



October 2009

## **iSecurity Audit Case Study at DnBNOR Bank, Luxembourg**

### **General**

iSecurity Audit is being used by the Luxembourg subsidiary of DnBNOR Bank (formerly Union Bank of Norway), which is part of Norway's largest financial services group with total combined assets of nearly \$300B.

This document will discuss various aspects of configuring and implementing iSecurity Audit at DnBNOR Bank and can serve as a valuable reference for all iSecurity Audit customers worldwide.

Raz-Lee Security would like to take this opportunity to thank Mr. Michael Neylon of DnBNOR's internal auditing department for his assistance in defining the auditing requirements and implementing iSecurity Audit as described in this Case Study, as well as Mr. Gerd Gesner and Mr. Bertrand Wauters of our Belgium distributor.

This document is divided into the following sections:

1. System Audit Options
2. Audit Values
3. Audit Reports. Report details appear in Appendix A.
4. Printer Files
5. Audit Scheduler
6. Displaying System Values
7. Checking User Audit Settings
8. Using Object Auditing
9. Log & Journal Retention Maintenance
10. Real Time Detection

1. System Audit Options (individual options listed below can be accessed by choosing Option 1 and then Option 1 again, from the Audit main menu)

- **APPN filter violation**

Audit violations detected by the APPN firewall. Directory search filter and endpoint filter violations are audited. Also known as the **\*NETCMN** option for the QAUDLVL system value.

- **Authorization failure**

Audit unsuccessful attempts to sign on the system and to access objects. Use authorization failures to regularly monitor users trying to perform unauthorized functions on the system. You can also use authorization failures to assist with migration to a higher security level and to test resource security for a new application. Also known as the **\*AUTFAIL** option for the QAUDLVL system value.

- **Job tasks**

Audit actions that affect a job, such as starting, stopping, holding, releasing, canceling, or changing the job. Use job tasks to monitor who is running batch jobs. Also known as the **\*JOBDTA** option for the QAUDLVL system value.

- **Object creation**

Audit the creation or replacement of an object. Use object creation to monitor when programs are created or recompiled. Also known as the **\*CREATE** option for the QAUDLVL system value.

- **Object deletion**

Audit the deletion of an object. Also known as the **\*DELETE** option for the QAUDLVL system value.

- **Object management**

Audit an object rename or move operation. Use object management to detect copying confidential information by moving the object to a different library. Also known as the **\*OBJMGT** option for the QAUDLVL system value.

- **Object restore**

Audit the restore of an object. Use object restore to detect attempts to restore unauthorized objects. Also known as the **\*SAVRST** option for the QAUDLVL system value.

- **Office tasks**

Audit changes to the system distribution directory and opening of a mail log. Actions performed on specific items in the mail log are not recorded. Use office tasks to detect attempts to change how mail is routed or to monitor opening another user's mail log. Also known as the **\*OFCSRVR** option for the QAUDLVL system value.

- **Optical tasks**

Audit optical functions, such as adding or removing an optical cartridge, or changing the authorization list used to secure an optical volume. Other functions include copying, moving, or renaming an optical file, saving or releasing a held optical file, and so on. Also known as the **\*OPTICAL** value for the QAUDLVL system value.

- **Printing functions**

Audit the printing of a spooled file, printing directly from a program, or sending a spooled file to a remote printer. Use printing functions to detect printing confidential information. Also known as the **\*PRTDTA** option for the QAUDLVL system value.

- **Program adoptions**

Audit the use of adopted authority to gain access to an object. Use program adoption to test where and how a new application uses adopted authority. Also known as the **\*PGMADP** option for the QAUDLVL system value.

- **Security tasks**

Audit events related to security, such as changing a user profile or system value. Use security tasks to detect attempts to circumvent security by using service tools or collecting traces in which security sensitive data is retrieved. Also known as the **\*SECURITY** option for the QAUDLVL system value.

- **Service tasks**

Audit the use of service tools, such as the Dump Object and Start Copy Screen commands. Use service tasks to detect attempts to circumvent security by using service tools. Also known as the **\*SERVICE** option for the QAUDLVL system value.

- **Spool management**

Audit actions performed on spooled files, including creating, copying, and sending. Use spool management to detect attempts to print or send confidential data. Also known as the **\*SPLFDTA** option for the QAUDLVL system value.

- **System integrity violations**

Audit program domain violations when a program causes an integrity error. Use system integrity violation to assist with migration to a higher security level or to test a new application. Also known as the **\*PGMFAIL** option for the QAUDLVL system value.

- **System management**

Audit system management activities, such as changing a reply list or the power-on and -off schedule. Use system management to detect attempts to use system management functions to circumvent security controls. Also known as the **\*SYSMGT** option for the QAUDLVL system value.



## 2. Audit Values

System Audit Values assure that actions occurring in your system can be traced to their original users. This auditing system is delivered with a full range of auditing capabilities to assure compliance with industry and government standards.

Audit control features should be turned **ON** at the system level.

Each of the sixteen possible system wide auditing values has been enabled. The status of these audit values are as follows:

### **Audit Value    Description System**

\***AUTFAIL**    Log Authority failures  
Journal Entry Type: **AF, AU, CV, DI, GR, KF, IP, PW, VO, VC, VN, VP**  
Available on **QAUDLVL** System Value = **yes**  
Available on **CHGUSRAUD** Command = **no**

\***DELETE**    Log deletion of objects  
Journal Entry Type: **DO, DI**  
Available on **QAUDLVL** System Value = **yes**  
Available on **CHGUSRAUD** Command = **yes**

\***OBJMGT**    Log object management changes  
Journal Entry Type: **DI, OM**  
Available on **QAUDLVL** System Value = **yes**  
Available on **CHGUSRAUD** Command = **yes**

\***SYSMGT**    Log changes to certain system management areas  
Journal Entry Type: **DI, SM, VL**  
Available on **QAUDLVL** System Value = **yes**  
Available on **CHGUSRAUD** Command = **yes**

\***SAVRST**    Log restore actions to security sensitive objects  
Journal Entry Type: **OR, RA, RJ, RO, RP, RQ, RU, RZ**  
Available on **QAUDLVL** System Value = **yes**  
Available on **CHGUSRAUD** Command = **yes**



- \*SECURITY** Log security related changes  
Journal Entry Type: **AD, CA, CP, CQ, CV, CY, DI, DS, EV, GR, GS, IP, JD, KF, NA, OW, PA, PG, PS, SE, SO, SV, VA, VU, X0**  
Available on **QAUDLVL** System Value = **yes**  
Available on **CHGUSRAUD** Command = **yes**
- \*SERVICE** Log usage of the system and hardware service tools  
Journal Entry Type: **ST, VV**  
Available on **QAUDLVL** System Value = **yes**  
Available on **CHGUSRAUD** Command = **yes**
- \*PGMFAIL** Log Program failures caused by security violations  
Journal Entry Type: **AF**  
Available on **QAUDLVL** System Value = **yes**  
Available on **CHGUSRAUD** Command = **no**
- \*CREATE** Log creation of new objects  
Journal Entry Type: **CO, DI**  
Available on **QAUDLVL** System Value = **yes**  
Available on **CHGUSRAUD** Command = **yes**
- \*JOBDTA** Log job events such as start and stop.  
Journal Entry Type: **JS, SG, VC, VN, VS**  
Available on **QAUDLVL** System Value = **yes**  
Available on **CHGUSRAUD** Command = **yes**
- \*PGMADP** Log usage of programs that adopt authority  
Journal Entry Type: **AP**  
Available on **QAUDLVL** System Value = **yes**  
Available on **CHGUSRAUD** Command = **yes**
- \*NETCMN** Log APPN firewall events  
Journal Entry Type: **CU, CV, IR, IS, ND, NE, SK**  
Available on **QAUDLVL** System Value = **yes**  
Available on **CHGUSRAUD** Command = **no**
- \*OFCSRV** Log Office Vision/400 security changes  
Journal Entry Type: **ML, SD**  
Available on **QAUDLVL** System Value = **yes**  
Available on **CHGUSRAUD** Command = **yes**
- \*OPTICAL** Log usage of optical storage devices  
Journal Entry Type: **O1, O2, O3**  
Available on **QAUDLVL** System Value = **yes**  
Available on **CHGUSRAUD** Command = **yes**



- \***PRTDTA**      Log printing functions  
Journal Entry Type: **PO**  
Available on **QAUDLVL** System Value = **yes**  
Available on **CHGUSRAUD** Command = **no**
  
- \***SPLFDTA**      Log usage of spooled files (reports)  
Journal Entry Type: **SF**  
Available on **QAUDLVL** System Value = **yes**  
Available on **CHGUSRAUD** Command = **yes**



### 3. Audit Reports

iSecurity Audit is provided with ready-to-be-used predefined reports for all the Journal Entry Types listed above.

Each such report can be restricted to a time group (for example: after working hours, weekends, etc.). The reports may be filtered and output fields can be defined in accordance with your particular needs. Each such report can be run automatically, for example daily, weekly, etc.

The bank uses a weekly report scheduled to run each Sunday at 01:00 AM, which reports on all of the following events for the past week.

Note the suffix BK (i.e. bank) which has been added to the names of all the iSecurity-provided audit reports.

Each report's specific parameters appear in Appendix A.

**C@ shows the changes on User Profiles. Note that this is a unique entry which exists only in iSecurity!**

**AF shows all authority failures.**

**CA shows all authority changes within libraries L1DMLIB and L9DMLIB.**

**CD shows all commands executed by selected users.**

**CO displays which users have created new objects, except for a specific list of users: SIOWNER etc.**

**CP shows who has changed, created or restored user profiles and how.**

**DS shows who has reset the DST password.**

**DO shows who has deleted objects excluding users LIOWNER, TIOWNER etc.**

**JS is only switched "on" during non-working-hours and weekends, and shows who has signed on to the system.**

**OR show who restored any objects on the system.**

**OM shows who moved or restored objects on the system.**

**OW shows who changed the ownership of an object except SIOWNER etc.**



**PW shows all users who tried to sign on with a wrong password.**

**RA is written during a restore of objects/libraries etc. if any authority changes are made.**

**RJ shows restoration of objects with changes to user profile specifications.**

**RP shows who restored programs that adopt authorities.**

**SM shows who made system management changes.**

**ST shows who used the service tool (SST).**

**SV shows who changed system values.**

**ZC shows who opened an object with the Change option.**

**CM shows the executed commands by selected users (all users except users within the IT department and special programs).**





#### 4. Printer Files

The following printer files within library SMZ4 should be changed in order to direct the audit reports defined above to a specific output queue (the Bank uses outq **PRTAUDIT**):

<i>AUACTNPF</i>	<i>*FILE</i>	<i>PRTF</i>	<i>AU-mail/message Print</i>
<i>AUAUDPRT</i>	<i>*FILE</i>	<i>PRTF</i>	<i>Audit Print Entries</i>
<i>AUAUDSRT</i>	<i>*FILE</i>	<i>PRTF</i>	<i>AU print audit options</i>
<i>AUQRYPRT</i>	<i>*FILE</i>	<i>PRTF</i>	<i>Audit Print Entries</i>
<i>AURPTSP</i>	<i>*FILE</i>	<i>PRTF</i>	<i>AU Report summary pages</i>
<i>AUTIMPP</i>	<i>*FILE</i>	<i>PRTF</i>	<i>AU-Print Time Groups</i>
<i>GSIPWDP</i>	<i>*FILE</i>	<i>PRTF</i>	<i>GS Work with Operators - PRINT</i>
<i>GSSYSPRT</i>	<i>*FILE</i>	<i>PRTF</i>	<i>System non-described printer file</i>

In order to print all audit reports to outq **PRTAUDIT**, change the printer file **AUQRYPRT** with the following native command:

**CHGPRTF FILE(SMZ4/AUQRYPRT) OUTQ(\*LIBL/PRTAUDIT)**



5. Audit Scheduler (the window below can be accessed by choosing Option 1 and then Option 11 from the Audit main menu)

The bank uses the Audit Scheduler with 3 Shifts:

```

Work with Audit Scheduler

Type choices, press Enter.

Activate Audit Scheduler . . . Y (Y/N)

Change pre-defined settings at:
Time . . . . 7:00 19:00 _____ :00 _____ :00

Pre-defined settings to be activated at the above times:
Monday . . . SHIFT1 SHIFT2 _____ _____
Tuesday . . . SHIFT1 SHIFT2 _____ _____
Wednesday . . . SHIFT1 SHIFT2 _____ _____
Thursday . . . SHIFT1 SHIFT2 _____ _____
Friday . . . SHIFT1 SHIFT2 _____ _____
Saturday . . . SHIFT3 _____ _____
Sunday . . . SHIFT3 _____ _____
  
```

The parameters above mean that system values **QAUDCTL** and **QAUDLVL** will be changed in accordance with the defined SHIFT values. For example, SHIFT2 will take effect at 7PM Monday-Friday until 7AM the next day with the following settings:

```

Modify Audit Settings

Set . . . : SHIFT2 Outside of working hours, between 19:00-07:00

Type choices, press Enter.
Y=Yes

Current Modified Parameter Description
Main Audit Control Parameters (QAUDCTL)
Y Y *AUDLVL Activity auditing (as selected below)
Y Y *OBJAUD Object access auditing
Y Y *NOQTEMP Do not audit QTEMP objects
Action Auditing Values (in effect only if *AUDLVL = "Y")
Y Y *AUTFAIL Authority failure events
Y Y *CREATE Create objects
Y Y *DELETE Delete objects
Y Y *JOBDBTA Start, End, Hold, Release, Change job
Y Y *NETCMN APPN filter violation
Y Y *OBJMGT Move, Rename objects
Y Y *OFCSRV Sys distribution directory, Office mail
Y Y *OPTICAL Optical volume tasks

F3=Exit F4=Prompt F8=Print F12=Cancel
  
```

## 6. Displaying System Values

The native OS/400 command **WRKSYSVAL** (work with system values) will show the changed values:

```

Work with System Values
System: S720
Position to . . . . . Starting characters of system value
Subset by Type . . . . . *ALL F4 for list

Type options, press Enter.
2=Change 5=Display

System
Option Value Type Description
█ QASTLVL *SYSCTL User assistance level
- QATNPGM *SYSCTL Attention program
- QAUDCTL *SEC Auditing control
- QAUBENDACN *SEC Auditing end action
- QAUDERCLVL *SEC Force auditing data
- QAUDLVL *SEC Security auditing level
- QAUTOCFG *SYSCTL Autoconfigure devices
- QAUTORMT *SYSCTL Autoconfigure of remote controllers
  
```

Following are the Auditing Options for System Value **QAUDCTL**:

```

System value . . . . . : QAUDCTL
Description . . . . . : Auditing control

Auditing
control
*AUDLVL
*OBJAUD
*NOQTEMP
  
```

Following are the Auditing Options for System Value **QAUDLVL**:



```
System value . . . . . : QAUDLVL
Description . . . . . : Security auditing level

Auditing options
*DELETE
*JOBDTA
*NETCMN
*OBJMGT
*OFCSRV
*OPTICAL
*PGMADP
*PGMFAIL
*PRDTA
*SAVRST
*SECURITY

Auditing options
*SERVICE
*SPLFDTA
*SYSMGT
```

## 7. Checking User Audit Settings

Using option **OS/400 Audit Features** (Option 1) and then Option 31, **User Audit Settings**, the bank obtains the following information (which uses system command **CHGUSRAUD** (Change User Auditing)):

```

1=Select      3=Copy      4=Delete
5=Display

                !! !!! !O! ! !S!S!S!
                !C!D!J!O!O!P!P!S!E!E!P!S
                !R!E!O!B!F!T!G!A!C!R!L!Y
                !E!L!B!J!C!I!M!V!U!V!F!S
                C!A!E!D!M!S!C!A!R!R!I!D!M
                M!T!T!G!R!A!D!S!I!C!T!G
                D!E!E!A!T!V!L!P!T!T!E!A!T
Opt  User/Group  Object      Action      D!E!E!A!T!V!L!P!T!T!E!A!T  Previous  Change
      USER1      *ALL        *LIST      Y Y Y Y Y Y Y Y Y Y      19/10/05  7:30
      USER2      *CHANGE     *LIST      Y Y Y Y Y Y Y Y Y Y      23/02/06  14:57

```

These defined audit changes will be written into the appropriate user profile e.g. USER2. The OS/400 native command **WRKUSRPRF** shows the changes made to this user profile:

### Display User Profile - Basic

```

User profile .....: USER2

Object auditing value .....: *CHANGE
Action auditing values .....: *CMD
                               *OBJMGT
                               *OPTICAL
                               *SAVRST
                               *SECURITY
                               *SERVICE
                               *SYSMGT

User ID number .....: 317
Group ID number .....: *NONE

```



## 8. Using Object Auditing

Using option **OS/400 Audit Features** (Option 1) and then either Option 41, **Native Object Auditing** or Option 42, **IFS Object Auditing**, the bank audits objects as follows:

```

QGPL    QSTRUP150  *PGM    *ALL    13/06/05 13:49
QSYS    CHGUSRAUD *CMD    *CHANGE 30/04/05 10:13
QSYS    CHGUSRPRF *CMD    *ALL    22/03/05 17:32
  
```

In the example above, PGM QSTRUP150 will be audited. Any changes to this program will be audited/reported. This object can be checked using OS/400 native command **WRKOBJ**. Then select Option 8=Display description, in order to determine whether this object is being audited:

```

Type options, press Enter.
  2=Edit authority    3=Copy    4=Delete    5=Display authority    7=Rename
  8=Display description 13=Change description

Opt  Object          Type          Library      Attribute    Text
  8   QSTRUP150      *PGM          QGPL         CLP          Startprogramm modif.

Object . . . . . : QSTRUP150      Attribute . . . . . : CLP
Library . . . . . : QGPL          Owner . . . . . : USER2
Type . . . . . : *PGM          Primary group . . . . . : *NONE

User-defined information:
Attribute . . . . . :
Text . . . . . : Startprogramm modif. 13.06.05 GG

Creation information:
Creation date/time . . . . . : 13.06.05 13:43:27
Created by user . . . . . : USER2
System created on . . . . . : S4441890
Object domain . . . . . : *USER

Change/Usage information:
Change date/time . . . . . : 23.02.06 15:25:12
Usage data collected . . . . . : YES
Last used date . . . . . : 23.02.06
Days used count . . . . . : 142
Reset date . . . . . :
Allow change by program . . . . . : YES

Auditing information:
Object auditing value . . . . . : *ALL    ←===== Object Audit
  
```

## 9. Log & Journal Retention Maintenance

From the main Audit menu select Option 81, **System Configuration** and then Option 9, **Log and Journal Retention**. You will see the following screen:

```

Log & Journal Retention                                29/10/07 13:41:27

Type options, press Enter.
Log retention period (days) . . . . 32                Days, 99=*NOMAX
Backup program for logs . . . . . AULOGBP             Name, *STD, *NONE
  Backup program library. . . . . USER2
A specified backup program may run before deleting old logs. It will backup
all data deleted after the retention period expires. The *STD (default)
backup program is SMZ4/AUSOURCE AULGBKP.

The following parameters apply to the audit journal receivers. This is
the primary data source for Audit. You should always backup the journal
receiver because it may contain data not logged in Audit.

Journal retention period (days) . 08                Days, 99=*NOMAX
Backup program for journal . . . . *NONE             Name, *STD, *NONE
  Backup program library . . . . .
A specified backup program may run before deleting old journal receivers.
It will backup data deleted after the retention period expires. The *STD
program is SMZ4/AUSOURCE AUJRNBP
  
```

The Audit logs will be kept for 32 days. Each log will be written into the file AUXX within library SMZ4DTA as a daily member (e.g L060111). The maintenance job **AU#MNT** within the scheduler looks for this parameter = 32 and will delete all members older than 32 days.

The Audit Journal receiver is kept for 8 days; as long as this receiver is available you may create any audit report using the receiver. If the journal receivers are saved on tape before they are deleted, you will be able to access data not being logged in Audit.



## 10. Real-Time Detection

In order for all of the above auditing features to be available, Real-Time Detection **must** be activated and running!

- Activation**
1. **Activate** Real-Time Detection
  2. De-activate Real-Time Detection
  5. **Work with Active Jobs**

The bank starts Real-Time Detection at IPL within SBS QSYSWRK as an Autostart Job Entry:

*Display Autostart Job Entries*

*Subsystem description: QSYSWRK      Status: ACTIVE*

<i>Job</i>	<i>Job Description</i>	<i>Library</i>	
<i>AU#STRRTAU</i>	<i>AU#STRRTAU</i>	<i>SMZ4DTA</i>	<i>←==== Job entry</i>
<i>QDB2MULTI</i>	<i>QQTEMP</i>	<i>QSYS</i>	
<i>QFSIOPJOB</i>	<i>QFSIOPWK</i>	<i>QSYS</i>	



## Appendix A

Following are the detailed report parameters in use by the bank. Filter Conditions appear in bold because of their importance in generating the specific report.

**1. Entry C@ shows the changes on User Profiles. Note that this is a unique entry which exists only in iSecurity!**

**Z8C@BK** – Changes to user profiles.

**Filter Condition = Name of program NE QMNCGPWD**

Output Fields = Name of program  
 Current user profile  
 Type of entry  
 User profile  
 Status  
 User class  
 \*ALLOBJ authority  
 \*JOBCTL authority  
 \*SAVSYS authority  
 \*SECADM authority  
 \*SPLCTL authority  
 \*SERVICE authority  
 \*IOSYSCFG authority  
 Group profile  
 Owner  
 Group authority  
 Initial menu  
 Initial program  
 Limited capability  
 Storage  
 Attention program  
 \*CMD audit value  
 \*CREATE audit value  
 \*DELETE audit value  
 \*JOBDTA audit value  
 \*OBJMT audit value  
 \*OFCSRV audit value  
 \*OPTICAL audit value  
 \*PGMADP audit value  
 \*SAVRST audit value  
 \*SECURITY audit value  
 \*SERVICE audit value  
 \*SPLFDTA audit value  
 Group authority  
 Supplemental groups  
 Timestamp of entry  
 Command name

Sort fields = NONE



## 2. Entry AF shows all authority failures:

**Z8AFBK** – Authority failure      Journal entry type=AF  
**Filter condition = NONE**  
Output fields = Name of program  
                  User profile name  
                  Name of object  
                  Library name  
                  Object type  
                  Name of job  
                  Name of user  
                  User profile name  
                  Date & time    yyyy-mm-dd-hh.mm  
Sort fields    = NONE

## 3. Entry CA shows all authority changes within libraries L1DMLIB and L9DMLIB:

**Z8CABK** – Authority changes      Journal entry type = CA  
**Filter condition = Library name EQ L1DMLIB & L9DMLIB**  
Output fields = Name of program  
                  User profile name  
                  Type of entry  
                  Name of object  
                  Library name  
                  Object type  
                  User profile name  
                  Authorization list name  
                  Y – Object Existence  
                  Y – Object Management  
                  Y – Object Operational  
                  Y – Authorization List Management  
                  Y - \*AUTL authority  
                  Y – Read  
                  Y – Add  
                  Y – Update  
                  Y – Exclude  
                  Y – Execute  
                  Y – Object Alter  
                  Y – Object Reference  
                  GRT–Grant RVK–Revoke USR-GRTUSRAUT  
                  Field name  
                  Office user name  
                  Folder or document name  
                  Office on behalf of user  
                  Y – Personal status changed  
                  A – Add access code R-Remove access code



Access code  
Object name country ID  
Object name language ID  
Parent directory file ID  
Object file ID  
Object name  
Object file ID  
ASP name  
ASP number  
Path name country ID  
Path name language ID  
Absolute path name indicator  
Relative file ID of path name  
Date & Time    yyyy-mm-dd-hh.mm  
Sort fields =    NONE

**4. Entry CD shows all commands executed by selected users:**

**Z8CDBK** - Command string audit    Journal entry type = **CD**  
    **Filter condition = Y-Command run from CL pgm NE Y**  
    **Name of program EQ QCMD**  
    **User of job = USER1, USER2...USERn**

Output fields = Name of program  
User profile name  
Type of entry  
Name of object  
Library name  
Object type  
Y-Command run from CL pgm or REXX proc  
Date & Time    yyyy-mm-dd-hh.mm  
Time            hh.mm.ss  
User profile description  
Sort fields    = NONE

**5. Entry CO displays which users have created new objects, except for a specific list of users: SOWNER etc.:**

**Z8COBK** – Create Object            Journal entry type = **CO**  
    **Filter condition = User profile name NLIST SOWNER**  
  **SOWNER1**  
  **SOWNERn**  
    **Name of program NLIST OUTQ99**  
  **ABC0019**



Output fields = Name of program  
User profile name  
Type of entry  
Name of object  
Object type  
Date & Time yyyy-mm-dd-hh.mm  
Sort fields = NONE

## 6. Entry CP shows who has changed, created or restored userprofiles and how:

**Z8CPBK** – User profile changed, created or restored Journal entry type=**CP**

**Filter condition = NONE**

Output fields = Name of program  
User profile name  
System name  
Type of entry  
User profile name  
Library name  
Object type  
CHG, CRT, DST, RST  
Y - Password changed  
Y - Password \*NONE  
Y - Password expired  
Y - \*ALLOBJ special authority  
Y - \*JOBCTL special authority  
Y - \*SAVSYS special authority  
Y - \*SECADM special authority  
Y - \*SPLCTL special authority  
Y - \*SERVICE special authority  
Y - \*AUDIT special authority  
Y - \*IOSYSCFG special authority  
Group profile name  
Owner of objects  
Group authority  
Initial program name  
Initial program library  
Initial menu name  
Initial menu library  
Current library name  
Limit capabilities  
User class  
Priority limit  
Status  
Group authority type  
Supplemental groups  
User ID number

Group ID number  
Date & Time yyyy-mm-dd-hh.mm  
Time hh.mm.ss  
Name of Job  
User of Job  
Number of Job  
User description  
User profile description  
Sort fields = NONE

### 7. Entry DS shows who has reset the DST password:

**Z8DSBK** – DST security password reset      Journal entry type=**DS**  
**Filter condition = NONE**  
Output fields = Name of program  
User profile name  
Type of entry  
Y – Request to reset to DST password  
DST Profile type: \*SECURITY \*FULL \*BASIC  
New DST user profile  
Y – Password changed  
New DST user profile  
Requesting DST user profile  
Date & Time yyyy-mm-dd-hh.mm  
Sort fields = NONE

### 8. Entry DO shows who has deleted objects excluding users LIOWNER, TIOWNER etc.:

**Z8DOBK** – Delete object      Journal type=**DO**  
**Filter condition = User of job NLIST SIOOWNER  
SIOOWNER1  
SIONWERN**  
**Name of program NLIST OUTQ99  
ABC019**  
**Name of object NLIKE QHST%**  
Output fields = Name of program  
User profile name  
Type of entry  
Name of object  
Object type  
Date & Time yyyy-mm-dd-hh.mm  
Sort fields = NONE



**9. Entry JS is only switched “on” during non-working-hours and weekends, and shows who has signed on to the system:**

**Z8JSBK** – LogOns outside work      Journal entry type=**JS**  
**Filter condition = User profile name NLIST USER1, USER2,...USERn**

**Name of job NLIKE SAV%**  
**Type of Entry NE M**  
**Type of job NLIST B W**  
Output fields = User profile name  
                  Job name  
                  Job queue  
                  Real user  
                  Date & Time    yyyy-mm-dd-hh.mm  
Sort fields     = NONE

**10. Entry OR show who restored any objects on the system:**

**Z8ORBK** – Object restore      Journal entry type=**OR**  
**Filter condition = NONE**  
Output fields = Name of program  
                  User profile name  
                  Type of entry  
                  Restore object name  
                  Object type  
                  Save object name  
                  Date & Time    yyyy-mm-dd-hh.m  
Sort fields     = NONE

**11. Entry OM shows who moved or restored objects on the system:**

**Z8OMBK** – Object move or rename      Journal entry type=**OM**  
**Filter condition = User of job NLIST S1OWNER**  
**S1OWNER1**  
**S1OWNERn**  
**Name of program NE OUTQ99**  
Output fields = Name of program  
                  User profile name  
                  Type of entry  
                  Old object name  
                  Object type  
                  New object name

Sort fields Date & Time yyy-mm-dd-hh.mm  
= NONE

## 12. Entry OW shows who changed the ownership of an object except SOWNER etc.:

**Z8OWBK** – Object ownership changed Journal entry type=**OW**  
**Filter condition = Old owner name NLIST SOWNER**  
**SOWNER1**  
**SOWNERn**  
**New owner name NLIST NOWNER**  
**NOWNER1**  
**NOWNERn**

Output fields = Name of program  
User profile name  
Name of object  
Object type  
Old owner name  
New owner name  
Date & Time yyyy-mm-dd-hh.mm  
Name of job  
Sort fields = NONE

## 13. Entry PW shows all users who tried to sign on with a wrong password:

**Z8PWBK** – Invalid password Journal entry type=**PW**  
**Filter condition = NONE**  
Output fields = Name of program  
User profile name  
P-Pwd U-User name A-APPC D-DST user+  
E-DST Pwd  
Device name  
Remote location name  
Local location name  
Network ID  
Date & Time yyyy-mm-dd-hh.mm  
Name of job  
Sort fields = NONE



**14. Entry RA is written during a restore of objects/libraries etc. if any authority changes are made:**

**Z8RABK** – Authority change during restore Journal entry type=**RA**

**Filter condition = NONE**

Output fields = Name of program  
User profile name  
Type of entry  
Name of object  
Library name  
Object type  
Authorization list name removed  
Y – Public authority set to \*EXCLUDE  
Y – Privat authority removed  
Y – Authorization list removed  
Date & Time yyyy-mm-dd-hh.mm  
Sort fields = NONE

**15. Entry RJ shows restoration of objects with changes to user profile specifications:**

**Z8RJBK** – Restoring job description with profile spec. Journal entry=**RJ**

**Filter condition = NONE**

Output fields = Name of program  
User profile name  
Type of entry  
Job description name  
Library name  
Object type  
User name  
Date & Time yyyy-mm-dd-hh.mm  
Sort fields = NONE

**16. Entry RP shows who restored programs that adopt authorities:**

**Z8RPBK** – Restoring adopted authority program Journal entry type=**RP**

**Filter condition = NONE**

Output fields = Name of program  
User profile name  
Type of entry  
Program name  
Library name  
Object type  
Owner name





Sort fields                      Date & Time      yyyy-mm-dd-hh.mm  
= NONE

**17. Entry SM shows who made system management changes:**

**Z8SMBK** – System management changes      Journal entry type=**SM**

**Filter condition**    = **NONE**  
Output fields        = Name of program  
                          User profile name  
                          System name  
                          Type of entry  
                          Type of access  
                          Sequence number  
                          Message ID  
                          Name of relational data base  
                          Name of HFS file system  
                          Date & Time      yyyy-mm-dd-hh.mm  
Sort fields            = NONE

**18. Entry ST shows who used the service tool (SST):**

**Z8STBK** – Use of service tools                      Journal entry type=**ST**

**Filter condition**    = **User profile name NE QSVRDRCTR**  
Output fields        = Name of program  
                          User profile name  
                          Type of entry  
                          Name of service tool  
                          Name of object  
                          Name of object library  
                          Type of object  
                          Service tools profile  
                          Date & Time      yyyy-mm-dd-hh.mm  
Sort fields            = NONE

**19. Entry SV shows who changed system values:**

**Z8SVBK** – System value changed                      Journal entry type=**SV**

**Filter condition**    = **User profile name NE SECURITY2P**  
Output fields        = Name of program  
                          User profile name  
                          System value name  
                          New value  
                          Date & Time      yyyy-mm-dd-hh.mm  
Sort fields            = NONE

**20. Entry ZC shows who opened an object with the Change option:**

**Z8ZCBK** – Object accessed (change)                      Journal entry type=**ZC**

**Filter condition**        = **NONE**  
**Output fields**            = Name of program  
                                   User profile name  
                                   Type of entry  
                                   Name of object  
                                   Library name  
                                   Object type  
                                   Type of access  
                                   Object data  
                                   Type of access (text)  
                                   Object name country ID  
                                   Object name language ID  
                                   Parent directory file ID  
                                   Object file ID  
                                   Object name  
                                   Object file ID  
                                   ASP name  
                                   ASP number  
                                   Path name country ID  
                                   Path name language ID  
                                   Absolute path name indicator  
                                   Relative file ID of path name  
  
**Sort fields**                = **NONE**

**21. Entry CM shows the executed commands by selected users (all users except users within the IT department and special programs):**

**Z9CMBK** – Commands run by a user or program.    Journal entry=**CD**

**Filter condition**        = **User profile name NLIST USER1, USER2,...,USERn**  
**Name of object**        **NE SIGNOFF**  
**Name of program**      **NLIKE PGM1%,..., PGMn%**  
                                   **NLIST PGMA, ..., PGMZ**  
                                   **NLIKE ABC%,...,XYZ%**  
  
**Output fields**            = **Name of job NE AU#MNT**  
                                   = Name of program  
                                   User profile name  
                                   Type of object  
                                   Name of object  
                                   Library name  
                                   Object type  
                                   Y-CMD run from CL pgm or REXX proc  
                                   Date & Time    yyyy-mm-dd-hh.mm



Sort fields      Name of job  
                    Number of job  
                    = NONE

The comparison parameters of the filter condition and the meaning of these parameters:

- NE**      **Not equal**
- GT**      **Greater than**
- LT**      **Less than**
- GE**      **Greater than or equal to**
- LE**      **Less than or equal to**
- RANGE** **Range (between Value1 and Value2, or equals a value)**
- IS**      **NULL**
- ISNOT** **NULL**
- LIST**    **List (field equals Value1, or equals Value2,...)**
- NLIST** **Not list (field does not equal Value1, or....)**
- LIKE**    **Like (field starts with, ends with, or matches the pattern in Value)**
- NLIKE** **Not like (field does not start with, does not end with, or does not match the pattern in value)**

AH Technology Pty Ltd  
PO Box 205 Malvern Victoria 3144

Tel: +613 9885 4877 Fax: +613 8678-0665  
Email: [info@ahtech.com.au](mailto:info@ahtech.com.au) [www.ahtechnology.com.au](http://www.ahtechnology.com.au)

