The SQLXPress Audit Facility

SQLXPress Audit Services

SQLXPress is a client-server application. The client runs on a PC workstation and sends commands to a server program which runs on the NSK system. In order to use any client facilities, the user must enter a valid logon name and password, which is encrypted and sent to the SQLXPress server, which in turn logs on to the NSK system. Thereafter, functions performed by the server are subject to standard Guardian and Safeguard security settings.

SQLXPress version 3.40 and above is capable of auditing various levels of activity of the users of the SQLXPress product. The auditing is performed by a unique NonStop process pair. All components of SQLXPress send audit to the audit process, which then writes data to the audit trail. Auditing is a critical component of SQLXPress: if the audit process fails, SQLXPress will refuse to perform any audited function (This includes logon and logoff operations).

The audit trail is owned by, and accessible to, a specific userid known as the audit administrator. The audit administrator is not required to be the same userid that owns the SQLXPress installation.

The type and amount of information that is audited is controlled by the AUDITLEVEL setting. AUDITLEVEL can be one of the following:

1. NONE: no audit is produced.
2. BASIC: logons and logoffs are audited, and various background activities are audited.
3. CHANGE: in addition to BASIC audit, operations which cause a change to data are audited.
4. ACCESS: in addition to CHANGE audit, operations which access data are audited.

SQLXPress audit is controlled by the PAM program, running as a named NonStop process pair. All potentially auditable events are passed to the PAM server, which then makes a decision about whether or not to audit the event. In a future release, the PAM server will also be responsible for *permissions* (i.e. it will determine if an individual event is permitted). In the SQLXPress 3.4 release, the PAM server is configured to provide audit services only, that is, the permissions features are turned off, and all events are attempted. Of course, the security systems provided by SQL/MX, SQL/MP, and Safeguard are applied to any operation.

The PAM server is *PROGID* to the SQLXPress audit administrator userid. This userid is initially the same as the SQLXPress installation owner, but can be changed through a two step give-accept procedure. Using the *PROGID* feature means that all audit files are owned by the audit administrator-id.

Auditing

When audit is required, the data is written to the current audit file. Audit files can be located in a different volume/subvolume from the SQLXPress installation, and in fact this is recommended. Audit filenames are formed using the 3 character product prefix (SQX), the 2 character audit trail identifier (AT) and three numeric digits. Audit trail numbers start at 0 and continue to 999, when they reset.

This means a maximum of 1000 audit trail files can be retained. You can configure SQLXPress with either or both a mimumum number of audit trail files to keep, and a minimum number of days of audit to keep.

Configuration Data.

Configuration data is kept in the following locations:

The LICENSE file

The LICENSE file may contain a setting for OPTION_AUDIT_LEVEL. This specifies the minimum acceptable audit level for the installation.

The SQXINI file

The SQXINI file contains a [PAM] section, which provides the information necessary to start the PAM server.

The PROCESS=$pname setting specifies the name of the PAM server process. This setting is required.

The SUBVOL=$vol.sub setting specifies the location of the audit trail files. If not specified, the SQLXPress installation subvolume is used.

The CPU, PRIORITY, SERVERIN and SERVEROUT parameters are optional.

The SQXINI file also contains a [SETUP] section, which provides information that is used at SETUP time.

The AUDITLEVEL setting in the [SETUP] section is used to initially configure the SQLXPress audit level.

The SQXATCNF file

The SQXATCNF file is located in the audit trail subvolume. SQXATCNF must have security OOOO and must belong to the audit administrator.

SQXATCNF contains

1. Information about the physical properties of the audit trail files (e.g. extent sizes).
2. Information about the minimum number of audit trail files to keep, and the minimum number of days of audit to keep.
3. The current auditing level.

Securing the SQLXPress Installation

Installation Considerations for SQLXPress

To maximize the security of an SQLXPress installation, consider the following before installing the product.

1. Select a Guardian user-id that will be used to install SQLXPress. This user-id needs no special Guardian privileges. (This is referred to as the SQLXPress administrator).
2. Select a different user-id to be used as the SQLXPress audit administrator. Again, no special Guardian privileges are required.
3. Select a Guardian subvolume for each of the following purposes. Security is maximized if they are distinct subvolumes:
    1. the installation subvolume, that will contain program files, license and configuration data,
    2. a subvolume for temporary Guardian files, which include scripts and other background task data,
    3. an audit trail subvolume.
4. Determine if you plan to use SQL/MX or SQL/MP for the SQLXPress database. The SQLXPress database contains information about queries, programs, and other objects that can be managed with SQLXPress. All users of SQLXPress will require read and write access to it. For an SQL/MX database, you need to identify the catalog and schema. For SQL/MP, you need to identify a catalog and subvolume. The subvolume should be different from any of the ones used above.

Post-installation tasks

1. From a TACL process logged on as the SQLXPress administrator:
    1. Secure all SQLXPress program files with Guardian security “OONO”.
    2. Use the AX program to give the audit administrator responsibility to the audit administrator.
    3. Create a Safeguard subvolume record that allows file creation in the installation subvolume for only the SQLXPress administrator-id and the audit administrator-id.
    4. Create a Safeguard subvolume record that allows access to the audit trail subvolume for the audit administrator-id alone.

2. From a TACL process logged on as the audit administrator:
    1. Use the AX program to accept audit administrator responsibility.
    2. Review the settings for audit file extents and change as required.
    3. Review the settings for audit file retention, and change as required.
    4. Review the auditlevel and change if necessary.

The AX Program

The AX program is a TACL based program that is used to manage SQLXPress audit. It is also the program that is used by the SQLXPress Auditor GUI to extract audit data from the audit trails.

Almost all of the functions performed by AX can be invoked through the SQLXPress Auditor GUI. Notable exceptions are the give and accept functions.

AX performs functions based on options supplied on the command line. Options begin with a single or double dash character e.g. the command ***RUN AX –shutdown*** causes AX to shut down the PAM process.

Option	Function Performed
-h	Help. Prints a list of AX options and functions.
--shutdown	Causes the PAM process to shutdown gracefully. PAM does not shutdown until all users of SQLXPress have logged off.
--list	Lists information about the configuration of the SQLXPress audit files, and informaion about each audit file.
--give <userid>	When run by the current audit administrator, begins the process of giving audit administrator responsibility to another user. The give function cannot be performed if the PAM process is running. Once the give operation has been performed, SQLXPress will not run until the new audit administrator has performed the accept function.
--accept	This is performed by the new audit administrator to accept audit administrator responsibility.
--auditlevel <level>	Sets the auditlevel to one of: NONE, BASIC, CHANGE, ACCESS.
--nextfile	Forces the current audit file be completed and auditing to the next audit file.
--setextents <p> <s>	Sets the primary and secondary extents for audit files.
--setmaxextents <n>	Sets the maxextents value for audit files.
--setretention <f> <d>	Sets the minimum number of audit files to retain, and the minimum number of days of audit.
--print	Prints selected audit records.
--mxtables <schema>	Extracts selected records to an MX database.
--mptables <catalog> <subvol>	Extracts selected records to an MP database.

When using the print, mxtables, or mptables options, various other criteria can be provided:

Option	Function Performed
--caid <userid>	Select records with a particular caid
--client <pattern>	Select records from clients matching <pattern>
--file <filename>	Specifies a specific audit file.
--fp <fingerprint>	Select records with a particular fingerprint. You can abbreviate the fingerprint to the last four digits if they are not zero.
--from <datetime>	Specifies the start of the period of interest. Datetime is of the form: dd-

	mmm-yyyy,hh:mm:ss. Datetime can also be specified as a negative number of hours and minutes from the current time.
--paid <userid>	Select records with a particular paid
--program <pattern>	Select records from programs matching <pattern>
--quiet	Suppresses various status messages.
-r [CONTROL| SESSION |EVENT [<action>]| OUTCOME [SUCCESS| FAIL [<error>]]]	CONTROL - Select control operations SESSION - Select open, close EVENT - Select events OUTCOME - Select event outcomes
--session <sid>	Select records from a session. You can abbreviate the session id to the last three digits if they are not zero.
--to <datetime>	Specifies the end of the period of interest. Datetime is of the form: dd-mmm-yyyy,hh:mm:ss. Datetime can also be specified as a negative number of hours and minutes from the current time.
--transid <tid>	Select records with a particular transid
-u <userid> --user <userid>	Select records with a either paid or caid
-v <subvol>	Specifies the subvolume containing the audit trails.

When using the mxtables, or mptables options, more criteria can be provided:

Option	Function Performed
--extents <p> <s> <m>	Specifies the primary and secondary extent sizes and the maxetents setting for the AEVENT and AEVENTX tables.
--txrecords <n>	Specifies the number of audit records to extract in each TMF transaction the maxextents value for audit files.
--mptables <catalog> <subvol>	Extracts selected records to an MP database.

