NetIQ Security Solutions for IBM i
TGAudit 2.1
Report Reference Guide
Revised August 2019

Legal Notice

Table of Contents

TABLE OF CONTENTS ..... **III**

1. INTRODUCTION **12**

2. CONFIGURATION MANAGEMENT REPORTS **13**

2.1. Access Control List Changes 15
2.2. Actions that Affect a Job are Audited 16
2.3. Active Job Information 17
2.4. Adopting Authority from a Program Owner is Audited 17
2.5. All Deletions of External Objects on the System are Audited 18
2.6. All Object Creations are Audited 19
2.7. All Optical Functions are Audited 20
2.8. All Security Functions are Audited 21
2.9. Alternate Subsystem Configurations 23
2.10. Attention Events are Audited 23
2.11. Auditing End Action set to Power Down System 24
2.12. Authority Changes to Restored Objects 25
2.13. Authorization Failures are Audited 25
2.14. Authorization List or Object Authority Changes 27
2.15. Basic Product Information on the System 27
2.16. Certificate Details 28
2.17. Certificates Expired 28
2.18. Certificates Expiring in 90 Days 29
2.19. Change Request Descriptor Changes 29
2.20. Change Request Descriptors Restored 30
2.21. Cross Reference Physical File 31
2.22. Cryptographic Configuration Changes 31
2.23. Current Cumulative PTF Level 32
2.24. Current Job's Reply List Entry Information 33
2.25. Database Content 33
2.26. Dependencies of Row Permissions and Column Masks 34
2.27. Directory Server Extensions 34
2.28. Disk Information 35
2.29. DRDA and DDM User Access 36
2.30. EIM Attribute Changes 36
2.31. Environment Variable Changes 37
2.32. Function Usage Configuration Details 38
2.33. Function Usage Identifiers 38
2.34. Group PTFs Information 39
2.35. IBM i Temporary Storage Pool Detail 39
2.36. IPv4 and IPv6 Network Connection Details 40
2.37. Installed Products 40
2.38. Job Description Details 41
2.39. Job Descriptions that Contain User Profile Names were Restored 41
2.40. Job Descriptions – USER Parameter Changes 42
2.41. Job Descriptions with Logging 43
2.42. Job Descriptions with Request Data 43

2.43. Job Descriptions with Specific Initial Library Lists....44
2.44. Job Schedule Entry Information....44
2.45. Journal and Remote Journal Information....45
2.46. Key Ring File Changes....45
2.47. Limit Device Sessions Not Enabled....46
2.48. Line Description Details....47
2.49. Media Library Status Details....47
2.50. Memory Pool Details....48
2.51. Message Queue Data for All Queues....48
2.52. Message Queue Data QSYSOPR....49
2.53. Message Queue Data Severity Greater than 30....50
2.54. Message Queue Details....50
2.55. Networking and Communications Functions are Audited....51
2.56. Object Auditing Attribute Changes....52
2.57. Object Lock Information....53
2.58. Object Management Tasks are Audited....53
2.59. OfficeVision Tasks are Audited....54
2.60. Operating System Product Info....55
2.61. Output Queue Details....55
2.62. Ownership Changes for Restored Objects....56
2.63. Partition Information....57
2.64. Permission or Column Mask Defined....57
2.65. Primary Group Changes for Restored Objects....58
2.66. Printing Functions are Audited....58
2.67. Product Information on the System....59
2.68. Product Registration ID Information....60
2.69. Products License Information....61
2.70. Products with Load Errors....61
2.71. Program Changes to Adopt Owner Authority....62
2.72. Program Failures are Audited....63
2.73. Programs Restored that Adopt Owner Authority....64
2.74. Programs that Adopt Authority were Executed....64
2.75. PTF Status for all Products....65
2.76. PTFs Applied to the Licensed Internal Code....66
2.77. PTFs for WDS....66
2.78. PTFs Requiring IPL....67
2.79. PTFs that are Loaded but not Applied....67
2.80. Record Lock Information....68
2.81. Restrict use of Use Adopted Authority....69
2.82. Save and Restore Information is Audited....69
2.83. Schedule Master File....71
2.84. Security Auditing Level....71
2.85. Security System Values....72
2.86. Server Security Data is Retained....73
2.87. Server Security User Information Actions....74
2.88. Service Tasks are Audited....75
2.89. Service Tools Actions....76
2.90. Spooled File Functions are Audited....76
2.91. Spooled File in Output Queue....77
2.92. Storage Usage by User Profile....78
2.93. Strong System Security Level....78
2.94. Subsystem Autostart Details....79
2.95. Subsystem Communication Details....79

2.96. Subsystem Information Details 80
2.97. Subsystem Job Queue Details 80
2.98. Subsystem Pool Data Details 81
2.99. Subsystem Prestart Job Details 82
2.100. Subsystem Remote Entries 82
2.101. Subsystem Routing Entries 83
2.102. Subsystem Routing Entry Changes 83
2.103. Subsystem Workstation Names 84
2.104. Subsystem Workstation Types 85
2.105. Superseded PTFs 85
2.106. System, User, and Object Auditing Control Configuration 86
2.107. System Management Tasks are Audited 86
2.108. System Software Resources 87
2.109. System Value Changes 88
2.110. Systems Management Changes 89
2.111. Time Adjustment Software Installed 90
2.112. User Profile Changes 90
2.113. User Profile Information 91

3. NETWORK MANAGEMENT REPORTS 93

3.1. Actions to IP Rules 94
3.2. APPN Endpoint Filter Violations 95
3.3. Asynchronous Signals Processed 95
3.4. Authority Failures 96
3.5. Cluster Operations 97
3.6. Connection Verifications 98
3.7. Connections Started, Ended, or Rejected 98
3.8. Controller Description Details 99
3.9. Controllers and Attached Devices 100
3.10. Database Server Initialization Report 100
3.11. Database Server Native DB Report 101
3.12. Database Server Object Info Report 101
3.13. Database Server SQL Request Report 102
3.14. Device Description Details 102
3.15. Device Descriptions - *APPC 103
3.16. DNS Configuration Details 103
3.17. Integrated File System Exits Installed 104
3.18. Internet Security Management Events 105
3.19. Inter-process Communication Events 105
3.20. Intrusion Monitor Events 106
3.21. Network Attribute Changes 107
3.22. Network Attribute Details 108
3.23. Network Authentication Events 109
3.24. Network Connection Details 110
3.25. Network Interface Details IPv4 110
3.26. Network Interface Details IPv6 111
3.27. Network Route Details IPv4 111
3.28. Network Route Details IPv6 112
3.29. Network Server Descriptions 113
3.30. Network Server Encryption Status 113
3.31. Network Servers with Encryption Verified 113
3.32. Network Servers with Failed or Unknown Encryption 114
3.33. Object Management Changes 114

3.34. OfficeVision Mail Services Actions 115
3.35. Remote Power On and IPL 116
3.36. Remote Service Attribute 117
3.37. Remote Sign-on Control 117
3.38. Secure Socket Connections 118
3.39. Server Sessions Started or Ended 119
3.40. Service Status Change Events 120
3.41. Sockets-related Exit Points Not Secured 121
3.42. SSL Cipher List and Specification List 121
3.43. TCP/IP IPv4 Stack Attributes 122
3.44. TCP/IP IPv6 Stack Attributes 123
3.45. Unsecured Remote Server Exit Points 123

4. PROFILE MANAGEMENT REPORTS 125

4.1. All User Profiles 126
4.2. Authority Failures 126
4.3. Authority Restored for User Profiles 127
4.4. Authorization Lists with Public Access 128
4.5. Block Password Change 128
4.6. Changes to Service Tools Profiles 129
4.7. Connection Verifications 130
4.8. Directory Server Extensions 130
4.9. Disable Profile After Maximum Failed Signon Attempts 131
4.10. Duplicate Password Control 131
4.11. Enabled IBM Profiles 132
4.12. Exceeded Account Limit Events 133
4.13. Group Profile Information 134
4.14. Group Profiles with *ALLOBJ *SECADM or *SERVICE Special Authorities 134
4.15. Group Profiles with Special Authorities 135
4.16. IBM Profile Details Report 136
4.17. Identity Token Events 136
4.18. Inactive Job Message Queue 137
4.19. Inactive Job Time-out 138
4.20. Invalid Sign-on Attempts 139
4.21. Limit Adjacent Digits in Password 140
4.22. Limit Characters in Password 140
4.23. Limit Password Character Positions 141
4.24. Limit Repeating Characters in Password 142
4.25. Limit Security Officer Device Access 143
4.26. Maximum Password Length 143
4.27. Minimum Password Length 144
4.28. Network Attribute Changes 145
4.29. Network Log on and Logoff Events 145
4.30. Network Password Errors 146
4.31. Network Profile Changes 147
4.32. Object Authorities of User Profiles 148
4.33. Ownership Changes for Restored Objects 148
4.34. Password Expiration Interval 149
4.35. Password Expiration Warning 150
4.36. Password Level 150
4.37. Password Rules 151
4.38. Password Security Reports 152
4.39. Password Validation Program 152

4.40. Powerful User Profiles 153
4.41. Profile Object Auditing Values 154
4.42. Profile with Password Expiration Interval not *SYSVAL 155
4.43. Profiles that are *DISABLED 155
4.44. Profiles with Expired Passwords 156
4.45. Profiles with Limit Capabilities = *NO 157
4.46. Profiles with Multiple Groups 157
4.47. Profiles with Pwd = *NONE or *DISABLED 158
4.48. Publicly Accessible User Profiles 158
4.49. Require Digit in Password 159
4.50. Security Officer Profiles 160
4.51. Service Tool Security Attributes 161
4.52. Swap Profile Events 161
4.53. System Service Tools Users 162
4.54. User Profile = Password 164
4.55. User Profiles Not Used in 90 Days 164
4.56. Users with Job Control Special Authority 165
4.57. Users with Save System Special Authority 166
4.58. Users with Unlimited Device Sessions 167

5. RESOURCE MANAGEMENT REPORTS 169

5.1. *PUBLIC User with *RWX Authorities -*PUBLIC with *ALL 170
5.2. Actions on Validation Lists 171
5.3. Allow Object Restore Option 172
5.4. Allow User Domain Objects in Libraries 173
5.5. ASCII Files Stored in the IFS 173
5.6. Attributes for /QSYS.LIB 174
5.7. Authority Collection for IFS Objects 175
5.8. Authority Collection for Native Objects 175
5.9. Authorization List Details 176
5.10. Authorization Lists with Public Access 176
5.11. Authorized Users via Authorization Lists 177
5.12. Change Request Descriptors Restored 178
5.13. Close Operations on Server Files 178
5.14. Commands Available in QSH 179
5.15. Commands Executed 180
5.16. Configuration Files 181
5.17. Create Operations 181
5.18. Database Files Larger than 100Mb 182
5.19. Database Files with Over 1,000,000 Read Operations 182
5.20. Database Files with Over 100,000 Delete Operations 183
5.21. Database Files with Over 100,000 Insert Operations 183
5.22. Database Files with Over 1,000 Delete Operations 184
5.23. Db2 Mirror Communication Services 184
5.24. Db2 Mirror Product Services 185
5.25. Db2 Mirror Replication Services 186
5.26. Db2 Mirror Replication State 186
5.27. Db2 Mirror Setup Tools 187
5.28. Delete Operations 187
5.29. Directory Link, Unlink, and Search Operations 188
5.30. Directory Search Violations 189
5.31. DLO Object Changes 190
5.32. DLO Object Reads 190

5.33. Dual Optical Object Accesses 191
5.34. Exit Point Maintenance Operations 192
5.35. File Statistics 193
5.36. File Usage Information 194
5.37. Files Checked Out Status 194
5.38. Files not Secured by Authorization Lists 195
5.39. Files with RWX Authorities 196
5.40. HTTP Server and Web Files Status 196
5.41. HTTP Server File Authorities 197
5.42. IFS Directory Information 197
5.43. IFS Files Being Journaled 198
5.44. Integrated File System Content 198
5.45. Integrated File System Security 199
5.46. Job Changes 200
5.47. Job Descriptions - USER Parameter Changes 201
5.48. Largest Files Report > 100Mb 201
5.49. LDAP Operations 202
5.50. Library QGPL Database Files not Backed up in 30 Days 203
5.51. Library Statistics 204
5.52. Maximum sign-on attempts allowed is NOMAX 205
5.53. Network Resource Accesses 205
5.54. Object Authority 206
5.55. Object Changes 207
5.56. Object Details 207
5.57. Object Management Changes 208
5.58. Object Ownership Changes 209
5.59. Object Reads 209
5.60. Object Statistics 210
5.61. Objects Restored 211
5.62. Optical Volume Accesses 212
5.63. Primary Group Changes 213
5.64. Printer Output Changes 214
5.65. Program Reference Details 214
5.66. Programs that Adopt Authority 215
5.67. PTF Object Changes 216
5.68. PTF Operations 216
5.69. Public Access to Commands in QSYS 217
5.70. Public Access to Devices 218
5.71. Public Access to Journal Receivers in QGPL 218
5.72. Public Access to Objects in QGPL 219
5.73. Regular Files on the IFS 220
5.74. Row and Column Access Control 220
5.75. Single Optical Object Accesses 221
5.76. Socket Descriptor Details 222
5.77. Spooled File Actions 222
5.78. System Directory Changes 223
5.79. System Security Audit Journal Exists 224
5.80. TGAudit Report Configuration 225
5.81. TGCentral Agent Configuration 226
5.82. User-defined File Systems (UDFS's) 227
5.83. Verify Object on Restore 228

6. LOG MANAGEMENT REPORTS 231

6.1. JOB ACTIVITY DETAILS 231
6.2. JOB ACTIVITY SUMMARY 231
7. APPENDIX 233
7.1. APPENDIX - COLLECTORS 233

What's New

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 - 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

1. Introduction

This reference guide provides information about each build-it report 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.

Please refer to the TGAudit User Guide for detailed information and concepts on how to use TGAudit.

2. Configuration Management Reports

This section of reports provides details regarding your security configuration.

- 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
- Change Request Descriptors Restored
- Cross Reference Physical File
- Cryptographic Configuration Changes
- Current Cumulative PTF Level
- Current Job's Reply List Entry Information
- Database Content
- Dependencies of Row Permissions and Column Masks
- Directory Server Extensions
- Disk Information
- DRDA and DDM User Access
- EIM Attribute Changes
- Environment Variable Changes
- 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 for All Queues
- Message Queue Data QSYSOPR
- Message Queue Data Severity Greater than
- 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
- Save and Restore Information is Audited
- Schedule Master File
- Security Auditing Level
- Security System Values
- Server Security Data is Retained
- Server Security User Information Actions
- Service Tasks are Audited
- Service Tools Actions
- 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
- Systems Management Changes
- Time Adjustment Software Installed
- User Profile Changes
- User Profile Information

2.1. 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.

The report is based on the following collector:

- QSYS2.ACTIVE_JOB_INFO

PASS = VA journal entries were not found in QAUDJRN.

FAIL = VA journal entries were found in QAUDJRN.

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

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

2.2. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

2.3. Active Job Information

This report displays a list of active jobs.

The report is based on the following collector:

- 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**.

Note: 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

2.4. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

2.5. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

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

2.6. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

2.7. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

2.8. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

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

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

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

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.

2.9. 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.

The report is based on the following collector:

- 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**.

Note: 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

2.10. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

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

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

2.11. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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**.

Note: 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

2.12. 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.

The report is based on the following collector:

- JOURNAL_RA

PASS = RA journal entries were not found in QAUDJRN.

FAIL = RA journal entries were found in QAUDJRN.

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.

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

2.13. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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 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

2.14. 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.

The report is based on the following collector:

- JOURNAL_CA

PASS = CA journal entries were not found in QAUDJRN.

FAIL = CA journal entries were found in QAUDJRN.

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

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

2.15. Basic Product Information on the System

This report displays product information.

The report is based on the following collector:

- 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

2.16. Certificate Details

This report displays the details of your security certificates.

The report is based on the following collector:

- KEYSTORE_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 **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

2.17. Certificates Expired

This report displays expired security certificates.

The report is based on the following collector:

- KEYSTORE_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 **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

2.18. Certificates Expiring in 90 Days

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

The report is based on the following collector:

- KEYSTORE_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 **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

2.19. 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.

The report is based on the following collector:

- JOURNAL_CQ

PASS = CQ journal entries were not found in QAUDJRN.

FAIL = CQ journal entries were found in QAUDJRN.

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

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

2.20. Change Request Descriptors Restored

This report displays restore operations for Change Request Descriptor (*CRQD) objects that adopts 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.

The report is based on the following collector:

- JOURNAL_RQ

PASS = RQ journal entries were not found in QAUDJRN.

FAIL = RQ journal entries were found in QAUDJRN.

For RQ journal entries to be generated, the QAUDLVL system value must contain *SAVRST.

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 **14** (Change Request Descriptors 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

2.21. 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 file (objects) in the specified library.

The report is based on the following collector:

- 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 **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

2.22. 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.

The report is based on the following collector:

- JOURNAL_CY

PASS = CY journal entries were not found in QAUDJRN.

FAIL = CY journal entries were found in QAUDJRN.

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

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

2.23. 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.

The report is based on the following collector:

- PTF_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** (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

2.24. Current Job's Reply List Entry Information

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

The report is based on the following collector:

- 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**.

Note: 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

2.25. 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.

The report is based on the following collector:

- 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

2.26. Dependencies of Row Permissions and Column Masks

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

The report is based on the following collector:

- 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**.

Note: 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

2.27. 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.

The report is based on the following collector:

- JOURNAL_XD

PASS = XD journal entries were not found in QAUDJRN.

FAIL = XD journal entries were found in QAUDJRN.

For XD journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL, *CREATE, and *DELETE.

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

Configuration Management Reports

2.28. Disk Information

This report displays information about the disk.

The report is based on the following collector:

- 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**.

Note: 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

2.29. DRDA and DDM User Access

This report displays DRDA and DDM User access.

The report is based on the following collector:

- 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**.

Note: 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

2.30. 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.

The report is based on the following collector:

- JOURNAL_AU

PASS = AU journal entries were not found in QAUDJRN.

FAIL = AU journal entries were found in QAUDJRN.

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

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

2.31. 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.

The report is based on the following collector:

- JOURNAL_EV

PASS = EV journal entries were not found in QAUDJRN.

FAIL = EV journal entries were found in QAUDJRN.

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

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

2.32. 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.

The report is based on the following collector:

- 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**.

Note: 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

2.33. Function Usage Identifiers

This report displays details about function usage identifiers.

The report is based on the following collector:

- 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**.

Note: 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

2.34. Group PTFs Information

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

The report is based on the following collector:

- 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**.

Note: 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

2.35. IBM i Temporary Storage Pool Detail

This report displays the IBM i temporary storage pool detail.

The report is based on the following collector:

- QSYS2.SYSTMPSTG

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**.

Note: 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

2.36. IPv4 and IPv6 Network Connection Details

This report displays IPv4 and IPv6 connection details.

The report is based on the following collector:

- 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**.

Note: 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

2.37. Installed Products

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

The report is based on the following collector:

- 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 **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

2.38. Job Description Details

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

The report is based on the following collector:

- JOB_DESCSRIPTIONS

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

2.39. 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.

The report is based on the following collector:

- JOURNAL_RJ

PASS = RJ journal entries were not found in QAUDJRN.

FAIL = RJ journal entries were found in QAUDJRN.

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

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

2.40. 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.

The report is based on the following collector:

- JOURNAL_JD

PASS = JD journal entries were not found in QAUDJRN.

FAIL = JD journal entries were found in QAUDJRN.

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

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**.

Note: 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

2.41. 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.

The report is based on the following collector:

- JOB_DESCSRIPTIONS

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

2.42. Job Descriptions with Request Data

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

The report is based on the following collector:

- JOB_DESCSRIPTIONS

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.

2.43. 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.

The report is based on the following collector:

- JOB_DESCSRIPTIONS

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

2.44. 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.

The report is based on the following collector:

- 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**.

Note: 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

2.45. 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.

The report is based on the following collector:

- 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**.

Note: 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

2.46. 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.

The report is based on the following collector:

- JOURNAL_KF

PASS = KF journal entries were not found in QAUDJRN.

FAIL = KF journal entries were found in QAUDJRN.

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

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

2.47. Limit Device Sessions Not Enabled

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

The report is based on the following collector:

- SYSTEM_VALUES

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

FAIL = System value QLMTDEVSSN is set to 0.

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.

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**.

Note: 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

2.48. 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.

The report is based on the following collector:

- LINE_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 **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

2.49. Media Library Status Details

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

The report is based on the following collector:

- 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**.

Note: 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

2.50. Memory Pool Details

This report displays one row for every pool.

The report is based on the following collector:

- 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**.

Note: 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

2.51. 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.

The report is based on the following collector:

- 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

2.52. 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.

The report is based on the following collector:

- 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

2.53. 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.

The report is based on the following collector:

- 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 **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

2.54. 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.

The report is based on the following collector:

- 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

2.55. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

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

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)

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

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

2.56. 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.

The report is based on the following collector:

- JOURNAL_AD

PASS = AD journal entries were not found in QAUDJRN.

FAIL = AD journal entries were found in QAUDJRN.

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.

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

2.57. Object Lock Information

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

The report is based on the following collector:

- 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**.

Note: 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

2.58. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

2.59. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

2.60. 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.

The report is based on the following collector:

- SOFTWARE_RESOURCES

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

2.61. Output Queue Details

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

The report is based on the following collector:

- OUTPUT_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 **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

2.62. 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.

The report is based on the following collector:

- JOURNAL_RO

PASS = RO journal entries were not found in QAUDJRN.

FAIL = RO journal entries were found in QAUDJRN.

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.

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

2.63. Partition Information

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

The report is based on the following collector:

- 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**.

Note: 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

2.64. 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.

The report is based on the following collector:

- 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**.

Note: 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

2.65. 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.

The report is based on the following collector:

- JOURNAL_RZ

PASS = RZ journal entries were not found in QAUDJRN.

FAIL = RZ journal entries were found in QAUDJRN.

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.

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

2.66. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

Configuration Management Reports

2.67. 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.

The report is based on the following collector:

- PRODUCT_INFO

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 **30** (Work with Reports).
3) Press **Enter**.

Note: 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

2.68. Product Registration ID Information

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

The report is based on the following collector:

- PRODUCT_INFO

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

2.69. Products License Information

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

The report is based on the following collector:

- 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**.

Note: 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

2.70. 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.

The report is based on the following collector:

- 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 **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

2.71. Program Changes to Adopt Owner Authority

This report displays 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.

The report is based on the following collector:

- JOURNAL_PA

PASS = PA journal entries were not found in QAUDJRN.

FAIL = PA journal entries were found in QAUDJRN.

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

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 Reports

2.72. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

2.73. Programs Restored that Adopt Owner Authority

This report displays restored programs that inherit 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.

The report is based on the following collector:

- JOURNAL_RP

PASS = RP journal entries were not found in QAUDJRN.

FAIL = RP journal entries were found in QAUDJRN.

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

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

2.74. 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.

The report is based on the following collector:

- JOURNAL_AP

PASS = AP journal entries were not found in QAUDJRN.

FAIL = AP journal entries were found in QAUDJRN.

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

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

2.75. 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.

The report is based on the following collector:

- PTF_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** (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

2.76. 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.

The report is based on the following collector:

- PTF_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** (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

2.77. PTFs for WDS

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

The report is based on the following collector:

- PTF_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** (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

2.78. 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.

The report is based on the following collector:

- PTF_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** (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

2.79. 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.

The report is based on the following collector:

- PTF_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** (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

2.80. Record Lock Information

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

The report is based on the following collector:

- 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**.

Note: 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

2.81. Restrict use of Use Adopted Authority

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

The report is based on the following collector:

- SYSTEM_VALUES

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

2.82. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

2.83. Schedule Master File

This report returns the IBM internal job schedule.

The report is based on the following collector:

- 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 **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

2.84. Security Auditing Level

This report displays the security auditing levels.

The report is based on the following collector:

- SYSTEM_VALUES

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**.

Note: 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

2.85. Security System Values

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

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

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

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**.

Note: 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

2.86. Server Security Data is Retained

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

The report is based on the following collector:

- SYSTEM_VALUES

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.

N**ote**: 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

2.87. 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.

The report is based on the following collector:

- JOURNAL_SO

PASS = SO journal entries were not found in QAUDJRN.

FAIL = SO journal entries were found in QAUDJRN.

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

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

2.88. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

2.89. 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.

The report is based on the following collector:

- JOURNAL_ST

PASS = ST journal entries were not found in QAUDJRN.

FAIL = ST journal entries were found in QAUDJRN.

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

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

2.90. Spooled File Functions are Audited

This report displays status of spooled file functions.

The report is based on the following collector:

- SYSTEM_VALUES

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

2.91. 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.

The report is based on the following collector:

- 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**.

Note: 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

2.92. Storage Usage by User Profile

This report displays details about storage by user profile.

The report is based on the following collector:

- 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**.

Note: 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

2.93. Strong System Security Level

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

The report is based on the following collector:

- SYSTEM_VALUES

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

2.94. Subsystem Autostart Details

This report displays subsystem description information for autostart job entries.

The report is based on the following collector:

- SUBSYSTEM_AUTOSTART

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

2.95. Subsystem Communication Details

This report displays subsystem description information for communication entries.

The report is based on the following collector:

- 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

2.96. Subsystem Information Details

This report displays general subsystem description information.

The report is based on the following collector:

- 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

2.97. Subsystem Job Queue Details

This report displays subsystem description information for job queue entries.

The report is based on the following collector:

- 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

2.98. Subsystem Pool Data Details

This report displays subsystem description information for pool definitions.

The report is based on the following collector:

- 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

2.99. Subsystem Prestart Job Details

This report displays subsystem description information for prestart job entries.

The report is based on the following collector:

- SUBSYSTEM_PRESTART

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

2.100. Subsystem Remote Entries

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

The report is based on the following collector:

- SUBSYSTEM_REMOTE

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

2.101. Subsystem Routing Entries

This report displays subsystem description information for routing entries.

The report is based on the following collector:

- SUBSYSTEM_ROUTING

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

2.102. Subsystem Routing Entry Changes

This report displays changes of 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.

The report is based on the following collector:

- JOURNAL_SE

PASS = SE journal entries were not found in QAUDJRN.

FAIL = SE journal entries were found in QAUDJRN.

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

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

2.103. Subsystem Workstation Names

This report displays subsystem description information for workstation name entries.

The report is based on the following collector:

- 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

2.104. Subsystem Workstation Types

This report displays subsystem description information for workstation type entries.

The report is based on the following collector:

- 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

2.105. 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.

The report is based on the following collector:

- PTF_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** (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

2.106. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

2.107. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

2.108. System Software Resources

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

The report is based on the following collector:

- SOFTWARE_RESOURCES

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

2.109. System Value Changes

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

The report is based on the following collector:

- JOURNAL_SE

PASS = SV journal entries were not found in QAUDJRN.

FAIL = SV journal entries were found in QAUDJRN.

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

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

2.110. 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.

The report is based on the following collector:

- JOURNAL_SM

PASS = SM journal entries were not found in QAUDJRN.

FAIL = SM journal entries were found in QAUDJRN.

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

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

2.111. 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.

The report is based on the following collector:

- SYSTEM_VALUES

See also

Configuration Management Reports

2.112. 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.

The report is based on the following collector:

- JOURNAL_CP

PASS = CP Journal entries were not found in QAUDJRN.

FAIL = CP Journal entries were found in QAUDJRN.

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

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

2.113. User Profile Information

This report displays information about user profiles.

The report is based on the following collector:

- QSYS2.USER_INF

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**.

Note: 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

3. Network Management Reports

This section of reports provides details on potential security vulnerabilities related to network access to your system.

- Actions to IP Rules
- APPN Endpoint Filter Violations
- Asynchronous Signals Processed
- Authority Failures
- Cluster Operations
- Connection Verifications
- 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 Request Report
- Device Description Details
- Device Descriptions - *APPC
- DNS Configuration Details
- Integrated File System Exits Installed
- Internet Security Management Events
- Inter-process Communication Events
- Intrusion Monitor Events
- Network Attribute Changes
- 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
- Service Status Change Events
- Sockets-related Exit Points Not Secured
- SSL Cipher List and Specification List

- TCP/IP IPv4 Stack Attributes
- TCP/IP IPv6 Stack Attributes
- Unsecured Remote Server Exit Points

3.1. Actions to IP Rules

This report displays actions to IP Rules. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is IR.

The report is based on the following collector:

- JOURNAL_IR

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.

The following are event types:

- 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 search for any report using the **Work with Reports** (TGWRKRPT) interface.

See also

Network Management Reports

3.2. 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.

The report is based on the following collector:

- JOURNAL_NE

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

See also

Network Management Reports

3.3. 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.

The report is based on the following collector:

- JOURNAL_SG

PASS = SG journal entries were not found in QAUDJRN.

FAIL = SG journal entries were found in QAUDJRN.

For SG journal entries to be generated, the QAUDLVL system value must contain *JOBDTA.

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

See also

Network Management Reports

3.4. Authority Failures

This report displays authority failures that have occurred on the system. The data displayed in this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with these events is AF.

The report is based on the following collector:

- JOURNAL_AF

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.

The following are 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

See also

Network Management Reports

3.5. 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.

The report is based on the following collector:

- JOURNAL_CU

PASS = CU journal entries were not found in QAUDJRN.

FAIL = CU journal entries were found in QAUDJRN.

For CU journal entries to be generated, the QAUDLVL system value must contain *NETCLU and *NETCMN.

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

See also

Network Management Reports

3.6. 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.

The report is based on the following collector:

- JOURNAL_CV

PASS = CV journal entries were not found in QAUDJRN.

FAIL = CV journal entries were found in QAUDJRN.

For CV journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL, *NETBAS, *NETCMN, and *SECURITY.

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 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

Network Management Reports

3.7. Connections Started, Ended, or Rejected

This report displays information for connections that were started, ended, or rejected 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 VC.

The report is based on the following collector:

- JOURNAL_VC

PASS = VC journal entries were not found in QAUDJRN.

FAIL = VC journal entries were found in QAUDJRN.

For VC journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL and *JOBDTA.

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

See also

Network Management Reports

3.8. Controller Description Details

This report displays information about controller descriptions available on the system.

The report is based on the following collector:

- 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 search for any report using the **Work with Reports** (TGWRKRPT) interface.

See also

Network Management Reports

3.9. Controllers and Attached Devices

This report displays information about controller descriptions on the system and the related devices attached to each controller description.

The report is based on the following collector:

- 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 search for any report using the **Work with Reports** (TGWRKRPT) interface.

See also

Network Management Reports

3.10. Database Server Initialization Report

This report displays DB server transactions of type DBINIT - Perform server initiation.

The report is based on the following collectors:

- NETWORK_TRANS_DATABASE
- NETWORK_TRANSACTIONS_DATABASE

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**.

Note: 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

3.11. Database Server Native DB Report

This report displays DB server transactions of type DBNDB - Perform native database request.

The report is based on the following collectors:

- NETWORK_TRANS_DATABASE
- NETWORK_TRANSACTIONS_DATABASE

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**.

Note: 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

3.12. Database Server Object Info Report

This report displays DB server transactions of type DBROI - Retrieve object information and catalog function.

The report is based on the following collectors:

- NETWORK_TRANS_DATABASE
- NETWORK_TRANSACTIONS_DATABASE

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**.

Note: 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

3.13. Database Server SQL Request Report

This report displays DB server transactions of type DBSQL - Perform SQL requests

The report is based on the following collectors:

- NETWORK_TRANS_DATABASE
- NETWORK_TRANSACTIONS_DATABASE

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**.

Note: 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

3.14. Device Description Details

This report displays information about device descriptions configured on the system.

The report is based on the following collector:

- 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 search for any report using the **Work with Reports** (TGWRKRPT) interface.

See also

Network Management Reports

3.15. Device Descriptions - *APPC

This report displays details about *APPC device descriptions configured on the system. *APPC devices are for advanced program-to-program communications.

The report is based on the following collector:

- 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 search for any report using the **Work with Reports** (TGWRKRPT) interface.

See also

Network Management Reports

3.16. DNS Configuration Details

This report displays the DNS configuration of the system.

The report is based on the following collector:

- NETWORK_TCPIP_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 **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 search for any report using the **Work with Reports** (TGWRKRPT) interface.

See also

Network Management Reports

3.17. 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.

The report is based on the following collector:

- EXIT_POINTS

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**.

Note: 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

3.18. Internet Security Management Events

This report displays information about Internet Security Management 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 IS.

The report is based on the following collector:

- JOURNAL_IS

PASS = IS journal entries were not found in QAUDJRN.

FAIL = IS journal entries were found in QAUDJRN.

For IS journal entries to be generated, the QAUDLVL system value must contain *NETBAS and *NETCMN.

The following are 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 search for any report using the **Work with Reports** (TGWRKRPT) interface.

See also

Network Management Reports

3.19. 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.

The report is based on the following collector:

- JOURNAL_IP

PASS = IP journal entries were not found in QAUDJRN.

FAIL = IP journal entries were found in QAUDJRN.

For IP journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL, *SECIPC, and *SECURITY.

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

See also

Network Management Reports

3.20. Intrusion Monitor Events

This report displays information about Intrusion Monitor 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 IM.

The report is based on the following collector:

- JOURNAL_IM

PASS = IM journal entries were not found in QAUDJRN.

FAIL = IM journal entries were found in QAUDJRN.

For IM journal entries to be generated, the QAUDLVL system value must contain *ATNEVT.

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

See also

Network Management Reports

3.21. 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.

The report is based on the following collector:

- JOURNAL_NA

PASS = NA journal entries were not found in QAUDJRN.

FAIL = NA journal entries were found in QAUDJRN.

For NA journal entries to be generated, the QAUDLVL system value must contain *SECCFG and *SECURITY.

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

Network Management Reports

3.22. 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.

The report is based on the following collector:

- NETWORK_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 **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 search for any report using the **Work with Reports** (TGWRKRPT) interface.

See also

Network Management Reports

3.23. 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.

The report is based on the following collector:

- JOURNAL_X0

PASS = X0 journal entries were not found in QAUDJRN.

FAIL = X0 Journal entries were found in QAUDJRN.

For X0 journal entries to be generated, the QAUDLVL system value must contain *SECNAS and *SECURITY.

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

See also

Network Management Reports

3.24. Network Connection Details

This report displays information about network connections to the system. The data is similar to netstat data, showing details such as local and remote IP addresses, port numbers, server information, SSL enabled status, TCP state, and connection type information.

The report is based on the following collector:

- NETWORK_CONNECTIONS

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

See also

Network Management Reports

3.25. Network Interface Details IPv4

This report displays IPv4 network interface information for the system.

The report is based on the following collector:

- 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 search for any report using the **Work with Reports** (TGWRKRPT) interface.

See also

Network Management Reports

3.26. Network Interface Details IPv6

This report displays IPv6 network interface information for the system.

The report is based on the following collector:

- 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 **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 search for any report using the **Work with Reports** (TGWRKRPT) interface.

See also

Network Management Reports

3.27. Network Route Details IPv4

This report displays IPv4 routing information on the system.

The report is based on the following collector:

- NETWORK_ROUTE_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 search for any report using the **Work with Reports** (TGWRKRPT) interface.

See also

Network Management Reports

3.28. Network Route Details IPv6

This report displays IPv6 routing information on the system.

The report is based on the following collector:

- NETWORK_ROUTE_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 search for any report using the **Work with Reports** (TGWRKRPT) interface.

See also

Network Management Reports

3.29. Network Server Descriptions

This report displays information about network server descriptions defined on the system.

The report is based on the following collector:

- 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 search for any report using the **Work with Reports** (TGWRKRPT) interface.

See also

Network Management Reports

3.30. Network Server Encryption Status

This report displays information about remote servers and whether or not communication to those servers is encrypted.

The report is based on the following collector:

- NETWORK_SVR_ENCRYPT_STATUS

See also

Network Management Reports

3.31. Network Servers with Encryption Verified

This report displays remote servers on the system that are able to complete a successful SSL handshake.

The report is based on the following collector:

- NETWORK_SVR_ENCRYPT_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 **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 search for any report using the **Work with Reports** (TGWRKRPT) interface.

See also

Network Management Reports

3.32. 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.

The report is based on the following collector:

- NETWORK_SVR_ENCRYPT_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 **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 search for any report using the **Work with Reports** (TGWRKRPT) interface.

See also

Network Management Reports

3.33. 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.

The report is based on the following collector:

- JOURNAL_OM

PASS = OM journal entries were not found in QAUDJRN.

FAIL = OM journal entries were found in QAUDJRN.

For OM journal entries to be generated, the QAUDLVL system value must contain *OBJMGT.

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

See also

Resource Management Reports

3.34. 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.

The report is based on the following collector:

- JOURNAL_ML

PASS = ML Journal entries were not found in QAUDJRN.

FAIL = ML Journal entries were found in QAUDJRN.

For ML journal entries to be generated, the QAUDLVL system value must contain *OFCSRV.

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

See also

Network Management Reports

3.35. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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**.

Note: 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

3.36. Remote Service Attribute

This report displays the value of the QRMTSRVATR (Remote Service Attribute) system value if a vulnerability is found.

The report is based on the following collector:

- SYSTEM_VALUES

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**.

Note: 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

3.37. Remote Sign-on Control

This report displays the value of the QRMTSIGN (Remote Sign-on Control) system value if a vulnerability is found.

The report is based on the following collector:

- SYSTEM_VALUES

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

See also

Network Management Reports

3.38. 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.

The report is based on the following collector:

- JOURNAL_SK

PASS = SK journal entries were not found in QAUDJRN.

FAIL = SK journal entries were found in QAUDJRN.

For SK journal entries to be generated, the QAUDLVL system value must contain *NETCMN, *NETFAIL, and *NETSCK.

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

See also

Network Management Reports

3.39. 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.

The report is based on the following collector:

- JOURNAL_VS

FAIL = VS journal entries were found in QAUDJRN.

For VS journal entries to be generated, the QAUDLVL system value must contain *JOBDTA.

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

See also

Network Management Reports

3.40. Service Status Change Events

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

The report is based on the following collector:

- JOURNAL_VV

PASS = VV Journal entries were not found in QAUDJRN.

FAIL = VV Journal entries were found in QAUDJRN.

For VV journal entries to be generated, the QAUDLVL system value must contain *SERVICE.

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

See also

Network Management Reports

3.41. Sockets-related Exit Points Not Secured

This report evaluates whether or not exit programs are installed on the sockets-related exit points.

The report is based on the following collector:

- EXIT_POINTS

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 sockets-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 sockets-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 sockets-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 search for any report using the **Work with Reports** (TGWRKRPT) interface.

See also

Network Management Reports

3.42. SSL Cipher List 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

See also

Network Management Reports

3.43. TCP/IP IPv4 Stack Attributes

This report displays TCP/IP stack attribute information for IPv4 communication.

The report is based on the following collector:

- NETWORK_TCPIP_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 **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 search for any report using the **Work with Reports** (TGWRKRPT) interface.

See also

Network Management Reports

3.44. TCP/IP IPv6 Stack Attributes

This report displays TCP/IP stack attribute information for IPv6 communication.

The report is based on the following collector:

- NETWORK_TCPIP_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 **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 search for any report using the **Work with Reports** (TGWRKRPT) interface.

See also

Network Management Reports

3.45. Unsecured Remote Server Exit Points

This report evaluates whether or not exit programs are installed on remote server exit points.

The report is based on the following collector:

- EXIT_POINTS

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

See also

Network Management Reports

4. Profile Management Reports

This section of reports provides details on potential security vulnerabilities related to user profiles on your system.

- All User Profiles
- Authority Failures
- Authority Restored for User Profiles
- Authorization Lists with Public Access
- Block Password Change
- Changes to Service Tools Profiles
- Connection Verifications
- Directory Server Extensions
- Disable Profile After Maximum Failed Sign-on 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 Logon and Logoff Events
- Network Password Errors
- Network Profile Changes
- Object Authorities of User Profiles
- Ownership Changes for Restored Objects
- Password Expiration Interval
- Password Expiration Warning
- Password Level
- Password Rules
- Password Security Reports
- 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

4.1. All User Profiles

This report displays a list of all the user profiles that exist on the system and their associated settings.

The report is based on the following collector:

- USER_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 **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

4.2. 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.

The report is based on the following collector:

- JOURNAL_AF

PASS = AF journal entries were not found in QAUDJRN.

FAIL = AF journal entries were found in QAUDJRN.

For AF journal entries to be generated, the QAUDLVL system value must contain *SAVRST.

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

4.3. 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.

The report is based on the following collector:

- JOURNAL_RU

PASS = RU journal entries were not found in QAUDJRN.

FAIL = RU journal entries were found in QAUDJRN.

For RU journal entries to be generated, the QAUDLVL system value must contain *SAVRST.

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

4.4. Authorization Lists with Public Access

This report displays public access information for authority 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 CA.

The report is based on the following collector:

- JOURNAL_CA

See also

Profile Management Reports

4.5. Block Password Change

This report displays the value of the QPWDCHGBLK (Block Password Change) system value if a vulnerability is found.

The report is based on the following collector:

- JOURNAL_CA

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

4.6. 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.

The report is based on the following collector:

- JOURNAL_DS

PASS = DS journal entries were not found in QAUDJRN.

FAIL = DS journal entries were found in QAUDJRN.

For DS journal entries to be generated, the QAUDLVL system value must contain *SECCFG and *SECURITY.

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

4.7. Connection Verifications

This report displays connection verifications. 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.

The report is based on the following collector:

- JOURNAL_CV

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**.

Note: 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

4.8. Directory Server Extensions

This report displays 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.

The report is based on the following collector:

- JOURNAL_XD

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**.

Note: 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

4.9. 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).

The report is based on the following collector:

- SYSTEM_VALUES

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**.

Note: 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

4.10. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

4.11. 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.

The report is based on the following collector:

- USER_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

4.12. 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.)

The report is based on the following collector:

- JOURNAL_VL

PASS = VL journal entries were not found in QAUDJRN.

FAIL = VL journal entries were found in QAUDJRN.

For VL journal entries to be generated, the QAUDLVL system value must contain *SYSMGT.

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

4.13. 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.

The report is based on the following collector:

- USER_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

4.14. 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.

The report is based on the following collector:

- USER_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 **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

4.15. 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.

The report is based on the following collector:

- USER_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 **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

4.16. IBM Profile Details Report

This report displays configuration information for the Q* IBM user profiles on the system.

The report is based on the following collector:

- USER_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 **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

4.17. 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.

The report is based on the following collector:

- JOURNAL_X1

PASS = X1 journal entries were not found in QAUDJRN.

FAIL = X1 journal entries were found in QAUDJRN.

For X1 journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL, *SECURITY, and *SECVFY.

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

4.18. Inactive Job Message Queue

This report displays the value of the QINACTMSGQ (Inactive Job Message Queue) system value if a vulnerability is found.

The report is based on the following collector:

- SYSTEM_VALUES

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**.

Note: 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

4.19. Inactive Job Time-out

This report displays the value of the QINACTITV (Inactive Job Time-out) system value if the value is *NONE.

The report is based on the following collector:

- SYSTEM_VALUES

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.

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**.

Note: 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

4.20. 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.

The report is based on the following collector:

- JOURNAL_PW

PASS = PW Journal entries were not found in QAUDJRN.

FAIL = PW Journal entries were found in QAUDJRN.

For PW journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL.

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 user profile is disabled.
- R - Attempted sign-on (user authentication) failed because 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

4.21. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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

4.22. Limit Characters in Password

This report displays the value of the QPWDLMTCHR (Limit Characters in Password) system value if a vulnerability is found.

The report is based on the following collector:

- SYSTEM_VALUES

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

4.23. Limit Password Character Positions

This report displays the value of the QPWDPOSDIF (Limit Password Character Positions) system value if a vulnerability is found.

The report is based on the following collector:

- SYSTEM_VALUES

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).

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

4.24. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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.)

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

4.25. Limit Security Officer Device Access

This report displays the value of the Limit Security Officer Device Access (QLMTSECOFR) system value.

The report is based on the following collector:

- SYSTEM_VALUES

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**.

Note: 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

4.26. Maximum Password Length

This report displays the value of the QPWDMAXLEN (Maximum Password Length) system value if a vulnerability is found.

The report is based on the following collector:

- SYSTEM_VALUES

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.

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

4.27. Minimum Password Length

This report displays the value of the QPWDMINLEN (Minimum Password Length) system value if the value is less than 7.

The report is based on the following collector:

- SYSTEM_VALUES

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.

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

4.28. Network Attribute Changes

This report displays changes made to network attributes.

The report is based on the following collector:

- JOURNAL_NA

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**.

Note: 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

4.29. 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.)

The report is based on the following collector:

- JOURNAL_VN

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

4.30. 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.

The report is based on the following collector:

- JOURNAL_VP

PASS = VP journal entries were not found in QAUDJRN.

FAIL = VP journal entries were found in QAUDJRN.

For VP journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL.

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

4.31. 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.

The report is based on the following collector:

- JOURNAL_VU

PASS = VU journal entries were not found in QAUDJRN.

FAIL = VU journal entries were found in QAUDJRN.

For VU journal entries to be generated, the QAUDLVL system value must contain *SECCFG and *SECURITY.

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

4.32. Object Authorities of User Profiles

This report displays the object authorities of all user profile objects on the system.

The report is based on the following collector:

- USER_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

4.33. Ownership Changes for Restored Objects

This report displays changes to object ownership.

The report is based on the following collector:

- JOURNAL_RO

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**.

Note: 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

4.34. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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).

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

4.35. Password Expiration Warning

This report displays the value of the QPWDEXPWRN (Password Expiration Warning) system value if the value is less than 14.

The report is based on the following collector:

- SYSTEM_VALUES

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.

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

4.36. Password Level

This report displays the value of the QPWDLVL (Password Level) system value if the value is set to 0.

The report is based on the following collector:

- SYSTEM_VALUES

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

4.37. Password Rules

This report displays the value of the QPWDRULES (Password Rules) system value if the value is not *PWDSYSVAL.

The report is based on the following collector:

- SYSTEM_VALUES

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.

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

4.38. Password Security Reports

Password Security Reports provide information on the security configuration for passwords on your system. There are many system values and system settings that can put controls in place to enhance the security of passwords on your system. These reports evaluate these settings and determine if the configuration is strong.

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**.

Note: 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

4.39. Password Validation Program

This report displays the value of the QPWDVLDPGM (Password Validation Program) system value if the value is not *NONE.

The report is based on the following collector:

- SYSTEM_VALUES

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.

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

4.40. 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.

The report is based on the following collector:

- USER_PROFILES

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. The special authorities available are:

- *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

It is highly 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

4.41. Profile Object Auditing Values

This report displays profile information for users that have object auditing turned on.

The report is based on the following collector:

- USER_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 **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

4.42. 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.

The report is based on the following collector:

- USER_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 **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

4.43. 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.

The report is based on the following collector:

- USER_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 **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

4.44. 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.

The report is based on the following collector:

- USER_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 **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

4.45. 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.

The report is based on the following collector:

- USER_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 **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

4.46. 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.

The report is based on the following collector:

- USER_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 **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

4.47. 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.

The report is based on the following collector:

- USER_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 **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

4.48. 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.

The report is based on the following collector:

- USER_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 **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

4.49. 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.

The report is based on the following collector:

- SYSTEM_VALUES

PASS = System value QPWDRQDDGT is not set to 0.

FAIL = System value QPWDRQDDGT is set to 0.

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.

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

4.50. Security Officer Profiles

This report displays user profile information about user profiles with security officer (*SECOFR) user class.

The report is based on the following collector:

- USER_PROFILES

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.

User profiles with security officer class authority typically have all object authority and have little to no restrictions on the system.

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

4.51. Service Tool Security Attributes

This report returns the attributes of the service tool.

Note: This report is only available for OS 7.4 or higher.

The report is based on the following collector:

- 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

4.52. 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.

The report is based on the following collector:

- JOURNAL_PS

PASS = PS journal entries were not found in QAUDJRN.

FAIL = PS journal entries were found in QAUDJRN.

For PS journal entries to be generated, the QAUDLVL system value must contain *SECURITY and *SECVFY.

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

4.53. System Service Tools Users

This report lists detailed information, including status and privileges, of System Service Tools (SST) users that are not system-supplied.

The report is based on the following collector:

- SYSTEM_TOOL_USERS

PASS = One additional SST user exists on the system.

FAIL = Many additional SST users exist on the system.

SST allows you to work with system-level tools. Tasks such as adding or removing disk units can be done through SST.

The following are possible 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

4.54. 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.

The report is based on the following collector:

- USER_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 **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

4.55. 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.

The report is based on the following collector:

- USER_PROFILES

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 left over 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.

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

4.56. Users with Job Control Special Authority

This report displays user profile information for users with Job Control (*JOBCTL) special authority.

The report is based on the following collector:

- USER_PROFILES

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.

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

4.57. Users with Save System Special Authority

This report displays user profile information for users that have the Save System (*SAVSYS) special authority.

The report is based on the following collector:

- USER_PROFILES

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.

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

4.58. 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.

The report is based on the following collector:

- USER_PROFILES

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.

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

5. Resource Management Reports

This section of reports provides details on potential security vulnerabilities related to resources on your system.

- *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
- Authority Collection for IFS Objects
- Authority Collection for Native Objects
- Authorization List Details
- Authorization Lists with Public Access
- Authorized Users through Authorization Lists
- Change Request Descriptors Restored
- Close Operations on Server Files
- Commands Available in QSH
- Commands Executed
- Configuration Files
- Create Operations
- 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 Over 1000 Delete Operations
- Db2 Mirror Communication Services
- Db2 Mirror Product Services
- Db2 Mirror Replication Services
- Db2 Mirror Replication State
- Db2 Mirror Setup Tool
- 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 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
- 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
- Object Authority
- Object Changes
- Object Details
- Object Management Changes
- Object Ownership Changes
- Object Reads
- Objects Restored
- 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
- Row and Column Access Control
- Single Optical Object Accesses
- Socket Descriptor Details
- Spooled File Actions
- System Directory Changes
- System Security Audit Journal Exists
- TGAudit Report Configuration
- TGCentral Agent Configuration
- User-defined File Systems (UDFS's)
- Verify Object on Restore

*5.1. *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.

The report is based on the following collector:

- IFS_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 **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

5.2. 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.

The report is based on the following collector:

- JOURNAL_VO

PASS = VO journal entries were not found in QAUDJRN.

FAIL = VO journal entries were found in QAUDJRN.

For VO journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL, *SECURITY, and *SECVLDL.

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

5.3. Allow Object Restore Option

This report displays the value of the QALWOBJRST (Allow Object Restore Option) system value if a vulnerability is found.

The report is based on the following collector:

- SYSTEM_VALUES

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.

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**.

Note: 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

5.4. 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.

The report is based on the following collector:

- SYSTEM_VALUES

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.

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**.

Note: 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

5.5. 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.

The report is based on the following collector:

- IFS_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 **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

5.6. Attributes for /QSYS.LIB

This report displays attributes of objects found in QSYS.LIB.

The report is based on the following collector:

- IFS_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

5.7. Authority Collection for IFS Objects

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.

The report is based on the following collector:

- AUTHORITIES_COLLECTION

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 **25** (Authority Collection for IFS 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

Resource Management Reports

5.8. Authority Collection for Native Objects

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.

The report is based on the following collector:

- AUTHORITIES_COLLECTION

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 **7** (Authority Collection for Native 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

Resource Management Reports

5.9. Authorization List Details

This report displays all authorization lists that exist on the system.

The report is based on the following collector:

- AUTHORITIES_LIST

PASS = N/A

FAIL = N/A

Unnecessary authorization lists should be deleted. Verify the necessary authorization lists are used to secure sensitive 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 **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

5.10. Authorization Lists with Public Access

This report displays authorization lists that do not have *PUBLIC authority set to *EXCLUDE.

The report is based on the following collector:

- AUTHORITIES_LIST

PASS = *PUBLIC authority for authorization lists is set to *EXCLUDE.

FAIL = *PUBLIC authority for authorization lists is not set to *EXCLUDE.

*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

5.11. 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.

The report is based on the following collector:

- 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**.

Note: 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

5.12. Change Request Descriptors Restored

This report displays all restored change request descriptors.

The report is based on the following collector:

- JOURNAL_RQ

For RQ 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**.

Note: 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

5.13. 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.

The report is based on the following collector:

- JOURNAL_VF

PASS = VF journal entries were not found in QAUDJRN.

FAIL = VF journal entries were found in QAUDJRN.

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.

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

Resource Management Reports

5.14. Commands Available in QSH

This report displays all binary commands available in the QSH and PASE environments. These commands are Unix operating system commands.

The report is based on the following collector:

- IFS_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 **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

5.15. 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.

The report is based on the following collector:

- JOURNAL_CD

PASS = CD journal entries were not found in QAUDJRN.

FAIL = CD journal entries were found in QAUDJRN.

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.

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

5.16. 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.

The report is based on the following collector:

- IFS_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 **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

5.17. 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.

The report is based on the following collector:

- JOURNAL_CO

PASS = CO journal entries were not found in QAUDJRN.

FAIL = CO journal entries were found in QAUDJRN.

For CO journal entries to be generated, the QAUDLVL system value must contain *CREATE.

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

5.18. Database Files Larger than 100Mb

This report returns database files with over 100,000 delete operations.

The report is based on the following collector:

- SYSTABLESTAT

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**.

Note: 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

5.19. Database Files with Over 1,000,000 Read Operations

This report returns database files larger with over 100,000 read operations.

The report is based on the following collector:

- SYSTABLESTAT

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**.

Note: 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

5.20. Database Files with Over 100,000 Delete Operations

This report returns database files larger with over 100,000 delete operations.

The report is based on the following collector:

- SYSTABLESTAT

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**.

Note: 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

5.21. Database Files with Over 100,000 Insert Operations

This report returns database files larger with over 100,000 insert operations.

The report is based on the following collector:

- SYSTABLESTAT

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**.

Note: 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

5.22. Database Files with Over 1,000 Delete Operations

This report returns database files larger with over 1,000 delete operations.

The report is based on the following collector:

- SYSTABLESTAT

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**.

Note: 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

5.23. Db2 Mirror Communication Services

This report returns Db2 mirror communication services details

The report is based on the following collector:

- JOURNAL_M6

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

5.24. Db2 Mirror Product Services

This report returns Db2 mirror product services details

Note: This report is only available for OS 7.4 or higher.

The report is based on the following collector:

- JOURNAL_M8

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

5.25. Db2 Mirror Replication Services

This report returns Db2 mirror replication services details.

Note: This report is only available for OS 7.4 or higher.

The report is based on the following collector:

- JOURNAL_M7

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

5.26. Db2 Mirror Replication State

This report returns Db2 mirror replication state details.

Note: This report is only available for OS 7.4 or higher.

The report is based on the following collector:

- JOURNAL_M9

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

5.27. Db2 Mirror Setup Tools

This report returns the Db2 mirror setup tool details.

Note: This report is only available for OS 7.4 or higher.

The report is based on the following collector:

- JOURNAL_M0

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

5.28. 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.

The report is based on the following collector:

- JOURNAL_DO

PASS = DO journal entries were not found in QAUDJRN.

FAIL = DO journal entries were found in QAUDJRN.

For DO journal entries to be generated, the QAUDLVL system value must contain *DELETE, *SECCFG, and *SECURITY.

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

5.29. Directory Link, Unlink, and Search Operations

This report displays 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.

The report is based on the following collector:

- JOURNAL_LD

PASS = LD journal entries were not found in QAUDJRN.

FAIL = LD journal entries were found in QAUDJRN.

For LD journal entries to be generated, object auditing must be turned on for directories by using the CHGAUD command.

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

Resource Management Reports

5.30. 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.

The report is based on the following collector:

- JOURNAL_ND

PASS = ND journal entries were not found in QAUDJRN.

FAIL = ND journal entries were found in QAUDJRN.

For ND journal entries to be generated, the QAUDLVL system value must contain *NETBAS and *NETCMN.

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

5.31. DLO Object Changes

This report displays change details for DLO objects. The data related to this report is retrieved from system security audit journal (QAUDJRN). The journal entry type associated with this event is YC.

The report is based on the following collector:

- JOURNAL_YC

PASS = YC journal entries were not found in QAUDJRN.

FAIL = YC journal entries were found in QAUDJRN.

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.

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

5.32. 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.

The report is based on the following collector:

- JOURNAL_YR

PASS = YR journal entries were not found in QAUDJRN.

FAIL = YR journal entries were found in QAUDJRN.

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.

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

5.33. 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.

The report is based on the following collector:

- JOURNAL_02

PASS = 02 journal entries were not found in QAUDJRN.

FAIL = O2 journal entries were found in QAUDJRN.

For O2 journal entries to be generated, the QAUDLVL system value must contain *OPTICAL.

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

5.34. 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.

The report is based on the following collector:

- JOURNAL_GR

PASS = GR journal entries were not found in QAUDJRN.

FAIL = GR journal entries were found in QAUDJRN.

For GR journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL, *SECCFG, and *SECURITY.

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

5.35. File Statistics

This report contains the list of statistics related to an object.

The report is based on the following collector:

- TGMOBJINF

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 *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

5.36. 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.

The report is based on the following collector:

- IFS_ATTRIBUTES

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 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

5.37. 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.

The report is based on the following collector:

- IFS_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 **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

5.38. 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.

The report is based on the following collector:

- IFS_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 **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

5.39. 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. The *RWX allows all operations on the object except those that are limited to the owner or controlled by the object rights. The IFS uses *R, *W, and *X authorities to grant read, write, and execute rights respectively. They can be combined, so *RWX gives the equivalent of *ALL authority.

The report is based on the following collector:

- IFS_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 **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

5.40. HTTP Server and Web Files Status

This report displays status information for the HTTP server and related web files in the "/www" directory.

The report is based on the following collector:

- IFS_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

5.41. HTTP Server File Authorities

This report displays authorities for files in the "/www" IFS folder.

The report is based on the following collector:

- IFS_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 **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

5.42. IFS Directory Information

This report displays all the directories on the Integrated File System (IFS). Only objects with type *DIR will be shown.

The report is based on the following collector:

- IFS_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 **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

5.43. IFS Files Being Journaled

This report displays the extended journaling information for objects.

The report is based on the following collector:

- IFS_JOURNALING

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

5.44. Integrated File System Content

This report returns content from the Integrated File System (IFS).

The report is based on the following collector:

- DATABASE_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

5.45. Integrated File System Security

This report displays the value of the QSCANFSCTL (Scan File Systems) system value if a vulnerability is found.

The report is based on the following collector:

- SYSTEM_VALUES

PASS = System value QSCANFS is not set to *NONE.

FAIL = System value QSCANFS is set to *NONE.

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, the i5/OS IFS is a good hiding place for viruses.

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.

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

5.46. 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.

The report is based on the following collector:

- JOURNAL_JS

PASS = JS journal entries were not found in QAUDJRN.

FAIL = JS journal entries were found in QAUDJRN.

For JS journal entries to be generated, the QAUDLVL system value must contain *JOBBAS, *JOBCHGUSR, and *JOBDTA.

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

5.47. Job Descriptions - USER Parameter Changes

This report displays user parameter changes.

The report is based on the following collector:

- JOURNAL_JD

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**.

Note: 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

5.48. Largest Files Report > 100Mb

This report displays stream files that are larger than 100Mb.

The report is based on the following collector:

- IFS_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 **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

5.49. LDAP Operations

This report displays 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.

The report is based on the following collector:

- JOURNAL_DI

For DI journal entries to be generated, the QAUDLVL system value must contain:

- *AUTFAIL
- *CREATE
- *DELETE
- *OBJMGT
- *SECDIRSRV
- *SECURITY
- *SYSMGT

PASS = DI journal entries were not found in QAUDJRN.

FAIL = DI journal entries were found in QAUDJRN.

Object Auditing should also be enabled by using the CHGOBJAUD command.

Types of LDAP operations:

- CI - Create 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

5.50. 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.

The report is based on the following collector:

- OBJECT_DETAILS

T**o run this report**

1) Access the TGAudit **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**.

Note: 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

5.51. Library Statistics

This report contains the list of statistics related to a library.

The report is based on the following collector:

- TGMOBJINF

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: *LIB
OBJOWNER	Owner of objefct
OBJDEFINER	Creator of object
OBJCREATED	Date on which object was created
OBJSIZE	Size of object
OBJTEXT	Description of object

See also

Resource Management Reports

5.52. 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.

The report is based on the following collector:

- SYSTEM_VALUES

PASS = System value QMAXSIGN is set to a value other than *NOMAX.

FAIL = System value QMAXSIGN is set to *NOMAX.

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.

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**.

Note: 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

5.53. 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.

The report is based on the following collector:

- JOURNAL_VR

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

5.54. Object Authority

This report contains the list of details related to an authority object.

The report is based on the following collector:

- OBJECT_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 **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

5.55. 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.

The report is based on the following collector:

- JOURNAL_ZC

PASS = ZC journal entries were not found in QAUDJRN.

FAIL = ZC journal entries were found in QAUDJRN.

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.

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

5.56. Object Details

This report contains the list of details related to system objects.

The report is based on the following collector:

- OBJECT_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 **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

5.57. 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.

The report is based on the following collector:

- JOURNAL_OM

PASS = OM journal entries were not found in QAUDJRN.

FAIL = OM journal entries were found in QAUDJRN.

For OM journal entries to be generated, the QAUDLVL system value must contain *OBJMGT.

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

See also

Resource Management Reports

5.58. 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.

The report is based on the following collector:

- JOURNAL_OW

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

5.59. Object Reads

This report displays read operations of 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.

The report is based on the following collector:

- JOURNAL_ZR

PASS = ZR journal entries were not found in QAUDJRN.

FAIL = ZR journal entries were found in QAUDJRN.

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.

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

5.60. Object Statistics

This report contains the list of statistics related to an object.

The report is based on the following collector:

- TGMOBJINF

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: *CMD - Command *CLS - Class *DTAARA - Data area *FILE - File *JOBD - Job description *JOBQ - Job queue *JRNRCV - Journal receiver *MODULE - Module *OUTQ - Output queue *PGM - Program *SBSD - Subsystem description *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

5.61. 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.

The report is based on the following collector:

- JOURNAL_OR

PASS = OR journal entries were not found in QAUDJRN.

FAIL = OR journal entries were found in QAUDJRN.

For OR journal entries to be generated, the QAUDLVL system value must contain *SAVRST.

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

5.62. 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.

The report is based on the following collector:

- JOURNAL_03

PASS = O3 journal entries were not found in QAUDJRN.

FAIL = O3 journal entries were found in QAUDJRN.

For O3 journal entries to be generated, the QAUDLVL system value must contain *OPTICAL.

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

5.63. 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.

The report is based on the following collector:

- JOURNAL_PG

PASS = PG journal entries were not found in QAUDJRN.

FAIL = PG journal entries were found in QAUDJRN.

For PG journal entries to be generated, the QAUDLVL system value must contain *SECRUN and *SECURITY.

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

5.64. 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.

The report is based on the following collector:

- JOURNAL_PO

PASS = PO journal entries were not found in QAUDJRN.

FAIL = PO journal entries were found in QAUDJRN.

For PO journal entries to be generated, the QAUDLVL system value must contain *PRTDTA.

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

Resource Management Reports

5.65. 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.

The report is based on the following collector:

- 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

5.66. 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.

The report is based on the following collector:

- 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 **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

5.67. 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.

The report is based on the following collector:

- JOURNAL_PU

PASS = PU journal entries were not found in QAUDJRN.

FAIL = PU journal entries were found in QAUDJRN.

For PU journal entries to be generated, the QAUDLVL system value must contain *PTFOBJ.

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

5.68. 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.

The report is based on the following collector:

- JOURNAL_PF

PASS = PF journal entries were not found in QAUDJRN.

FAIL = PF journal entries were found in QAUDJRN.

For PF journal entries to be generated, the QAUDLVL system value must contain *PTFOPR.

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

5.69. 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.

The report is based on the following collector:

- OBJECT_AUTHORITIES

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.

*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.

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**.

Note: 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

5.70. Public Access to Devices

This report displays information about devices that do not have *PUBLIC authority set to *EXCLUDE or *AUTL.

The report is based on the following collector:

- OBJECT_AUTHORITIES

PASS = *PUBLIC authority for devices is set to *EXCLUDE or *AUTL.

FAIL = *PUBLIC authority for devices is not set to *EXCLUDE or *AUTL.

*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.

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**.

Note: 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

5.71. 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.

The report is based on the following collector:

- OBJECT_AUTHORITIES

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.

*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.

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**.

Note: 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

5.72. 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.

The report is based on the following collector:

- OBJECT_AUTHORITIES

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.

*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.

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**.

Note: 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

5.73. 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 (/).

The report is based on the following collector:

- IFS_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 **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

5.74. 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.

The report is based on the following collector:

- JOURNAL_AX

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

5.75. 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.

The report is based on the following collector:

- JOURNAL_01

PASS = 01 journal entries were not found in QAUDJRN.

FAIL = O1 journal entries were found in QAUDJRN.

For O1 journal entries to be generated, the QAUDLVL system value must contain *OPTICAL.

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

5.76. 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.

The report is based on the following collector:

- JOURNAL_GS

PASS = GS journal entries were not found in QAUDJRN.

FAIL = GS journal entries were found in QAUDJRN.

For GS journal entries to be generated, the QAUDLVL system value must contain *SECSCKD and *SECURITY.

Types of entries:

- G - Give descriptor
- R - Received descriptor
- U - Unable to use 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

Resource Management Reports

5.77. 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.

The report is based on the following collector:

- JOURNAL_SF

PASS = SF journal entries were not found in QAUDJRN.

FAIL = SF journal entries were found in QAUDJRN.

For SF journal entries to be generated, the QAUDLVL system value must contain *SPLFDTA.

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

5.78. 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.

The report is based on the following collector:

- JOURNAL_SD

PASS = SD journal entries were not found in QAUDJRN.

FAIL = SD journal entries were found in QAUDJRN.

For SD journal entries to be generated, the QAUDLVL system value must contain *OFCSRV.

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**.

Note: 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

5.79. System Security Audit Journal Exists

This report displays object details for the System Security Audit Journal (QAUDJRN) if it exists on the system.

The report is based on the following collector:

- OBJECT_DETAILS

PASS = System Security Audit Journal exists.

FAIL = System Security Audit Journal does not exist.

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.

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**.

Note: 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

5.80. TGAudit Report Configuration

This report returns TG Audit configuration details.

The report is based on the following collector:

- DATABASE_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 **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

5.81. TGCentral Agent Configuration

This report returns the TG Central configuration details.

The report is based on the following collector:

- DATABASE_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 **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
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

5.82. 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.

This report returns IFS attributes of objects that are *TYPE2 format.

The report is based on the following collector:

- IFS_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 **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

5.83. Verify Object on Restore

This report displays the value of the QVFYOBJRST (Verify Object on Restore) system value if a vulnerability is found.

The report is based on the following collector:

- SYSTEM_VALUES

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. This value applies to objects of types: *CMD, *PGM, *SRVPGM, *SQLPKG and *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.

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**.

Note: 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

6. Log Management Reports

6.1. Job Activity Details

This report displays the activities identified for monitoring by the Job Activity Monitor.

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**.

Note: 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**.

6.2. Job Activity Summary

This report displays a summary of the activities identified for monitoring by the Job Activity Monitor.

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**.

Note: 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**.

7. Appendix

7.1. APPENDIX - Collectors

Collector ID	Collector Name	Collector Category
ACCESS_ESCAL_ACC_CONTROLS	Access Escalation Access Controls	Network
ACCESS_ESCAL_DEFAULTS	Access Escalation Defaults	Network
ACCESS_ESCAL_ENTITLEMENTS	Access Escalation Entitlements	Network
ACCESS_ESCAL_FILE_EDITORS	Access Escalation File Editors	Network
ACCESS_ESCALATION_USAGE	Access Escalation Usage	Network
AUTH_USERS_VIA_AUTH_LISTS	Authorized Users through Authorization Lists	Resource
AUTHORITY_COLLECTION	Authority Collection Data	Journal
AUTHORITY_COMPLIANCE	Authority Compliance	Resource
AUTHORITY_LIST	Authority List Data	System
BLUEPRINT_3RD_PARTY_FILE	Blueprint 3rd Party Integration File	Profile
BLUEPRINT_AUTH_SETTINGS_FILE	Blueprint Authority List Settings File	Profile
BLUEPRINT_MASTER	Blueprint Master	Profile
BLUEPRINT_NON_COMPLIANCE_USER	Blueprint Non-Compliance User Profiles	Profile
BLUEPRINT_OBJECT_AUTH_FILE	Blueprint Object Authority File	Profile
BLUEPRINT_PARAMETER_FILE	Blueprint Parameter File	Profile
CONTROLLER_ATTACHED_DEVICES	Controller Attached Device Information	Network
CONTROLLER_DESCRIPTION_DATA	Controller Description Information	Network
DATA_AREA_AUDITING	Audit data area changes	Network
DATABASE_AUDITING	Monitor Database changes	Network
DATABASE_CONTENT	Database Content	Configuration
DET_ACT_HISTORY	Detect Activity History	Network
DET_CMD_RULES	Command Monitor Rules	Configuration
DET_JRN_SEIM_RULES	Journal Monitor Rules for SEIM	Configuration
DET_JRNMON_ALERTS	Journal Monitor Alerts	Configuration
DET_JRNMON_RULES	Journal Monitor Rules	Configuration

Collector ID	Collector Name	Collector Category
DET_MON_MASTER	Monitor Master	Configuration
DET_MSQ_CMD_ALR	Message Queue and Command Alerts	Configuration
DET_MSQ_RULES	Message Queue Rules	Configuration
DET_SEIM_PROVIDERS	SEIM Providers	Configuration
DET_SNMP_TRP_PCKG	SNMP Trap Packages	Configuration
DEVICE_DESCRIPTION_APPC	Device Description APPC Information	Network
DEVICE_DESCRIPTION_DATA	Device Description Information	Network
EXIT_POINTS	Display Exit Point Data	Network
FIELD_AUTHORITY	Display Field Level Authorities	Object
IFS_ATTRIBUTES	Display the attributes for the IFS objects	Resource
IFS_AUTHORITIES	Display the public and private authorities associated with the object	Resource
IFS_CONTENT	IFS Content	Configuration
IFS_JOURNALING	Display extended journaling information for the IFS object	Resource
IFS_STATUS	Display status information about an IFS file	Resource
ISL_CONFIGURATION_SETTINGS	ISL Configuration Settings	Network
ISL_DISCONNECT_OPTIONS	ISL Disconnect Options	Network
ISL_RULES	ISL Inclusion Exclusion Rules	Network
JOB_ACTIVITY_DETAILS	Job Activity Details	Log
JOB_ACTIVITY_SUMMARY	Job Activity Summary	Log
JOB_DESCRIPTIONS	Job Description Data	Configuration
JOURNAL_AD	Object Auditing Attribute Changes	Configuration
JOURNAL_AF	Authority Failures	Profile
JOURNAL_AP	Programs that Adopt Authority were Executed	Configuration
JOURNAL_AU	EIM Attribute Changes	Configuration
JOURNAL_AX	Row and Column Access Control	Resource
JOURNAL_CA	Authorization List or Object Authority Changes	Profile
JOURNAL_CD	Commands Executed	Resource
JOURNAL_CO	Create Operations	Resource
JOURNAL_CP	User Profile Changes	Configuration
JOURNAL_CQ	Change Request Descriptor Changes	Configuration

Collector ID	Collector Name	Collector Category
JOURNAL_CU	Cluster Operation	Network
JOURNAL_CV	Connection Verification	Profile
JOURNAL_CY	Cryptographic Configuration Changes	Configuration
JOURNAL_DI	LDAP Operations	Resource
JOURNAL_DO	Delete Operations	Resource
JOURNAL_DS	Changes to Service Tools Profiles	Profile
JOURNAL_EV	Environment Variable Changes	Profile
JOURNAL_GR	Exit Point Maintenance Operations	Resource
JOURNAL_GS	Socket Descriptor Details	Resource
JOURNAL_IM	Intrusion Monitor Events	Network
JOURNAL_IP	Inter-process Communication Events	Network
JOURNAL_IR	Actions to IP Rules	Network
JOURNAL_IS	Internet Security Management Events	Network
JOURNAL_JD	Job Descriptions – USER Parameter Changes	Resource
JOURNAL_JS	Job Changes	Resource
JOURNAL_KF	Key Ring File Changes	Configuration
JOURNAL_LD	Directory Link, Unlink, and Search Operations	Resource
JOURNAL_M0	Db2 Mirror Setup Tools	Resource
JOURNAL_M6	Db2 Mirror Communication Services	Resource
JOURNAL_M7	Db2 Mirror Replication Services	Resource
JOURNAL_M8	Db2 Mirror Product Services	Resource
JOURNAL_M9	Db2 Mirror Replication State	Resource
JOURNAL_ML	OfficeVision Mail Services Actions	Configuration
JOURNAL_NA	Network Attribute Changes	Profile
JOURNAL_ND	Directory Search Violations	Resource
JOURNAL_NE	APPN Endpoint Filter Violations	Network
JOURNAL_O1	Single Optical Object Accesses	Resource
JOURNAL_O2	Dual Optical Object Accesses	Resource
JOURNAL_O3	Optical Volume Accesses	Resource
JOURNAL_OM	Object Management Changes	Resource
JOURNAL_OR	Objects Restored	Resource

Collector ID	Collector Name	Collector Category
JOURNAL_OW	Object Ownership Changes	Resource
JOURNAL_PA	Program Changes to Adopt Owner Authority	Configuration
JOURNAL_PF	PTF Operations	Resource
JOURNAL_PG	Primary Group Changes	Resource
JOURNAL_PO	Printer Output Changes	Resource
JOURNAL_PS	Swap Profile Events	Configuration
JOURNAL_PU	PTF Object Changes	Profile
JOURNAL_PW	Invalid Sign-on Attempts	Profile
JOURNAL_RA	Authority Changes to Restored Objects	Configuration
JOURNAL_RJ	Job Descriptions that Contain User Profile Names were Restored	Configuration
JOURNAL_RO	Ownership Changes for Restored Objects	Profile
JOURNAL_RP	Programs Restored that Adopt Owner Authority	Configuration
JOURNAL_RQ	Change Request Descriptors Restored	Resource
JOURNAL_RU	Authority Restored for User Profiles	Profile
JOURNAL_RZ	Primary Group Changes for Restored Objects	Configuration
JOURNAL_SD	System Directory Changes	Resource
JOURNAL_SE	Subsystem Routing Entry Changes	Configuration
JOURNAL_SF	Spooled File Actions	Resource
JOURNAL_SG	Asynchronous Signals Processed	Network
JOURNAL_SK	Secure Socket Connections	Network
JOURNAL_SM	Systems Management Changes	Configuration
JOURNAL_SO	Server Security User Information Actions	Configuration
JOURNAL_ST	Service Tools Actions	Configuration
JOURNAL_SV	System Values Changes	Configuration
JOURNAL_VA	Access Control List Changes	Configuration
JOURNAL_VC	Connections Started, Ended, or Rejected	Network
JOURNAL_VF	Close Operations on Server Files	Resource
JOURNAL_VL	Exceeded Account Limit Events	Profile
JOURNAL_VN	Network Log On and Off Events	Configuration
JOURNAL_VO	Actions on Validation Lists	Resource

Collector ID	Collector Name	Collector Category
JOURNAL_VP	Network Password Errors	Profile
JOURNAL_VR	Network Resource Accesses	Resource
JOURNAL_VS	Server Sessions Started or Ended	Network
JOURNAL_VU	Network Profile Changes	Profile
JOURNAL_VV	Service Status Change Events	Network
JOURNAL_X0	Network Authentication Events	Network
JOURNAL_X1	Identity Token Events	Profile
JOURNAL_XD	Directory Server Extensions	Profile
JOURNAL_YC	DLO Object Changes	Resource
JOURNAL_YR	DLO Object Reads	Resource
JOURNAL_ZC	Object Changes	Resource
JOURNAL_ZR	Object Reads	Resource
KEYSTORE_DATA	KeyStore	Configuration
LINE_DESCRIPTION_DATA	Line Description Information	Configuration
MESSAGE_QUEUE	Message Queue Details	Configuration
MESSAGE_QUEUE_DATA	Message Queue Data	Configuration
NETWORK_ATTRIBUTES	Network Attribute Information	Network
NETWORK_CONNECTIONS	Network Connections Ipv4 and Ipv6	Network
NETWORK_EXIT_CONFIG	Exit Point Configuration Report	Network
NETWORK_INTERFACE_IPV4	Network Interface Data Ipv4	Network
NETWORK_INTERFACE_IPV6	Network Interface Data Ipv6	Network
NETWORK_ROUTE_IPV4	Network Route Data Ipv4	Network
NETWORK_ROUTE_IPV6	Network Route Data Ipv6	Network
NETWORK_SERVER_DESCRIPTIONS	Network Server Description Data	Network
NETWORK_SVR_ENCRYPT_STATUS	Network Server Encryption Status	Network
NETWORK_TCPIP_IPV4	TCP/IP Ipv4 Stack Attributes	Network
NETWORK_TCPIP_IPV4	Remote Exit Rules	Network
NETWORK_TCPIP_IPV6	TCP/IP Ipv6 Stack Attributes	Network
NETWORK_TCPIP_IPV6	Remote Exit Rules	Network
NETWORK_TRANS_CENTRAL	Central Server Transactions	Network
NETWORK_TRANS_COMMAND	Remote Command Transactions	Network

Collector ID	Collector Name	Collector Category
NETWORK_TRANS_DATABASE	Remote Exit Rules	Network
NETWORK_TRANS_DATAQ	Remote Exit Rules	Network
NETWORK_TRANS_DDM	Remote Exit Rules	Network
NETWORK_TRANS_SHOWCASE	Network Trans Showcase	Network
NETWORK_TRANSACTIONS_FILE	Remote Exit Rules	Network
NETWORK_TRANSACTIONS_FTP_REXEC	Remote Exit Rules	Network
NETWORK_TRANSACTIONS_PRINTER	Remote Exit Rules	Network
NETWORK_TRANSACTIONS_SIGNON	Remote Exit Rules	Network
NETWORK_TRANSACTIONS_TELNET	Remote Exit Rules	Network
OBJECT_AUTHORITY	Display Object Authority	Resource
OBJECT_DETAILS	Display Object Details	Resource
OUTPUT_QUEUE	Output Queue Information	Configuration
PRODUCT_INFO	Basic Information about a software product	Configuration
PROFILE_COMPLIANCE	Profile Compliance Data	Profile
PROFILE_INACTIVITY_SETTINGS	Profile Inactivity Settings	Profile
PROFILE_MANAGER_DEFAULTS	Profile Manager Defaults	Profile
PROGRAM_ADOPT	Programs that Adopt Authority	Resource
PROGRAM_REFERENCE_DATA	Program Reference Data	Resource
PTF_DATA	Program Temporary Fix Data	Configuration
QSYS2.ACTIVE_JOB_INFO	Active job information	Configuration
QSYS2.DRDA_AUTHENTICATION	DRDA and DDM User access	Configuration
QSYS2.FUNCTION_INFO	Function usage identifiers	Configuration
QSYS2.FUNCTION_USAGE	Function usage configuration details.	Configuration
QSYS2.GROUP_PTF_INFO	Group PTFs Information	Configuration
QSYS2.JOURNAL_INFO	Journal and remote journal information	Configuration
QSYS2.LICENSE_INFO	Products license information.	Configuration
QSYS2.MEDIA_LIBRARY_INFO	Media Library Status details	Configuration
QSYS2.MEMORY_POOL	Memory pool details	Configuration
QSYS2.MEMORY_POOL_INFO	Active memory pools	Configuration
QSYS2.NETSTAT_JOB_INFO	IPv4 and IPv6 network connection details.	Configuration
QSYS2.OBJECT_LOCK_INFO	Object lock information	Configuration

Collector ID	Collector Name	Collector Category
QSYS2.OUTPUT_QUEUE_ENTRIES	Spooled file in output queue	Configuration
QSYS2.RECORD_LOCK_INFO	Record lock information	Configuration
QSYS2.REPLY_LIST_INFO	Current job's reply list entry information	Configuration
QSYS2.SCHEDULED_JOB_INFO	Job Schedule Entry information	Configuration
QSYS2.SERVER_SBS_ROUTING	Alternate subsystem configurations	Configuration
QSYS2.SYSCONTROLS	Permissions or column mask defined	Configuration
QSYS2.SYSCONTROLSDEP	Dependencies of row permissions and column masks	Configuration
QSYS2.SYSDISKSTAT	Disk Information	Configuration
QSYS2.SYSTEM_STATUS_INFO	Partition information	Configuration
QSYS2.SYSTMPSTG	IBM i temporary storage pool detail	Configuration
QSYS2.USER_INFO	User Profile Information	Configuration
QSYS2.USER_STORAGE	Storage usage by user profile	Configuration
REMOTE_TRAN_SUMMARY_BY_SERVER	Remote Summary Server	Network
REMOTE_TRAN_SUMMARY_BY_USER	Remote Summary User	Network
RSC_MGR_COMPLIANCE_DATA	Resource Manager Authority Out of compliance data	Network
RSC_MGR_CONFIG	Resource Manager Configuration	Network
RSC_MGR_SCHEMA_DETAILS	Resource Manager Authority Schema Details	Network
RSC_MGR_SCHEMA_HEADER	Resource Manager Authority Schema Header	Network
SERVICE_TOOL_SECURITY_ATTR	Service Tool Security Attributes	Profile
SERVICE_TOOL_USERS	Service Tool User Data	Profile
SOCKET_SUMMARY_BY_SERVER	Socket Summary by Server	Network
SOCKET_SUMMARY_BY_USER	Socket Summart by User	Network
SOCKET_TRAN_RULES	Socket Rules	Network
SOCKET_TRANSACTIONS	Socket Transactions	Network
SOFTWARE_RESOURCES	Installed Software Resources Data	Configuration
SUBSYSTEM_AUTOSTART	Subsystem Autostart Jobs	Configuration
SUBSYSTEM_COMMUNICATIONS	Subsystem Communication Entries	Configuration
SUBSYSTEM_INFORMATION	Subsystem Information Details	Configuration
SUBSYSTEM_JOB_QUEUE	Subsystem Job Queue	Configuration
SUBSYSTEM_POOL_DATA	Subsystem Pool Data	Configuration

Collector ID	Collector Name	Collector Category
SUBSYSTEM_PRESTART	Subsystem Prestart Jobs	Configuration
SUBSYSTEM_REMOTE	Subsystem Remote Entries	Configuration
SUBSYSTEM_ROUTING	Subsystem Routing Entries	Configuration
SUBSYSTEM_WORKSTATION_NAMES	Subsystem Workstation Names	Configuration
SUBSYSTEM_WORKSTATION_TYPES	Subsystem Workstation Types	Configuration
SYSCOLAUTH	Privileges granted on a column	Configuration
SYSCONTROLS	Permission or column mask defined	Configuration
SYSCONTROLSDEP	Dependencies of row permissions and column masks	Configuration
SYSCONTROLSDEP	Privileges granted on a row	Configuration
SYSFIELDS	Columns with field procedures	Configuration
SYSPACKAGEAUTH	Privileges granted on a package	Configuration
SYSPROGRAMSTAT	Program, service program, and module with SQL statements	Configuration
SYSROUTINEAUTH	Privileges granted on a routine	Configuration
SYSSCHEMAAUTH	Privileges granted on a schema	Configuration
SYSSEQUENCEAUTH	Privileges granted on a sequence	Configuration
SYSTABAUTH	Privileges granted on a table or view	Configuration
SYSTABLESTAT	Table statistics include all partitions and members	Configuration
SYSTEM_VALUES	Display System Value Data	System
SYSTOOLS.GROUP_PTF_CURRENCY	PTF Groups installed per IBM Recommendations	Configuration
SYSTOOLS.GROUP_PTF_DETAILS	PTFs within PTF Groups installed per IBM Recommendations	Configuration
SYSUDTAUTH	Privileges granted on a type	Configuration
SYSVARIABLEAUTH	Privileges granted on a global variable	Configuration
SYSXSROBJECTAUTH	Privileges granted on an XML schema	Configuration
TGMOBJINF	Object Information	Resource
TG_NETWORK_GROUPS	TG Network Groups	Network
TG_OBJECT_GROUPS	TG Object Groups	Network
TG_OPERATION_GROUPS	TG Operation Groups	Network
TG_USER_GROUPS	TG User Groups	Network

Collector ID	Collector Name	Collector Category
USER_OBJECT_AUTHORITIES	User Profile Object Authorities	Profile
USER_PRF_VIA_BLUEPRINT	User Profile via Blueprint	Profile
USER_PROFILE_ACTIVITY	User Profile Activity	Profile
USER_PROFILE_EXCLUSIONS	User Profile Exclusions	Profile
USER_PROFILES	Display User Profile Data	Profile