Technical Note

SQLXPress Data Blacklist Facility

Document Version 1.03

Introduction

The SQLXPress data blacklist facility provides a means for security administrators to ensure that sensitive business data is not exposed to DBAs, operations and development staff, and other users of systems where SQLXPress is deployed.

The facility is helpful in two scenarios:

1. Where the system contains live production data.
2. Where the system contains test data that has been copied from a production database. Such data can be altered for the purposes of testing, but may contain private or otherwise sensitive information that cannot be transmitted off the system, and cannot be exposed to developers or testers.

The data blacklist facility requires SQLXPress release 3.21.7 or above. For release 3.40 and above, it works for both SQL/MX and SQL/MP. For releases prior to 3.40, it works only for SQL/MX data.

Data can be blacklisted at the catalog, schema, or table level. Blacklisted data is immediately discarded by the SQLXPress server code that is running on the NSK system. The I/O buffer used by SQLXpress is immediately overwritten, so the data will not be present in a process memory dump. Blacklisted data is not passed to any other NSK process and is not transmitted off the system.

All client and server components of SQLXPress that access SQL data are affected. This includes server based scripts and client access via the data browser or ad hoc queries.

DDL operations such as CREATE, DROP, etc., are not affected by the blacklist.

For SQL/MX only, access to catalog metadata is not normally prevented by the catalog level blacklist. This means that users can still view the object definitions for objects in a blacklisted catalog, and that the shape of the tables, indexes, etc. is exposed. However, it is possible to blacklist the metadata schema itself – this will prevent a user from viewing any information about the objects in the catalog.

Background

SQLXPress is a client-server application. The client runs on a PC workstation and sends commands to a set of server programs which run on the NSK system. The server programs are installed in a Guardian subvolume on the system.

Configuration Procedure

Once SQLXPress has been installed, the SQLXPress administrator creates a Guardian edit-file called MXSECURE in the SQLXPress installation subvolume to control SQL/MX blacklists and an edit-file called MPSECURE to control SQL/MP blacklists. Both file's Guardian security setting should be "NOOO". This allows anyone to read the file, but allows only the security administrator to modify it. Each contains a "BLACKLIST" section.

MXSECURE

The [BLACKLIST] section contains entries that refer to specific Catalogs, Schemas, or Tables. These entries can contain % or _ wildcard characters. SQLXPress will suppress data from SELECTs that reference these tables. This includes indexes and non-blacklisted views that refer to blacklisted tables. SQLXPress does this by examining the execution plan generated by SQL/MX before each statement is executed. If the plan contains any nodes that reference objects in the blacklist, then data from the execution of the statement is discarded.

For example:

```
[BLACKLIST]
C PRODCAT
S DEVCAT.TEST%
T DEVCAT.OTHER.SECRET
```

In the case of a catalog blacklist entry, the DEFINITION_SCHEMA which contains catalog metadata is excluded (i.e. not blacklisted) by default. To prevent access to the metadata, both a catalog entry (for the catalog) and a schema entry (for the metadata) are required, for example:

```
[BLACKLIST]
C PRODCAT
S PRODCAT.DEFINITION_SCHEMA_VERSION_%
```

SQL/MX Verification Procedure

Once the MXSECURE file has been created and you have added the blacklist entries, make sure the Guardian security setting for this file is "NOOO".

Start the SQLXpress client and log on. Choose *Tools*, then *Execute SQL/MX Statements* from the menu. Enter the statement "SELECT COUNT(*) FROM catalog.schema.tablename" (where catalog, schema, and tablename refer to the table to be verified). Press the lightning-bolt button to execute the query. The query results row should show "0 row retrieved". Click on the statistics tab. The statistics value for the "Accessed Rows" attribute should be the actual number of rows in the table. This procedure confirms that SQLXpress is suppressing data from the blacklisted table.

MPSECURE

The [BLACKLIST] section contains entries that refer to specific tables. These entries can contain *, ?, and + wildcard characters. A * matches any sequence of characters, a ? matches a single character, and a + matches a numeric character. SQLXPress will suppress data from SELECTs that reference these tables. This includes indexes and non-blacklisted views that refer to blacklisted tables. SQLXPress does this by parsing each SQL/MP statement before it is executed. SQLXPress resolves defines and views to determine what tables are being accessed. If the statement references objects in the blacklist, then data from the execution of the statement is discarded.

For example:

```
[BLACKLIST]
T $D1.MSTEST.D*
```

SQL/MP Verification Procedure

Once the MPSECURE file has been created and you have added the blacklist entries, make sure the Guardian security setting for this file is "NOOO".

Start the SQLXpress client and log on. Choose *Tools*, then *Execute SQL/MP Statements* from the menu. Enter the statement "SELECT COUNT(*) FROM tablename" (where tablename refers to the table to be verified). Press the lightning-bolt button to execute the query. The query results row should show "0 row retrieved". Click on the statistics tab. The statistics value for the "Accessed Rows" attribute should be the actual number of rows in the table. This procedure confirms that SQLXpress is suppressing data from the blacklisted table.