEVICE_DESCRIPTION_DATA

**Report ID**: DEVICE_DESCRIPTION_DATA

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **7** (Device Details Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **1** (Device Description Details).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Device Descriptions - *APPC

This report displays details about *APPC device descriptions configured on the system.  *APPC devices are for advanced program-to-program communications.

**Collector ID**: DEVICE_DESCRIPTION_APPC

**Report ID**: DEVICE_DESCRIPTION_APPC

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **7** (Device Details Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **2** (Device Descriptions - *APPC).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# DNS Configuration Details

This report displays the DNS configuration of the system.

**Collector ID**: NETWORK_TCPIP_IPV6

**Report ID**: TCPIP_IPV6_STACK_ATTRIBUTES

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Network Settings Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **16** (DNS Configuration Details).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Integrated File System Exits Installed

This report displays information about exit programs installed on the QIBM_QP0L_SCAN_OPEN and QIBM_QP0L_SCAN_CLOSE exit points.

**Collector ID**: EXIT_POINTS

**Report ID**: INTEGRATED_FILE_EXITS

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Network Management Reports

# Internet Security Management Events

This report displays information about Internet Security Management Events. The data relating to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is IS.

**Collector ID**: JOURNAL_IS

**Report ID**: *BASE

> **Tip**: For IS journal entries to be generated, the QAUDLVL system value must contain *NETBAS and *NETCMN.

PASS = IS journal entries were not found in QAUDJRN.

FAIL = IS journal entries were found in QAUDJRN.

**Types of entries**

A - Fail (starting in V7R1, this type is no longer used)

C - Normal (starting in V7R1, this type is no longer used)

U - Mobile User (starting in V7R1, this type is no longer used)

1 - IKE Phase 1 SA Negotiation

2 - IKE Phase 2 SA Negotiation

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **3** (Network Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **10** (Internet Security Management Events).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

**Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Inter-process Communication Events

This report displays details about Inter-process Communication Events. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is IP.

**Collector ID**: JOURNAL_IP

**Report ID**: *BASE

> **Tip**: For IP journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL, *SECIPC, and *SECURITY.

PASS = IP journal entries were not found in QAUDJRN.

FAIL = IP journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **8** (Inter-process Communication Events).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Intrusion Monitor Events

This report displays information about Intrusion Monitor Events. The data relating to this report is retrieved from the system security audit journal (QAUDJRN. The journal entry type associated with this event is IM.

**Collector ID**: JOURNAL_IM

**Report ID**: *BASE

> **Tip**: For IM journal entries to be generated, the QAUDLVL system value must contain *ATNEVT.

PASS = IM journal entries were not found in QAUDJRN.

FAIL = IM journal entries were found in QAUDJRN.

The following are the types of intrusions monitored:

ACKSTORM - TCP ACK storm

ADRPOISN - Address poisoning

FLOOD - Flood event

FRAGGLE - Fraggle attack

ICMPRED - ICMP (Internet Control Message Protocol) redirect

IPFRAG - IP fragment

MALFPKT - Malformed packet

OUTRAW - Outbound Raw

PERPECH - Perpetual echo

PNGDEATH - Ping of death

RESTOPT - Restricted IP options

RESTPROT - Restricted IP protocol

SMURF - Smurf attack

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **3** (Network Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **7** (Intrusion Monitor Events).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# NetServer Configuration

This report displays the list of IBM® i NetServer configuration information.

**Collector ID**: NETSERVER_CONFIG

**Report ID**: NETSERVER_CONFIG

> **Note**: See IBM documentation for additional information: https://www.ibm.com/docs/en/i/7.4?topic=ssw_ibm_i_74/apis/qzlslsti.htm

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Network Settings Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **18** (NetServer Configuration).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# NetServer Shares

This report displays the list of IBM® i NetServer shares. Alternatively, you can use List Server Information (QZLSLSTI) and Open List of Server Information (QZLSOLST) APIs.

**Collector ID**: NETSERVER_SHARES

**Report ID**: NETSERVER_SHARES

> **Note**: See IBM documentation for additional information: https://www.ibm.com/docs/en/i/7.4?topic=ssw_ibm_i_74/apis/qzlslsti.htm

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Network Settings Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **17** (NetServer Shares).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Network Attribute Details

This report displays all network attributes available on the system similar to what is displayed using the Display Network Attribute (DSPNETA) command.  If there are attributes that are not configured correctly, you can update them using the Change Network Attribute (CHGNETA) command.

**Collector ID**: NETWORK_ATTRIBUTES

**Report ID**: NETWORK_ATTRIBUTES_DETAILS

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **3** (Network Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **2** (Network Settings Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **9** (Network Attribute Detail).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Network Authentication Events

This report displays information about Network Authentication Events. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is X0.

**Collector ID**: JOURNAL_X0

**Provider ID**: *BASE

> **Tip**: For X0 journal entries to be generated, the QAUDLVL system value must contain *SECNAS and *SECURITY.

PASS = X0 journal entries were not found in QAUDJRN.

FAIL = X0 Journal entries were found in QAUDJRN.

**Types of entries:**

1 - Service ticket valid

2 - Service principals do not match

3 - Client principals do not match

4 - Ticket IP address mismatch

5 - Decryption of the ticket failed

6 - Decryption of authenticator failed

7 - Realm is not within client local realms

8 - Ticket is a replay attempt

9 - Ticket not yet valid

A - Decrypt of KRB_AP_PRIV or KRB_AP_SAFE checksum error

B - Remote IP address mismatch

C - Local IP address mismatch

D - KRB_AP_PRIV or KRB_AP_SAFE timestamp error

E - KRB_AP_PRIV or KRB_AP_SAFE replay error

F - KRB_AP_PRIV or KRB_AP_SAFE sequence order error

K - GSS accept — expired credential

L - GSS accept — checksum error

M - GSS accept — channel bindings

N - GSS unwrap or GSS verify expired context

O - GSS unwrap or GSS verify decrypt/decode

P - GSS unwrap or GSS verify checksum error

Q - GSS unwrap or GSS verify sequence error

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **19** (Network Authentication Events).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Network Connection Details

This report displays information about network connections to the system.  The data is similar to network data, showing details such as local and remote IP addresses, port numbers, server information, SSL enabled status, TCP state, and connection type information.

**Collector ID**: NETWORK_CONNECTIONS

**Report ID**: NETWORK_CONNECTION_DETAILS

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **3** (Network Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **1** (Network Connection Details).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Network Interface Details IPv4

This report displays IPv4 network interface information for the system.

**Collector ID**: NETWORK_INTERFACE_IPV4

**Report ID**: NETWORK_INTERFACE_IPv4

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Network Settings Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **5** (Network Interface Details IPv4).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Network Interface Details IPv6

This report displays IPv6 network interface information for the system.

**Collector ID**: NETWORK_INTERFACE_IPV6

**Report ID**: NETWORK_INTERFACE_IPV6

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Network Settings Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **6** (Network Interface Details IPv6).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Network Route Details IPv4

This report displays IPv4 routing information on the system.

**Collector ID**: NETWORK_ROUTE_IPV4

**Report ID**: NETWORK_ROUTE_DETAILS_IPV4

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Network Settings Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **7** (Network Route Details IPv4).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Network Route Details IPv6

This report displays IPv6 routing information on the system.

**Collector ID**: NETWORK_ROUTE_IPV6

**Report ID**: NETWORK_ROUTE_DETAILS_IPV6

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Network Settings Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **8** (Network Route Details IPv6).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Network Server Descriptions

This report displays information about network server descriptions defined on the system.

**Collector ID**: NETWORK_SERVER_DESCRIPTIONS

**Report ID**: NETWORK_SERVER_DESCRIPTIONS

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Network Settings Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **13** (Network Server Descriptions).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Network Server Encryption Status

This report displays information about remote servers and whether or not communication to those servers is encrypted.

**Collector ID**: NETWORK_SVR_ENCRYPT_STATUS

**Report ID**: NETWORK_SVR_ENCRYPT_STATUS

**See also**

Network Management Reports

# Network Servers with Encryption Verified

This report displays remote servers on the system that are able to complete a successful SSL handshake.

**Collector ID**: NETWORK_SVR_ENCRYPT_STATUS

**Report ID**: NETWORK_SVR_ENCRYPT_VERIFIED

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **3** (Network Servers with Encryption Verified).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Network Servers with Failed or Unknown Encryption

This report displays remote servers on the system that return a failed or unknown status for an SSL handshake.

**Collector ID**: NETWORK_SVR_ENCRYPT_STATUS

**Report ID**: NETWORK_SVR_ENCRYPT_NOT_VERIF

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **2** (Network Servers with Failed or Unknown Encryption).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Object Management Changes

This report displays object management changes. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is OM.

**Collector ID**: JOURNAL_OM

**Report ID**: *BASE

> **Tip**: For OM journal entries to be generated, the QAUDLVL system value must contain *OBJMGT.

PASS = OM journal entries were not found in QAUDJRN.

FAIL = OM journal entries were found in QAUDJRN.

**Types of entries:**

M - Object moved to a different library.

R - Object renamed.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **7** (Object Management Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# OfficeVision Mail Services Actions

This report displays information about mail actions in OfficeVision. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is ML.

**Collector ID**: JOURNAL_ML

**Report ID**: *BASE

> **Tip**: For ML journal entries to be generated, the QAUDLVL system value must contain *OFCSRV.

PASS = ML Journal entries were not found in QAUDJRN.

FAIL = ML Journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **11** (OfficeVision Mail Services Actions).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Remote Power On and IPL

This report displays the value of the QRMTIPL (Remote Power On and IPL) system value if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QRMTIPL

PASS = System value QRMTIPL is set to 0.

FAIL = System value QRMTIPL is to 1.

The Remote Power On system value defines whether or not turning on power to the system can be done from a remote location.

The recommended value is 0.

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Network Management Reports

# Remote Service Attribute

This report displays the value of the QRMTSRVATR (Remote Service Attribute) system value if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QRMTSRVATR

PASS = System value QRMTSRVATR is set to 0.

FAIL = System value QRMTSRVATR is to 1.

The Remote service attribute system value specifies if service attributes can be changed from a remote location.

The recommended value is 0.

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Network Management Reports

# Remote Sign-on Control

This report displays the value of the QRMTSIGN (Remote Sign-on Control) system value if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QRMTSIGN

PASS = System value QRMTSIGN is set to 1.

FAIL = System value QRMTSIGN is to 0.

The Remote Sign-on Control system value specifies how the system handles remote sign-on requests.

The recommended value is 1.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Network Settings Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **1** (Remote Sign-on Control).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Secure Socket Connections

This report displays information about Secure Socket Connections. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is SK.

**Collector ID**: JOURNAL_SK

**Report ID**: *BASE

> **Tip**: For SK journal entries to be generated, the QAUDLVL system value must contain *NETCMN, *NETFAIL, and *NETSCK.

PASS = SK journal entries were not found in QAUDJRN.

FAIL = SK journal entries were found in QAUDJRN.

**Types of entries:**

A - Accept

C - Connect

D - DHCP address assigned

F - Filtered mail

P - Port unavailable

R - Reject mail

U - DHCP address not assigned

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **15** (Secure Socket Connections).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Server Sessions Started or Ended

This report displays Server Sessions that started or ended. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is VS.

**Collect ID**: JOURNAL_VS

**Report ID**: *BASE

> **Tip**: For VS journal entries to be generated, the QAUDLVL system value must contain *JOBDTA.

FAIL = VS journal entries were found in QAUDJRN.

**Types of entries:**

E - End session

S - Start session

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **17** (Server Sessions Started or Ended).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Server Share Information

This report displays the list of IBM® i NetServer shares.  Alternatively, you can use List Server Information (QZLSLSTI) and Open List of Server Information (QZLSOLST) APIs.

**Collector ID**: QSYS2.SERVER_SHARE_INFO

**Report ID**: SERVER_SHARE_INFO

> **Note**: See the IBM documentation for additional information: https://www.ibm.com/support/pages/ibm-i-74-tr3-enhancements

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Configuration Management Reports

# Service Status Change Events

This report displays changes to Service Status. The data relating to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is VV.

**Collector ID**: JOURNAL_VV

**Report ID**: *BASE

> **Tip**: For VV journal entries to be generated, the QAUDLVL system value must contain *SERVICE.

PASS = VV Journal entries were not found in QAUDJRN.

FAIL = VV Journal entries were found in QAUDJRN.

**Types of entries:**

C - Service status changed

E - Server stopped

P - Server paused

R - Server restarted

S - Server started

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **18** (Service Status Change Events).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Sockets-related Exit Points Not Secured

This report evaluates whether or not exit programs are installed on the sockets-related exit points.

**Collector ID**: EXIT_POINTS

**Report ID**: SOCKET_EXITS

PASS = Exit point programs are installed on sockets-related exit points or server is i5/OS release less than 7.1.

FAIL = No exit point programs are installed on socket-related exit points.

Clients for newer remote servers, such as Secure File Transfer Protocol (SFTP) and Secure Shell (SSH), communicate with i5/OS through sockets instead of the more well-known remote server exit points. There are also many applications that connect directly to the IBM i through proprietary protocols using socket communication. Since i5/OS 7.1, there are socket-related exit points available to help monitor and secure network traffic through sockets on your system.

At a minimum, exit point programs should be installed on socket-related exit points so you can monitor who is accessing the data on your system.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **3** (Network Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **2** (Network Settings Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **3** (Sockets-related Exit Points Not Secured).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# SSL Cipher Control and Specification List

This report displays the values of the QSSLCSL (SSL Cipher Specification List) and QSSLCSLCTL (SSL Specification List) system values if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: SECURE_SOCKET

PASS = System value QSSLCSL is *OPSYS and QSSLCSLCTL is *OPSYS.

FAIL = System value QSSLCSL is not *OPSYS and system value QSSLCSLCTL is not *OPSYS.

The Secure Sockets Layer (SSL) cipher specification list specifies the list of cipher suites that are supported by System SSL. The shipped value is *RSA_AES_128_CBC_SHA, *RSA_RC4_128_SHA, *RSA_RC4_128_MD5, *RSA_AES_256_CBC_SHA, *RSA_3DES_EDE_CBC_SHA, *RSA_DES_CBC_SHA, *RSA_EXPORT_RC4_40_MD5, *RSA_EXPORT_RC2_CBC_40_MD5, *RSA_NULL_SHA, and *RSA_NULL_MD5.

You must have *IOSYSCFG, *ALLOBJ, and *SECADM special authorities to change this system value.

System SSL uses the sequence of the values in QSSLCSL to order the System SSL default cipher specification list. The default cipher specification list entries are system defined and can change on release boundaries. A default cipher removed from QSSLCSL results in the cipher's removal from the default list. The default cipher is added back to the default cipher specification list when it is added back into QSSLCSL. It is not possible to add other ciphers to the default list beyond the system-defined set for the release.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **3** (Network Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **2** (Network Settings Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **2** (SSL Cipher Control and Specification List ).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

# TCP_IP IPv4 Stack Attributes

This report displays TCP/IP stack attribute information for IPv4 communication.

**Collector ID**: NETWORK_TCPIP_IPV4

**Report ID**: TCPIP_IPV4_STACK_ATTRIBUTES

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Network Settings Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **14** (TCP/IP IPv4 Stack Attributes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# TCP_IP IPv6 Stack Attributes

This report displays TCP/IP stack attribute information for IPv6 communication.

**Collector ID**: NETWORK_TCPIP_IPV6

**Report ID**: TCPIP_IPV6_STACK_ATTRIBUTES

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Network Settings Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **15** (TCP/IP IPv6 Stack Attributes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Network Management Reports

# Unsecured Remote Server Exit Points

This report evaluates whether or not exit programs are installed on remote server exit points.

**Collector ID**: EXIT_POINTS

**Report ID**: UNSECURED_REMOTE_EXITS

PASS = Exit programs are installed on remote server exit points.

FAIL = Exit programs are NOT installed on all remote server exit points.

Communication for ODBC, FTP, and TELNET transactions, along with transactions for numerous other remote servers such as RMTCMD, DDM, etc., pass through remote server exit points. Exit programs can be installed on remote server exit points to monitor and secure transactions. It is important to know who is accessing the data on your system so you can verify if the access is authorized or not.

While it is best to implement object-level and Integrated File System (IFS) security to protect your system, sometimes, due to application limitations, it may not be possible to implement this type of security effectively and an application may break if object-level security is implemented. In a situation like this, it is recommended you monitor all your remote connections and the data access. Remote server exit points are your only option in these scenarios.

At a minimum, it is recommended to have exit point programs monitoring remote server exit points so you can review who is accessing your data.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **3** (Network Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **2** (Network Settings Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **4** (Unsecured Remote Server Exit Points).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you can search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

# Profile Management Reports

This section includes descriptions of the following **Profile Management** reports:

- All User Profiles
- Authority Failures
- Authority Restored for User Profiles
- Block Password Change
- Changes to Service Tools Profiles
- Connection Verifications
- Directory Server Extensions
- Disable Profile After Maximum Failed Signon Attempts
- Duplicate Password Control
- Enabled IBM Profiles
- Exceeded Account Limit Events
- Group Profile Information
- Group Profiles with *ALLOBJ *SECADM or *SERVICE Special Authorities
- Group Profiles with Special Authorities
- IBM Profile Details Report
- Identity Token Events
- Inactive Job Message Queue
- Inactive Job Time-out
- Invalid Sign-on Attempts
- Limit Adjacent Digits in Password
- Limit Characters in Password
- Limit Password Character Positions
- Limit Repeating Characters in Password
- Limit Security Officer Device Access
- Maximum Password Length
- Minimum Password Length
- Network Attribute Changes
- Network Log on and Logoff Events
- Network Password Errors
- Network Profile Changes
- Object Authorities of User Profiles
- Ownership Changes for Restored Objects0
- Password Expiration Interval
- Password Expiration Warning
- Password Level
- Password Rules

- Password Validation Program
- Powerful User Profiles
- Profile Object Auditing Values
- Profile with Password Expiration Interval not *SYSVAL
- Profiles that are *DISABLED
- Profiles with Expired Passwords
- Profiles with Limit Capabilities = *NO
- Profiles with Multiple Groups
- Profiles with Pwd = *NONE or *DISABLED
- Publicly Accessible User Profiles
- Require Digit in Password
- Security Officer Profiles
- Service Tool Security Attributes
- Swap Profile Events
- System Service Tools Users
- User Profile = Password
- User Profiles Not Used in 90 Days
- Users with Job Control Special Authority
- Users with Save System Special Authority
- Users with Unlimited Device Sessions

**See also**

TGAudit Report Reference Introduction

# All User Profiles

This report displays a list of all the user profiles that exist on the system and their associated settings.

**Collector ID**: USER_PROFILES

**Report ID**: AllUSERS

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **5** (All User Profiles).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Authority Failures

This report displays information about restoring user profiles. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is AF.

**Collector ID**: JOURNAL_AF

**Report ID**: *BASE

> **Tip**: For AF journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL and *PGMFAIL.

PASS = AF journal entries were not found in QAUDJRN.

FAIL = AF journal entries were found in QAUDJRN.

**Types of failures**

A - Not authorized to object

B - Restricted instruction

C - Validation failure

D - Use of unsupported interface, object domain failure

E - Hardware storage protection error, program constant space violation

F - ICAPI authorization error

G - ICAPI authentication error

H - Scan exit program

I - System Java inheritance not allowed

J - Submit job profile error

K - Special authority violation

N - Profile token not a regenerable token

O - Optical Object Authority Failure

P - Profile swap error

R - Hardware protection error

S - Default sign-on attempt

T - Not authorized to TCP/IP port

U - User permission request not valid

V - Profile token not valid for generating new profile token

W - Profile token not valid for swap

X - System violation

Y - Not authorized to the current JUID field during a clear JUID operation.

Z - Not authorized to the current JUID field during a set JUID operation

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **4** (All Authority Failures).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Authority Restored for User Profiles

This report displays information about restoring authority to user profiles. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is RU. These entries are generated by using the RSTAUT command.

**Collector ID**: JOURNAL_RU

**Report ID**: *BASE

> **Tip**: For RU journal entries to be generated, the QAUDLVL system value must contain *SAVRST.

PASS = RU journal entries were not found in QAUDJRN.

FAIL = RU journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Profile Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **5** (Authority Restored for User Profiles).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Block Password Change

This report displays the value of the QPWDCHGBLK (Block Password Change) system value if a vulnerability is found.

**Collector ID**: JOURNAL_CA

**Report ID**: *BASE

PASS = System value QPWDCHGBLK is set to a value other than *NONE

FAIL = System value QPWDCHGBLK is set to *NONE.

The Block Password Change system value specifies the time period during which a password is blocked from being changed following the prior successful password change operation.  This system value does not restrict password changes made by the Change User Profile (CHGUSRPRF) command.

Consider changing this value from 1-99 to specify the number of hours before the next password change can be made after a successful password change.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **3** (Password-related System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **1** (Block Password Change).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Changes to Service Tools Profiles

This report displays changes to Service Tools profiles. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is DS.

**Collector ID**: JOURNAL_DS

**Report ID**: *BASE

> **Tip**: For DS journal entries to be generated, the QAUDLVL system value must contain *SECCFG and *SECURITY.

PASS = DS journal entries were not found in QAUDJRN.

FAIL = DS journal entries were found in QAUDJRN.

**Types of entries**

A - Reset of a service tools user ID password

C - Change to a service tools user ID

P - Service tools user ID password was changed

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Profile Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **2** (Changes to Service Tools Profiles).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

## Profile Management Reports

# Connection Verifications

This report displays information about Connection Verification events. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is CV.

**Collector ID**: JOURNAL_CV

**Report ID**: *BASE

> **Tip**: For CV journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL, *NETBAS, *NETCMN, and *SECURITY.

PASS = CV journal entries were not found in QAUDJRN.

FAIL = CV journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **3** (Network Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **6** (Connection Verifications).

9) Press **Enter**.

> **Note**: The criteria allow you to limit the data returned n the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Directory Server Extensions

This report displays changes to Directory Server Extensions. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is XD.

**Collector ID**: JOURNAL_XD

**Report ID**: *BASE

> **Tip**: For XD journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL, *CREATE, and *DELETE.

PASS = XD journal entries were not found in QAUDJRN.

FAIL = XD journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (System Configuration Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **22** (Directory Server Extensions).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Disable Profile After Maximum Failed Signon Attempts

This report displays the value of the QMAXSGNACN (Action to Take for Failed Sign-on Attempts) system value if the value is 1 (Disable Device Only).

**Collector ID**: SYSTEM_VALUES

**Report ID**: QMAXSGNACN

PASS = System value QMAXSGNACN is set to 2 or 3.

FAIL = System value QMAXSGNACN is not set to 1.

The Action to Take for Failed Sign-on Attempts system value specifies how the system reacts when the maximum number of consecutive, incorrect, sign-on attempts (see system value QMAXSIGN) is reached. A change to this system value takes effect the next time someone attempts to sign on the system.

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Profile Management Reports

# Duplicate Password Control

This report displays the value of the QPWDRQDDIF (Duplicate Password Control) system value if the value is 0 or is greater than 4.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QPWDRQDDIF

PASS = System value QPWDRQDDIF is set to 1, 2, or 3.

FAIL = System value QPWDRQDDIF is set to 0 or a value greater than 4.

The Duplicate Password Control system value limits how often a user can repeat the use of a password.

0 = Can be the same as old passwords

1 = Cannot be the same as last 32

2 = Cannot be the same as last 24

3 = Cannot be the same as last 18

4 = Cannot be the same as last 12

5 = Cannot be the same as last 10

6 = Cannot be the same as last 8

7 = Cannot be the same as last 6

8 = Cannot be the same as last 4

It is recommended to set this system value to 1, 2, or 3 to increase password security on your system.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **3** (Password-related System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **12** (Duplicate Password Control).

9) Press **Enter**.

10) Modify the run criteria as necessary.

**Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

**Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Enabled IBM Profiles

This report displays a list of user profiles on the system that begin with Q and have a *ENABLED status.  IBM profiles are shipped with the operating system and are used for system application functions.

**Collector ID**: USER_PROFILES

**Report ID**: ENABLED_IBM_PROFILES

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **6** (Enabled IBM Profiles).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Exceeded Account Limit Events

This report displays information about Account Limit Exceeded events. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is VL.

(*Obsolete in 7.2.)

**Collect ID**: JOURNAL_VL

**Report ID**: *BASE

> **Tip**: For VL journal entries to be generated, the QAUDLVL system value must contain *SYSMGT.

PASS = VL journal entries were not found in QAUDJRN.

FAIL = VL journal entries were found in QAUDJRN.

**Types of entries**

A - Account expired

D - Account disabled

L - Logon hours exceeded

U - Unknown or unavailable

W - Workstation not valid

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Profile Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **6** (Exceeded Account Limit Events).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

**Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Group Profile Information

This report displays configuration information about group profiles on the system.  User profiles inherit the special authorities of the group profiles of which they are members.  It is important to monitor the group profiles on your system and ensure they are configured correctly, with only the minimal amount of special authority required.

**Collector ID**: USER_PROFILES

**Report ID**: GROUP_PROFILES

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **11** (Group Profile Information).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Group Profiles with *ALLOBJ *SECADM or *SERVICE Special Authorities

This report displays configuration information for group profiles on the system that have all object, security administrator, or service special authorities. User profiles that are members of these group profiles will inherit these powerful special authorities. The number of user profiles on the system that have these special authorities should be limited as much as possible since they have access to all resources on the system and can perform critical system operations.

**Collector ID**: USER_PROFILES

**Report ID**: GROUP_PROFILE_ALL_SEC_SRV

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **17** (Group Profiles with *ALLOBJ *SECADM or *SERVICE Special Authorities).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Group Profiles with Special Authorities

This report displays configuration information for group profiles on the system that have any special authorities. Since user profiles who are members of these group profiles will inherit the special authorities of their groups, it is critical to evaluate and make sure the group profiles have the least amount of authority required for their specific job functions.

**Collector ID**: USER_PROFILES

**Report ID**: GROUP_PROFILE_SPECIAL_AUTH

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **16** (Group Profiles with Special Authorities).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# IBM Profile Details Report

This report displays configuration information for the Q* IBM user profiles on the system.

**Collector ID**: USER_PROFILES

**Report ID**: IBM_PROFILE_DETAILS

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **15** (IBM Profile Details Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Identity Token Events

This report displays Identity Token events. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is X1.

**Collector ID**: JOURNAL_X1

**Report ID**: *BASE

> **Tip**: For X1 journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL, *SECURITY, and *SECVFY.

PASS = X1 journal entries were not found in QAUDJRN.

FAIL = X1 journal entries were found in QAUDJRN.

**Types of entries**

D - Delegate of identity token was successful

F - Delegate of identity token failed

G - Get user from identity token was successful

U - Get user from identity token failed

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Profile Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **10** (Identity Token Events).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Inactive Job Message Queue

This report displays the value of the QINACTMSGQ (Inactive Job Message Queue) system value if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QINACTMSGQ

PASS = System value QINACTMSGQ is *ENDJOB or *DSCJOB.

FAIL = System value QINACTMSGQ is set to a message queue.

The Inactive Message Queue system value specifies the action the system takes when an interactive job has been inactive for an interval of time (the time interval is specified by the system value QINACTITV). The interactive job can be ended, disconnected, or message CPI1126 can be sent to the message queue you specify. The message queue must exist in the system auxiliary storage pool (ASP) or in a basic user ASP.

If the specified message queue does not exist or is damaged when the inactive time-out interval is reached, the messages are sent to the QSYSOPR message queue.

All of the messages in the specified message queue are cleared during an IPL. If you assign a user's message queue to be QINACTMSGQ, the user loses all messages that are in the user's message queue during each IPL.

A change to this system value takes effect immediately. The shipped value is *ENDJOB.

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Profile Management Reports

# Inactive Job Time-out

This report displays the value of the QINACTITV (Inactive Job Time-out) system value if the value is *NONE.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QINACTITV

PASS = System value QINACTITV is not *NONE.

FAIL = System value QINACTITV is *NONE.

The Inactive Job Time-out system value specifies when the system takes action on inactive interactive jobs. The system value QINACTMSGQ determines the action the system takes. Local jobs that are currently signed-on to a remote system are excluded. For example, a work station is directly attached to system A, and system A has QINACTITV set on. If display station pass-through or TELNET is used to sign on to system B, this work station is not affected by the QINACTITV value set on system A.

> **Note**: A change to this system value takes effect immediately.

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Profile Management Reports

# Invalid Sign-on Attempts

This report displays password validation failures. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is PW.

**Collector ID**: JOURNAL_PW

**Report ID**: *BASE

> **Tip**: For PW journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL.

PASS = PW Journal entries were not found in QAUDJRN.

FAIL = PW Journal entries were found in QAUDJRN.

**Types of entries**

A - APPC bind failure.

C - User authentication with the CHKPWD command failed.

D - Service tools user ID name not valid.

E - Service tools user ID password not valid.

P - Password not valid.

Q - Attempted sign-on (user authentication) failed because the user profile is disabled.

R - Attempted sign-on (user authentication) failed because the password was expired. This audit record might not occur for some user authentication mechanisms. Some authentication mechanisms do not check for expired passwords.

S - SQL Decryption password is not valid.

U - User name not valid.

X - Service tools user ID is disabled.

Y - Service tools user ID not valid.

Z - Service tools user ID password not valid.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Profile Activity Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **4** (Invalid Sign-on Attempts).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Limit Adjacent Digits in Password

This report displays the value of the QPWDLMTAJC (Limit Adjacent Digits in Password) system value if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QPWDLMTCHR

PASS = System value QPWDLMTAJC is set to 1 or higher.

FAIL = System value QPWDLMTAJC is set to 0.

The Limit Adjacent Digits in Password system value specifies whether adjacent numbers are allowed in passwords. This makes it difficult to guess passwords by preventing the use of dates or social security numbers as passwords.

Consider setting the value to limit adjacent digits in passwords to 1 or more, according to your password policy. Be sure to balance complexity and usability in your password policy.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **3** (Password-related System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **4** (Limit Adjacent Digits in Password).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Limit Characters in Password

This report displays the value of the QPWDLMTCHR (Limit Characters in Password) system value if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QPWDLMTCHR

PASS = System value QPWDLMTCHR is set to a value other than *NONE.

FAIL = System value QPWDLMTCHR is set to *NONE.

The Limit Characters in a Password system value provides password security by preventing certain characters (vowels, for example) from being in a password. This makes it difficult to guess passwords by preventing the use of common words or names as passwords.

Consider setting the value to limit characters in passwords to 1 or more, according to your password policy. Be sure to balance complexity and usability in your password policy.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **3** (Password-related System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **5** (Limit Characters in Password).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Limit Password Character Positions

This report displays the value of the QPWDPOSDIF (Limit Password Character Positions) system value if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QPWDPOSDIF

PASS = System value QPWDPOSDIF is not set to 0.

FAIL = System value QPWDPOSDIF is set to 0.

The Limit Password Character Positions system value controls the position of characters in a new password. This prevents the user from specifying the same character in a password corresponding to the same position in the previous password. For example, new password DJS2 could not be used if the previous password was DJS1 (the D, J, and S are in the same positions).

> **Tip**: Consider setting this system value to limit 1 or more password character positions. Be sure to balance complexity and usability in your password policy.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **3** (Password-related System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **10** (Limit Password Character Positions).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Limit Repeating Characters in Password

This report displays the value of the QPWDLMTREP (Limit Repeating Characters in Password) system value if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QPWDLMTREP

PASS = System value QPWDLMTREP is not set to 0.

FAIL = System value QPWDLMTREP is set to 0.

The Limit Repeating Characters in Password system value prevents a user from using the same character more than once in the same password.  (For example, AAAA.)

> **Tip**: Consider limiting repeating characters in passwords and set this value to a value higher than 0, according to your password policy.  Be sure to balance complexity and usability in your password policy.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **3** (Password-related System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **6** (Limit repeating Characters in Password).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Limit Security Officer Device Access

This report displays the value of the Limit Security Officer Device Access (QLMTSECOFR) system value.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QLMTSECOFR

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Profile Management Reports

# Maximum Password Length

This report displays the value of the QPWDMAXLEN (Maximum Password Length) system value if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QPWDMAXLEN

PASS = System value QPWDMAXLEN is set to 10 or higher.

FAIL = System value QPWDMAXLEN is set less than 10.

The Maximum Password Length system value specifies the maximum number of characters in a password.

> **Tip**: It is recommended to set this value to a minimum of 10.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Password-related System Values).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **8** (Maximum Password Length).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Minimum Password Length

This report displays the value of the QPWDMINLEN (Minimum Password Length) system value if the value is less than 7.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QPWDMINLEN

PASS = System value QPWDMINLEN is set to 7 or higher.

FAIL = System value QPWDMINLEN is set less than 7.

The Minimum Password Length system value specifies the minimum number of characters in a password.

> **Tip:** It is recommended to set this value at 7 or higher.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Password-related System Values).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **9** (Minimum Password Length).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Network Attribute Changes

This report displays changes to network attributes. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is NA.

**Collector ID**: JOURNAL_NA

**Report ID**: *BASE

> **Tip**: For NA journal entries to be generated, the QAUDLVL system value must contain *SECCFG and *SECURITY.

PASS = NA journal entries were not found in QAUDJRN.

FAIL = NA journal entries were found in QAUDJRN.

### Types of changes

A - Change to network attribute

T - Change to TCP/IP attribute

### To run this report

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **3** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Network Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **12** (Network Attribute Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

### See also

Profile Management Reports

# Network Log on and Logoff Events

This report displays logon or logoff operations on the network. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is VN.

(*Obsolete in 7.2.)

**Collector ID**: JOURNAL_VN

**Report ID**: *BASE

> **Tip**: For VN journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL and *JOBDTA.

PASS = VN journal entries were not found in QAUDJRN.

FAIL = VN journal entries were found in QAUDJRN.

**Types of entries**

F - Logoff requested

O - Logon requested

R - Logon rejected

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Profile Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **7** (Network Log On and Off Events).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Network Password Errors

This report displays events where incorrect network passwords were used. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is VP.

**Collector ID**: JOURNAL_VP

**Report ID**: *BASE

> **Tip**: For VP journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL.

PASS = VP journal entries were not found in QAUDJRN.

FAIL = VP journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Profile Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **8** (Network Password Errors).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Network Profile Changes

This report displays changes to network profiles. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is VU.

**Collector ID**: JOURNAL_VU

**Report ID**: *BASE

> **Tip**: For VU journal entries to be generated, the QAUDLVL system value must contain *SECCFG and *SECURITY.

PASS = VU journal entries were not found in QAUDJRN.

FAIL = VU journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Profile Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **9** (Network Profile Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Object Authorities of User Profiles

This report displays the object authorities of all user profile objects on the system.

**Collector ID**: USER_OBJECT_AUTHORITIES

**Report ID**: USERS_OBJECT_AUTHORITIES

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **23** (Object Authorities of User Profiles).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Ownership Changes for Restored Objects0

This report displays changes to object ownership.

**Collector ID**: JOURNAL_RO

**Report ID**: *BASE

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Profile Management Reports

# Password Expiration Interval

This report displays the value of the QPWDEXPITV (Password Expiration Interval) system value if the value is *NOMAX or greater than 90.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QPWDEXPITV

PASS = System value QPWDEXPITV is set to 90 or less.

FAIL = System value QPWDEXPITV is set to *NOMAX or a value greater than 90.

The Password Expiration Interval system value specifies the number of days for which passwords are valid. This provides password security by requiring users to change their passwords after a specified number of days. If the password is not changed within the specified number of days, the user cannot sign-on until the password is changed.

Seven days before the password ends, you are warned at sign-on time, even if you are not displaying sign-on information (see system value QDSPSGNINF).

**Tip**: 90 days is a good standard for the password expiration interval.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **3** (Password-related System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **2** (Password Expiration Interval).

9) Press **Enter**.

10) Modify the run criteria as necessary.

**Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

**Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Password Expiration Warning

This report displays the value of the QPWDEXPWRN (Password Expiration Warning) system value if the value is less than 14.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QPWDEXPWRN

PASS = System value QPWDEXPWRN is 14 or greater.

FAIL = System value QPWDEXPWRN is set to less than 14.

The Password Expiration Warning system value controls the number of days prior to a password expiring to begin displaying password expiration warning messages on the Sign-on Information display.

> **Tip**: It is recommended to set this value to 14 days or more.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Password-related System Values).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **3** (Password Expiration Warning).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Password Level

This report displays the value of the QPWDLVL (Password Level) system value if the value is set to 0.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QPWDLVL

PASS = System value QPWDLVL is not set to 0.

FAIL = System value QPWDLVL is set to 0.

The Password Level system value specifies the level of password support on the system. The password level of the system can be set to allow user profile passwords of 1-10 characters or to allow user profile passwords of 1-128 characters.

The password level can be set to allow a 'passphrase' as the password value. The term 'passphrase' is sometimes used in the computer industry to describe a password value which can be very long and has few, if any, restrictions on the characters used in the password value. Blanks can be used between letters in a passphrase, which allows you to have a password value that is a sentence or sentence fragment.

Changing the password level of the system from 1-10 character passwords or 1-128 character passwords requires careful consideration. If your system communicates with other systems in a network, then all systems must be able to handle the longer passwords.

A change to this system value takes effect at the next IPL. To see the current and pending password level values, use the CL command Display Security Attributes (DSPSECA). The shipped value is 0.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **3** (Password-related System Values).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **7** (Password Level).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Password Rules

This report displays the value of the QPWDRULES (Password Rules) system value if the value is not *PWDSYSVAL.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QPWDRULES

PASS = System value QPWDRULES is set to *PWDSYSVAL.

FAIL = System value QPWDRULES is not set to *PWDSYSVAL.

The Password Rules system value specifies the rules used to check whether a password is formed correctly.

> **Note**: Changes made to this system value take effect the next time a password is changed. The shipped value is *PWDSYSVAL.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Password-related System Values).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **13** (Password Rules).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Password Validation Program

This report displays the value of the QPWDVLDPGM (Password Validation Program) system value if the value is not *NONE.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QPWDVLDPGM

PASS = System value QPWDVLDPGM is set to *NONE.

FAIL = System value QPWDVLDPGM is not set to *NONE.

The Password Validation Program system value provides the ability for a user-written program to do additional validation on passwords. The program must exist in the system auxiliary storage pool (ASP) or in a basic user ASP.

Since a password validation program receives passwords in clear text, there is a risk of the program capturing and storing passwords. These programs should be used with extreme caution.

> **Tip**: It is recommended to set this value to *NONE. If a password validation program must exist, ensure it is designed securely and is from a trusted source.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Password-related System Values).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **14** (Password Validation Program).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Powerful User Profiles

This report displays information about the user profiles on your system that have *SECOFR user class or have *ALLOBJ or *SECADM special authorities.

**Collector ID**: USER_PROFILES

**Report ID**: POWER_USERS

PASS = 3 or fewer user profiles with *SECOFR user class or *ALLOBJ or *SECADM special authorities were found on your system.

FAIL = More than three user profiles with *SECOFR user class or *ALLOBJ or *SECADM special authorities were found on your system.

Special authorities determine the level of access a user profile has on the system.

**Types of Special Authorities**

*ALLOBJ – All object authority

*SECADM – Security administrator authority

*JOBCTL – Job control authority

*SPLCTL – Spool control authority

*SAVSYS – Save system authority

*SERVICE – Service authority

*AUDIT – Audit authority

*IOSYSCFG – System configuration authority

> **Tip**: It is recommended to minimize the number of user profiles with special authorities on your system. Assign the minimum authority necessary when creating user profiles. Also, periodically review user profiles to ensure assigned special authorities are still required.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **1** (Powerful User Profiles).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Profile Object Auditing Values

This report displays profile information for users that have object auditing turned on.

**Collector ID**: USER_PROFILES

**Report ID**: PROFILE_OBJECT_AUDIT

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **21** (Profile Object Auditing Values).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Profile with Password Expiration Interval not *SYSVAL

This report displays user profile configuration information for profiles that do not have the typical system standard of *SYSVAL for the Password Expiration Interval. If a user profile has a non-standard value for this setting, they may be attempting to bypass the system security policy. Ensure any non-standard settings are reviewed and approved.

**Collector ID**: USER_PROFILES

**Report ID**: USERS_PWDEXPITV

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **8** (Profile with Password Expiration Interval not *SYSVAL).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Profiles that are *DISABLED

This report displays user profiles that have a status of *DISABLED. These users cannot sign on to the system. Disabled users should be evaluated to determine if they should be deleted from the system due to inactivity. They should also be evaluated to check for instances of hacking attempts since typical system configuration is to disable users after 3 invalid sign-on attempts.

**Collector ID**: USER_PROFILES

**Report ID**: PROFILES_DISABLED

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **13** (Profiles that are *DISABLED).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Profiles with Expired Passwords

This report displays user profile information for users with expired passwords.  If a user's password has been expired for a long period of time, you may want to evaluate if that user can be deleted from the system since it may not be in use.

**Collector ID**: USER_PROFILES

**Report ID**: PROFILES_EXPIRED_PWD

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **14** (Profiles with Expired Passwords).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Profiles with Limit Capabilities = *NO

This report displays user profile configuration information for users that do not have limited capabilities on the system. Users without limited capabilities have greater access to system functions including command line access and the ability to change the initial program, initial menu, current library, and attention key handling programs.

**Collector ID**: USER_PROFILES

**Report ID**: USER_LIMIT_CAPABILITIES

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **12** (Profiles with Limit Capabilities = *NO).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Profiles with Multiple Groups

This report displays user profile configuration information for users with supplemental group profiles. Users inherit the special authorities of their group profiles, so make sure the group profiles assigned have the appropriate authorities to match the job functions of the users. If particular group profiles are not required for the user's job function, remove the group profile association.

**Collector ID**: USER_PROFILES

**Report ID**: PROFILES_MULTIPLE_GROUPS

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **18** (Profiles with Multiple Groups).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Profiles with Pwd = *NONE or *DISABLED

This report displays profile information for users with no password or users that are disabled. These users cannot sign on to the system and should be cleaned up on a regular basis. If these profiles are no longer needed, make sure they are removed.

**Collector ID**: USER_PROFILES

**Report ID**: PROFILES_PWD_NONE_DISABLED

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **19** (Profiles with Pwd = *NONE or *DISABLED).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Publicly Accessible User Profiles

This report displays user profiles where the *PUBLIC authority to the user profile object is not set to *EXCLUDE. In other words, for these users, the general "public" on the system have access to the user profile objects. Typically, the *PUBLIC authority on all user profile objects should be set to *EXCLUDE so unintentional or malicious changes to user profile objects cannot be made to corrupt user profile integrity.

**Collector ID**: USER_OBJECT_AUTHORITIES

**Report ID**: USERS_WITH_PUBLIC_ACCESS

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **22** (Publicly Accessible User Profiles).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Require Digit in Password

This report displays the value of the QPWDRQDDGT (Require digit in password) system value if the value is set to 0.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QPWDRQDDGT

> **Note**: The Require Digit in Password system value specifies whether a digit is required in a new password. This prevents the user from only using alphabetic characters.

PASS = System value QPWDRQDDGT is not set to 0.

FAIL = System value QPWDRQDDGT is set to 0.

> **Tip**: It is recommended to require at least 1 digit in passwords. Be sure to balance complexity and usability in your password policy.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Password-related System Values).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **11** (Require Digit in Password).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Security Officer Profiles

This report displays user profile information about user profiles with the security officer (*SECOFR) user class.

**Collector ID**: USER_PROFILES

**Report ID**: SECURITY_OFFICER

> **Note**: User profiles with security officer class authority typically have all object authority and have little to no restrictions on the system.

PASS = Three or fewer user profiles with *SECOFR user class exist on the system.

FAIL = More than three user profiles with *SECOFR user class exist on the system.

> **Tip**: The number of user-profiles with security officer privileges should be very minimal and reserved only for authorized administrators in your organization.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **2** (Security Officer Profiles).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Service Tool Security Attributes

This report returns the attributes of the service tool.

> **Important**: This report is only available for OS 7.4 or higher.

**Collector ID**: SERVICE_TOOL_SECURITY_ATTR

**Report ID**: SERVICE_TOOL_SECURITY_ATTR

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **24** (Service Tool Security Attributes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Swap Profile Events

This report displays information about any time a profile swap occurs on the system. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is PS.

**Collector ID**: JOURNAL_PS

**Report ID**: *BASE

> **Note**: For PS journal entries to be generated, the QAUDLVL system value must contain *SECURITY and *SECVFY.

PASS = PS journal entries were not found in QAUDJRN.

FAIL = PS journal entries were found in QAUDJRN.

**Types of entries**

A - Profile swap during pass-through

E - End work on behalf of relationship

H - Profile handle generated by the QSYGETPH API

I - All profile tokens were invalidated

M - Maximum number of profile tokens have been generated

P - Profile token generated for user

R - All profile tokens for a user have been removed

S - Start work on behalf of relationship

V - User profile authenticated

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Profile Activity Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **3** (Swap Profile Events).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# System Service Tools Users

This report lists detailed information, including status and privileges, of System Service Tools (SST) users that are not system-supplied.

SST allows you to work with system-level tools.  Tasks such as adding or removing disk units can be done through SST.

**Collector ID**: SYSTEM_TOOL_USERS

**Report ID**: SYSTEM_TOOL_USERS

PASS = One additional SST user exists on the system.

FAIL = Many additional SST users exist on the system.

**Privileges for SST users:**

- Disk units - operations
- Disk units - administration
- Disk units - read only
- System partitions - operations
- System partitions - administration
- Partition remote panel key
- Operator panel functions
- Operating system initial program load (IPL)
- Install
- Performance data collector
- Hardware service manager
- Display/Alter/Dump
- Main storage dump
- Product activity log
- Licensed Internal Code log
- Licensed Internal Code fixes
- Trace
- Dedicated service tools (DST) environment
- Remote service support
- Service tools security
- Service tools save and restore
- Debug
- System capacity - operations
- System capacity - administrator
- System security
- Start service tools
- Take over console

It is recommended to restrict SST access as much as possible since system availability and data integrity can be severely jeopardized through accidental or malicious use of these tools.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **4** (System Service Tools Users).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# User Profile = Password

This report displays user profiles whose password matches their user profile name.  This is a critical security vulnerability since it is the most easily guessed password available.  Best practice is to use a different default password other than the user profile name when creating new users and set any passwords to expire if they are the same as the profile name.  Expiring the password forces the user to change it at the time of their next sign-on.

**Collector ID**: USER_PROFILES

**Report ID**: PROFILES_SAME_PWD

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **20** (User Profile = Password ).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# User Profiles Not Used in 90 Days

This report displays user profile information for users on your system that have not been used in 90 days.

**Collector ID**: USER_PROFILES

**Report ID**: NOT_USED_90_DAYS

PASS = No users exist that have not been used in 90 days.

FAIL = Users exist on your system that have not been used in 90 days.

User profiles that have not been used in three months are typically no longer necessary on the system and are often leftover from employees that are no longer with the organization. The more of these unnecessary profiles that exist on your system, the higher the risk of someone exploiting access to your system.

> **Tip**: It is recommended to disable and eventually delete user profiles not being used.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **3** (User Profiles Not Used in 90 Days).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Users with Job Control Special Authority

This report displays user profile information for users with Job Control (*JOBCTL) special authority.

**Collector ID**: USER_PROFILES

**Report ID**: USERS_JOBCTL

PASS = Three or fewer user profiles with *JOBCTL special authority.

FAIL = More than three user profiles with *JOBCTL special authority.

User profiles with *JOBCTL special authority can change, display, hold, release, cancel, and clear all jobs that are running on the system or that are on a job queue or output queue that has OPRCTL (*YES) specified. The user also has the authority to start writers and stop active subsystems.

> **Tip**: The number of user profiles with Job Control special authority should be very minimal and reserved only for authorized administrators in your organization.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **9** (Users with Job Control Special Authority).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Users with Save System Special Authority

This report displays user profile information for users that have the Save System (*SAVSYS) special authority.

**Collector ID**: USER_PROFILES

**Report ID**: USERS_SAVSYS

PASS = Three or fewer user profiles with *SAVSYS special authority.

FAIL = More than three user profiles with *SAVSYS special authority.

User profiles with *SAVSYS authority have the authority to save, restore, and free storage for all objects on the system, with or without object management authority.

> **Tip**: The number of user profiles with Save System special authority should be very minimal and reserved only for authorized administrators in your organization.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **2** (Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **10** (Users with Save System Special Authority).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Users with Unlimited Device Sessions

This report displays user profile information for users on your system that have the Limit Device Sessions (LMTDEVSSN) parameter set to *NO.

**Collector ID**: USER_PROFILES

**Report ID**: USERS_LIMIT_DEVICE

PASS = All users have the Limit Device Sessions parameter set to a value other than *NO.

FAIL = Users exist on your system that have the Limit Device Sessions parameter set to *NO.

Setting the Limit Device Sessions parameter to *NO is considered bad practice since it enables profiles to be shared more easily.  If sessions are not limited, the same user profile can sign on at any number of device sessions.

> **Tip**: It is recommended to set the Limit Device Sessions parameter to *YES or *SYSVAL.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **2** (Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **7** (Users with Unlimited Device Sessions).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Profile Management Reports

# Resource Management Reports

This section includes descriptions of the following **Resource Management** reports:

- *PUBLIC User with *RWX Authorities -*PUBLIC with *ALL
- Actions on Validation Lists
- Allow Object Restore Option
- Allow User Domain Objects in Libraries
- ASCII Files Stored in the IFS
- Attributes for QSYS.LIB
- Authorization List Details
- Authorization Lists with Public Access
- Authorized Users via Authorization Lists
- Change Request Descriptors Restored
- Changed Data Files in Last 30 Days
- Close Operations on Server Files
- Commands Available in QSH
- Commands Executed
- Configuration Files
- Create Operations
- Damages Objects
- Data Queue Entries
- Database Files Larger than 100Mb
- Database Files with Over 1,000,000 Read Operations
- Database Files with Over 100,000 Delete Operations
- Database Files with Over 100,000 Insert Operations
- Database Files with 10000 Delete Records
- Db2 Mirror Communication Services
- Db2 Mirror Product Services
- Db2 Mirror Replication Services
- Db2 Mirror Replication State
- Db2 Mirror Setup Tools
- Delete Operations
- Directory Link, Unlink, and Search Operations
- Directory Search Violations
- DLO Object Changes
- DLO Object Reads
- Dual Optical Object Accesses
- Exit Point Maintenance Operations
- File Statistics

- File Usage Information
- Files Checked Out Status
- Files Not Secured by Authorization Lists
- Files Not Used in the Last 30 Days
- Files with RWX Authorities
- HTTP Server and Web Files Status
- HTTP Server File Authorities
- IFS Directory Information
- IFS Files Being Journaled
- Integrated File System Content
- Integrated File System Security
- Job Changes
- Job Descriptions - USER Parameter Changes
- Journaled Files
- Journaled Objects
- Largest Files Report >100Mb
- LDAP Operations
- Library QGPL Database Files not Backed up in 30 Days
- Library Statistics
- Maximum sign-on attempts allowed is NOMAX
- Network Resource Accesses
- New Data Files in Last 30 Days
- New Library in Last 30 Days
- New Objects in the Last 30 Days
- Object Authority
- Object Changes
- Object Details
- Object Ownership Changes
- Object Reads
- Object Source
- Object Statistics
- Objects Changed in the Last 30 Days
- Objects Created in the Last 30 Days
- Objects Larger than 100MB
- Objects Owned by QSECOFR
- Objects Restored
- Objects Used in the Last 30 Days
- Optical Volume Accesses
- Primary Group Changes

- Printer Output Changes
- Program Reference Details
- Programs that Adopt Authority
- PTF Object Changes
- PTF Operations
- Public Access to Commands in QSYS
- Public Access to Devices
- Public Access to Journal Receivers in QGPL
- Public Access to Objects in QGPL
- Regular Files on the IFS
- Restored Objects in the Last 30 Days
- Single Optical Object Accesses
- Socket Descriptor Details
- Source Changes in Last 30 Days
- Spooled File Actions
- System Directory Changes
- System Security Audit Journal Exists
- TGAudit Report Configuration
- TGCentral Agent Configuration
- Unsaved Objects in the Last 30 Days
- User-defined File Systems (UDFS's)
- Verify Object on Restore

**See also**

TGAudit Report Reference Introduction

# *PUBLIC User with *RWX Authorities -*PUBLIC with *ALL

This report displays the public and private authorities associated with the objects that have the User Data Authority attribute set to *RWX for the *PUBLIC user.  In the QSYS.LIB file system, this is the equivalent of having object authorities set to *ALL for *PUBLIC.

**Collector ID**: IFS_AUTHORITIES

**Report ID**: PUBLIC_USER_AUTH_FILES

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **19** (*PUBLIC User with RWX Authorities - *PUBLIC with *ALL).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Actions on Validation Lists

This report displays actions on validation lists. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is VO.

**Collector ID**: JOURNAL_VO

**Report ID**: *BASE

> **Tip**: For VO journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL, *SECURITY, and *SECVLDL.

PASS = VO journal entries were not found in QAUDJRN.

FAIL = VO journal entries were found in QAUDJRN.

**Types of entries**

A - Add validation list entry

C -Change validation list entry

F -Find validation list entry

R -Remove validation list entry

U -Unsuccessful verify of a validation list entry

V -Successful verify of a validation list entry

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **18** (Actions on Validation Lists).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

**Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Allow Object Restore Option

This report displays the value of the QALWOBJRST (Allow Object Restore Option) system value if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QALWOBJRST

PASS = System value QALWOBJRST is set to *NONE.

FAIL = System value QALWOBJRST is not set to *NONE.

The QALWOBJRST system value controls how the system handles attempts to restore objects with security-sensitive attributes. The value can be set to *ALL, *NONE, or a list of values. If *ALL is specified, any object can be restored to the system. If *NONE is specified, no objects with security-sensitive attributes can be restored.

> **Tip**: It is recommended to set this value to *NONE so objects with security-sensitive attributes cannot be unknowingly restored on your system. If there is a legitimate need for a security-sensitive object to be restored on your system, you will need to change this system value to allow the restore and then change it back to *NONE. This will prevent instances such as potentially harmful programs that inherit security officer authorities from being restored to your system without your knowledge. Always ensure security-sensitive objects are from trusted sources and designed correctly to avoid creating system vulnerabilities such as basic users being able to access the command line with security officer authorities.

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Resource Management Reports

# Allow User Domain Objects in Libraries

This report displays the value of the QALWUSRDMN (Allow User Domain Objects in Libraries) system value if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QALWUSRDMN

PASS = System value QALWUSRDMN is not set to *ALL.

FAIL = System value QALWUSRDMN is set to *ALL.

This system value controls which libraries may contain user domain user (*USRxxx) objects. You can specify up to 50 individual libraries or all libraries on the system.

> **Tip**: It is recommended you specify a list of libraries which is allowed to store object types such as user indexes (*USRIDX) and user spaces (*USRSPC).

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Resource Management Reports

# ASCII Files Stored in the IFS

This report displays details about ASCII files in the Integrated File System (IFS). ASCII files are determined by the CCSID and codepage attributes. These files contain stream file data and are in directory structures similar to Windows or Unix operating system environments.

**Collector ID**: IFS_ATTRIBUTES

**Report ID**: ASCII_FILES

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **9** (ASCII Files Stored in the IFS).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Attributes for QSYS.LIB

This report displays attributes of objects found in QSYS.LIB.

**Collector ID**: IFS_ATTRIBUTES

**Report ID**: QSYS.LIB_ATTRIBUTES

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **14** (Attributes for /QSYS.LIB).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Authorization List Details

This report displays all authorization lists that exist on the system.

**Collector ID**: AUTHORITIES_LIST

**Report ID**: AUTHORITIES_LIST_DETAILS

> **Tip**: Unnecessary authorization lists should be deleted. Verify the necessary authorization lists are used to secure sensitive data.

PASS = N/A

FAIL = N/A

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Object Information Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **4** (Authorization List Details).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Authorization Lists with Public Access

This report displays authorization lists that do not have *PUBLIC authority set to *EXCLUDE.

**Collector ID**: AUTHORITIES_LIST

**Report ID**: AUTHORITY_LIST_PUBLIC

PASS = *PUBLIC authority for authorization lists is set to *EXCLUDE.

FAIL = *PUBLIC authority for authorization lists is not set to *EXCLUDE.

> **Tip**: *PUBLIC represents all the users on the system. Allowing *PUBLIC access to authorization lists can be a security risk. If an individual user or group of users require access to objects secured by an authorization list, add the user or group to the authorization list.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Object Information Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **5** (Authorization Lists with Public Access).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Authorized Users via Authorization Lists

This report displays the user authorities of an object granted through authorization lists.  If an object is secured by an authorization list, the users in the authorization list and their related authorities will be displayed for that object.

**Collector ID**:  AUTH_USERS_VIA_AUTH_LISTS

**Report ID**: AUTH_USERS_VIA_AUTH_LISTS

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Resource Management Reports

# Change Request Descriptors Restored

This report displays restore operations for Change Request Descriptor (*CRQD) objects that adopt authority. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is RQ.

**Collector ID**: JOURNAL_RQ

**Report ID**: *BASE

> **Tip**: For RQ journal entries to be generated, the QAUDLVL system value must contain *SAVRST.

PASS = RQ journal entries were not found in QAUDJRN.

FAIL = RQ journal entries were found in QAUDJRN.

Use Change User Auditing (CHGUSRAUD) to start auditing commands or use the Change Object Auditing (CHGOBJAUD) command.

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Resource Management Reports

# Changed Data Files in Last 30 Days

Use this report to list the data file changes that occurred in the last 30 days.

**Collector ID**: OBJECT_DETAILS

**Report ID**: CHANGED_FILES_30

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **5** (Object Detail Reports).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Close Operations on Server Files

This report displays Close of Server Files. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is VF.

**Collector ID**: JOURNAL_VF

**Report ID**: *BASE

> **Tip**: For VF journal entries to be generated, use the Change User Auditing (CHGUSRAUD) to start auditing commands or use the Change Object Auditing (CHGOBJAUD) command.

PASS = VF journal entries were not found in QAUDJRN.

FAIL = VF journal entries were found in QAUDJRN.

**Types of entries:**

A - Administrative disconnection

N - Normal client disconnection

S - Session disconnection

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **17** (Close Operations on Server Files).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

# Commands Available in QSH

This report displays all binary commands available in the QSH and PASE environments. These commands are Unix operating system commands.

**Collector ID**: IFS_STATUS

**Report ID**: QSH_COMMANDS

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **23** (Commands Available in QSH).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Commands Executed

This report displays command executions. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is CD.

**Collector ID**: JOURNAL_CD

**Report ID**: *BASE

> **Tip**: For CD journal entries to be generated, use the Change User Auditing (CHGUSRAUD) to start auditing commands or use the Change Object Auditing (CHGOBJAUD) command. QAUDCTL must also be set to *OBJAUD in order for CD journal entries to be generated.

PASS = CD journal entries were not found in QAUDJRN.

FAIL = CD journal entries were found in QAUDJRN.

**Types of entries:**

C - Command run

L - OCL statement

O - Operator control command

P - S/36 procedure

S - Command run after command substitution took place

U - Utility control statement

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **1** (Commands Executed).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

**Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Configuration Files

This report displays file status information for files on the system with file extensions that are typical for configuration files like .conf, .ini, .cfg, .inf, and .cf.

**Collector ID**: IFS_STATUS

**Report ID**: CONFIGURATION_FILES

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **21** (Configuration Files).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Create Operations

This report displays objects created on the system. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is CO.

**Collector ID**: JOURNAL_CO

**Report ID**: *BASE

> **Tip**: For CO journal entries to be generated, the QAUDLVL system value must contain *CREATE.

PASS = CO journal entries were not found in QAUDJRN.

FAIL = CO journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **2** (Create Operations).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Damages Objects

Use this report to list all the objects with a damaged status. For recovery of damaged object you need to restore the object from another system or a backup.

**Collector ID**: OBJECT_DETAILS

**Report ID**: OBJECTS_DAMAGED

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **5** (Object Detail Reports).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Data Queue Entries

This report displays one or more messages from the specified data queue. The messages are not removed from the data queue. The message data is returned as characters, UTF-8, and binary data.

**Collector ID**: QSYS2.DATA_QUEUE_ENTRIES

**Report ID**: DATA_QUEUE_ENTRIES

### To run this report

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

### See also

Resource Management Reports

# Database Files Larger than 100Mb

This report returns database files with over 100,000 delete operations.

**Collector ID**: SYSTABLESTAT

**Report ID**: SYSTABLESTAT_LARGE_FILES

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Resource Management Reports

# Database Files with Over 1,000,000 Read Operations

This report returns database files larger with over 100,000 read operations.

**Collector ID**: SYSTABLESTAT

**Report ID**: SYSTABLESTAT_READ_OPERATIONS

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Resource Management Reports

# Database Files with Over 100,000 Delete Operations

This report returns database files larger with over 100,000 delete operations.

**Collector ID**: SYSTABLESTAT

**Report ID**: SYSTABLESTAT_DELETE_OPERATIONS

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Resource Management Reports

# Database Files with Over 100,000 Insert Operations

This report returns database files larger with over 100,000 insert operations.

**Collector ID**: SYSTABLESTAT

**Report ID**: SYSTABLESTAT_INSERT_OPERATIONS

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Resource Management Reports

# Database Files with 10000 Delete Records

This report returns database files larger with 10,000 delete records.

**Collector ID**: SYSTABLESTAT

**Report ID**: SYSTABLESTAT_DELETELD_RECORDS

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Resource Management Reports

# Db2 Mirror Communication Services

This report returns Db2 mirror communication services details

**Collector ID**: JOURNAL_M6

**Report ID**: *BASE

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **4** (Data Mirroring Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **5** (Db2 Mirror Communication Services).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Db2 Mirror Product Services

This report returns Db2 mirror product services details.

> **Important**: This report is only available for OS 7.4 or higher.

**Collector ID**: JOURNAL_M8

**Report ID**: *BASE

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **4** (Data Mirroring Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **3** (Db2 Mirror Product Services).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Db2 Mirror Replication Services

This report returns Db2 mirror replication services details.

> **Important**: This report is only available for OS 7.4 or higher.

**Collector ID**: JOURNAL_M7

**Report ID**: *BASE

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **4** (Data Mirroring Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **2** (Db2 Mirror Replication Services).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Db2 Mirror Replication State

This report returns Db2 mirror replication state details.

> **Important**: This report is only available for OS 7.4 or higher.

**Collector ID**: JOURNAL_M9

**Report ID**: *BASE

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **4** (Data Mirroring Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **4** (Db2 Mirror Replication State).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Db2 Mirror Setup Tools

This report returns the Db2 mirror setup tool details.

> **Important**: This report is only available for OS 7.4 or higher.

**Collector ID**: JOURNAL_M0

**Report ID**: *BASE

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **4** (Data Mirroring Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **1** (Db2 Mirror Setup Tools).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Delete Operations

This report displays all delete operations. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is DO.

**Collector ID**: JOURNAL_DO

**Report ID**: *BASE

> **Tip**: For DO journal entries to be generated, the QAUDLVL system value must contain *DELETE, *SECCFG, and *SECURITY.

PASS = DO journal entries were not found in QAUDJRN.

FAIL = DO journal entries were found in QAUDJRN.

**Types of entries:**

A - Object was deleted not under commitment control)

C - A pending object delete was committed

D - A pending object create was rolled back

I - Initialize environment variable space

P - The object delete is pending (the delete was performed under commitment control)

R - A pending object delete was rolled back

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **3** (Delete Operations).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

**Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Directory Link, Unlink, and Search Operations

This report displays the event link, unlink, and search directory operations. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is LD.

**Collector ID**: JOURNAL_LD

**Report ID:** *BASE

> **Tip**: For LD journal entries to be generated, object auditing must be turned on for directories by using the CHGAUD command.

PASS = LD journal entries were not found in QAUDJRN.

FAIL = LD journal entries were found in QAUDJRN.

**Types of entries:**

L - Link directory

U - Unlink directory

K - Search directory

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **3** (Directory Link, Unlink, and Search Operations).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

# Directory Search Violations

This report displays directory search filter violations. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is ND.

**Collector ID**: JOURNAL_ND

**Report ID:** *BASE

> **Tip**: For ND journal entries to be generated, the QAUDLVL system value must contain *NETBAS and *NETCMN.

PASS = ND journal entries were not found in QAUDJRN.

FAIL = ND journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **4** (Directory Search Violations).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# DLO Object Changes

This report displays change details for DLO objects. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is YC.

**Collector ID**: JOURNAL_YC

**Report ID:** *BASE

> **Tip**: For YC journal entries to be generated, object auditing on the object must be set to *CHANGE. To set object auditing, use the CHGOBJAUD command.

PASS = YC journal entries were not found in QAUDJRN.

FAIL = YC journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **5** (DLO Object Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# DLO Object Reads

This report displays read details for DLO objects. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is YR.

**Collector ID**: JOURNAL_YR

**Report ID:** *BASE

For YR journal entries to be generated, object auditing on the object must be set to *ALL. To set object auditing, use the CHGOBJAUD command.

PASS = YR journal entries were not found in QAUDJRN.

FAIL = YR journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **6** (DLO Object Reads).

9) Press **Enter**.

10) Modify the run criteria as necessary.

**Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

**Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Dual Optical Object Accesses

This report displays optical object access details. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is O2.

**Collector ID**: JOURNAL_02

**Report ID**: *BASE

> **Tip**: For O2 journal entries to be generated, the QAUDLVL system value must contain *OPTICAL.

PASS = 02 journal entries were not found in QAUDJRN.

FAIL = O2 journal entries were found in QAUDJRN.

**Types of entries**

C - Copy

R - Rename

B - Backup Dir or File

S - Save Held File

M - Move File

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **11** (Dual Optical Object Accesses).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Exit Point Maintenance Operations

This report displays exit point maintenance events. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is GR.

**Collector ID**: JOURNAL_GR

**Report ID**: *BASE

> **Tip**: For GR journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL, *SECCFG, and *SECURITY.

PASS = GR journal entries were not found in QAUDJRN.

FAIL = GR journal entries were found in QAUDJRN.

**Types of entries**

A - Exit program added

C - Operations Resource Monitoring and Control Operations

D - Exit program removed

F - Function registration operations

R - Exit program replaced

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **4** (Exit Point Maintenance Operations).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

**Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# File Statistics

This report contains the list of statistics related to an object (files).

**Collector ID**: OBJECT_STAT

**Report ID**: FILE_STAT

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Object Information Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **9** (File Statistics).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**Report Column Description**

| Column | Description |
|---|---|
| OBJNAME | Name assigned to the object |
| OBJTYPE | Type of object<br>*FILE - |
| OBJOWNER | Owner of the object |
| OBJDEFINER | Definer of object |
| OBJCREATED | Date on which object was created |
| OBJSIZE | Object size |
| OBJTEXT | Descriptive of object |

**See also**

Resource Management Reports

# File Usage Information

This report displays file usage information for files stored in the IFS. Fields returned indicate how often an object is used. Usage has different meanings according to the specific file system and according to the individual object types supported within a file system. Usage count is updated for operations such as opening and closing of a file or can refer to adding links, renaming, restoring, or checking out an object.

**Collector ID**: IFS_ATTRIBUTES

**Report ID**: FILE_USAGE_INFORMATION

**The attributes returned include**

- Days used count: The number of days an object has been used.
- Date object was most recently used: The date the object was last used.
- Date Days_used_cnt was Reset: The date the days used count was the last reset to zero (0).

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **12** (File Usage Information).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Files Checked Out Status

This report displays files checked out by users. When an object is checked out, other users can only read and copy the object. Only the user who has the object checked out can change the object.

**Collector ID**: IFS_ATTRIBUTES

**Report ID**: CHECKED_OUT_FILES

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **10** (Files Checked Out Status).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Files Not Secured by Authorization Lists

This report displays IFS files that are not secured by authorization lists. This report will also show public and private authorities associated with the files.

**Collector ID**: IFS_AUTHORITIES

**Report ID**: FILES_NOT_SECURED_WITH_AUTL

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **16** (Files not Secured by Authorization Lists).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Files Not Used in the Last 30 Days

Use this report to list files not used in the last 30 days.

**Collector ID**: OBJECT_DETAILS

**Report ID**: FILE_USAGE

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **5** (Object Detail Reports).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Files with RWX Authorities

This report displays the public and private authorities associated with the IFS files that have User Data Authority set to *RWX.  The User Data Authority attribute defines what permissions the user has to the file.

*RWX - Allows all operations on the object except those that are limited to the owner or controlled by the object rights

**Collector ID**: IFS_AUTHORITIES

**Report ID**: FILES_RWX_ENABLED

IFS uses the following to grant rights:

*R - Read

*W - Write

*X - Execute rights respectively.

> **Tip**: Read, write, and execute rights can be used in combined, so *RWX gives the equivalent of *ALL authority.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **17** (Files with RWX Authorities).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# HTTP Server and Web Files Status

This report displays status information for the HTTP server and related web files in the "/www" directory.

**Collector ID**: IFS_STATUS

**Report ID**: HTTP_WEB_FILES_STATUS

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **22** (HTTP Server and Web Files Status).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# HTTP Server File Authorities

This report displays authorities for files in the "/www" IFS folder.

**Collector ID**: IFS_AUTHORITIES

**Report ID**: HTTP_SERVER_FILES_AUTH

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **18** (HTTP Server File Authorities).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# IFS Directory Information

This report displays all the directories on the Integrated File System (IFS). Only objects with type *DIR will be shown.

**Collector ID**: IFS_ATTRIBUTES

**Report ID**: DIRECTORY_INFORMATION

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **11** (IFS Directory Information).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# IFS Files Being Journaled

This report displays the extended journaling information for objects.

**Collector ID**: IFS_JOURNALING

**Report ID**: FILES_BEING_JOURNALED

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **20** (IFS Files Being Journaled).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Integrated File System Content

This report returns content from the Integrated File System (IFS).

**Collector ID**: IFS_CONTENT

**Report ID**:  IFS_CONTENT

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **26** (Integrated File System Content).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Integrated File System Security

This report displays the value of the QSCANFSCTL (Scan File Systems) system value if a vulnerability is found.

> **Note**: Review the Scan File Systems (QSCANFS) system value and choose a value that is appropriate for your environment. Ensure QSCANFS is not set to *NONE.

**Collector ID**: SYSTEM_VALUES

**Report ID**: INTEGRATED_FILE_SECURITY

> **Tip**: Although the i5/OS is a virus-free system, if you do not monitor the IFS, it could be a virus carrier and affect your entire network. In fact, i5/OS IFS is a good hiding place for viruses.

PASS = System value QSCANFS is not set to *NONE.

FAIL = System value QSCANFS is set to *NONE.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **1** (Integrated File System Security).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Job Changes

This report displays job change events. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is JS.

**Collector ID**: JOURNAL_JS

**Report ID**: *BASE

> **Tip**: For JS journal entries to be generated, the QAUDLVL system value must contain *JOBBAS, *JOBCHGUSR, and *JOBDTA.

PASS = JS journal entries were not found in QAUDJRN.

FAIL = JS journal entries were found in QAUDJRN.

**Types of entries**

A - ENDJOBABN command

B - Submit

C - Change

E - End

H - Hold

I - Disconnect

J - The current job is attempting to interrupt another job

K - The current job is about to be interrupted

L - The interruption of the current job has completed

M - Change profile or group profile

N - ENDJOB command

P - Attach prestart or batch immediate job

Q - Change query attributes

R - Release

S - Start

T - Change profile or group profile using a profile token.

U - CHGUSRTRC

V - Virtual device changed by QWSACCDS API

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **6** (Job Changes).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Job Descriptions - USER Parameter Changes

This report displays user parameter changes.

**Collector ID**: JOURNAL_JD

**Report ID**: *BASE

> **Tip**: For JD journal entries to be generated, use the Change User Auditing (CHGUSRAUD) to start auditing commands or use the Change Object Auditing (CHGOBJAUD) command.

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Journaled Files

Use this report to list all database files associated with a journal.

**Collector ID**: OBJECT_DETAILS

**Report ID**: JOURNALED_FILES

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **5** (Object Detail Reports).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Journaled Objects

Use this report to display information about journaled objects.  Data returned is closely related to the values returned by the Retrieve Journal Information (QjoRetrieveJournalInformation) API and the Work with Journal Attributes (WRKJRNA) CL command.

**Collector ID**:  QSYS2.JOURNALED_OBJECTS

**Report ID**: JOURNALED_OBJECTS

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **5** (Object Detail Reports).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Largest Files Report >100Mb

This report displays stream files that are larger than 100Mb.

**Collector ID**: IFS_ATTRIBUTES

**Report ID**: LARGE_FILES_ON_IFS

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **13** (Largest Files Report > 100Mb).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# LDAP Operations

This report displays the Lightweight Directory Access Protocol (LDAP) operations. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is DI.

**Collector ID**: JOURNAL_DI

**Report ID**: *BASE

> **Tip**: Object Auditing should also be enabled by using the CHGOBJAUD command.

PASS = DI journal entries were not found in QAUDJRN.

FAIL = DI journal entries were found in QAUDJRN.

For DI journal entries to be generated, the QAUDLVL system value must contain:

- *AUTFAIL
- *CREATE
- *DELETE
- *OBJMGT
- *SECDIRSRV
- *SECURITY
- *SYSMGT

**Types of LDAP operations**

CI - Create an instance

CO - Object creation

CP - Password change

DI - Delete instance

DO - Object delete

EX - LDAP directory export

IM - LDAP directory import

OM - Object management (rename)

OW - Ownership change

PO - Policy change

PW - Password fail

RM - Replication management

UB - Successful unbind

ZC - Object change

ZR - Object read

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **2** (LDAP Operations).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Library QGPL Database Files not Backed up in 30 Days

This report displays file information for physical files in the QGPL library that have not been saved in 30 days.  It is good practice to ensure critical system files are backed up on a regular basis to ensure system availability.

**Collector ID**: OBJECT_DETAILS

**Report ID**: DATABASE_QGPL_30_DAYS

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**See also**

Resource Management Reports

# Library Statistics

This report contains the list of statistics related to a library.

**Collector ID**: LIBRARY_STAT

**Report ID**:  LIBRARY_STAT

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Object Information Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **10** (Library Statistics).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**Report Column Description**

| Column | Description |
|---|---|
| OBJNAME | Name assigned to object |
| OBJTYPE | Type of object:<br>*LIB |
| OBJOWNER | Owner of object |
| OBJDEFINER | Creator of object |
| OBJCREATED | Date on which object was created |
| OBJSIZE | Size of object |
| OBJTEXT | Description of object |

**See also**

Resource Management Reports

# Maximum sign-on attempts allowed is NOMAX

This report displays the value of the QMAXSIGN (Maximum Sign-on Attempts Allowed) system value if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QMAXSIGN

> **Tip**: The Maximum Sign-on Attempts Allowed system value controls the number of times a user can incorrectly attempt to sign on to the system. This value should be set to a reasonably low number to guard against unauthorized access attempts to your system.

PASS = System value QMAXSIGN is set to a value other than *NOMAX.

FAIL = System value QMAXSIGN is set to *NOMAX.

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Network Resource Accesses

This report displays network resource access details. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is VR.

**Collector ID**: JOURNAL_VR

**Report ID**: *BASE

> For VR journal entries to be generated, object auditing on the object must be set to *CHANGE. To set object auditing, use the CHGOBJAUD command.

PASS = VR journal entries were not found in QAUDJRN.

FAIL = VR journal entries were found in QAUDJRN.

### Types of entries

F - Resource access failed

S - Resource access succeeded

### To run this report

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **19** (Network Resource Accesses).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

### See also

Resource Management Reports

# New Data Files in Last 30 Days

Use this report to list new data files created in the last 30 days.

**Collector ID**: OBJECT_DETAILS

**Report ID**: NEW_DATA_30

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **5** (Object Detail Reports).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# New Library in Last 30 Days

Use this report to list new libraries created in the last 30 days.

**Collector ID**: OBJECT_DETAILS

**Report ID**: NEW_LIB_30

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **5** (Object Detail Reports).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# New Objects in the Last 30 Days

Use this report to list the new objects created in the last 30 days. The object creation date is used to select data included in this report.

**Collector ID**: OBJECT_DETAILS

**Report ID**: OBJECTS_NEW_30

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **5** (Object Detail Reports).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Object Authority

This report contains the list of details related to an authority object.

**Collector ID**: OBJECT_AUTHORITY

**Report ID**: *NONE

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Object Information Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **2** (Object Authority).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Object Changes

This report displays change operations to objects. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is ZC.

**Collector ID**: JOURNAL_ZC

**Report ID**: *BASE

> **Tip**: For ZC journal entries to be generated, object auditing on the object must be set to *CHANGE. To set object auditing, use the CHGOBJAUD command.

PASS = ZC journal entries were not found in QAUDJRN

FAIL = ZC journal entries were found in QAUDJRN

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **7** (Object Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Object Details

This report contains the list of details related to system objects.

**Collector ID**: OBJECT_DETAILS

**Report ID**: *NONE

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Object Information Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **1** (Object Details).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Object Ownership Changes

This report displays changes to object ownership. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is OW.

**Collector ID**: JOURNAL_OW

**Report ID**: *BASE

> **Tip**: For OW journal entries to be generated, the QAUDLVL system value must contain *SECRUN and *SECURITY.

PASS = OW journal entries were not found in QAUDJRN.

FAIL = OW journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **9** (Object Ownership Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Object Reads

This report displays the read operations for objects. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is ZR.

**Collector ID**: JOURNAL_ZR

**Report ID**: *BASE

> **Tip**: For ZR journal entries to be generated, object auditing on the object must be set to *ALL. To set object auditing, use the CHGOBJAUD command.

PASS = ZR journal entries were not found in QAUDJRN.

FAIL = ZR journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **8** (Object Reads).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Object Source

Use this report to list objects that were created using source files.

**Collector ID**: OBJECT_DETAILS

**Report ID**: OBJECT_SOURCE

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **5** (Object Detail Reports).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Object Statistics

This report contains the list of statistics related to an object.

**Collector ID**: OBJECT_STAT

**Report ID**: OBJECT_STAT

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Object Information Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **8** (Object Statistics).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**Report Column Description**

| Column | Description |
|---|---|
| OBJNAME | Name assigned to object |

| | |
|---|---|
| OBJTYPE | Type of object:<br>*CMD - Command<br>*CLS - Class<br>*DTAARA - Data area<br>*FILE - File<br>*JOBD - Job description<br>*JOBQ - Job queue<br>*JRNRCV - Journal receiver<br>*MODULE - Module<br>*OUTQ - Output queue<br>*PGM - Program<br>*SBSD - Subsystem description<br>*SQLPKG - SQL package |
| OBJOWNER | Owner of object |
| OBJDEFINER | Creator of object |
| OBJCREATED | Date on which object was created |
| OBJSIZE | Size of object |
| OBJTEXT | Description of object |

**See also**

Resource Management Reports

# Objects Changed in the Last 30 Days

Use this report to list objects that have changed in the last 30 days.

**Collector ID**: OBJECT_DETAILS

**Report ID**: OBJECT_CHANGED_30

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **5** (Object Detail Reports).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Objects Created in the Last 30 Days

Use this report to list objects create in the last 30 days. The report is sorted by the object creator's name.

**Collector ID**: OBJECT_DETAILS

**Report ID**: OBJECT_CREATED_30

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **5** (Object Detail Reports).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Objects Larger than 100MB

Use this report to list all objects larger than 100 MB (megabytes). The list is sorted by size in descending order.

**Collector ID**: OBJECT_DETAILS

**Report ID**: LARGEST_OBJECTS

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **5** (Object Detail Reports).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Objects Owned by QSECOFR

Use this report to list objects owned by QSECOFR.

**Collector ID**: OBJECT_DETAILS

**Report ID**: OBJECT_OWNED_QSECOFR

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **5** (Object Detail Reports).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Objects Restored

This report displays objects restored. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is OR.

**Collector ID**: JOURNAL_OR

**Report ID**: *BASE

> **Tip**: For OR journal entries to be generated, the QAUDLVL system value must contain *SAVRST.

PASS = OR journal entries were not found in QAUDJRN.

FAIL = OR journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **8** (Objects Restored).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Objects Used in the Last 30 Days

Use this report to list objects used in the last 30 days.

**Collector ID**: OBJECT_DETAILS

**Report ID**: OBJECT_USED_30

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **5** (Object Detail Reports).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Optical Volume Accesses

This report displays optical volume access details. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is O3.

**Collector ID**: JOURNAL_03

**Report ID**: *BASE

> **Tip**: For O3 journal entries to be generated, the QAUDLVL system value must contain *OPTICAL.

PASS = O3 journal entries were not found in QAUDJRN.

FAIL = O3 journal entries were found in QAUDJRN.

**Types of entries**

A - Change Volume Attributes

B - Backup Volume

C - Convert Backup Volume to Primary

E - Export

I - Initialize

K - Check Volume

L - Change Authorization List

M - Import

N - Rename

R - Absolute Read

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **12** (Optical Volume Accesses).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Primary Group Changes

This report displays Primary Group changes. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is PG.

**Collector ID**: JOURNAL_PG

**Report ID**: *BASE

> **Tip**: For PG journal entries to be generated, the QAUDLVL system value must contain *SECRUN and *SECURITY.

PASS = PG journal entries were not found in QAUDJRN.

FAIL = PG journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **14** (Primary Group Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Printer Output Changes

This report displays printer output changes. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is PO.

**Collector ID**: JOURNAL_PO

**Report ID**: *BASE

> **Tip**: For PO journal entries to be generated, the QAUDLVL system value must contain *PRTDTA.

PASS = PO journal entries were not found in QAUDJRN.

FAIL = PO journal entries were found in QAUDJRN.

**Types of output**

D - Direct print

R - Sent to remote system for printing

S - Spooled file printed

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **15** (Printer Output Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

# Program Reference Details

This report displays information about objects that are referenced by programs.  The data shown in this report is similar to what is displayed through the Display Program Reference (DSPPGMREF) command.

**Collector ID**: PROGRAM_REFERENCE_DATA

**Report ID**: PROGRAM_REFERENCE_DATA

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **2** (Object Information Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **6** (Program Reference Details).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Programs that Adopt Authority

This report contains the list of programs that adopted authority from previous call levels.  Adopt Authority allows a user to run programs with higher privileges; therefore, ensure that all programs listed are known programs. If you see any unknown programs in the list, you might want to investigate and remove the adoption capability for those programs.  You can perform this by running the Change Program Command (CHGPGM) and setting the Use Adopted Authority (USEADPAUT) option to *NO.

**Collector ID**: PROGRAM_ADOPT

**Report ID**: PROGRAMS_ADOPT_AUTHORITY

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **2** (Object Information Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **3** (Program Adopt Details).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# PTF Object Changes

This report displays changes to Program Temporary Fix (PTF) objects such as program or service program objects of a PTF. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is PU.

**Collector ID**: JOURNAL_PU

**Report ID**: *BASE

> **Tip**: For PU journal entries to be generated, the QAUDLVL system value must contain *PTFOBJ.

PASS = PU journal entries were not found in QAUDJRN.

FAIL = PU journal entries were found in QAUDJRN.

### To run this report

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **8** (PTF Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **9** (PTF Object Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

### See also

Resource Management Reports

# PTF Operations

This report displays Program Temporary Fix (PTF) operations such as loading, applying, or removing a PTF. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is PF.

**Collector ID**: JOURNAL_PF

**Report ID**: *BASE

> **Tip**: For PF journal entries to be generated, the QAUDLVL system value must contain *PTFOPR.

PASS = PF journal entries were not found in QAUDJRN.

FAIL = PF journal entries were found in QAUDJRN.

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **1** (Configuration Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **8** (PTF Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **8** (PTF Operation).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Public Access to Commands in QSYS

This report displays information about commands in the QSYS library that do not have *PUBLIC authority set to *EXCLUDE or *AUTL.

**Collector ID**: OBJECT_AUTHORITIES

**Report ID**: COMMAND_AUTHORITY_QSYS

> **Tip**: *PUBLIC represents all the users on the system. Allowing *PUBLIC access to commands in QSYS can be a security risk. If an individual user or a group of users requires access to commands, authorization lists should be used to secure the objects. Make sure the *PUBLIC authority on the authorization list is set to *EXCLUDE as well.

PASS = *PUBLIC authority for commands in QSYS is set to *EXCLUDE or *AUTL.

FAIL = *PUBLIC authority for commands in QSYS is not set to *EXCLUDE or *AUTL.

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Public Access to Devices

This report displays information about devices that do not have *PUBLIC authority set to *EXCLUDE or *AUTL.

**Collector ID**: OBJECT_AUTHORITIES

**Report ID**: DEVICE_AUTHORITY

> **Tip**: *PUBLIC represents all the users on the system. Allowing *PUBLIC access to devices can be a security risk. If an individual user or a group of users requires access to devices, authorization lists should be used to secure the objects. Make sure the *PUBLIC authority on the authorization list is set to *EXCLUDE as well.

PASS = *PUBLIC authority for devices is set to *EXCLUDE or *AUTL.

FAIL = *PUBLIC authority for devices is not set to *EXCLUDE or *AUTL.

**To run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**. The **Work with Reports** interface is displayed.
4) Locate the desired report using the search and sort options available.
5) In the **Opt** field for the desired report, enter **7** (Run).
6) Press **Enter**.
7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Public Access to Journal Receivers in QGPL

This report displays information about journal receivers that do not have *PUBLIC authority set to *EXCLUDE or *AUTL.

**Collector ID**: OBJECT_AUTHORITIES

**Report ID**: JOURNAL_AUTHORITY_QGPL

> **Tip**: *PUBLIC represents all the users on the system. Allowing *PUBLIC access to journal receivers can be a security risk since there can be sensitive data contained in journal receiver. If an individual user or a group of users requires access to journal receivers, authorization lists should be used to secure the objects. Make sure the *PUBLIC authority on the authorization list is set to *EXCLUDE as well.

PASS = *PUBLIC authority for journal receivers in QGPL is set to *EXCLUDE or *AUTL.

FAIL = *PUBLIC authority for journal receivers in QGPL is not set to *EXCLUDE or *AUTL.

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Public Access to Objects in QGPL

This report displays objects in the QGPL library that do not have *PUBLIC authority set to *EXCLUDE or *AUTL.

**Collector ID**: OBJECT_AUTHORITIES

**Report ID**: OBJECT_AUTH_QGPL

> **Tip**: *PUBLIC represents all the users on the system. Allowing *PUBLIC access to program and data can be a security risk. If an individual user or a group of users requires access to programs or data, authorization lists should be used to secure the objects. Make sure the *PUBLIC authority on the authorization list is set to *EXCLUDE as well.

PASS = *PUBLIC authority for objects in the QGPL library is set to *EXCLUDE or *AUTL.

FAIL = *PUBLIC authority for objects in the QGPL library is not set to *EXCLUDE or *AUTL.

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Regular Files on the IFS

This report displays the file status for regular files on the IFS. Regular is defined in the Property field. This report will look at files 3 levels deep from root ✓.

**Collector ID**: IFS_STATUS

**Report ID**: REGULAR_FILES

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **24** (Regular Files on the IFS).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Restored Objects in the Last 30 Days

Use this report to list objects restored in the last 30 days. The Object restore date is used to select the data used in the report.

**Collector ID**: OBJECT_DETAILS

**Report ID**: OBJECTS_RESTORED_30

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **5** (Object Detail Reports).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Single Optical Object Accesses

This report displays optical object access details. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is O1.

**Collector ID**: JOURNAL_01

**Report ID**: *BASE

> **Tip**: For O1 journal entries to be generated, the QAUDLVL system value must contain *OPTICAL.

PASS = 01 journal entries were not found in QAUDJRN.

FAIL = O1 journal entries were found in QAUDJRN.

**Types of entries**

R - Read

U - Update

D - Delete

C - Create Dir

X - Release Held File

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **10** (Single Optical Object Accesses).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Socket Descriptor Details

This report displays socket descriptor details. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is GS.

**Collector ID**: JOURNAL_GS

**Report ID**: *BASE

> **Tip**: For GS journal entries to be generated, the QAUDLVL system value must contain *SECSCKD and *SECURITY.

PASS = GS journal entries were not found in QAUDJRN.

FAIL = GS journal entries were found in QAUDJRN.

**Types of entries:**

G - Give descriptor

R - Received descriptor

U - Unable to use the descriptor

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **5** (Socket Descriptor Details).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

# Source Changes in Last 30 Days

Use this report to list objects with source changes in the last 30 days.

**Collector ID**: OBJECT_DETAILS

**Report ID**: SOURCE_CHANGES_30

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **5** (Object Detail Reports).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Spooled File Actions

This report display changes made to spooled output files. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is SF.

**Collector ID**: JOURNAL_SF

**Report ID**: *BASE

> **Tip**: For SF journal entries to be generated, the QAUDLVL system value must contain *SPLFDTA.

PASS = SF journal entries were not found in QAUDJRN.

FAIL = SF journal entries were found in QAUDJRN.

**Types of entries**

A - Spooled file read by someone other than the owner of the spooled file

C - Spooled file created

D - Spooled file deleted

H - Spooled file held

I - Create of inline file

R - Spooled file released

S - Spooled file saved

T - Spooled file restored

U - Security-relevant spooled file attributes changed

V - Only non-security-relevant spooled file attributes changed

X - Spooled file operation rejected by exit program

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **1** (Object Activity Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter the **16** (Spooled File Actions).

9) Press **Enter**.

10) Modify the run criteria as necessary.

**Note**:

> The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# System Directory Changes

This report displays System Directory changes. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is SD.

**Collector ID**: JOURNAL_SD

**Report ID**: *BASE

> **Tip**: For SD journal entries to be generated, the QAUDLVL system value must contain *OFCSRV.

PASS = SD journal entries were not found in QAUDJRN.

FAIL = SD journal entries were found in QAUDJRN.

**Types of entries**

ADD - Add directory entry

CHG - Change directory entry

COL - Collector entry

DSP - Display directory entry

OUT - Output file request

PRT - Print directory entry

RMV - Remove directory entry

RNM - Rename directory entry

RTV - Retrieve details

SUP - Supplier entry

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

**Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# System Security Audit Journal Exists

This report displays object details for the System Security Audit Journal (QAUDJRN) if it exists on the system.

**Collector ID**: OBJECT_DETAILS

**Report ID**: SYSTEM_JOURNAL_EXISTS

> **Tip**: If the System Security Audit Journal (QAUDJRN) does not exist, it guarantees there is no auditing of system events happening on the system at all. This is a big risk for the entire system. Without an audit journal for system events, there is no data repository to gather forensic information from if a security event should occur.

PASS = System Security Audit Journal exists.

FAIL = System Security Audit Journal does not exist.

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# TGAudit Report Configuration

This report returns TGAudit configuration details.

**Collector ID**: IFS_CONTENT

**Report ID**: IFS_TGAUDIT_RPT_CNFG

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **27** (TGAudit Report Configuration).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**Report Column Description**

| Column | Description |
|---|---|
| Home | Home path to TG product installation |
| Headings | Number of headings |
| Label | Label type |
| Encode | Encode status |
| Schema | Schema status |
| Field Delimiter | Field delimiter type |
| Output CCSID | Coded character set identifier |

**See also**

Resource Management Reports

# TGCentral Agent Configuration

This report returns the TG Central configuration details.

**Collector ID**: IFS_CONTENT

**Report ID**: IFS_TGCENTRAL_AGENT

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **28** (TGCentral Report Configuration).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**Report Column Description**

| Column | Description |
|---|---|
| TGcentral_IP1 | IP address for TGCentral |
| TGCenral_Name1 | Name of TGCentral instance |
| TGCentral_Port1 | Port used for TGCentral Integration |
| SSL | Secure socket layer certificate indicator |
| Poll_Time_Get | Ping value for get |
| Poll_Time_Set | Ping value for set |
| Page_Size | Page size |

| | |
|---|---|
| Debug_Level | Level at which to debug |
| JSONConv | JSON settings |
| LogFileAgtPath | Path to agent log file |
| LogFileSetPath | Path to set log file |
| LogFileGetPath | Path to get log file |
| LogFileJamPath | Path to Jam log file |
| LogFileSize | Log file size |
| LogArchiveFiles | Number of archive files |
| SendIncTrx | TRX indicator |
| BufferTriggers | Path to buffer t rigger file |
| PollTime | Ping value for poll time trigger |
| LogFileTgrPath | Path to trigger log  file |
| SendDetAlr | Send TGDetect alert indicator |
| PollTimeGet | Ping value for get |
| PollTimeSet | Ping value for set |

**See also**

Resource Management Reports

# Unsaved Objects in the Last 30 Days

Use this report to list objects that have not been saved in the last 30 days. It is recommended that you regularly backup your mission-critical data.

**Collector ID**: OBJECT_DETAILS

**Report ID**: UNSAVED OBJECT_30

**To run this report**

1) Access the TGAudit main menu.

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **4** (Resource Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter the **5** (Object Detail Reports).

7) Press **Enter**.

9) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

10) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# User-defined File Systems (UDFS's)

This report displays details about user-defined file systems (UDFS's). A user-defined file system *TYPE2 has high-performance file access. It has a minimum object size of 4096 bytes and a maximum object size of approximately one terabyte in the "root" QOpenSys and user-defined file systems. Otherwise, the maximum is approximately 256 gigabytes. A *TYPE2 *STMF is capable of memory mapping as well as the ability to specify an attribute to optimize disk storage allocation.

> **Note**: This report returns IFS attributes of objects that are *TYPE2 format.

**Collector ID**: IFS_ATTRIBUTES

**Report ID**: USER_DEFINED_FILE_SYSTEM

**To run this report**

1) Access the TGAudit main menu.
2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the **4** (Resource Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the **3** (Integrated File System Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter the **15** (User-defined File Systems (UDFS's)).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

11) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Verify Object on Restore

This report displays the value of the QVFYOBJRST (Verify Object on Restore) system value if a vulnerability is found.

**Collector ID**: SYSTEM_VALUES

**Report ID**: QVFYOBJRST

PASS = System value is set to 3 or higher.

FAIL = System value is set to 1 or 2.

This system value specifies the policy to be used for object signature verification during a restore operation.

These values apply to objects of types:

*CMD

*PGM

*SRVPGM

*SQLPKG

*MODULE

It also applies to *STMF objects which contain Java programs. This value also specifies the policy for PTFs applied to the system, including Licensed Internal Code fixes.

If Digital Certificate Manager is not installed on the system, all objects are treated as unsigned when determining the effects of this system value on those objects during a restore operation.

Program, service program and module objects that are created on a system with a release prior to V6R1 will be treated as unsigned when they are restored to a V6R1 or later system. Likewise, program, service program and module objects created or converted on a V6R1 or later release will be treated as unsigned when they are restored to a release previous to V6R1.

When an attempt is made to restore an object onto the system, three system values work together as filters to determine if the object is allowed to be restored, or if it is converted during the restore. The first filter is the verify object on restore (QVFYOBJRST) system value. It is used to control the restore of some objects that can be digitally signed. The second filter is the force conversion on restore QFRCCVNRST system value. This system value allows you to specify whether or not to convert programs, service programs, SQL packages, and module objects during the restore. It can also prevent some objects from being restored. Only objects that can get past the first two filters are processed by the third filter. The third filter is the allow object on restore QALWOBJRST system value. It specifies whether or not objects with security-sensitive attributes can be restored.

**Tip**: It is recommended to set this system value to 3 or higher.

**To run this report**

1) Access the TGAudit **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports** interface is displayed.

4) Locate the desired report using the search and sort options available.

5) In the **Opt** field for the desired report, enter **7** (Run).

6) Press **Enter**.

7) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report and choose the desired output format.

8) Press **Enter**.

> **Alternatively**, you search for any report using the **Work with Reports** (TGWRKRPT) interface.

**See also**

Resource Management Reports

# Appendices


- APPENDIX - TGAudit Report Reference Revisions
- APPENDIX - TGAudit Collectors

# APPENDIX - TGAudit Report Reference Revisions

This section includes enhancement by version.


- Version 2.4 - TGAudit Report Reference
- Version 2.3 - TGAudit Report Reference
- Version 2.2 - TGAudit Report Reference
- Version 2.1 - TGAudit Report Reference

# Version 2.4 - TGAudit Report Reference

### Collectors

The following new collectors are now available:

- SYS_VAL_CONFIG
- SYS_VAL_DEFAULT
- SYS_VAL_VALID
- NETSERVER_CONFIG
- NETSERVER_SHARES
- QSYS2.DATA_QUEUE_ENTRIES
- QSYS2.EXIT_POINT_INFO
- QSYS2.EXIT_PROGRAM_INFO
- QSYS2.JOURNALED_OBJECTS
- QSYS2.SERVER_SHARE_INFO
- QSYS2.SOFTWARE_PRODUCT

### Reports

#### Configuration Reports

The following new **Configuration** reports are now available:

- Exit Point Information
- Exit Program Information
- Software Product Information
- System Value Configuration Changes
- System Value Configuration Details
- System Value Default Changes
- System Value Defaults
- System Value Valid Value Changes
- System Value Valid Values

#### Network Reports

- NetServer Shares
- NetServer Configuration
- Server Share Information

#### Resource Reports

- Data Queue Entries
- Journaled Objects

# Version 2.3 - TGAudit Report Reference

This release includes the following:

**Collectors**

The following new collectors are available:

- DATABASE_FIELD_ACTIVITY
- ENCRYPT_DATABASE_FIELD
- ENCRYPT_DATABASE_FILE
- ENCRYPT_DATABASE_FILTER
- ENCRYPT_DATABASE_RULES
- ENCRYPTION_DEFAULTS
- QHST.MSG_INFO
- QSYS2.MESSAGE_QUEUE_INFO

**Reports**

The following new reports are available:

- QHST Message Information
- QHST Messages with Severity Greater than 40
- Message Queue Data by Date Range
- Columns with Field Procedures

# Version 2.2 - TGAudit Report Reference

### Collectors

The following new collectors are now available for use:

- AUTHORITY_COL_ALI
- AUTHORITY_COL_IFS
- AUTHORITY_COL_OBJECT
- DATABASE_ACCESS
- DATABASE_OPERATIONS
- DTBASE_OPERATIONS_JRN
- QHST_MSG_INFO
- SENSITIVE_DATABASE_CONTENT

### Authority Collection Reports

The following new reports are now available for use:

- Authority Collection for Object IFS Report
- Authority Collection for Object Native Report
- Authority Collection Report (*ALL)

### Configuration Reports

The following new reports are now available for use:

- QHST Message Information
- QHST Messages with Severity Greater Than 40

### Data Level Reports

The following new reports are now available for use:

- Database Access
- Database Operations
- Database Operations by Journal
- Sensitive Database Content

### Resource Reports

The following new reports are now available for use:

- Changed Data Files in Last 30 Days
- Damages Objects
- Files Not Used in the Last 30 Days
- Journaled Files
- New Data Files in Last 30 Days
- New Library in Last 30 Days
- New Objects in the Last 30 Days
- Object Source

- Objects Changed in the Last 30 Days
- Objects Created in the Last 30 Days
- Objects Larger than 100MB
- Objects Owned by QSECOFR
- Objects Used in the Last 30 Days
- Restored Objects in the Last 30 Days
- Source Changes in Last 30 Days
- Unsaved Objects in the Last 30 Days

> **Note**: The new **Resource** reports use the existing Object_Details collector.

# Version 2.1 - TGAudit Report Reference

This release includes the following:

### Collectors

The following new collectors are now available for use:

- DATABASE_CONTENT
- IFS_CONTENT
- JOURNAL_M0
- JOURNAL_M6
- JOURNAL_M7
- JOURNAL_M8
- JOURNAL_M9
- NETWORK_TRANS_SHOWCASE
- SERVICE_TOOL_SECURITY_ATTR
- TGMOBJINF

> **Note**: See APPENDIX - TGAudit Collectors for a complete list of available collectors.

### Reports

The following new reports are now available for use:

#### Configuration Reports

- Database Content
- Cross Reference Physical File
- Schedule Master File

#### Profile Reports

- Service Tool Security Attributes

#### Resources Reports

- Db2 Mirror Communication Services
- Db2 Mirror Product Services
- Db2 Mirror Replication Services
- Db2 Mirror Replication State
- Db2 Mirror Setup Tools
- File Statistics
- Integrated File System Content
- Library Statistics
- Object Statistics
- TGAudit Report Configuration
- TGCentral Agent Configuration

# APPENDIX - TGAudit Collectors

u

| Collector ID | Collector Name | Collector Category | Platform |
|---|---|---|---|
| ACCESS_ESCAL_ACC_CONTROLS | Access Escalation Access Controls | Network | IBMi |
| ACCESS_ESCAL_DEFAULTS | Access Escalation Defaults | Network | IBMi |
| ACCESS_ESCAL_ENTITLEMENTS | Access Escalation Entitlements | Network | IBMi |
| ACCESS_ESCAL_FILE_EDITORS | Access Escalation File Editors | Network | IBMi |
| ACCESS_ESCALATION_USAGE | Access Escalation Usage | Network | IBMi |
| AUTH_USERS_VIA_AUTH_LISTS | Authorized Users through Authorization Lists | Resource | IBMi |
| AUTHORITY_COL_ALI | Authority Collection Report (*ALL) | Resources | IBMi |
| AUTHORITY_COL_IFS | Auth Collection For Objects IFS Report | Resources | IBMi |
| AUTHORITY_COL_OBJECT | Auth Collection For Objects Native Report | Resources | IBMi |
| AUTHORITY_COLLECTION | Authority Collection Data | Journal | IBMi |
| AUTHORITY_COMPLIANCE | Authority Compliance | Resource | IBMi |
| AUTHORITY_LIST | Authority List Data | System | IBMi |
| BLUEPRINT_3RD_PARTY_FILE | Blueprint 3rd Party Integration File | Profile | IBMi |
| BLUEPRINT_AUTH_SETTINGS_FILE | Blueprint Authority List Settings File | Profile | IBMi |
| BLUEPRINT_MASTER | Blueprint Master | Profile | IBMi |
| BLUEPRINT_NON_COMPLIANCE_USER | Blueprint Non-Compliance User Profiles | Profile | IBMi |
| BLUEPRINT_OBJECT_AUTH_FILE | Blueprint Object Authority File | Profile | IBMi |
| BLUEPRINT_PARAMETER_FILE | Blueprint Parameter File | Profile | IBMi |
| BLUEPRINT_PERMISSION_FILE | Blueprint Permission File | Profile | IBMi |
| CMD_SEC_COMMANDS | Commands Allowed/Rejected via Command Security | Resources | IBMi |
| CMD_SEC_CONF_SETTINGS | Command Security Config Settings | Resources | IBMi |
| CMD_SEC_PARAM_LEVEL | Command Security Paramater Level | Resources | IBMi |
| CMD_SEC_RULES | Command Security Config Settings | Resources | IBMi |

| | | | |
|---|---|---|---|
| CONTROLLER_ATTACHED_DEVICES | Command Security Paramater Level | Network | IBMi |
| CONTROLLER_DESCRIPTION_DATA | Controller Description Information | Network | IBMi |
| DATA_AREA_AUDITING | Audit data area changes | Network | IBMi |
| DATABASE ACCESS | Database File Access | N/A | IBMi |
| DATABASE_AUDITING | Monitor Database changes | Network | IBMi |
| DATABASE_CONTENT | Database Content | Configuration | IBMi |
| DATABASE_FIELD_ACTIVITY | Database Field Activity | Resources | IBMi |
| DATABASE_OPERATIONS | Database Operations | N/A | IBMi |
| DET_ACT_HISTORY | Detect Activity History | Network | IBMi |
| DET_DEFAULTS | Detect Defaults | Configuration | IBMi |
| DET_CMD_RULES | Command Monitor Rules | Configuration | IBMi |
| DET_JRN_SEIM_RULES | Journal Monitor Rules for SEIM | Configuration | IBMi |
| DET_JRNMON_ALERTS | Journal Monitor Alerts | Configuration | IBMi |
| DET_JRNMON_RULES | Journal Monitor Rules | Configuration | IBMi |
| DET_MON_MASTER | Monitor Master | Configuration | IBMi |
| DET_MSQ_CMD_ALR | Message Queue and Command Alerts | Configuration | IBMi |
| DET_MSQ_RULES | Message Queue Rules | Configuration | IBMi |
| DET_SEIM_PROVIDERS | SEIM Providers | Configuration | IBMi |
| DET_SNMP_TRP_PCKG | SNMP Trap Packages | Configuration | IBMi |
| DEVICE_DESCRIPTION_APPC | Device Description APPC Information | Network | IBMi |
| DEVICE_DESCRIPTION_DATA | Device Description Information | Network | IBMi |
| DTBASE_OPERATIONS_JRN | Database Operations by Journal | N/A | IBMi |
| ENCRYPT_DATABASE_FIELD | Encryption Database Field Details | Resource | IBMi |
| ENCRYPT_DATABASE_FILE | Encryption Database File Details | Resource | IBMi |
| ENCRYPT_DATABASE_FILTER | Encryption Database File Details | Resource | IBMi |
| ENCRYPT_DATABASE_RULES | Encryption Database Rule Details | Resource | IBMi |
| ENCRYPTION_DEFAULTS | Encryption Defaults | Resource | IBMi |
| EXIT_POINTS | Display Exit Point Data | Network | IBMi |
| FIELD_AUTHORITY | Display Field Level Authorities | Object | IBMi |
| IFS_ATTRIBUTES | Display the attributes for the IFS objects | Resource | IBMi |

| | | | |
|---|---|---|---|
| IFS_AUTHORITIES | Display the public and private authorities associated with the object | Resource | IBMi |
| IFS_CONTENT | IFS Content | Configuration | IBMi |
| IFS_JOURNALING | Display extended journaling information for the IFS object | Resource | IBMi |
| IFS_STATUS | Display status information about an IFS file | Resource | IBMi |
| INACTIVITY_DISCONNECTS | Inactivity Disconnections | Configuration | IBMi |
| INCOMING_TRANSACTIONS | Incoming Transactions | Network | IBMi |
| ISL_CONFIGURATION_SETTINGS | ISL Configuration Settings | Network | IBMi |
| ISL_DISCONNECT_OPTIONS | ISL Disconnect Options | Network | IBMi |
| ISL_RULES | ISL Inclusion Exclusion Rules | Network | IBMi |
| JOB_ACTIVITY_DETAILS | Job Activity Details | Log | IBMi |
| JOB_ACTIVITY_SUMMARY | Job Activity Summary | Log | IBMi |
| JOB_DESCRIPTIONS | Job Description Data | Configuration | IBMi |
| JOURNAL_AD | Object Auditing Attribute Changes | Configuration | IBMi |
| JOURNAL_AF | Authority Failures | Profile | IBMi |
| JOURNAL_AP | Programs that Adopt Authority were Executed | Configuration | IBMi |
| JOURNAL_AU | EIM Attribute Changes | Configuration | IBMi |
| JOURNAL_AX | Row and Column Access Control | Resource | IBMi |
| JOURNAL_CA | Authorization List or Object Authority Changes | Profile | IBMi |
| JOURNAL_CD | Commands Executed | Resource | IBMi |
| JOURNAL_CO | Create Operations | Resource | IBMi |
| JOURNAL_CP | User Profile Changes | Configuration | IBMi |
| JOURNAL_CQ | Change Request Descriptor Changes | Configuration | IBMi |
| JOURNAL_CU | Cluster Operation | Network | IBMi |
| JOURNAL_CV | Connection Verification | Profile | IBMi |
| JOURNAL_CY | Cryptographic Configuration Changes | Configuration | IBMi |
| JOURNAL_DI | LDAP Operations | Resource | IBMi |
| JOURNAL_DO | Delete Operations | Resource | IBMi |
| JOURNAL_DS | Changes to Service Tools Profiles | Profile | IBMi |
| JOURNAL_EV | Environment Variable Changes | Profile | IBMi |
| JOURNAL_GR | Exit Point Maintenance Operations | Resource | IBMi |

| | | | |
|---|---|---|---|
| JOURNAL_GS | Socket Descriptor Details | Resource | IBMi |
| JOURNAL_IM | Intrusion Monitor Events | Network | IBMi |
| JOURNAL_IP | Inter-process Communication Events | Network | IBMi |
| JOURNAL_IR | Actions to IP Rules | Network | IBMi |
| JOURNAL_IS | Internet Security Management Events | Network | IBMi |
| JOURNAL_JD | Job Descriptions – USER Parameter Changes | Resource | IBMi |
| JOURNAL_JS | Job Changes | Resource | IBMi |
| JOURNAL_KF | Key Ring File Changes | Configuration | IBMi |
| JOURNAL_LD | Directory Link, Unlink, and Search Operations | Resource | IBMi |
| JOURNAL_M0 | Db2 Mirror Setup Tools | Resource | IBMi |
| JOURNAL_M6 | Db2 Mirror Communication Services | Resource | IBMi |
| JOURNAL_M7 | Db2 Mirror Replication Services | Resource | IBMi |
| JOURNAL_M8 | Db2 Mirror Product Services | Resource | IBMi |
| JOURNAL_M9 | Db2 Mirror Replication State | Resource | IBMi |
| JOURNAL_ML | OfficeVision Mail Services Actions | Configuration | IBMi |
| JOURNAL_NA | Network Attribute Changes | Profile | IBMi |
| JOURNAL_ND | Directory Search Violations | Resource | IBMi |
| JOURNAL_NE | APPN Endpoint Filter Violations | Network | IBMi |
| JOURNAL_O1 | Single Optical Object Accesses | Resource | IBMi |
| JOURNAL_O2 | Dual Optical Object Accesses | Resource | IBMi |
| JOURNAL_O3 | Optical Volume Accesses | Resource | IBMi |
| JOURNAL_OM | Object Management Changes | Resource | IBMi |
| JOURNAL_OR | Objects Restored | Resource | IBMi |
| JOURNAL_OW | Object Ownership Changes | Resource | IBMi |
| JOURNAL_PA | Program Changes to Adopt Owner Authority | Configuration | IBMi |
| JOURNAL_PF | PTF Operations | Resource | IBMi |
| JOURNAL_PG | Primary Group Changes | Resource | IBMi |
| JOURNAL_PO | Printer Output Changes | Resource | IBMi |
| JOURNAL_PS | Swap Profile Events | Configuration | IBMi |
| JOURNAL_PU | PTF Object Changes | Profile | IBMi |
| JOURNAL_PW | Invalid Sign-on Attempts | Profile | IBMi |
| JOURNAL_RA | Authority Changes to Restored Objects | Configuration | IBMi |

| | | | |
|---|---|---|---|
| JOURNAL_RJ | Job Descriptions that Contain User Profile Names were Restored | Configuration | IBMi |
| JOURNAL_RO | Ownership Changes for Restored Objects | Profile | IBMi |
| JOURNAL_RP | Programs Restored that Adopt Owner Authority | Configuration | IBMi |
| JOURNAL_RQ | Change Request Descriptors Restored | Resource | IBMi |
| JOURNAL_RU | Authority Restored for User Profiles | Profile | IBMi |
| JOURNAL_RZ | Primary Group Changes for Restored Objects | Configuration | IBMi |
| JOURNAL_SD | System Directory Changes | Resource | IBMi |
| JOURNAL_SE | Subsystem Routing Entry Changes | Configuration | IBMi |
| JOURNAL_SF | Spooled File Actions | Resource | IBMi |
| JOURNAL_SG | Asynchronous Signals Processed | Network | IBMi |
| JOURNAL_SK | Secure Socket Connections | Network | IBMi |
| JOURNAL_SM | Systems Management Changes | Configuration | IBMi |
| JOURNAL_SO | Server Security User Information Actions | Configuration | IBMi |
| JOURNAL_ST | Service Tools Actions | Configuration | IBMi |
| JOURNAL_SV | System Values Changes | Configuration | IBMi |
| JOURNAL_VA | Access Control List Changes | Configuration | IBMi |
| JOURNAL_VC | Connections Started, Ended, or Rejected | Network | IBMi |
| JOURNAL_VF | Close Operations on Server Files | Resource | IBMi |
| JOURNAL_VL | Exceeded Account Limit Events | Profile | IBMi |
| JOURNAL_VN | Network Log On and Off Events | Configuration | IBMi |
| JOURNAL_VO | Actions on Validation Lists | Resource | IBMi |
| JOURNAL_VP | Network Password Errors | Profile | IBMi |
| JOURNAL_VR | Network Resource Accesses | Resource | IBMi |
| JOURNAL_VS | Server Sessions Started or Ended | Network | IBMi |
| JOURNAL_VU | Network Profile Changes | Profile | IBMi |
| JOURNAL_VV | Service Status Change Events | Network | IBMi |
| JOURNAL_X0 | Network Authentication Events | Network | IBMi |
| JOURNAL_X1 | Identity Token Events | Profile | IBMi |
| JOURNAL_XD | Directory Server Extensions | Profile | IBMi |
| JOURNAL_YC | DLO Object Changes | Resource | IBMi |
| JOURNAL_YR | DLO Object Reads | Resource | IBMi |
| JOURNAL_ZC | Object Changes | Resource | IBMi |

| | | | |
|---|---|---|---|
| JOURNAL_ZR | Object Reads | Resource | IBMi |
| KEYSTORE_DATA | KeyStore | Configuration | IBMi |
| LIBRARY_STAT | Library Statistics | Resources | IBMi |
| LINE_DESCRIPTION_DATA | Line Description Information | Configuration | IBMi |
| MESSAGE_QUEUE | Message Queue Details | Configuration | IBMi |
| MESSAGE_QUEUE_DATA | Message Queue Data | Configuration | IBMi |
| NETSERVER_CONFIG | NetServer Configuration | Network | IBMi |
| NETSERVER_SHARES | NetServer Shares | Network | IBMi |
| NETWORK_ATTRIBUTES | Network Attribute Information | Network | IBMi |
| NETWORK_CONNECTIONS | Network Connections Ipv4 and Ipv6 | Network | IBMi |
| NETWORK_EXIT_CONFIG | Exit Point Configuration Report | Network | IBMi |
| NETWORK_INTERFACE_IPV4 | Network Interface Data Ipv4 | Network | IBMi |
| NETWORK_INTERFACE_IPV6 | Network Interface Data Ipv6 | Network | IBMi |
| NETWORK_ROUTE_IPV4 | Network Route Data Ipv4 | Network | IBMi |
| NETWORK_ROUTE_IPV6 | Network Route Data Ipv6 | Network | IBMi |
| NETWORK_SERVER_DESCRIPTIONS | Network Server Description Data | Network | IBMi |
| NETWORK_SVR_ENCRYPT_STATUS | Network Server Encryption Status | Network | IBMi |
| NETWORK_TCPIP_IPV4 | TCP/IP Ipv4 Stack Attributes/Remote Exit Rule | Network | IBMi |
| NETWORK_TCPIP_IPV6 | TCP/IP Ipv6 Stack Attributes/Remote Exit Rule | Network | IBMi |
| NETWORK_TRANS_CENTRAL | Central Server Transactions | Network | IBMi |
| NETWORK_TRANS_COMMAND | Remote Command Transactions | Network | IBMi |
| NETWORK_TRANS_DATABASE | Remote Exit Rules | Network | IBMi |
| NETWORK_TRANS_DATAQ | Remote Exit Rules | Network | IBMi |
| NETWORK_TRANS_DDM | Remote Exit Rules | Network | IBMi |
| NETWORK_TRANS_FILE | Remote Exit Rules | Network | IBMi |
| NETWORK_TRANS_FTP_REXEC | Remote Exit Rules | Network | IBMi |
| NETWORK_TRANS_PRINTER | Remote Exit Rules | Network | IBMi |
| NETWORK_TRANS_SHOWCASE | Network Trans Showcase | Network | IBMi |
| NETWORK_TRANS_SIGNON | Remote Exit Rules | Network | IBMi |
| NETWORK_TRANS_TELNET | Remote Exit Rules | Network | IBMi |

| | | | |
|---|---|---|---|
| OBJECT_AUTHORITY | Display Object Authority | Resource | IBMi |
| OBJECT_DETAILS | Display Object Details | Resource | IBMi |
| OBJECT_STAT | Object/File Statistics | Resource | IBMi |
| OUTPUT_QUEUE | Output Queue Information | Configuration | IBMi |
| PRODUCT_INFO | Basic Information about a software product | Configuration | IBMi |
| PROFILE_COMPLIANCE | Profile Compliance Data | Profile | IBMi |
| PROFILE_INACTIVITY_SETTINGS | Profile Inactivity Settings | Profile | IBMi |
| PROFILE_MANAGER_DEFAULTS | Profile Manager Defaults | Profile | IBMi |
| PROGRAM_ADOPT | Programs that Adopt Authority | Resource | IBMi |
| PROGRAM_REFERENCE_DATA | Program Reference Data | Resource | IBMi |
| PTF_DATA | Program Temporary Fix Data | Configuration | IBMi |
| QHST_MSG_INFO | QHST History Log Information | Configuration | IBMi |
| QSYS2.ACTIVE_JOB_INFO | Active job information | Configuration | IBMi |
| QSYS2.DATA_QUEUE_ENTRIES | Data Queue Entries | Resource | IBMi |
| QSYS2.DRDA_AUTHENTICATION | DRDA and DDM User access | Configuration | IBMi |
| QSYS2.EXIT_POINT_INFO | Exit Point Information | Configuration | IBMi |
| QSYS2.EXIT_PROGRAM_INFO | Exit Program Information | Configuration | IBMi |
| QSYS2.FUNCTION_INFO | Function usage identifiers | Configuration | IBMi |
| QSYS2.FUNCTION_USAGE | Function usage configuration details. | Configuration | IBMi |
| QSYS2.GROUP_PTF_INFO | Group PTFs Information | Configuration | IBMi |
| QSYS2.JOURNAL_INFO | Journal and remote journal information | Configuration | IBMi |
| QSYS2.JOURNALED_OBJECTS | Journal object information | Resource | IBMi |
| QSYS2.LICENSE_INFO | Products license information. | Configuration | IBMi |
| QSYS2.MEDIA_LIBRARY_INFO | Media Library Status details | Configuration | IBMi |
| QSYS2.MEMORY_POOL | Memory pool details | Configuration | IBMi |
| QSYS2.MEMORY_POOL_INFO | Active memory pools | Configuration | IBMi |
| QSYS2.MESSAGE_QUEUE_INFO | Message Queue | Configuration | IBMi |

| | | | |
|---|---|---|---|
| QSYS2.NETSTAT_JOB_INFO | IPv4 and IPv6 network connection details. | Configuration | IBMi |
| QSYS2.OBJECT_LOCK_INFO | Object lock information | Configuration | IBMi |
| QSYS2. OUTPUT_QUEUE_ENTRIES | Spooled file in output queue | Configuration | IBMi |
| QSYS2.RECORD_LOCK_INFO | Record lock information | Configuration | IBMi |
| QSYS2.REPLY_LIST_INFO | Current job's reply list entry information | Configuration | IBMi |
| QSYS2. SCHEDULED_JOB_INFO | Job Schedule Entry information | Configuration | IBMi |
| QSYS2. SERVER_SBS_ROUTING | Alternate subsystem configurations | Configuration | IBMi |
| QSYS2. SERVER_SHARE_INFO | Server Share Information | Configuration | IBMi |
| QSYS2. SOFTWARE_PRODUCT | Server Software Product information | Configuration | IBMi |
| QSYS2.SYSCONTROLS | Permissions or column mask defined | Configuration | IBMi |
| QSYS2.SYSCONTROLSDEP | Dependencies of row permissions and column masks | Configuration | IBMi |
| QSYS2.SYSDISKSTAT | Disk Information | Configuration | IBMi |
| QSYS2. SYSTEM_STATUS_INFO | Partition information | Configuration | IBMi |
| QSYS2.SYSTMPSTG | IBM i temporary storage pool detail | Configuration | IBMi |
| QSYS2.USER_INFO | User Profile Information | Configuration | IBMi |
| QSYS2.USER_STORAGE | Storage usage by user profile | Configuration | IBMi |
| REMOTE_TRAN_SUMMARY_ BY_SERVER | Remote Summary Server | Network | IBMi |
| REMOTE_TRAN_SUMMARY_ BY_USER | Remote Summary User | Network | IBMi |
| RSC_MGR_COMPLIANCE_DA TA | Resource Manager Authority Out of compliance data | Network | IBMi |
| RSC_MGR_CONFIG | Resource Manager Configuration | Network | IBMi |
| RSC_MGR_SCHEMA_DETAILS | Resource Manager Authority Schema Details | Network | IBMi |
| RSC_MGR_SCHEMA_HEADER | Resource Manager Authority Schema Header | Network | IBMi |
| SENSITIVE_DATABASE_CON TENT | Sensitive Database Content | Profile | IBMi |
| SERVICE_TOOL_SECURITY_ ATTR | Service Tool Security Attributes | Profile | IBMi |
| SERVICE_TOOL_USERS | Service Tool User Data | Profile | IBMi |

| | | | |
|---|---|---|---|
| SOCKET_SUMMARY_BY_SERVER | Socket Summary by Server | Network | IBMi |
| SOCKET_SUMMARY_BY_USER | Socket Summary by User | Network | IBMi |
| SOCKET_TRAN_RULES | Socket Rules | Network | IBMi |
| SOCKET_TRANSACTIONS | Socket Transactions | Network | IBMi |
| SOFTWARE_RESOURCES | Installed Software Resources Data | Configuration | IBMi |
| SUBSYSTEM_AUTOSTART | Subsystem Autostart Jobs | Configuration | IBMi |
| SUBSYSTEM_COMMUNICATIONS | Subsystem Communication Entries | Configuration | IBMi |
| SUBSYSTEM_INFORMATION | Subsystem Information Details | Configuration | IBMi |
| SUBSYSTEM_JOB_QUEUE | Subsystem Job Queue | Configuration | IBMi |
| SUBSYSTEM_POOL_DATA | Subsystem Pool Data | Configuration | IBMi |
| SUBSYSTEM_PRESTART | Subsystem Prestart Jobs | Configuration | IBMi |
| SUBSYSTEM_REMOTE | Subsystem Remote Entries | Configuration | IBMi |
| SUBSYSTEM_ROUTING | Subsystem Routing Entries | Configuration | IBMi |
| SUBSYSTEM_WORKSTATION_NAMES | Subsystem Workstation Names | Configuration | IBMi |
| SUBSYSTEM_WORKSTATION_TYPES | Subsystem Workstation Types | Configuration | IBMi |
| SYS_VAL_CONFIG | System Value Configuration | Configuration | IBMi |
| SYS_VAL_DEFAULT | System Value Default | Configuration | IBMi |
| SYS_VAL_VALID | System Value Default | Configuration | IBMi |
| SYSCOLAUTH | Privileges Granted on a Column | Configuration | IBMi |
| SYSCONTROLS | Permission or Column Mask Defined | Configuration | IBMi |
| SYSCONTROLSDEP | Dependencies of Row Permissions and Column Masks | Configuration | IBMi |
| SYSCONTROLSDEP | Privileges Granted on a Row | Configuration | IBMi |
| SYSFIELDS | Columns with Field Procedures | Configuration | IBMi |
| SYSPACKAGEAUTH | Privileges Granted on a Package | Configuration | IBMi |
| SYSPROGRAMSTAT | Program, Service Program, and Module with SQL Statements | Configuration | IBMi |
| SYSROUTINEAUTH | Privileges Granted on a Routine | Configuration | IBMi |
| SYSSCHEMAAUTH | Privileges Granted on a Schema | Configuration | IBMi |
| SYSSEQUENCEAUTH | Privileges Granted on a Sequence | Configuration | IBMi |
| SYSTABAUTH | Privileges Granted on a Table or View | Configuration | IBMi |

| | | | |
|---|---|---|---|
| SYSTABLESTAT | Table Statistics Include all Partitions and Members | Configuration | IBMi |
| SYSTEM_VALUES | Display System Value Data | System | IBMi |
| SYSTOOLS. GROUP_PTF_CURRENCY | PTF Groups Installed per IBM Recommendations | Configuration | IBMi |
| SYSTOOLS. GROUP_PTF_DETAILS | PTFs within PTF Groups Installed per IBM Recommendations | Configuration | IBMi |
| SYSUDTAUTH | Privileges Granted on a Type | Configuration | IBMi |
| SYSVARIABLEAUTH | Privileges Granted on a Global Variable | Configuration | IBMi |
| SYSXSROBJECTAUTH | Privileges Granted on an XML Schema | Configuration | IBMi |
| TGMOBJINF | Object Information | Resource | IBMi |
| TG_NETWORK_GROUPS | TG Network Groups | Network | IBMi |
| TG_OBJECT_GROUPS | TG Object Groups | Network | IBMi |
| TG_OPERATION_GROUPS | TG Operation Groups | Network | IBMi |
| TG_USER_GROUPS | TG User Groups | Network | IBMi |
| USER_OBJECT_AUTHORITIES | User Profile Object Authorities | Profile | IBMi |
| USER_PRF_VIA_BLUEPRINT | User Profile via Blueprint | Profile | IBMi |
| USER_PROFILE_ACTIVITY | User Profile Activity | Profile | IBMi |
| USER_PROFILE_ARCHIVE | User Profile Archive | Profile | IBMi |
| USER_PROFILE_EXCLUSIONS | User Profile Exclusions | Profile | IBMi |
| USER_PROFILES | Display User Profile Data | Profile | IBMi |