NetIQ Security Solutions for IBM i
TGAudit 1.7
Report Reference Guide
Revised February 2018

Legal Notice

Table of Contents

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.

2.1. 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.

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.

2.2. System Auditing Level Reports

This section of reports is based on values of the QAUDLVL (Auditing level) and QAUDLVL2 (Auditing level extension) system values. The values specified in these system values define what is audited on your system.

2.2.1. 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.

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

2.2.2. 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.

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

2.2.3. 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.

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)

2.2.4. 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.

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)

2.2.5. 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.

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

2.2.6. 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.

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

2.2.7. 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.

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.

2.2.8. 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.

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).

2.2.9. 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.

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

2.2.10. 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.

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

2.2.11. 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.

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

2.2.12. 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.

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.

2.2.13. 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.

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

2.2.14. 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.

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

2.2.15. 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.

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

2.2.16. Spooled File Functions are Audited

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

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

2.2.17. 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.

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

2.3. 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.

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.

2.4. 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.

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.

2.5. 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.

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.

2.6. 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.

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.

2.7. 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.

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.

2.8. 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.

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.

2.9. 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.

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.

2.10. 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.

2.11. 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.

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.

2.12. 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.

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.

2.13. 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.

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.

2.14. Installed Products

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

2.15. Job Description Details

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

2.16. 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.

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.

2.17. 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.

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.

2.18. 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

2.19. Job Descriptions with Request Data

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

2.20. 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.

2.21. 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.

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.

2.22. Limit Device Sessions Not Enabled

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

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.

2.23. 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.

2.24. 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.

2.25. 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.

2.26. 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.

2.27. 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.

2.28. 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.

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.

2.29. 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.

2.30. Output Queue Details

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

2.31. 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.

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.

2.32. 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.

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.

2.33. 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 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.

2.34. 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 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.

2.35. 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.

2.36. 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.

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.

2.37. 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.

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.

2.38. 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.

2.39. 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.

2.40. PTFs for WDS

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

2.41. 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.

2.42. 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.

2.43. Restrict use of Use Adopted Authority

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

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.

2.44. 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

2.45. Server Security Data is Retained

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

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.

2.46. 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.

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.

2.47. 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.

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.

2.48. Strong System Security Level

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

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.

2.49. Subsystem Autostart Details

This report displays subsystem description information for autostart job entries.

2.50. Subsystem Communication Details

This report displays subsystem description information for communication entries.

2.51. Subsystem Information Details

This report displays general subsystem description information.

2.52. Subsystem Job Queue Details

This report displays subsystem description information for job queue entries.

2.53. Subsystem Pool Data Details

This report displays subsystem description information for pool definitions.

2.54. Subsystem Prestart Job Details

This report displays subsystem description information for prestart job entries.

2.55. Subsystem Remote Entries

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

2.56. Subsystem Routing Entries

This report displays subsystem description information for routing entries.

2.57. 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.

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.

2.58. Subsystem Workstation Names

This report displays subsystem description information for workstation name entries.

2.59. Subsystem Workstation Types

This report displays subsystem description information for workstation type entries.

2.60. 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.

2.61. System Software Resources

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

2.62. 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.

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.

2.63. 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.

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

2.64. 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.

3. Network Management Reports

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

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.

PASS = IR journal entries were not found in QAUDJRN.

FAIL = IR journal entries were found in QAUDJRN.

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

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).

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.

PASS = NE journal entries were not found in QAUDJRN.

FAIL = NE journal entries were found in QAUDJRN.

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

Types of changes:

- A - Change to network attribute
- T - Change to TCP/IP attribute

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.

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.

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.

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 *AUTFAIL and *PGMFAIL.

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

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.

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.

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.

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.

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.

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

3.8. Controller Description Details

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

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.

3.10. Device Description Details

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

3.11. Device Descriptions - *APPC

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

3.12. DNS Configuration Details

This report displays the DNS configuration of the system.

3.13. 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.

3.14. 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.

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

3.15. 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.

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.

3.16. 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.

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

3.17. 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.

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

3.18. 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.

3.19. 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.

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

3.20. 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.

3.21. Network Interface Details IPv4

This report displays IPv4 network interface information for the system.

3.22. Network Route Details IPv4

This report displays IPv4 routing information on the system.

3.23. Network Server Descriptions

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

3.24. Network Server Encryption Status

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

3.25. Network Servers with Encryption Verified

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

3.26. 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.

3.27. 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.

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.

3.28. 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.

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.

3.29. Remote Service Attribute

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

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.

3.30. Remote Sign-on Control

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

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.

3.31. 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.

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

3.32. 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.

PASS = VS journal entries were not found in QAUDJRN.

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

3.33. 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.

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

3.34. Sockets-related Exit Points Not Secured

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

3.35. 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.

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.

3.36. TCP/IP IPv4 Stack Attributes

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

3.37. TCP/IP IPv6 Stack Attributes

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

3.38. Unsecured Remote Server Exit Points

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

4. Profile Management Reports

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

4.1. 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.

4.1.1. Block Password Change

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

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.

4.1.2. 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.

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.

4.1.3. 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.

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.

4.1.4. Limit Characters in Password

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

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.

4.1.5. Limit Password Character Positions

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

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.

4.1.6. 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.

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.

4.1.7. Maximum Password Length

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

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.

4.1.8. Minimum Password Length

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

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.

4.1.9. 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.

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.

4.1.10. Password Expiration Warning

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

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.

4.1.11. Password Level

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

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.

4.1.12. Password Rules

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

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.

4.1.13. Password Validation Program

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

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.

4.1.14. 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.

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.

4.2. All User Profiles

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

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.

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.

4.4. 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.

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

4.5. Disable Profile After Maximum Failed Sign-on 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).

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.

4.6. 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.

4.7. 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.)

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

4.8. 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.

4.9. 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.

4.10. 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.

4.11. IBM Profile Details Report

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

4.12. 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.

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

4.13. Inactive Job Message Queue

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

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.

4.14. Inactive Job Time-out

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

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.

4.15. 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.

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.

4.16. Limit Security Officer Device Access

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

4.17. Network Logon 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.)

PASS = VN journal entries were not found in QAUDJRN.

FAIL = VN journal entries were found in QAUDJRN.

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

Types of entries:

- F - Logoff requested
- O - Logon requested
- R - Logon rejected

4.18. 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.

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.

4.19. 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.

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.

4.20. Object Authorities of User Profiles

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

4.21. 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.

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.

4.22. Profile Object Auditing Values

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

4.23. 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.

4.24. 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.

4.25. 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.

4.26. 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.

4.27. 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.

4.28. 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.

4.29. 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.

4.30. Security Officer Profiles

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

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.

4.31. 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.

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

4.32. System Service Tools Users

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

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.

4.33. 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.

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.

4.34. 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.

4.35. 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.

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.

4.36. Users with Job Control Special Authority

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

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.

4.37. Users with Save System Special Authority

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

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.

4.38. 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.

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.

5. Resource Management Reports

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

5.1. 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.

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

5.2. Allow Object Restore Option

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

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.

5.3. 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.

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).

5.4. Authorization List Details

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

PASS = N/A

FAIL = N/A

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

5.5. Authorization Lists with Public Access

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

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.

5.6. 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.

PASS = VF journal entries were not found in QAUDJRN.

FAIL = VF journal entries were found in QAUDJRN.

For VF journal entries to be generated, object auditing is required and can be turned on by using the CHGOBJAUD command.

Types of entries:

- A - Administrative disconnection
- N - Normal client disconnection
- S - Session disconnection

5.7. 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.

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

5.8. 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.

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.

5.9. 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.

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

5.10. 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.

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

5.11. 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.

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.

5.12. 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.

PASS = YC journal entries were not found in QAUDJRN.

FAIL = YC journal entries were found in QAUDJRN.

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.

5.13. 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.

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.

5.14. 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.

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

5.15. 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.

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

5.16. Integrated File System Security

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

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.

5.17. 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.

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

5.18. 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.

PASS = DI journal entries were not found in QAUDJRN.

FAIL = DI journal entries were found in QAUDJRN.

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

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

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

5.19. 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.

PASS = VR journal entries were not found in QAUDJRN.

FAIL = VR journal entries were found in QAUDJRN.

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.

Types of entries:

- F - Resource access failed
- S - Resource access succeeded

5.20. 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.

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.

5.21. 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.

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.

5.22. 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.

PASS = OW journal entries were not found in QAUDJRN.

FAIL = OW journal entries were found in QAUDJRN.

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

5.23. 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.

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.

5.24. 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.

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.

5.25. 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.

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

5.26. 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.

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.

5.27. 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.

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

5.28. 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.

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.

5.29. 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.

5.30. 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.

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.

5.31. Public Access to Devices

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

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.

5.32. 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.

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.

5.33. 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.

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.

5.34. 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.

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

5.35. 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.

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

5.36. 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.

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

5.37. 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.

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

5.38. System Security Audit Journal Exists

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

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.

5.39. Verify Object on Restore

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

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.

5.40. Integrated File System (IFS) Reports

5.41. Integrated File System (IFS) Reports

5.41.1. *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.

5.41.2. 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.

5.41.3. Attributes for /QSYS.LIB

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

5.41.4. Commands Available in QSH

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

5.41.5. 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.

5.41.6. 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 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).

5.41.7. 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.

5.41.8. 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.

5.41.9. 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.

5.41.10. HTTP Server and Web Files Status

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

5.41.11. HTTP Server File Authorities

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

5.41.12. IFS Directory Information

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

5.41.13. IFS Files Being Journaled

This report displays the extended journaling information for objects.

5.41.14. Largest Files Report > 100Mb

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

5.41.15. 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 (/).

5.41.16. 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.

5.42. 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.

5.43. 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.

5.44. Authorized Users through 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.

5.45. 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.

5.46. 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.

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.

5.47. Program Reference Data

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.

5.48. 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.

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.

5.49. 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.

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.

5.50. 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.

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