

# SirScan

Managing the performance and reliability of a Model 204 system is a very complex task. Finding the diagnostic information required to tune applications or react to system outages is time consuming and labor intensive. In order to aid this troubleshooting, Model 204 keeps a log of events, or audit trail, in a sequential, binary format dataset called CCAJRNL.

The kinds of information logged in this dataset includes error messages, communications with the operator console, input lines from online terminals or User Language procedures, and resource utilization and accounting statistics.

Model 204 programmers and operations support staff spend significant amounts of time examining this information, trying to tune performance or reconstruct the events which may have caused a problem with the Model 204 system. In online environments, the ability to quickly and accurately access the correct information is critical to making the system available for users.

Because CCAJRNL is in binary format and it contains non-text recovery information, it must be processed by a utility called AUDIT204 before the audit trail can be easily examined. It is also possible to have the audit trail data copied as it is produced to a sequential, text format dataset called CCAAUDIT. Because CCAAUDIT is a text format dataset, it can be printed or scanned directly with a text editor. Usually, CCAAUDIT is sent to system spool space so that it must be examined with a spool file browsing utility such as SDSF.

In summary, the methods that have been available to access audit trail data are to use AUDIT204 to scan the CCAJRNL or to browse CCAAUDIT with SDSF or an equivalent editing utility.

There are several disadvantages in using these methods:

- *They are slow.*
- *They cannot be used from within Model 204.*
- *They are inefficient.*
- *They create lapses in security*

## SirScan Overcomes These Problems

To address these critical shortcomings, Sirius Software has developed SirScan. SirScan is a Model 204 subsystem that provides users direct access to the Model 204 audit trail from inside the Model 204 online address space.

- *SirScan provides fast access.*

SirScan allows a user to browse audit trail entries for a specific range of time. It uses direct access I/O to quickly and efficiently find the starting point of the range. It then uses an optimized sequential full track I/O technique to find the end of range specification.

Since SirScan uses direct access I/O on CCAJRNL, it can get to the appropriate starting point in less than a second, using less than 20 I/Os, regardless of the journal size. In contrast, AUDIT204 must sequentially scan the journal to get to the starting point, performing thousands of I/O's against the online journal dataset. Not only does this take time, but it adversely affects performance in the Model 204 online. The SDSF approach also requires sequentially scanning CCAAUDIT so that it can take minutes, even hours to get to the appropriate starting point.

```
-----Journal Scan Criteria for: ULSPF303 -----93/03/09 10:13:17
***                                     SCLASS: ADMIN_R1

Start time (HH:MM:SS) ==> -10          Start date (YY/MM/DD) ==>
Interval (Minutes)   ==> 5            (Refresh to current time if blank).

User                 ==> S.G.alan*,10DEV3
Line Width ==> 79

Maximum I/O's ==> 1000   Maximum records ==> 10000

Display - entry dates? (Y/N) ==> N      server numbers? (Y/N) ==> N
         entry times? (Y/N) ==> Y       user numbers? (Y/N)   ==> Y
         entry types? (Y/N) ==> Y

Format Entry types:  ST ==> Y   AA ==> Y

AD ==> N   CI ==> N   CP ==> N   CD ==> N   ER ==> N   LI ==> N   LP ==> N
LE ==> N   ME ==> N   OI ==> N   OO ==> N   RE ==> N   US ==> N

-----
L/Help          /quit
```

*SirScan Facilitates Specifying Search Criteria*



- **SirScan is user friendly.**

SirScan provides a full screen interface that allows a user to easily specify the audit trail scanning requirements. SirScan provides flexibility in formatting and subsetting audit trail data. It eliminates the need to search through thousands of lines of extraneous data looking for user-specific information.

- **SirScan is used within Model 204.**

The other methods require that the user exit Model 204 to scan the audit trail and get back into Model 204 to implement any changes. This is time consuming. With SirScan the user is not required to leave the Model 204 environment to scan the Audit Trail data.

- **SirScan is efficient.**

With SirScan, it is unnecessary to have an on-line CCAAUDIT. This eliminates the CPU overhead of producing the on-line CCAAUDIT and, more importantly, the spool space wasted by logging data to system spool when it is already logged to the journal. With a large audit trail, especially in a 7 X 24 shop, this can take several full packs of DASD.

- **SirScan provides Audit Trail access security.**

SirScan makes it possible to limit users to examining their own audit trail entries.

- **SirScan is flexible.**

SirScan transparently handles ring and concatenated journals. With AUDIT204, the user must guess the correct journal to examine. If the time range of interest happens to overlap more than one ring member, the user must manually put the pieces together. SirScan can get data directly from the in-storage journal buffers and AUDIT204 cannot. Thus, if the audit trail entries of interest have not yet been flushed from storage they cannot be examined with AUDIT204.

## Summary

SirScan brings the Model 204 audit trail under control providing several clear benefits:

- *Improved service by rapid access to the audit trail.*
- *CPU and audit trail I/O savings from efficient processing.*
- *Improved productivity from eliminating time searching the audit trail.*

SirScan runs under Model 204 version 2.1 and later. It is available under MVS and VM/CMS operating systems.

```

---- Scan ULSPP303 93/03/09 10:18:00 - 93/03/09 10:23:00----93/03/09 10:28:57
****                               Line: 1      Col: 1      To 73
10180496  7  MS M204.0131: CHECKPOINT COMPLETED ON  93.088 10:16:41.69
10180520  7  AD M204.0440: DEVPRO DISK UPDATE COMPLETED
10180520  7  ST USERID='ALAN' ACCOUNT='ALAN' LAST='EDIT' SUBSYSTEM='SIRPRO'
          PROC-FILE='DEVPRO' PROC='PUPE-EDIT2' QTRL=1091 TTRL=8 PDL=1332
          OUTP=1257 CMT=90 CPU=448 DCRD=5 DCRW=9 OUT=12 IN=12 PCPU=5
          RQTM=781 SCREENS=12 DEPR=2519
10180522  7  ST USERID='ALAN' ACCOUNT='ALAN' LAST='CMPL' SUBSYSTEM='SIRPRO'
          PROC-FILE='DEVPRO' PROC='PUPE-EDIT2' NTRL=2 QTRL=28 STBL=194
          VTRL=10 PDL=432 CPU=13 PCPU=1090 RQTM=13 DEPR=16
10180522  7  ST USERID='ALAN' ACCOUNT='ALAN' LAST='EVAL' SUBSYSTEM='SIRPRO'
          PROC-FILE='DEVPRO' PROC='PUPE-EDIT2' NTRL=2 QTRL=1093 QTRL=28
          STBL=176 VTRL=10 PDL=432 CPU=2 PCPU=2808 RQTM=1
10180522  7  MS INCLUDE PUPE-EDIT2
10180522  7  ST USERID='ALAN' ACCOUNT='ALAN' LAST='LOAD' SUBSYSTEM='SIRPRO'
          PROC-FILE='SIRPRO' PROC='PUPE-EDIT2' NTRL=351 QTRL=1619
          STBL=7872 VTRL=540 PTRL=178 PRCH=4720 CPU=4 PCPU=800 RQTM=5
          DEPR=7
10180611  7  ST USERID='ALAN' ACCOUNT='ALAN' LAST='EVAL' SUBSYSTEM='SIRPRO'
-----
1/Help      2/Scale on  3/Quit      4/FFkey off  5/Int. up    6/Int. down
7/Up       8/Down     9/Repeat    10/Left     11/Right

```

Online Audit Trail Data Can Be Searched and Scrolled