DBARS

FAQ

Version 4.4

www.sprdb2.com

Software Support: sup@sprdb2.com

What is the purpose of DBARS?

DBARS as an auditing solution

DBARS has been designed as an auditing solution for Db2 on z/OS. The product intercepts all accesses to the Db2 tables that contain vital or confidential data. Those tables have been designated as “to-be-audited” during DBARS startup. The intercepted Db2 accesses are stored into the DBARS **Recorder** dataset.

In addition, the product provides following services:

- Automatic archiving of the Recorder to offline storage media. Recorded Db2 accesses can be retained for an unlimited period of time.
- DBARS can be requested to issue alerts for Db2 accesses that are possibly fraudulent.
- DBARS can be requested to block such Db2 accesses.

DBARS as a Db2 access recorder

All facilities described under “DBARS as an auditing solution” are also available when DBARS is used to record accesses to defined Db2 tables. The archiving, alerting and blocking facilities are available as well.

Even if there is no need for DBARS as an auditing solution, DBARS may be useful as an access recorder for application developers and for application quality assurance. In an operational context DBARS archiving allows to maintain extensive historical logs of all accesses ever made to Db2.

What are the DBARS software requirements?

DBARS requires:

- z/OS 1.6 up to z/OS 2.4
- Db2 Server for z/OS Versions 9, 10, 11 or 12
- The workstations where the DBARS Graphical User Interface program DBARSGUI is invoked, should have Java Runtime Environment 1.8 or higher installed

What are the DBARS hardware requirements?

DBARS does not require specific hardware. Since Db2 access interception is done by software only, hardware appliances are not required to intercept Db2 related network traffic.

Because DBARS has its own interface to Db2, the product intercepts both local and remote Db2 accesses.

How does one install and setup DBARS?

DBARS is delivered as a ZIP file. The unzipped components are transferred from Windows to the mainframe using the DBARSFTP program, which is part of the distribution.

After transfer to the mainframe, several JCL procedures are available:

- to define the DBARS tables
- to link the DBARS components
- to bind the DBARS packages

DBARS operation is controlled by a startup parameter dataset, for which a default model is provided in the distribution. The startup parameters define, among other things, the Db2 tables to be monitored by DBARS.

How does DBARS work?

Actual interception of Db2 accesses is performed by a DBARS component that integrates with the Db2 address space DBM1. Therefore, all accesses to Db2 are intercepted, whatever their origin. The DBARS Intercept component stores the captured Db2 accesses into the DBARS Audit Queue. The Audit Queue is a 64-bit memory object.

The DBARS Writer component that executes in the DBARS address space, constantly polls the Audit Queue. When a stored access is found in the queue, it is written to the DBARS Recorder dataset.

To intercept Db2 accesses, DBARS does **NOT** depend on Db2 tracing or Db2 logging.

Can we block suspect Db2 accesses or issue an alert?

DBARS can issue an alert for a suspicious Db2 access. Also, if requested, suspect Db2 accesses can be blocked by DBARS.

The conditions for alerting or blocking are stated in the DBARS **RULES** dataset.

The following rule ensures that the EMPLOYEE table can be accessed from the CICS environment only:

```
Block when table EMPLOYEE and connection not CICS
```

By stating the above rule as Alert when, DBARS will issue an alert rather than block the access.

When an alert or a block event occurs

- the questionable Db2 access is written to the DBARS Recorder with an appropriate SQLCODE
- the Db2 access is also written to the DBARS Exception table

When a block event occurs

- a DBARS message is written to the z/OS console
- the user is cancelled and its LUW is rolled back
- if the DBARSNAX facility has been activated, an email will be sent to one or more email addresses when blocking or alerting occurs

What data are recorded by DBARS?

An intercepted Db2 access records following data items:

- the date and time of access
- the name of the Db2 application server accessed
- the name of the Db2 application requester
- the Db2 and z/OS userid
- the correlation ID (for example, the z/OS job name for batch access)
- the type of connection (BATCH, CICS, TSO,DDF)
- the type of access (dynamic or static)
- the LUW_id
- the external application name if remote access
- the workstation name if remote access
- the name of the program used for access
- the number of rows modified by the statement
- the statement's SQLCODE (indicating successful or failing access)
- the text of the SQL statement executed, with all input variables (“host variables”) in the statement replaced by their contents.

What is the DBARS Recorder?

The Db2 accesses intercepted by DBARS are stored into the DBARS Recorder.

During DBARS installation, the Recorder is defined as:

- A VSAM cluster, which is the recommended installation option.

  The Recorder cluster is created with the ESDS organization. In addition, a Recorder Index is created as a KSDS. The Recorder Index is used to speed up online scanning of the Recorder.

- A BSAM dataset

  The Recorder is created as a flat file. No indexing dataset is created.

- A Db2 table

  For performance reasons, this option should be used on lightly loaded Db2 systems only.

When the Recorder is created during DBARS installation, a primary and a secondary Recorder are defined. Dual recording is needed when the active Recorder is archived. During archiving, DBARS writes its audit data to the secondary Recorder.

What is the DBARS Centralized Recorder?

When DBARS monitors multiple Db2 subsystems, a DBARS address space is required for each Db2 subsystem. Each DBARS address space should be equipped with a Recorder dataset.

As an alternative, a Centralized Recorder can be defined.

The Centralized Recorder service is provided by the Centralized Recorder server, executing in its own address space.

When the DBARS startup parameters for a given DBARS instance request access to the Centralized Recorder service, that DBARS instance will send its audit data to the Centralized Recorder server, instead of directly writing to the Recorder.

The server and the sending DBARS instances communicate using TCP/IP sockets. DBARS instances that reside in the same z/OS system as the Centralized Recorder server may communicate using a storage resident request queue.

Which are the most common DBARS startup options?

These are the most common DBARS startup options. They are specified in the sample EXECPARM member, that is included in the DBARS/JCL distribution folder.

- DB2_SUBSYS xxxx

  Name of the Db2 subsystem to be audited.

  Required.

- Q2_SIZE 4096

  Size of the audit queue in MB.

  Required.

- SEQREC VSAM

  Uses a VSAM Recorder.

  Recommended.

- OPTIONS NOMASK

  OPTION NOMASK enables hostvar substitution.

  Recommended.

- RECORD DDL UTIL CMND

  DBARS records all Db2 accesses (DML).

  These additional recording options will record DDL statements, Db2 utility executions and Db2 commands.

  Recommended.

- AUDITNAMES

  This should be the last statement in the startup member.

  Specify the names of the Db2 tables to be monitored as *owner.tablename*. Both owner and tablename may be generic by including a trailing % character.

  Required.

How can we display the data recorded by DBARS?

DBARS offers several utilities to show recorded audit data, based on selection criteria specified by the user.

These utilities may inspect:

- all events available in the online DBARS Recorder
- the alert or block events recorded in the DBARS Exception table
- events recorded in the DBARS Archives

- For the TSO environment DBARS provides programs to obtain audit data
  - from the online Recorder
  - from the DBARS Exception table

- Batch utilities are provided to print selected data
  - from the online Recorder
  - from the DBARS Exception table
  - from a DBARS archive

- DBARSGUI is a Windows application that provides a modern graphical user interface to obtain selected audit data
  - from the online Recorder
  - from the DBARS Exception table
  - from a DBARS archive

How does DBARS archiving work?

When the DBARS Recorder must be archived, the DBARS archiving procedures work as follows:

- DBARS recording switches from the current Recorder dataset to the alternate Recorder
- the alternate Recorder now receives new audit data
- the now inactive Recorder is written to offline media, such as [virtual] tape

Typically, archiving is called from a started task that is scheduled at regular time intervals, depending on the size of the online Recorder and the number of audit events stored.

How do we stop DBARS?

To stop DBARS, the z/OS STOP command or the DBARS command STOP can be used.

However, if Db2 command recording has been requested in the DBARS startup parameters, DBARS will automatically stop when the monitored Db2 system is stopped.

Manually stopping DBARS while Db2 is still active should be avoided, because Db2 accesses will no longer be recorded after DBARS shutdown.

What is the DBARSGUI facility?

The DBARSGUI application provides a modern graphical user interface to access the data recorded by DBARS. DBARSGUI is a Java application executing on Windows workstations.

DBARSGUI Architecture

The DBARSGUI facility consists of a mainframe and a workstation component. These components communicate using TCP/IP sockets. The DBARSGUI address space on z/OS provides access services to the DBARSGUI workstation component.

The DBARSGUI program on z/OS listens on a specified TCP/IP port for requests sent by the workstation component.

DBARSGUI on the workstation is started from a Windows BAT file that specifies the IP address of the z/OS system where the DBARS Recorder resides. The BAT also specifies the TCP/IP port where the z/OS component is listening on.

When starting DBARSGUI, the workstation user is requested to enter a Db2 user-id and its password. After successful logon, the user is connected to the DBARSGUI service on the mainframe.

When the workstation user requests DBARS data, its request is passed to the z/OS component. This component accesses the DBARS Recorder data and sends the resulting data stream to the workstation. The workstation program converts the input stream to a GUI stream and shows it on the workstation.

Accessing multiple Db2 subsystems from DBARSGUI

- Given the 2 Db2 subsystems:
  - Db2 SYSA IP-address 212.313.45.2 on LPARx
  - Db2 SYSB IP-address 212.314.45.2 on LPARy
- There is a DBARS instance and a Recorder in both LPARs.
- The DBARSGUI started task is running in both LPARs and listens on port 4444.
- The workstation's desktop has 2 icons:
  - DBARSGUI_A.BAT

    Contains the DBARSGUI call: *"java -jar DBARS.jar 212.313.45.2 4444"*
  - DBARSGUI_B.BAT

    Contains the DBARSGUI call: *"java -jar DBARS.jar 212.314.45.2 4444"*

Note

DBARSGUI setup would be simpler when a Centralized Recorder is used for the DBARS instances on LPARx and LPARy. If the Centralized Recorder server would run on LPAR x, the workstation call

"java -jar DBARS.jar 212.313.45.2 4444"

would allow to access the audit data of both Db2 systems.

What is the DBARSNAX facility?

The DBARSNAX facility is associated with DBARS access alerting and blocking, as described in this paragraph.

DBARSNAX operates as follows:

- DBARSNAX on z/OS continuously interrogates the DBARS Exception table. When a new entry is found, it is sent to the DBARSNAX program running on the Windows workstation using TCP/IP.
- DBARSNAX on the workstation then sends an email with the Db2 access details to one or more email addresses. The target email addresses are specified in a parameter file.

How to start the DBARSNAX facility is described in the DBARS User's Guide.

Which Address Spaces are used by DBARS?

Required address space

A DBARS address space is required for every Db2 subsystem monitored by DBARS. The address space should also be equipped with a DBARS Recorder dataset, unless the Centralized Recorder facility is used.

Optional address spaces

- DBARSGUI
  If the DBARS Graphical User Interface should be available to Windows workstations, a DBARSGUI address space should be started in every DBARS address space. The address space communicates with the DBARSGUI application on the Windows desktop.

- DBARSCRS
  The DBARSCRS address space is required when the Centralized Recorder facility will be used. The Centralized Recorder server executes in this address space.

- DBARSNAX
  The address space is required when DBARS alert of blocking events should be sent to defined email addresses. The address space communicates with the DBARSNAX program on the Windows desktop.

How to secure the data recorded by DBARS?

DBARS records the SQL statements that access confidential or vital Db2 data.

Although the Db2 data do not appear in the DBARS recordings, there may be situations where the recorded SQL statements should be protected as well.

Consider the following options:

- The DBARS Recorder and archive datasets can be protected using z/OS security software such as RACF.
- It is possible to encrypt the DBARS audit data using the hardware assisted encryption services, offered by z/OS DFSMS. These services are completely transparent to the user and the DBARS software. DFSMS is able to encrypt both VSAM and sequential BSAM datasets.

Technical questions

Why does DBARS startup result in SQLCODE –991?

As the first SQL statement during initialization, DBARS issues an
EXEC SQL VALUES (CURRENT SERVER)

When this statement results in SQLCODE -991 (system code 00F30011), it is retried every second.

The explanation of the 00F30011 system code in Messages and Codes:

> *A connection or other work request was received, but the designated Db2 subsystem is not active*.

The SQLCODE -991 is normal if Db2 is not yet active when DBARS is being started.

However, if Db2 is active, a problem does exist.

Please check the following:

- Did the DBARS plans successfully bind to the Db2 subsystem?
- DSNHDECP should point to the intended Db2 subsystem. The STEPLIB DD in the DBARS startup JCL should specify the Db2 LOADLIBs in the correct order. **SDSNEXIT** should usually be the first in the concatenation, because its DSNHDECP usually points to the correct Db2 subsystem.
- The userid executing the DBARS plans should have SYSADM authority, to be able to load the plans. Otherwise SQLCODE –991 system code 00F30034 will result.

  IEF695I START DBARS WITH JOBNAME DBARS IS ASSIGNED TO USER STCUSR
- The userid STCUSR should have authority to load all plans.
- Did the following RACF command complete normally?
  rdefine started dbars.dbars stdata (user(stcusr)) setropts refresh

Initially, you could try to run the DBARS startup using normal JCL. This would exclude possible complexities associated with the started task environment and its Db2 related definitions.

Why is a warning received when binding DBARSW?

DSNX100I -BIND SQL WARNING

DBRM=DBARSW

STATEMENT=11455

xxxxxx.TEMP_TAB IS NOT DEFINED

The warning is issued because the TEMP_TAB table is created and dropped during DBARSW execution. This table does not exist at bind time. Hence the bind warning, which can be ignored.

Why are the “Db2 Command” recordings not shown when scanning the DBARS Recorder?

During Recorder scanning under TSO or Windows, recorded audit data are shown for the current userid. Db2 commands however are executed under the SYSOPR userid.

If the SYSOPR userid is specified in the scan selection criteria, Db2 command recordings will be shown.

Where is the DBARS License key located?

The License key is in the same library as the DBARS startup parameters, that is, in the DBARS JCLLIB.

Why does DBARS need the MONITOR1 privilege?

DBARS intercepts all Db2 accesses using its proprietary interface, without depending on Db2 tracing.

Db2 tracing however is needed when the OPTION startup statement requests recording of the Db2 utilities or Db2 commands.

For the vast majority of Db2 activity, DBARS does not need tracing.