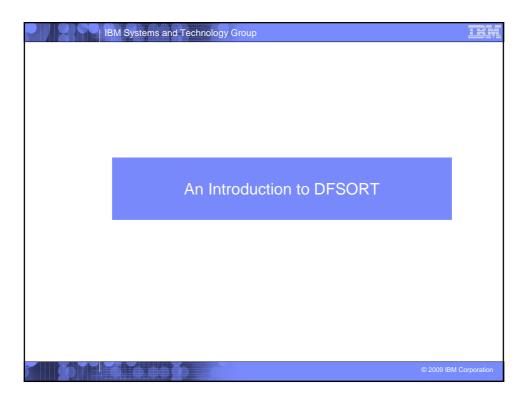
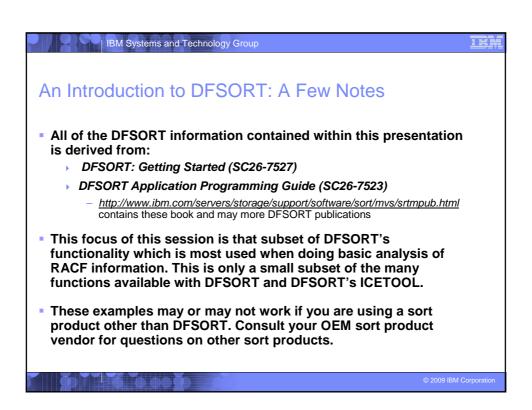


The Shortest Overview of IRRxxU00 Ever The RACF Database Unload Utility (IRRADU00) and the RACF SMF Unload Utility (IRRADU00) convert security information from its terse and cryptic format to a "flat file" format Unloaded format is easy to read and import into data-analysis tools such as DB2®, Microsoft® Excel®, SAS®, DFSORT, and even ISPF edit or browse Everything is unloaded, with the exception of security-sensitive fields (such as passwords and keys) and information which is "reserved for IBM use" The output of these utilities is documented in "RACF Macros and Interface" RACF ships default 30+ sample reports in 'SYS1.SAMPLIB(IRRICE)'









An Introduction to DFSORT: The Big Picture

- IBM's DFSORT is a high-performance product that you can use to sort data, merge data, copy data, select data, reformat data, and create reports.
- DFSORT works on information that is contained within data sets.
- A <u>record</u> is a collection of related information that is managed as a unit, such as an employee record.
- A <u>field</u> is a specific portion of a record that defines a particular category of data, such as an employee's name.
 - In DFSORT, each field is identified by a starting position, a length, and a data type (format).
 - DFSORT supports a large number of data types, such as CH, ZD, PD, BI, FS, UFF, SFF, Y2K, etc.).
 - DFSORT can also parse delimited fields, such as CSV data, into fixed fields

© 2009 IBM Corporation

IBM Systems and Technology Group



An Introduction to DFSORT: Sorting Data

- As its name implies, sorting is one of the main functions of DFSORT, and is invoked with the SORT statement:
 - SORT FIELDS=(startingPosition,length,dataType,sortOrder)
 - sortOrder: 'A' for ascending, 'D' for descending
 - dataType: 'CH' for character (EBCDIC) data
- For example, to sort the output of the RACF SMF Unload Utility by the type of record:
 - SORT FIELDS=(5,8,CH,A)



An Introduction to DFSORT: Sorting Data...

- You can sort on multiple fields by specifying multiple sort fields.
- For example, to sort on the type of record, the date, and the time, code:

```
SORT FIELDS=(5,8,CH,A,32,10,CH,A,23,8,CH,A)
```

Tip: If all of the fields have the same data type, you can code the FORMAT= keyword, which applies the specified data type to all of the fields in the statement:

```
SORT FORMAT=CH, FIELDS=(5,8,A,32,10,A,23,8,A)
```

© 2009 IBM Corporation

IBM Systems and Technology Group



An Introduction to DFSORT: Selecting Records

- DFSORT can be used to select records using the INCLUDE and OMIT statements.
 - INCLUDE COND=(startingPosition,length,dataType,testType,value)
 - OMIT COND=(startingPosition,length,dataType,testType,value)
- You can specify either a constant value (C'YES ') or another field in the record (39,4,CH) for the value.
- You can code multiple selection criteria, joined together with the Boolean AND and OR operators
 - INCLUDE COND=(startingPosition,length,dataType,testType,value,AND|OR, startingPosition,length,dataType,testType...)
 - OMIT COND=(startingPosition,length,dataType,testType,value,AND|OR,
 - startingPosition,length,dataType,testType...)
- You can code only one INCLUDE or OMIT statement per sort operation



An Introduction to DFSORT: Selecting Records...

- You must code a SORT, MERGE, or COPY statement with your INCLUDE or OMIT statement
 - SORT FIELD=COPY or OPTION COPY can be used instead of SORT FIELDS=(....) if you
 don't want to or need to sort the input data
- Example: Select all of the RACF Database Unload records ('0200' in columns 5-8) which define users who have the SPECIAL, OPERATIONS, or AUDITOR attribute ('YES' in columns 44-46, 49-51, or 390-392)

© 2009 IBM Corporation

IBM Systems and Technology Group



An Introduction to DFSORT: The Substring Operator

 You can use the DFSORT substring ("SS") comparison test to find a specified character string anywhere in a field

```
INCLUDE COND=(10,44,CH,SS,C'*')
```

- selects any record in which the character '*' appears within columns 10 to 53
- Consider this example:

 Which finds all general resource profiles (record type '0500') which are not generic (record offset 266 contains 'NO') but have a generic character in the name (the "SS" operands)

IBM Systems and Technology Group An Introduction to DFSORT: Reformatting Records DFSORT allows extensive reformatting of records using the OUTREC statement and/or the INREC statement The OUTREC statement defines the format of the output record The OUTREC statement indicates: What columns are to be copied to the output data set (startingPosition,length) What other data is to be inserted into the record Constant values System generated data · Edited or converted numeric values Justified or squeezed data Sequence numbers Results of arithmetic expressions Example: To copy the user ID, programmer name, and owner of the IRRDBU00 User Basic Data record, with a blank between each field, code: SORT FIELDS=COPY INCLUDE COND=(5,4,CH,EQ,C'0200') OUTREC FIELDS=(1,4,10,8,X,78,20,X,30,8) OPTION VLSHRT We'll talk about what "1,4" means in a moment

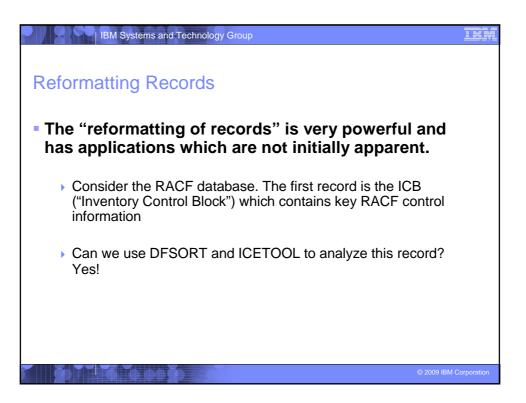
An Introduction to DFSORT: Reformatting Records... One very powerful feature of OUTREC is the ability to insert text into a record during the reformatting processing Can be very useful in transforming data into more usable forms Example: To copy the user ID, programmer name, and owner of the IRRDBU00 User Basic Data record, with a blank between each field, you would code: SORT FIELDS=COPY INCLUDE COND=(5,4,CH,EQ,C'0200') OUTREC FIELDS=(1,4,C'The owner of ID ',10,8,C' is ', 30,8,C' and is assigned to ',79,20) OPTION VLSHRT

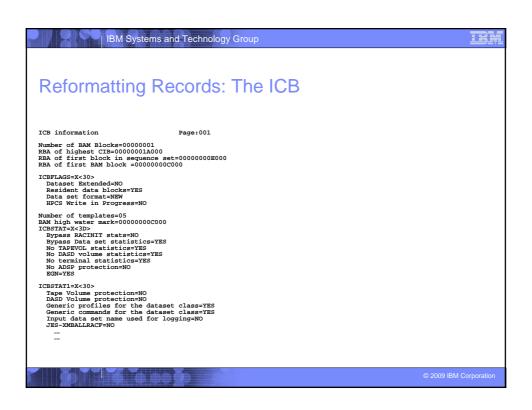
```
IBM Systems and Technology Group
An Introduction to DFSORT: Reformatting Records...
The owner of ID AUDTR01 is MARKN
                               and is assigned to EXTERNAL AUDITOR 01
The owner of ID AUDTR02 is MARKN
                               and is assigned to EXTERNAL AUDITOR 02
                     is MARKN
The owner of TD A6
                              The owner of ID BBB4
                     is MARKN
                               The owner of ID FRED
                     is MARKN
                               and is assigned to FRED THE OPERATOR
Some other powerful features of OUTREC are the ability to:
    Reformat different records in different ways using IFTHEN clauses

    Overlay selected bytes of a record using OVERLAY fields

    Extract delimited fields (such as CSV) into fixed fields

     Justify and squeeze data
```





```
Reformatting Records: The ICB ...

OPTION COPY
ALTSEQ CODE=(005C)
OUTFIL STARTREC=1, ENDREC=1, LINES=255,
HEADER2=(3/,C'ICB information', 20X, C'Page:', PAGE=(EDIT=(TTT)), 3/),
BUILD=(C'Number of BAM Blocks=',5,4, HEX,/,
C'RBA of highest CIB=',9,6, HEX,/,
C'RBA of first block in sequence set=',15,6, HEX,/,
C'RBA of first block in sequence set=',15,6, HEX,/,
C'ICBFLAGS=X<',27,1, HEX,C'>',/,
C'ICBFLAGS=X<',27,1, HEX,C'>',/,
C'Dataset Extended=',
27,1, CHANGE=(3,B'1.....',C'YES',B'0.....',C'NO'),/,
...

...
```

An Introduction to DFSORT: OUTFIL

IBM Systems and Technology Group

- The OUTFIL statement allows you to create one or more output data sets from a single pass of your input data
 - The output data sets can be complete copies of the input data set or may contain only selected records
 - You can select the records go into each output data set
 - · Based on values within the record
 - Based on relative record number
 - "Round robin" or "one rotation" assignment
 - · Every "nth" record
 - You can reformat the selected records in various ways
 - Very useful if you want to partition your RACF data base information or SMF
 - OUTFIL can also be used to create reports.

© 2009 IBM Corporation

IBM Systems and Technology Group

TEM

An Introduction to DFSORT: OUTFIL...

To put all of the IRRADU00 ACCESS records in one data set, all of the JOBINIT records into a second data set, and the remaining records into a third data set, you could code:

```
//SELECT
           EXEC PGM=SORT
//SYSOUT
         DD SYSOUT=*
         DD DISP=SHR,DSN=MARKN.TEST.IRRADU00
//SORTIN
//ACCESS
           DD DISP=SHR,DSN=MARKN.ACCESS.IRRADU00
//JOBINIT DD DISP=SHR,DSN=MARKN.JOBINIT.IRRADU00
//OTHERS
          DD DISP=SHR,DSN=MARKN.OTHERS.IRRADU00
//SYSIN DD *
SORT FIELDS=COPY
OUTFIL FNAMES=ACCESS, INCLUDE=(5,4,CH,EQ,C'ACCESS')
OUTFIL FNAMES=JOBINIT, INCLUDE=(5,4,CH,EQ,C'JOBINIT')
OUTFIL FNAMES=OTHERS, SAVE
```



An Introduction to DFSORT: Symbols

- DFSORT allows you to define symbols that can be used to replace fields, constants, and output columns in DFSORT and ICETOOL statements with easy-to-read labels
 - USBD_OPER could be used as a symbol for 44,1,CH
- The RACFICE package on the "Downloads" section of the RACF web site (http://www.ibm.com/servers/eserver/zseries/zos/racf/) contains DFSORT symbols for all of the IRRADU00 and IRRDBU00 fields. Using these symbols you can specify:

```
SORT FIELDS=(USBD_NAME,A)

INCLUDE COND=(GRBD_RECORD_TYPE,EQ,C'0500',AND,

GRBD_GENERIC,EQ,C'NO ',AND,

(GRBD_NAME,SS,EQ,C'*',OR,

GRBD_NAME,SS,EQ,C'%',OR,

GRBD_NAME,SS,EQ,C'&'))
```

© 2009 IBM Corporation

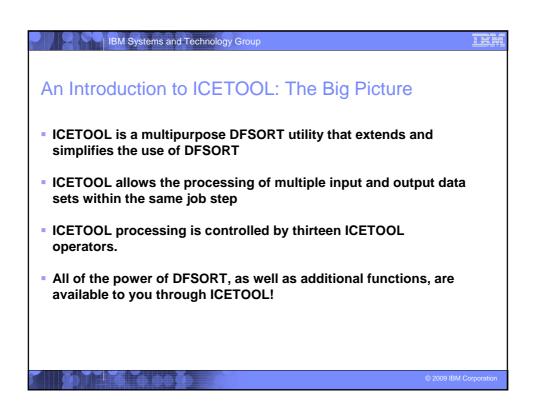
IBM Systems and Technology Group

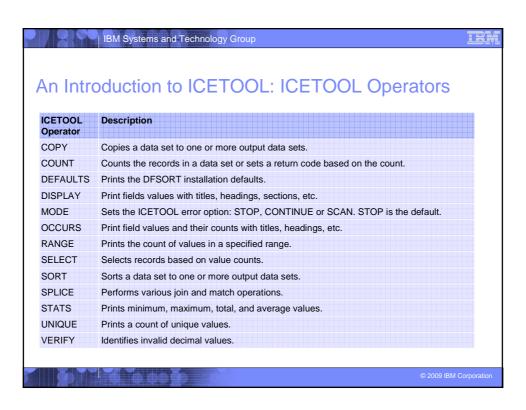


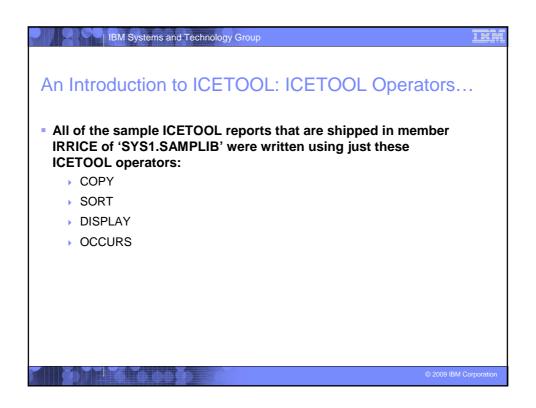
An Introduction to DFSORT: Variable Length Records

- In z/OS, there are two data set structures:
 - Fixed-length records, in which all records in the data set have the same length (RECFM=F, or FB) and
 - Variable-length records, in which the records in the data seta do not have to have the same size records (RECFM=V,VB, VS, or VBS). Each record must have a length with is less than the maximum record length specified for the data set.
 - Each variable length record is prefixed with a four-byte record descriptor word (RDW) that contains the length of the record in the first two bytes.
- When specifying the starting position, the RDW must by included.
 - ... which means that you must add 4 to all of the starting positions documented for the IRRADU00 and IRRDBU00 output in RACF Macros and Interfaces. The DFSORT Symbols mentioned previously already have the RDW built into their starting positions.











An Introduction to ICETOOL: SORT

- The SORT operator allows you to sort data, select the records which are of interest, reformat the records, etc.
- The syntax is:

```
SORT FROM(indd) USING(cntl) TO(outdd)
```

- ...where
 - indd is the input data set DD name
 - outdd is the output data set DD name
 - cntl is the one to four character prefix for the DD name that contains the DFSORT control statements
 - The DD name is formed by appending "CNTL" to the USING value

© 2009 IBM Corporation

| IBM Systems and Technology Group

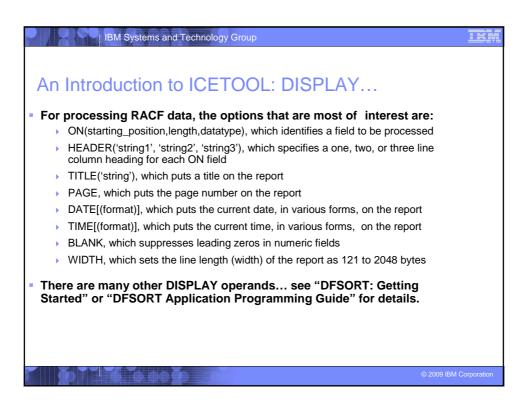


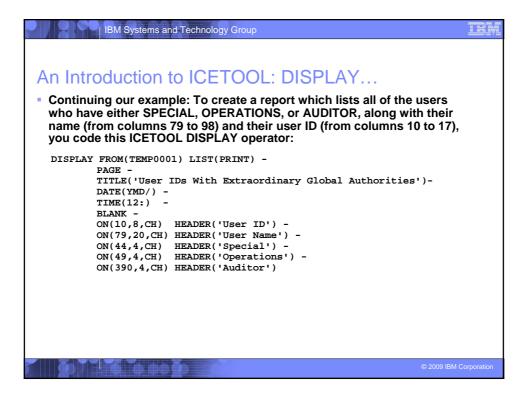
An Introduction to ICETOOL: SORT...

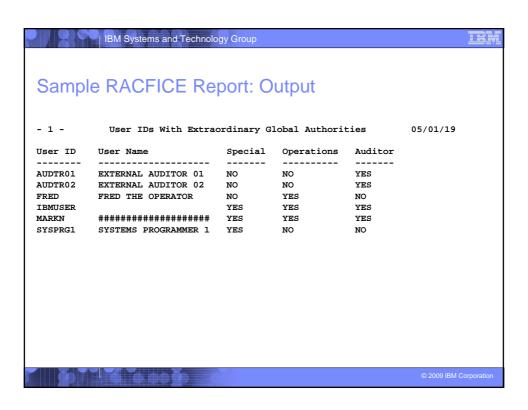
- Let's create a realistic example. To create a report that lists all of the users who have either SPECIAL, OPERATIONS, or AUDITOR, we have to find all of the user basic data records (which have '0200' in columns 5 to 9) and which have a 'Y' in column 44, column 49, or column 390.
- The DFSORT INCLUDE statement which does this is:

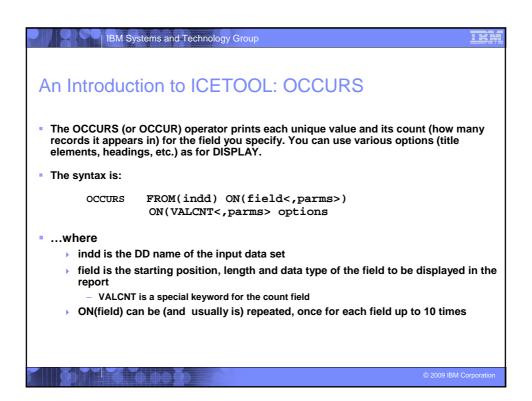
© 2009 IBM Corporati

An Introduction to ICETOOL: DISPLAY The DISPLAY operator allows you to: Select the information that is going to be in your report Specify single line or multi-line column headings Specify the title elements The syntax is: DISPLAY FROM(indd) ON(field, <parms>) LIST(listdd) options ...where indd is the DD name of the input data set ifield is the starting position, length and data type of the field that is to be in displayed the report listdd is the DD name of the report data set ON(field) can be (and usually is) repeated, once for each field in the report, up to 20 times









```
An Introduction to ICETOOL: OCCURS...

Example: Create a report which counts all of the RACF events by hour

The time is in hh:mm:ss format starting in column 23

The ICETOOL OCCURS statement for this is:

OCCURS FROM(IRRADU00) LIST(PRINT) -

PAGE -

TITLE('RACF Activity by Hour') -

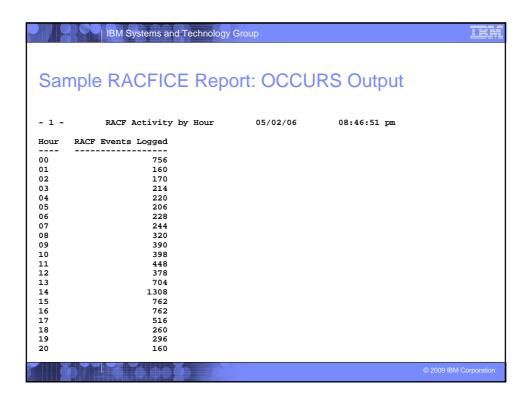
DATE(YMD/) -

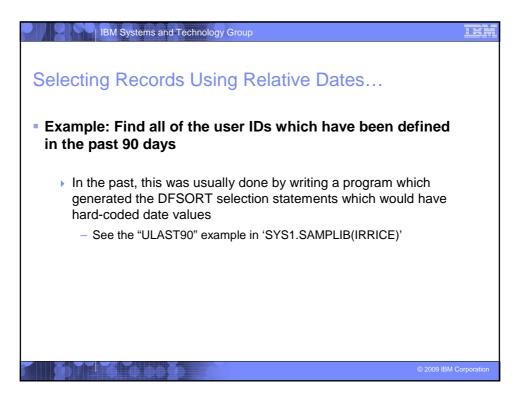
TIME(12:) -

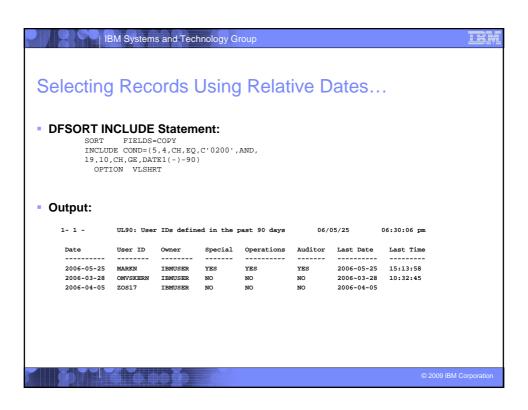
BLANK -

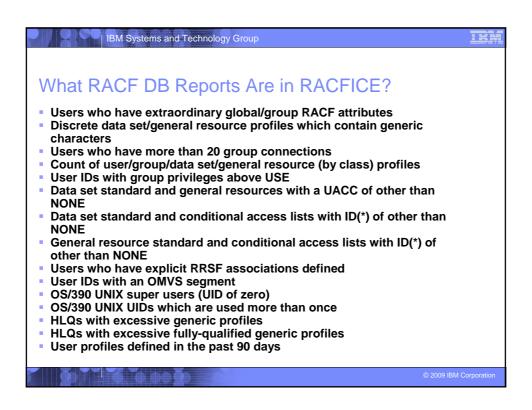
ON(23,2,CH) HEADER('Hour') -

ON(VALCNT) HEADER('RACF Events Logged')
```

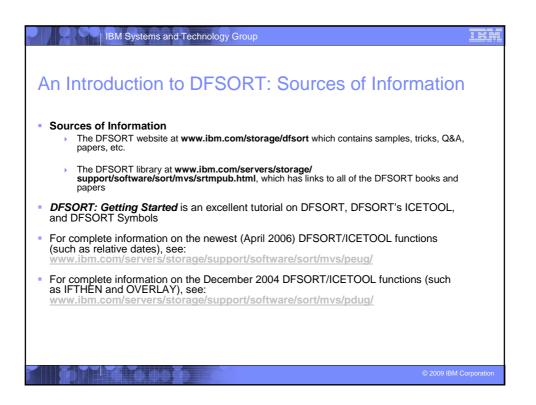








What SMF RACFICE Reports are in RACFICE? Events associated with a specific user User IDs with excessive incorrect passwords Terminals with excessive incorrect passwords Accesses allowed due to WARNING mode profiles Accesses allowed because the user has OPERATIONS Users who are using Automatic Command Direction Users who are directing command explicitly User who log on with LOGON BY RACLINK audit records Users who are using password synchronization Access violations



Disclaimer

The information contained in this document is distributed on as "as is" basis, without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used. Functionally equivalent programs that do not infringe IBM's intellectual property rights may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

It is possible that this material may contain references to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.

IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.

© 2009 IBM Corporation

TER